ANNEX A

REQUIREMENT SPECIFICATIONS FOR CATEGORY A (CORE SYSTEM)

Table of Contents

1 IMPLEMENTATION PLAN

1.1 The production rollout shall be completed according to the Implementation Plan. Major milestone dates are highlighted in **bold** in the timetables, Tables 7A-1.3(I) to (III), below. Tenderers shall observe these major milestones when working out the detailed Implementation Plan as they are essential requirements. The Contractor shall equally treat the dates specified in bold as fixed and incorporate the same into the final Implementation Plan to be prepared by it shortly after the commencement of the Implementation Period. All activities shall be performed by the Contractor unless otherwise expressly specified.

1.2 If any of the Contract in relation to any of the other Categories cannot be awarded at the same time as this Contract and the Government decides to cancel or postpone the implementation of such Category, and yet the Government still at its discretion awards this Contract in relation to Category A, the Government reserves the right to make further changes to the Implementation Plan below including the Completion Date to duly take into account of the Implementation Period which will be shortened arising from the cancellation or postponement of the other Categor(ies). Any decision of the Government shall be binding on the Contractor in the absence of manifest error.

1.3 If there is any delay in the implementation of any of the other Categories (regardless of whether or not such Category is covered by this Contract), and the Government decides to terminate or postpone the implementation of such Category but not this Category, the Government reserves the right to make further changes to the Implementation Plan below including the Completion Date to duly take into account of the Implementation Period which will be shortened arising from the termination or postponement of the other Categor(ies). Any decision of the Government shall be binding on the Contractor in the absence of manifest error.

Stage	Activity Description	Number of months after the Contract Date (Note (a))	
		Latest Start Date	End Date
A0	**Stage A0** **Project Initiation**	0	0
A0.1	Delivery of Documentation	0	0
Core System Implementation Activities			
A1	**Stage A1** **System Analysis and Design**	0	3
A1.1	System Analysis and Design ("SA&D")	0	3
A1.2	Delivery of Documentation	0	3
A2	**Stage A2** **System Development & Testing (A2.1 – A2.5)**	2	**8**
A2.1	Development Environment Setup	2	3
A2.1.1	Hardware and Software Delivery	2	2
A2.1.2	Installation Test and Functional Test (for Hardware and Software)	2	3
A2.2	Testing Environment Setup	6	7
A2.2.1	Hardware and Software Delivery	6	6
A2.2.2	Installation Test and Functional Test (for Hardware and Software)	6	7
A2.3	System Development and Testing	2	8
A2.3.1	System Development	2	7
A2.3.2	Functional Test	5	7
A2.3.3	System Integration Test ("SIT")	7	**8**
A2.4	Delivery of Documentation for stages A2.1 to A2.3	3	**8**
A2.5	System of Category A is "Ready for Overall SMARTICS-2 System Integration Tests"	N/A	**8**

Stage	Activity Description	Number of months after the Contract Date (Note (a))	
		Latest Start Date	End Date
A3	**Stage A3** **User Acceptance (A3.1)**	9	14
A3.1	User Acceptance Tests ("UAT") for the System only conducted by the Government and assisted by the Contractor	9	14
A5	**Stage A5** **Pre-production Setup and Production Rollout (A5.1.1 to A5.1.4)**	5	**15**
A5.1	Data Conversion and Migration	5	**15**
A5.1.1	Preparation and overall planning	5	6
A5.1.2	Program development and testing	7	8
A5.1.3	Conversion, migration and verification for image files	8	**15**
A5.1.4	Converted and migrated image files	N/A	**15**

Table 7A-1.3(I) Implementation Plan for Core System (Category A)

Stage	Activity Description	Number of months after the date all of the Systems of Categories B to E and ITI are "Ready for Overall SMARTICS-2 System Integration Tests" (Note (b))	
		Latest Start Date	End Date
A2	**Stage A2 (cont'd)** **System Development & Testing (A2.6 – A2.8)**	0	**1**
A2.6	Overall SMARTICS-2 System Integration Tests conducted by the Contractor of Category A and assisted and participated by the Contractors of all the other Categories and participated by the Government and ITI project team	0	**1**
A2.7	Delivery of Documentation for stage A2.6	0	**1**

Stage	**Activity Description**	**Number of months after the date all of the Systems of Categories B to E and ITI are "Ready for Overall SMARTICS-2 System Integration Tests"** **(Note (b))**	
		Latest Start Date	**End Date**
A2.8	System of Category A is "Ready for Overall SMARTICS-2 UAT"	N/A	**1**

Table 7A-1.3(II) Implementation Plan for Core System (Category A)

Stage	**Activity Description**	**Number of months after the date all of the Systems of Categories B to E and ITI are "Ready for Overall SMARTICS-2 UAT"** **(Note (c))**	
		Latest Start Date	**End Date**
A3	**Stage A3 (cont'd)** **User Acceptance (A3.2 – A3.5)**	0	**3**
A3.2	Overall SMARTICS-2 UAT conducted by the Government and assisted by the Contractors of all Categories	0	3
A3.3	Load Test and Resilience Test conducted by the Contractor in the presence of the Government	2	**3**
A3.4	Disaster Recovery Drill	2	**3**
A3.5	Delivery of Documentation for stages A3.2 to A3.4	1	**3**
A4	**Stage A4** **Training**	0	**3**
A4.1	Training Environment Setup at HQ and / or location to be designated by the Government	0	1
A4.1.1	Hardware and Software Delivery	0	0

Stage	**Activity Description**	**Number of months after the date all of the Systems of Categories B to E and ITI are "Ready for Overall SMARTICS-2 UAT"** **(Note (c))**	
		Latest Start Date	**End Date**
A4.1.2	Installation Test and Functional Test (for each item of Hardware and Software)	0	1
A4.2	Setup of Training Database	2	2
A4.3	Preparing and conducting Training	2	**3**
A4.4	Delivery of Documentation	1	**3**
A5	**<u>Stage A5 (cont'd)</u>** **Pre-production Setup and Production Rollout (A5.1.5 – A5.8)**	0	**8**
A5.1	Data Conversion and Migration (cont'd)	0	**4**
A5.1.5	Rehearsal and Production Data Conversion and Migration	0	4
A5.1.6	Converted and migrated data	N/A	**4**
A5.2	Site Preparation at all of the Locations	0	7
A5.3	Phase 1 Production Sites	1	**5**
A5.3.1	Phase 1 Production Environment Setup [d]	1	3
A5.3.1.1	Delivery of Hardware and Software to Phase 1 Production Sites	1	1
A5.3.1.2	Installation Test and Functional Test (for each item of Hardware and Software) at Phase 1 Production Sites	2	3
A5.3.2	Production Data Setup at Phase 1 Production Sites	3	3
A5.3.3	Trial run at Phase 1 Production Sites	4	4
A5.3.4	Reliability Test at Phase 1 Production Sites	5	**5**
A5.3.5	Core System complete production rollout at Phase 1 Production Sites	N/A	**5**
A5.4	Phase 2 Production Sites	4	**8**
A5.4.1	Phase 2 Production Environment Setup [d]	4	6
A5.4.1.1	Delivery of Hardware and Software to Phase 2 Production Sites	4	4

Stage	Activity Description	**Number of months after the date all of the Systems of Categories B to E and ITI are "Ready for Overall SMARTICS-2 UAT"** **(Note (c))**	
		Latest Start Date	**End Date**
A5.4.1.2	Installation Test and Functional Test (for each unit of Hardware and Software) at Phase 2 Production Sites	5	6
A5.4.2	Production Data Setup at Phase 2 Production Sites	6	6
A5.4.3	Trial run at Phase 2 Production Sites	7	7
A5.4.4	Reliability Test at Phase 2 Production Sites	8	**8**
A5.4.5	Core System complete production rollout at Phase 2 Production Sites	N/A	**8**
A5.5	Delivery of Documentation	2	8
A5.6	Start of Transition Period	4	N/A
A5.7	Completion of Transition Period	N/A	**8**
A5.8	Completion Date for the System of Category A (i.e. System is Ready for Use)	N/A	**8**
A6	**Stage A6** **Old System Removal**	9	9
A6.1	Removal and Collection of Trade-in Items	9	9
A6.2	Delivery of Documentation	9	9
A7	**Stage A7** **System Nursing**	4	**14**
A7.1	System Nursing Period	4	14
A7.2	Post Implementation Review	9	14
A7.3	Delivery of Documentation	9	14
A7.4	Completion of System Nursing Period	N/A	**14**

Table 7A-1.3(III) Implementation Plan for Core System (Category A)

Notes:

(a) Unless otherwise specified, for Stages A0, A1, A2 (except for A2.6, A2.7 and A2.8), A3.1 and A5.1 (except for A5.1.5 and A5.1.6), for a start date expressed as certain specified number of months, that date shall be the first working day of that number of months after the Contract Date, and for an end date expressed as certain specified number of months, the date shall be the last working day of the relevant number of months after the Contract Date. To illustrate, if the Contract Date is 3 January 2017:

Number of month(s) after the Contract Date	The first day of number of month(s) after the Contract Date	The last day of number of month(s) after the Contract Date	The latest start date of number of month(s) after the Contract Date	The end date of number of month(s) after the Contract Date
0	3 Jan 2017 Tue	2 Feb 2017 Thu	3 Jan 2017 Tue	2 Feb 2017 Thu
1	3 Feb 2017 Fri	2 Mar 2017 Thu	3 Feb 2017 Fri	2 Mar 2017 Thu
2	3 Mar 2017 Fri	2 Apr 2017 Sun	3 Mar 2017 Fri	31 Mar 2017 Fri
3	3 Apr 2017 Mon	2 May 2017 Tue	3 Apr 2017 Mon	2 May 2017 Tue
4	3 May 2017 Wed*	2 Jun 2017 Fri	4 May 2017 Thu	2 Jun 2017 Fri
5	3 Jun 2017 Sat	2 Jul 2017 Sun	5 Jun 2017 Mon	30 Jun 2017 Fri
6	3 Jul 2017 Mon	2 Aug 2017 Wed	3 Jul 2017 Mon	2 Aug 2017 Wed
7	3 Aug 2017 Thu	2 Sep 2017 Sat	3 Aug 2017 Thu	1 Sep 2017 Fri
8	3 Sep 2017 Sun	2 Oct 2017 Mon*	4 Sep 2017 Mon	29 Sep 2017 Fri
9	3 Oct 2017 Tue	2 Nov 2017 Thu	3 Oct 2017 Tue	2 Nov 2017 Thu
10	3 Nov 2017 Fri	2 Dec 2017 Sat	3 Nov 2017 Fri	1 Dec 2017 Fri

* Public Holiday

Without prejudice to the proper interpretation of the Note (a) above, by way of example, if the Contract Date is 3 January 2017, the latest start date of Stage A0 will be 3 January 2017 and the end date of the same will be 2 February 2017. Similarly, if given the same Contract Date, the latest start date of Stage A2.1, which is the first working day of 2 months after 3 January 2017 (the Contract Date), will be 3 March 2017 and the end date of the same, which is the last working day of 3 months after 3 January 2017 (the Contract Date), will be 2 May 2017.

(b) For Stages A2.6, A2.7 and A2.8, for a start date expressed as certain specified number of months, that date shall be the first working day of that number of months after the actual date the Systems of Categories B to E and ITI become Ready for Overall SMARTICS-2 System Integration Tests (in each case as notified by the Government (whose notification shall be conclusive in the absence of manifest error)), and for an end date expressed as certain specified number of months, the date shall be the last working day of the relevant number of months after the Systems of Categories B to E and ITI actually become Ready for Overall SMARTICS-2 System Integration Tests. If the dates on which the Systems of Categories B to E and ITI becoming Ready for Overall SMARTICS-2 System Integration Tests are different, the latest of these dates shall be adopted to determine the completion dates for the aforesaid stages.

(c) For Stages A3 (except A3.1), A4, A5 (except A5.1.1 to A5.1.4), A6 and A7, for a start date expressed as certain specified number of months, that date shall be the first working day of that number of months after the actual date the Systems of Categories B to E and ITI become Ready for Overall SMARTICS-2 UAT (in each case as notified by the Government in writing whose notification shall be binding and conclusive in the absence of manifest error), and for an end date expressed as certain specified number of months, the date shall be the last working day of the relevant number of months after the Systems of Categories B to E and ITI actually become Ready for Overall SMARTICS-2 UAT. If the dates on which the Systems of Categories B to E and ITI becoming Ready for Overall SMARTICS-2 UAT are different, the latest of these dates shall be adopted to determine the completion dates for the aforesaid stages.

(d) For Stages A5.3.1 and A5.4.1, the production environment may be set up during phase 1 at designated sites of ROP branch offices other than the existing location, for the renovation of existing sites of ROP branch offices, if temporary relocation of ROP branch offices to be adopted. After the completion of renovation, the ROP branch offices will be moved back to the existing location. As such, additional services to set up the System and data for ROP branch offices may be required before phase 2. The production rollout approach will be subject to any modifications as confirmed by the Government in the SA&D stage.

2 FUNCTIONAL REQUIREMENTS

2.1 System Objectives

2.1.1 The System shall meet the following objectives for Core System:

(a) support all business functionalities of Registration of Persons ("ROP") processes, including but not limited to, registration and issuance of HKICs with enhancements:

- to deliver more self-service means, online electronic services and automation so as to provide greater convenience to the public; and
- to maintain stringent safeguards for privacy protection of ROP data;

(b) support the provision of other ROP related services for ImmD and other Government bureaux / departments for specific purposes as allowed by the law;

(c) support a territory-wide HKIC replacement exercise within a period of around four years for the entire population of the HKSAR; and

(d) provide the system infrastructure for Core System so as to support normal ROP operation and the territory-wide HKIC replacement exercise.

2.2 System Overview

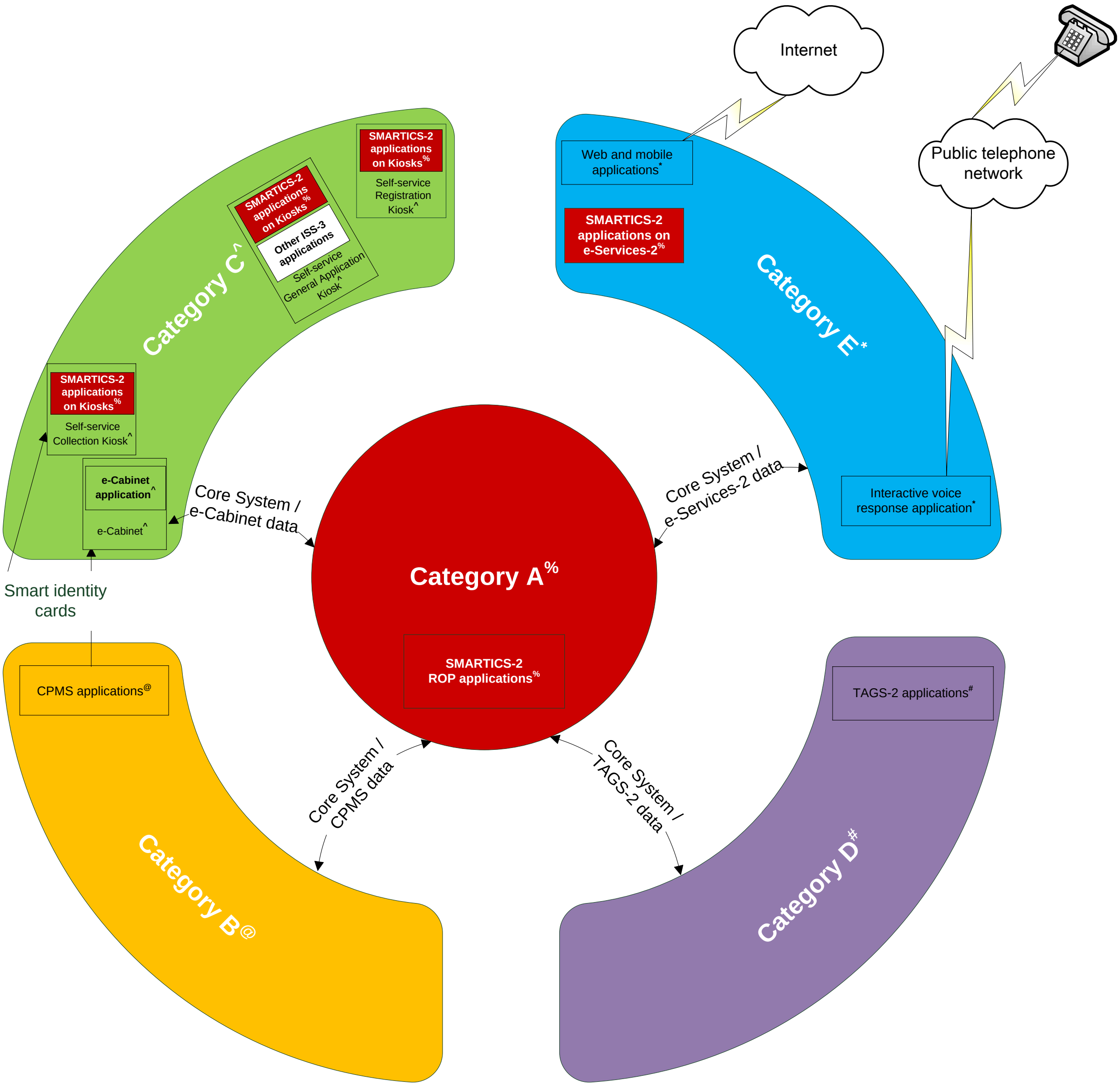
2.2.1 The System to be implemented under this Category A shall cover the following service components:

(a) handling applications for registration of Identity Card ("IC") (including overseas application for Permanent Identity Card ("PIC") from Hong Kong permanent resident staying abroad in connection with overseas application for a HKSAR passport, Minor Permanent Identity Card ("MPIC") for those aged under 11 in connection with application for HKSAR Passport and Consular Corps Identity Card ("CCIC") for consular staff);
(b) replacement of the aforesaid Identity Card;
(c) applications for Certificate of Registered Particulars ("CRP"), Certificate of Exemption ("EC"); and
(d) change of personal particulars of the registrants.

2.2.2 In addition to the normal over-the-counter operation, the above service components shall be provided through self-service general application kiosk ("MSK_GEN"), self-service registration kiosk ("MSK_REG"), self-service collection kiosk ("SCK") and Next Generation Electronic Services System ("e-Services-2") platform. The e-Services-2 platform may be accessed online via PC or other mobile devices.

2.2.3 Application Overview

2.2.3.1 The diagram below indicates the high-level major applications for the System and the integration with the Systems of other Categories:


Internet
Public telephone network
Web and mobile applications*
SMARTICS-2 applications on e-Services-2%
Category E*
Interactive voice response application*
Category C^
SMARTICS-2 applications on Kiosks%
Self-service Registration Kiosk^
SMARTICS-2 applications on Kiosks%
Other ISS-3 applications
Self-service General Application Kiosk^
SMARTICS-2 applications on Kiosks%
Self-service Collection Kiosk^
e-Cabinet application^
e-Cabinet^
Smart identity cards
Core System / e-Cabinet data
Core System / e-Services-2 data
Category A%
SMARTICS-2 ROP applications%
CPMS applications@
Core System / CPMS data
Core System / TAGS-2 data
TAGS-2 applications#
Category B@
Category D#

%Core System	Category A	🟥
@Smart Card and CPMS	Category B	🟨
^MSKS and CabS	Category C	🟩
#TAGS-2	Category D	🟪
*E-Services-2	Category E	🟦

Figure 7A-2.2.3.1 High-level Major Applications for the System

2.2.3.2 Without prejudice to the generality of Section 2.2.1 of this Annex, the business services provided by the System shall support all of the major functions listed in Sections 2.2.3.3 to 2.2.3.16 of this Annex below.

2.2.3.3 Appointment Booking

(a) The System shall provide appointment booking and pre-filling of registration details functions which shall be run on the e-Services-2 platform provided by the Contractor of Category E. The System shall allow the applicant to choose a date within a duration for making appointment. Booking can be made through the Internet (and mobile platforms) or by the telephone via the Interactive Voice Response System ("IVRS"), which is provided by the e-Services-2 under Category E; and

(b) On the e-Services-2 platform, the applicant shall make appointment booking according to the application type and the quota available on a selected date. The applicant will be advised, but not compulsory, to input his / her information in the application form, as part of the registration process (known as application pre-filling). The successful booking, together with the application pre-filling details, if any, will be stored in the database of the e-Services-2 platform and shall be transferred to the System pending retrieval during registration. The applicant can change or cancel the appointment or input again the application pre-filling details before the appointment date.

2.2.3.4 Reception

(a) On the appointment date, the applicant brings the necessary documents to the reception desk of the desired office at the appointment date and time;

(b) For applicants having made appointment, they can approach self-service tag issuing kiosk (to be provided under Category D) to collect printed tags by various ways, including but not limited to, scanning of barcodes or inputting of applicant's identity card number or travel document number themselves. Alternatively, they can approach reception desk and an officer can check from the System to see whether the applicant has reserved an appointment using the applicant's identity card number or travel document number;

(c) If no appointment has been reserved, a "walk-in" tag may be provided to the applicant through TAGS-2 subject to the availability of "walk-in" quota;

(d) The applicant then waits for calling by the registration officer. TAGS-2 shall provide functions to display the tag number to be called next, as well as the latest tag number for each functional unit; and

(e) All tag functions shall be provided under Category D. The Contractor of this category shall coordinate with the Contractor of Category D to work out solutions for application workflow at ROP branch offices and SIDCCs. The System shall match the related information of the applicants to the corresponding tag.

2.2.3.5 Application Registration

<u>At ROP Branch Offices</u>

(a) The System shall provide function(s) for the registration officer to retrieve applicant's personal data from the database if the applicant has previously applied for HKIC and / or has pre-filled personal information during appointment booking for application processing. The System shall provide function(s) for officer to perform record check, as well as for the applicant to check the correctness of the information he / she provided during the registration and he / she is allowed to make changes before confirmation. If no pre-filling of application form is performed, applicant can fill the application form electronically via equipment installed on the registration desk. After record checking, the System shall provide function(s) for the registration officer to print the completed application form for the applicant to append signature on the printed form;

(b) The System shall provide function(s) for the registration officer to capture the applicant’s two fingerprints into digital images, the System shall convert the fingerprint images into templates to be stored in the chip of the new smart identity card and the database. In addition, the new fingerprints captured shall also be verified against the applicant’s historical fingerprints, if any;

(c) The System shall provide function(s) for the registration officer to capture the applicant's facial appearance into digital photo image and perform facial recognition against historical records;

(d) The System shall provide function(s) for the registration officer to scan the signed application form and any relevant supporting document(s) for digital storage; and

(e) The applicant then waits for calling by the assessment officer to go through the application assessment process.

At SIDCC

(f) To kick start the registration process, the applicant shall be required to first perform registration in the self-service registration kiosk. The kiosk will be provided by the Contractor of Category C while the application and the fingerprint scanner (enrolment) shall be provided by the Contractor of Category A. To start the self-service registration in the kiosk, the System shall first perform identity verification by comparing live captured fingerprint with the templates stored in the existing smart identity card and those in the database. After successful identity verification, the System shall provide function(s) for the applicant to fill in the application form in electronic format. If the applicant has pre-filled the electronic application form during online appointment booking, the System shall display the form on screen for applicant to review, allow applicant to confirm the details on the form and print out the form to sign. The kiosk shall support live capturing of two fingerprints of applicant in self-service mode and the new fingerprint images shall be converted to templates to be stored in the chip of the new smart identity card for subsequent identity verification purposes. Upon completion of first part of the registration process (i.e. self-service registration at self-service registration kiosk), application shall be passed to the manned registration desk for second part of the registration process;

(g) In case of failed fingerprint verification or help-through is required, such as the elderly, disabled person, children, etc., they shall be handled in normal registration workflow (i.e. manned registration desk) in the replacement centres, like aforesaid in ROP branch offices;

(h) After performing first part of the registration in the self-service registration kiosks, the applicant will then wait to be called (through TAGS-2) for the second part of registration in the manned registration desk. Before starting the second part of the registration process, the System shall provide function(s) for the registration officer to verify the applicant’s identity by fingerprint verification. After the identity is successfully verified, the System shall provide function(s) for the registration officer to capture the applicant's facial appearance into digital photo image, perform facial recognition against historical records and scan the signed application form submitted by the applicant. Automatic Record Check (“ARC”) shall also be performed by conducting a series of record checks on the applications based on the pre-defined criteria automatically. The design of the System shall facilitate registration officer to complete the workflow (as described in this Section 2.2.3.5 (h))within 6 minutes; and

(i) After the registration process, the applicant then waits for calling by an assessment officer. If no irregularity is noted, the registration officer may also print a Notice of Collection (“NOC”) to inform the applicant about the date of collection of the new identity card before the applicant is allowed to leave.

2.2.3.6 Assessment

(a) At the assessment desk, after the applicant has completed registration as described in Section 2.2.3.5 of this Annex above, the System shall perform ARC for all HKIC applications in daily ROP and SIDCC operation based on some pre-defined criteria. Upon interview with the applicant, the assessment officer will assess the application based on ARC checking results and other application information (including but not limited to, the applicant’s personal details, photo, fingerprint and other related document images). The System shall provide function(s) for the assessment officer to conduct liveliness checking of the applicant’s fingerprints and to compare with those captured during registration and the historical fingerprints, if any;

(b) For HKIC renewals at SIDCCs and replacements in ROP branch offices of which the payment of fee is not required, after assessment, a NOC, or an acknowledgement form of application for an identity card (“acknowledgement form” / “ROP140”) shall be printed by the assessment officer and issued to the applicant showing the date of collection of the new HKIC;

(c) If a payment of a fee is required (e.g. due to damage, loss or change in personal particulars, etc.), after assessment, the applicant will be required to pay in shroff office, after fee payment (e.g. by cash, cheque or others), the System shall provide function(s) for issuance of the acknowledgement form (i.e. ROP140A). The details of the shroff transaction shall be recorded in the System; and

(d) The applicant will then leave the office.

2.2.3.7 Verification

After the application is assessed in a ROP office or SIDCC, the application will be passed to the Verification Office, where the System shall perform checking on duplication of applications and allow final verification be performed against all digitised application data and historical record (including images), if any, before card personalisation.

(a) All the verification tasks for applications after assessment at the ROP branch offices and SIDCCs will be processed centrally in the Headquarters;

(b) In the Verification Office, the applicant’s registration details shall be retrieved from the System for checking against the previous identity card application records, other record checking shall also be performed;

(c) For the application with applicant's previous digital fingerprint images to be kept in the Image Management System (“IMS”) to be developed by the Contractor and more particularly specified in Section 2.3.3.2.31 of this Annex, automatic fingerprint matching shall be performed to compare the fingerprints in the previous application against those in the current application;

(d) The matching result and the fingerprint image shall be displayed on screen; and

(e) The System shall provide function(s) for random spot check by supervisors.

2.2.3.8 Card Personalisation

After the application is verified at the Verification Office, the application is ready for personalisation. The System shall pass the necessary details to the card personalisation system provided under Category B for personalisation of new smart identity cards. The System shall keep inventory records of cards personalised with information obtained from CPMS (provided by the Contractor of Category B), as well as records of cards to be checked in into electronic cabinet for cards (“e-Cabinet”) or self-service collection kiosks which will be provided by the Cabinet System (“CabS”) under Category C.

2.2.3.9 Card Issue

(a) The System shall provide functions to allow the applicants to collect personalised new smart identity cards in a self-service manner. The metal cover of the self-service collection kiosk together with peripherals will be provided by the Contractor of Category C. Under the self-service smart identity card collection workflow, the applicant shall first approach a self-service tag issuing kiosk of TAGS-2 provided by Contractor of Category D or reception desk, based on the information provided by the applicant (such as the barcode on the NOC or ROP140 / ROP140A, or HKIC number), the System shall provide information of the self-service collection kiosk (or counter) that the applicant should approach to pick up the new smart identity card. In case of self-service tag issuing kiosk, the System shall interface with TAGS-2 to provide relevant information to the applicant;

(b) The applicant will then approach the self-service collection kiosk and insert his / her existing smart identity card or ROP140 / ROP140A into the kiosk. The kiosk shall verify the genuineness of the existing smart identity card or ROP140 / ROP140A. If the verification fails, the kiosk shall return the card or the ROP140 / ROP140A and direct the applicant to the manned collection desk. If the genuineness is verified, the identity card or the ROP140 / ROP140A will be collected and the applicant will be prompted to conduct identity verification by checking the live captured facial and fingerprint images against those stored in the database or in the chip of existing smart identity card, if applicable. If identity verification is successful, the dispenser inside self-service collection kiosk (which is provided under Category C) shall retrieve the new smart identity card from the secure storage and dispense to the applicant after his / her identity is verified with facial image and fingerprint template stored in the chip of new smart identity card and his / her presence in front of the kiosk is confirmed. The Contractor shall coordinate with Contractor of Category B to verify and ensure that no unique serial number of the chip can be read via contactless interface without authorised mutual authentication ("MA") once it is issued to the applicant. For any abnormal scenario, the new smart identity card shall not be issued to the applicant and the System shall alert supervisor to handle;

(c) e-Cabinet (to be provided under Category C) shall be installed in the card collection office in ROP branch offices and SIDCCs for storage and automatic retrieval of newly personalised smart identity cards which will be issued by a card issuing officer over counter. The System shall interface with the e-Cabinet which will provide automatic card dispensation function with automatic check-in, storage, retrieval and dispensing mechanism. During the retrieval process, the System shall obtain information from the counter regarding the new smart identity card to be issued, such as by ways of inputting the HKIC number, or scanning of barcode at collection desk or from TAGS-2 (viz. the self-service tag issuing kiosk), and pass the information to e-Cabinet of Category C for auto-dispensation of the new smart identity card. The personalised new smart identity card will be collected by the card issuing officer and be issued to the applicant or the proxy over the collection desk;

(d) When a batch of personalised new smart identity cards is delivered to respective ROP branch office or SIDCC, the cards will be checked in into the secure storage of the e-Cabinet or self-service collection kiosk and the System shall obtain information from the CabS (to be provided under Category C) on the cards stored and dispensed for record purpose;

(e) The System shall provide function(s) for the card issuing officer to verify the applicant's live fingerprint and facial appearance against the fingerprint and photo stored in the new smart identity card via contact and contactless interfaces. The System shall coordinate with Contractor of Category B to verify and ensure that no unique serial number of the chip can be read via contactless interface without authorised mutual authentication before the new smart identity card is issued;

(f) If the card is collected by a proxy, the proxy will directly approach the collection desk, the card issuing officer will check the photo on the existing smart identity card / ROP140 or ROP140A against the photo in the database and scan the collection authorisation form. When the checking is completed successfully, the card issuing officer will issue the new smart identity card to the proxy. The System shall update the card status automatically;

(g) The System shall provide function(s) for an applicant to check the chip data of the new smart identity card using MSK_GEN (to be provided under Category C) after fingerprint verification; and

(h) In case if the applicant fails to verify fingerprint / facial image in the self-service collection kiosk or changes to collect the new smart identity card by proxy, the System shall work with CabS to provide secure means for the card issuing officer to retrieve the new smart identity card stored in the self-service collection kiosk and perform the manual workflow of card issuance at the collection desk.

2.2.3.10 Minor Permanent Identity Card (“MPIC”) / Overseas Permanent Identity Card (“OPIC”) Applications

(a) The System shall process MPIC / OPIC application submitted together with passport application by post / in person (with application form in paper format). OPIC application is referred to Travel Documents and Nationality (Application) (“TDNA”) Section by respective Chinese Embassy;

(b) Staff of TDNA Section captures the application data and supporting documents (if any) into Electronic Passport System (“e-Passport”) and sends the relevant ROP application form and supporting documents to staff of Registration of Persons (Records) (“ROP(R)”) Section for ROP application indexing;

(c) The System shall provide functions to create new MPIC / OPIC application, perform application indexing and scan document images, including photo, fingerprints and any supporting documents to proceed with the application assessment. The processing of MPIC / OPIC application shall be handled by workflow engine;

(d) Upon the implementation of Next Generation Electronic Passport System (“e-Passport-2”), the System shall provide function(s) for new MPIC / OPIC application to be indexed automatically by receiving personal particulars interfaced from e-Passport-2. The System shall provide functions for supporting such interface with e-Passport-2, which will be implemented in early 2019 tentatively;

(e) The System shall conduct ARC after indexing and the case shall be routed to a case officer for assessment. Approved case shall then be sent to Card Personalisation and Management System (“CPMS”) (to be provided under Category B) for production of new MPIC / OPIC;

(f) An e-Cabinet shall be provided by the Contractor of Category C and installed in the Travel Documents (Issue) (“TDI”) Section for storage of newly personalised MPIC and OPIC for arrangement of speedy retrieval and matching with the corresponding HKSAR passport. The System shall interface with the e-Cabinet for management of inventory; and

(g) The System shall provide functions to support, including but not limited to, linking up of records for the MPIC / OPIC and the respective passport, processing status and card status of MPIC / OPIC to e-Passport-2 and receiving information from e-Passport-2 for retrieval of cards from e-Cabinet installed in TDI Section, as well as any related system interface between the System and e-Passport-2, which will be implemented in early 2019 tentatively. The details of system interface will be confirmed during SA&D stage.

2.2.3.11 Consular Corps Identity Card ("CCIC") Application

(a) The System shall provide function(s) for an officer in the Registration of Persons (Support) ("ROP(S)") Section to perform indexing and scanning of relevant documents for case creation. The System shall provide function(s) for the officer to scan portrait photo provided by the applicant and any other relevant documents into the system. Record check shall be conducted based on pre-defined rules and a specific card number will be allotted and the application will be registered in a control register. The System shall provide function(s) for the officer to assess and approve the application through workflow engine. The System shall also scan and store an image of the prepared CCIC for retention; and

(b) The System shall provide function to prepare and generate the covering letter for issuance of CCIC.

2.2.3.12 Amendment of Registered Particulars Application

(a) HKIC holders can apply for change of personal and registered particulars, whether or not appear on the card face of identity card, through the submission of forms "Notification of Change of Particulars Previously Registered" ("ROP18"), "Notification of Change of Address" ("ROP18A") and "Application for Amendment of Registered Particulars of Hong Kong Identity Card" ("ROP73"). Applicants who want to amend their registered particulars can submit the forms by post, e-mail (using Digital Certificate ("e-Cert")) and online submission through ImmD homepage or mobile platform (riding on the e-Services-2 platform to be provided by the Contractor of Category E). Change of address and telephone number can also be submitted through MSK_GEN;

(b) For application for amendment of registered particulars which requires re-issuance of HKIC, the System shall allow officers to allot the application to respective ROP office responsible for the case. For application received by post, the System shall provide functions for case initiation, data input, scanning of relevant documents, performing application indexing and record checking. The System shall then route the case to relevant ROP office for assessment;

(c) The System shall provide function(s) for putting up the case to senior officers for approval if required; and

(d) For application for amendment of registered particulars which does not require re-issuance of HKIC (such as address, name of spouse, etc.), applications submitted (by post or electronic means) will be processed by ROP(S). The System shall provide function(s) for officers in ROP(S) Section to perform indexing, inputting and scanning of relevant documents into the System. If application is submitted through electronic means, the amendment details will be updated to the relevant record automatically after reviewed, clarification and approval by officers.

2.2.3.13 Certificate of Registered Particulars ("CRP") Application

(a) The System shall provide online appointment booking for CRP application with submission of necessary information (filling required data in pre-defined electronic application form);

(b) Reception officer of the respective ROP office shall initiate the case under workflow and provide a tag number to CRP applicant (through TAGS-2 as provided under Category D);

(c) Upon attending the interview, applicant is required to confirm the data provided in the application. After confirmation, the System shall provide function(s) for a case officer to scan supporting documents (if any), perform application indexing and accept payment at ROP branch office;

(d) The CRP application shall be routed to the ROP(S) Section for preparation and production of CRP;

(e) Post in application shall be handled by ROP(S) Section by performing indexing and case creation through workflow;

(f) The System shall provide templates for different CRP contents and support the auto-filling of registered particulars into CRP templates (if data already in text format). The System shall provide function(s) for the officer to update the CRP contents and create / amend CRP templates; and

(g) The System shall route the CRP application between ROP(S) and ROP branch office and the completed case shall be routed to the respective ROP branch office for review and updating of the case result and the physical CRP in paper form shall be printed for issuance to applicant. The System shall provide function(s) to scan the signed CRP copy and record the issuance of CRP in ROP branch office.

2.2.3.14 Certificate of Exemption ("EC") Application

(a) Once an EC application is received by post or in ROP office, the System shall provide functions for officers to scan all supporting documents, input all application details and perform indexing. The officer will conduct checking of application information such as whether written and signed request and recent portrait photo of applicant have been provided. The System shall provide functions for EC application, scanning of portrait photo and sending an acknowledgement to the applicant (or the representative). In case if further clarification is required for assessment, the System shall provide function(s) to prepare and generate a request for clarification or further supporting documents and send the request to the applicant / representative. The System shall retrieve all details from the database for processing. The officer will check all details and summarise the case, input remarks relating to the application (if necessary) and submit the application through system workflow to a senior officer for cross-checking and approval. After approval, the System shall print the personalised EC (including portrait image), input audit number of respective EC for completion of the transaction and the EC will be printed for signature by the senior officer. Letter to applicant / representative informing the collection of EC at ROP branch office or by registered post will be prepared and issued through system workflow. Designated ROP branch office will issue the EC upon collection; and

(b) The System shall provide function(s) for submission of application for EC through applications on e-Services-2 platform. The System shall provide function(s) for the applicant to fill in the electronic form and attach / upload supporting documents for the EC application. The System shall support case creation, processing, approval and issuance in the system workflow. The System shall generate corresponding statistical reports automatically.

2.2.3.15 Potential Juror Selection

(a) The Jury Unit within the ROP(S) Section is responsible for counter-checking eligible persons to act as jurors in accordance with the Jury Ordinance and providing information to the Judiciary for updating the computerised Juror Information System. The System shall provide function(s) for compiling potential jurors list on daily basis. The potential juror list will be generated as follows:

(i) based on pre-defined criteria, the System shall compile a list of potential jurors every day from the HKIC applications received and the lists submitted by universities regarding names and identity card numbers of students who graduate recently from the universities (in electronic format and hardcopy);

(ii) the System shall provide convenient means to assist officers in Jury Unit of ROP(S) Section to send out stencil forms (such as by e-mail) to university graduates requesting them for updated addresses. The System shall also provide tools to assist officer to capture and update the new addresses as reported by the university graduates using stencil forms into the System, such as by means of handwriting character recognition software; and

(iii) the System shall provide functions for Jury Unit to generate eligible juror list (together with all necessary information) and send the potential juror list generated by ROP Jury Unit to the Judiciary through encrypted electronic means via the Government network. The compiled juror list shall be able to be retrieved from the System easily;

(b) The consolidated list of potential jurors shall be retained in the System for record purposes; and

(c) The public can submit the ROP18 (or ROP18A) by post, e-mail or via applications on e-Services-2 platform and the change of address application can also be submitted through MSK_GEN. The System shall compile the potential jurors list based on information obtained from these various means.

2.2.3.16 Fingerprint Verification

(a) Staff of Verification Unit of ROP(R) Section performs manual fingerprint verification for more than 200 cases daily. Such verification process requires the case officer to compare the new fingerprint images with the existing ones in database by visual inspection in order to ensure that they are identical to each other. The officers are also required to check the scanned documents against historical information;

(b) The System shall implement mechanism and software to visually identify the minutia points on the fingerprint images or on ridge lines to facilitate the manual verification process; and

(c) The System shall display minutia points generated from the digitalised fingerprint images on screen in order to facilitate the case officer for visual inspection. As a result, case officer can perform manual fingerprint verification in a more effective way. The System shall provide function(s) to print hardcopies of fingerprint images.

2.2.4 Infrastructure Overview

2.2.4.1 The system architecture of SMARTICS-2 shall comprise multiple service layers, namely the **Front-end Service Layer**, **Local Service Layer**, **Central Service Layer** and **ITI Service Layer** with physical locations across the PDC(KC), DDC(FL), ROP offices (including branches located outside HQ), SIDCCs, control points, HQ and other immigration offices outside HQ. Section 1.2.4 of Part VII sets out the description on the system architecture of SMARTICS-2.

2.2.4.2 The diagram below shows the high-level conceptual infrastructure topology of the Core System:

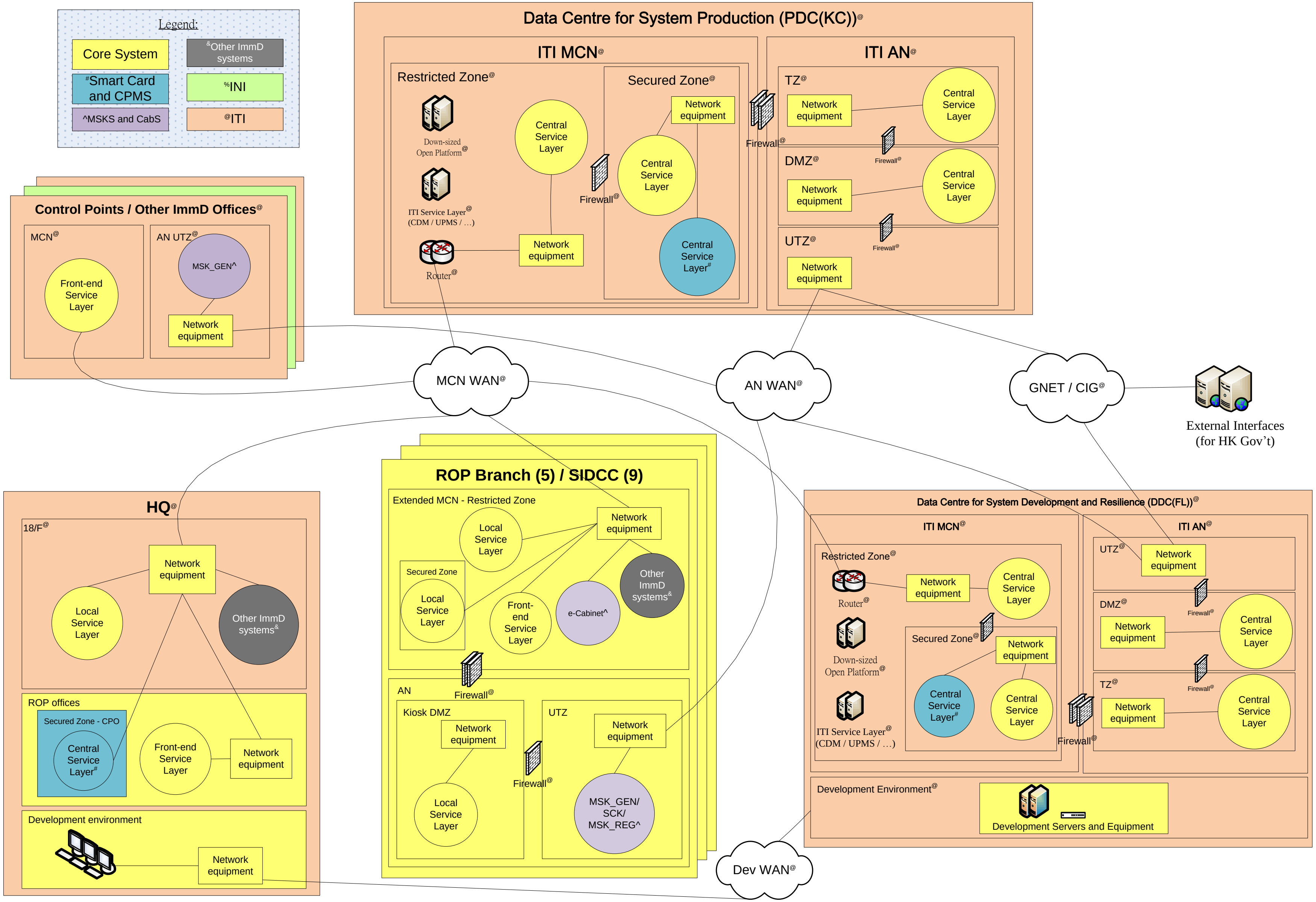


Figure 7A-2.2.4.2 High-level Conceptual Infrastructure Topology of the System

2.2.4.3 New Information Technology Infrastructure ("ITI"), comprising the Administrative Network ("AN") and the Mission Critical Network ("MCN"), is implemented at the PDC(KC) and DDC(FL) to support the ISS-3 systems and other future systems for ImmD. It involves an IP network that is interoperable with existing Immigration New Infrastructure ("INI"), on which existing ISS-2 systems of ImmD are riding. Details of INI are described in Section 2 of Appendix C – "Description of IT Infrastructure of ImmD" to Part VII. The Contractor in the implementation of the network for the System shall have to extend the MCN to other physical locations including all ROP branch offices and all SIDCCs ("Extended MCN") and establish the local kiosk network in all ROP branch offices and all SIDCCs ("Local Kiosk Network"). It is the scope of the Implementation Services to supply and install network equipment for all ROP branch offices and all SIDCCs to connect to the ITI MCN network at the PDC(KC) and DDC(FL) and set up the Extended MCN and Local Kiosk Network for all ROP branch offices and all SIDCCs. The diagram below illustrates the high-level concept for the Extended MCN and Local Kiosk Network.

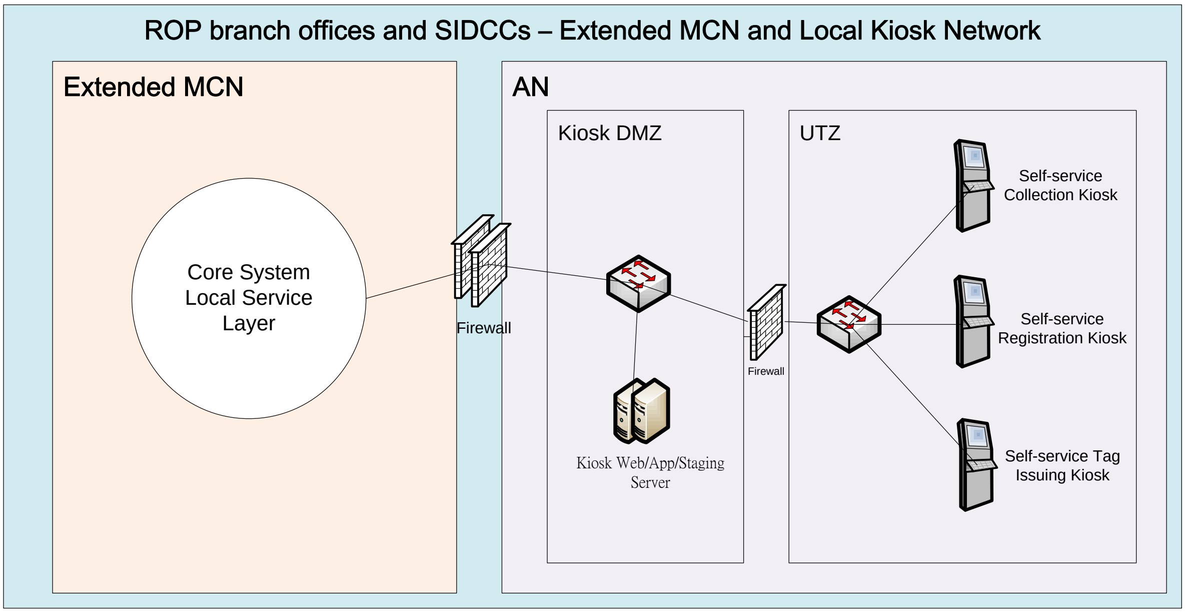

ROP branch offices and SIDCCs – Extended MCN and Local Kiosk Network
Extended MCN
AN
Kiosk DMZ
UTZ
Core System Local Service Layer
Firewall
Firewall
Kiosk Web/App/Staging Server
Self-service Collection Kiosk
Self-service Registration Kiosk
Self-service Tag Issuing Kiosk

Figure 7A-2.2.4.3 Extended MCN and Local Kiosk Network Diagram for the System

The scope of the Implementation Services does not include the provision of network equipment to connect to the MCN network as those offices will make use of existing ISS-2 systems, which are riding on INI network, to support the business operation until its respective ISS-3 systems (e.g. e-Passport-2) are implemented; or some offices are already riding on ITI network (e.g. ICONS would be rolled out in control points via the ITI network in 2016). For other immigration offices which are riding on INI network, the workstations of the System shall make use of the INI network to connect to the System until the respective ISS-3 project procuring network equipment to extend the MCN to the related immigration offices.

2.2.4.4 The Contractor shall have to establish the general kiosk network in the locations, including all ROP branch offices, all SIDCCs, all control points and the immigration offices inside and outside HQ ("General Kiosk Network"). It is also the scope of the Implementation Services to supply and install network equipment for all ROP branch offices, all SIDCCs, all control points and the immigration offices inside and outside HQ to connect to the ITI AN at the PDC(KC) and DDC(FL) and set up the General Kiosk Network to support self-service general application kiosks (where the kiosks are to be provided under Category C).

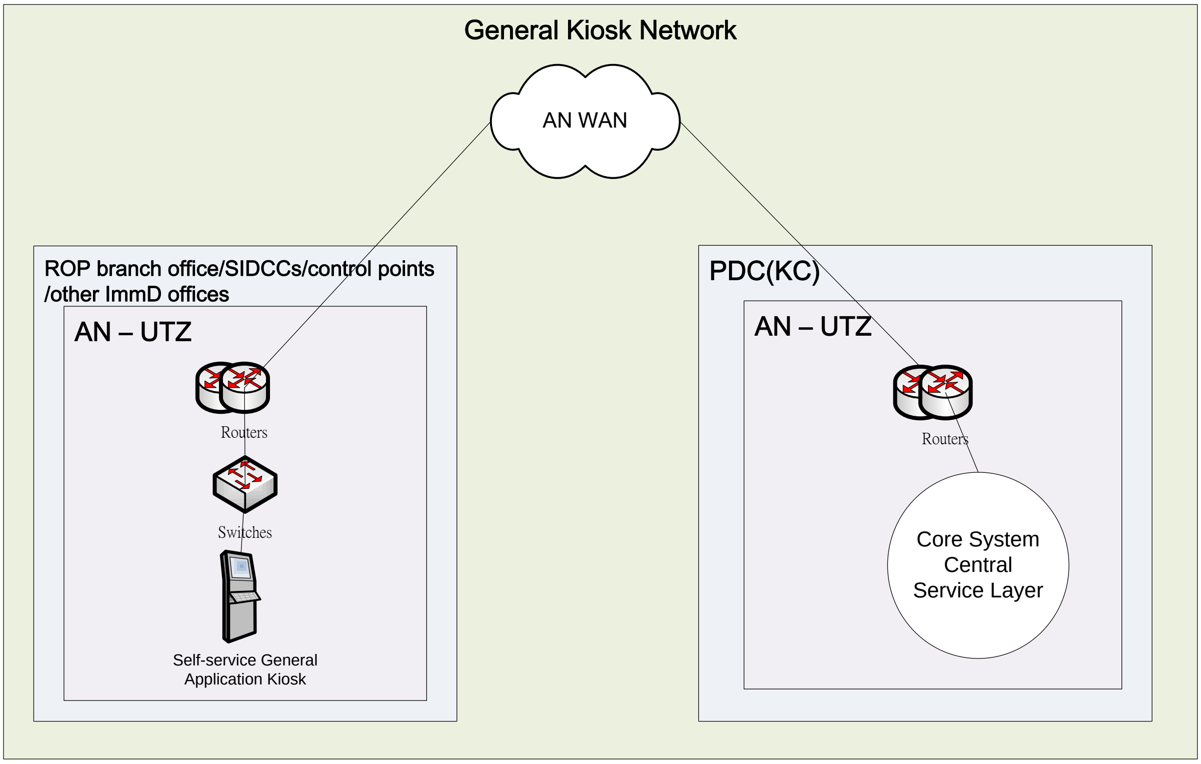

General Kiosk Network
AN WAN
ROP branch office/SIDCCs/control points /other ImmD offices
AN – UTZ
Routers
Switches
Self-service General Application Kiosk
PDC(KC)
AN – UTZ
Routers
Core System Central Service Layer

Figure 7A-2.2.4.4 General Kiosk Network Diagram for the System

2.2.4.5 The system infrastructure of the System shall be compatible and fully integrated with ITI. Without prejudice to the recommendations set out in Appendix B which have been incorporated in this Annex as essential requirements, the selected technical system options described in Section 5 in Appendix B – "Extract of the Feasibility Study Report on the Implementation of SMARTICS-2" and Appendix C – "Description of IT Infrastructure of ImmD" to Part VII shall be complied with in the design and implementation of the System.

2.2.4.6 The system infrastructure for the System provides network equipment, servers, storage, related software and services across different physical locations, including PDC(KC), DDC(FL), ROP branch offices, SIDCCs, HQ, control points and other immigration offices outside HQ via the ITI MCN, Extended MCN, Local Kiosk Network, ITI AN or General Kiosk Network as indicated in the diagrams. Workstations for the System, self-service kiosks (including self-service registration kiosks, self-service general application kiosks and self-service collection kiosks) at these locations will access the System functions through the aforesaid network directly. Nonetheless, there are still workstations of existing ISS-2 or ISS-3 systems at these locations to support business operation of ImmD. The system infrastructure for the System shall be able to support these workstations at these locations to access respective ISS-2 or ISS-3 systems which primarily hosted at HQ or PDC(KC) respectively. Section 2.3.5.3.8 of this Annex sets out the system infrastructure for the System at ROP branch offices and SIDCCs.

2.2.4.7 Some workstations for the System will be installed at control points or immigration offices (at HQ or outside HQ), which is riding on ITI or INI at these immigration offices. As only INI is available at some immigration offices, the system infrastructure for the System shall support the workstations for the System at these locations to access functions for the System hosted at PDC(KC) and DDC(FL) via the INI (and subsequently via ITI when all existing ISS-2 systems become obsolete). Sections 2.3.5.3.9 and 2.3.5.3.10 of this Annex sets out the system infrastructure of Core System at HQ, control points and immigration offices outside HQ.

2.2.4.8 SMARTICS-2 is a mission-critical application, which shall be built mainly on the infrastructure of ITI MCN, the Extended MCN and the Local Kiosk Network, with other supporting functions to be built on ITI AN and the General Kiosk Network. The communication and interfaces between SMARTICS-2 and other Government departments shall be built on the AN, which is connected to the Government Backbone Network (“GNET”).

2.2.4.9 The infrastructure of the Core System shall consist of the following infrastructure components, which are to be described in details from Sections 2.3.4 to 2.3.13:

(a) network and communication infrastructure;

(b) server and storage infrastructure;

(c) data management infrastructure;

(d) application services infrastructure;

(e) business services provisions;

(f) system management and backup infrastructure;

(g) cryptography and security infrastructure;

(h) development, testing and training environments; and

(i) development and testing tools.

2.2.4.10 The equipment installed at ROP branch offices, SIDCCs, HQ, control points and other immigration offices outside HQ shall not require computer operators and shall require very minimal user intervention during situations such as activation of peripheral equipment, system recovery, etc. All remote system operations shall be centrally and remotely managed at each of PDC(KC), DDC(FL) and HQ.

2.2.4.11 The System shall adopt the latest Information and Communication Technology (“ICT”) trends to enhance system performance and availability with possibilities to reduce ImmD resources and workload. The adopted system architecture shall also be technology proof, with the alignment of the ITI future development, for system scalability and technology upgrades on core functional components.

2.2.4.12 The System shall be of high availability and resilience and redundancy shall be incorporated according to the requirements specified in the Project Specifications and wherever appropriate.

2.2.4.13 The design of the System shall be modular. The interdependency between the front-end and back-end systems shall be minimised. Therefore, even in the very rare case when the back-end system is not available, the System shall still provide front-line identity card registration and collection services as long as the equipment at the registration and collection desks are functioning.

2.2.4.14 The System shall maintain repository at data centres, ROP branch offices and SIDCCs to store ROP records with biometric information in order to support the ROP business services in ROP offices and the territory-wide HKIC replacement exercise in SIDCCs.

2.2.4.15 The System shall maintain repository at ROP branch offices and SIDCCs to store essential information in order to enhance the service resilience in ROP branch offices and SIDCCs for any network or centralised server service outage.

2.3 Functional Specifications

2.3.1 Tenderer's Responsibility

2.3.1.1 The System shall be easy to operate, manage and maintain. Tenderers shall illustrate in Schedule 4 – "Technical Proposal and System Configuration" of Part V how the proposed technical solution can meet the requirements. Tenderers shall also propose solution to streamline the system operation, management and maintenance.

2.3.1.2 Tenderers shall state in Schedule 3 – "Specifications" of Part V their approach and methodology in quality management and assurance and project management.

2.3.1.3 Tenderers shall propose the bandwidth requirements for the communication lines to be supplied by the Government for the implementation of the System with respect to the WAN infrastructure for MCN and AN in Schedule 3 – "Specifications" of Part V.

2.3.1.4 Tenderers shall provide an overall configuration of the System in Schedule 4 – "Technical Proposal and System Configuration" of Part V, in particular its effectiveness in catering for high stability and performance requirements, the resilience and redundancy support, the scalability requirements, as well as the resources configuration of individual partition or virtual machine for each server and equipment.

2.3.1.5 In Schedule 4 – "Technical Proposal and System Configuration" of Part V, Tenderers shall propose the overall infrastructure for the Core System in PDC(KC), DDC(FL), ROP offices, SIDCCs, HQ, control points and ImmD offices outside HQ, including the infrastructure and network equipment to support MSK_GEN, MSK_REG, SCK and e-Cabinet (the front-end service layer to be provided under Category C), the infrastructure services and uninterruptible power supply ("UPS") requirements in ROP branch offices and SIDCCs.

2.3.1.6 Tenderers shall provide the preliminary design of Custom Programs for the System in Schedule 5 – "Preliminary Design for the Custom Programs" of Part V.

2.3.1.7 Tenderers shall propose in Schedule 5 – "Preliminary Design for the Custom Programs" of Part V the batch functions including filing of images to IMS, generation of reports and statistics, system and database backup for the System, record uploading, data synchronisation, online printing and secure printing for confidential reports. Tenderers shall also propose the schedule of batch functions and the length of overall batch window.

2.3.1.8 To extent applicable, Tenderers may provide in Table 5-4.2(A) of Schedule 4 of Part V the desirable features and functions including flexibility, reliability and resilience, integration of system components as a total solution and security respectively for assessment as specified in Annex C – "Marking Scheme for the Technical Assessment of Category A" to Part II – "Conditions of Tender", with detailed elaboration on how such features and functions can be fulfilled in the technical design and configuration of the System. For tender evaluation, **marks** will be given to the Tenderers if the desirable features and functions are relevant and such features and functions are provided in Table 5-4.2(A) of Schedule 4 of Part V. Tenderers shall note that a tender which fails to obtain the pass mark for assessment criterion 3 "Tenderer's Proposed Technical Solution" in Annex C to Part II will not be considered further as specified in Annex A – "Tender Evaluation Procedures and Assessment Criteria" to Part II – "Conditions of Tender".

2.3.1.9 Without prejudice to the recommendations set out in Appendix B to Part VII which have been incorporated in this Annex as essential requirements, the selected technical options described in Section 5 in Appendix B – "Extract of the Feasibility Study Report on the Implementation of SMARTICS-2" and Appendix C – "Description of IT Infrastructure of ImmD" to Part VII shall be complied with in the design and implementation of the System.

2.3.1.10 Tenderers shall propose any necessary contingency measures and provide the detailed contingency plan in Schedule 21 – "Information Summary" of Part V for catching up any possible project slippage. The contingency plan shall be exercised upon request by the Government in case of project slippage.

2.3.2 Contractor's Obligations concerning the Functional Requirements

2.3.2.1 The Contractor shall design and implement the System, which shall possess all functionalities to support the business functions specified in Section 2.2.3 of this Annex:

(a) all functionalities of the system of the SMARTICS (as described in Appendix A – "Description of Existing Systems" to Part VII, particularly in Sections 1.2, 1.3, 1.5 and 4);

(b) all functionalities proposed in the new business initiatives (as described in Appendix B – "Extract of the Feasibility Study Report on the Implementation of SMARTICS-2" to Part VII, particularly in Sections 4.5, 4.6, 4.7 and 5, as well as the related user requirements, data specifications and function specifications as described in Sections 1 to 3) unless any such functionalities or any part thereof are expressly stated to be implemented by the Contractor of another Category in another Annex to Part VII which relates to such Category;

(c) those functionalities as implemented by any system changes to the ROP System of the SMARTICS until the rollout of the System; and

(d) all new functions of the System as stated in this Annex,

but in each case of (a) to (d) subject to such System Design Refinements and Elaborations (as defined in Section 17.8.4 of Part VII) to be raised by the Government from time to time during the Implementation Period.

2.3.2.2 Brief descriptions of the existing functions and new user requirements are set out in Appendix A – "Description of Existing Systems" and Appendix B – "Extract of the Feasibility Study Report on the Implementation of SMARTICS-2" ("FSR") to Part VII respectively which form part of the Contract requirements. In the event of any inconsistency between these Appendices and this Annex A or another Annex to this Part VII, this Annex A or another Annex to this Part VII shall prevail.

2.3.2.3 The Contractor shall provide a total solution for the System and be responsible for the integration of the System with other systems as stipulated in Section 1.4.1 of Part VII (viz. the "Integral Systems").

2.3.2.4 When implementing the System, the Contractor shall adhere to the design as proposed in Schedule 4 – "Technical Proposal and System Configuration" - of Part V and subsequently to be further expanded and elaborated in the SA&D stage, which design must be compliant with all essential requirements, subject to any modifications as approved by the Government.

2.3.2.5 The Contractor of this Category shall implement the System as follows:

2.3.2.5.1 The Contractor shall provide a solution for the System that is highly flexible to cope with the future growth, in terms of both technology and workload.

2.3.2.5.2 The System shall be able to cater for the projected workload of ROP business for at least ten (10) years from the Completion Date, tentatively up to 2028, as specified in Section 5 of Part VII.

2.3.2.5.3 The System shall be scalable and expandable such that new ROP offices can be set up, identity card registration, assessment and collection workstations, self-service registration kiosks, self-service general application kiosks and self-service collection kiosks can be installed in any ROP branch offices and SIDCCs without the need for re-designing the System.

2.3.2.5.4 The System shall allow flexibility to support multiple modes of operation to meet different operational needs. The processes and mechanisms shall be flexible and robust enough to allow authorised control officers to adjust system parameters and switch between different modes of operations to cater for different operating environments.

2.3.2.5.5 The Contractor shall be responsible for the compatibility and interoperability of all Integral Systems as a whole.

2.3.2.5.6 The Contractor shall ensure quality and security of the data processed, handled or stored in the System. Data integrity shall be protected against all the possible threats, such as mis-keying, corruption of system or data, malfunction, unreliability or unavailability of the System service or component.

2.3.2.5.7 The Contractor shall protect the System against unauthorised data access. In this regard, security features for hardware, system software and application software must be provided. Moreover, the System shall be guarded against the interception of traffic, and hence access to data that can be replayed later as a means of achieving masquerade.

2.3.2.5.8 The Contractor shall adopt adequate privacy and security features for controlling the access and interface of the System with the External Systems (as defined in Section 1.4.1 of Part VII). The System shall provide different levels of access control to system data and resources to allow authorised control officers to operate the System securely. The System shall have measures to minimise the privacy risk and to improve system security and be compliance with the data privacy requirements as provided under PD(P)O.

2.3.2.5.9 The Contractor shall provide audit trailing and logging in the System so as to ensure that enough details are gathered for the effective detection and identification of the anomalies, the miscreants, the investigations performed, and the procedures and processes performed.

2.3.2.5.10 The Contractor shall provide a complete solution that is capable of supporting the input, storage, display and printing a mix of English and Chinese characters including the ImmD specific Chinese characters. The System shall support the input and display of textual messages in both English and Chinese. The latest version of ISO/IEC 10646 shall be adopted and used as the base of Unicode support of SMARTICS-2.

2.3.2.5.11 The Contractor shall provide the software and the Custom Programs that present user-friendly interface and online help facilities that are suitable for non-technical personnel.

2.3.2.5.12 The Contractor shall be aware of and analyse the potential impact of the System implementation to the other ImmD systems, propose the transitional arrangement and coordinate with the relevant parties to seamlessly cater for the changes.

2.3.2.6 The Contractor shall provide a complete and fully functional System, including Hardware, Software and Custom Programs.

2.3.2.7 Documentation for the Existing Systems may be made available for reference by the successful Contractor upon contract award. Regardless of whether or not it is available, the Contractor shall be required to review, clarify and confirm the requirements during SA&D stage ("user requirement affirmation process") but not relying on the existing documentation without going through the user requirement affirmation process. If so required (e.g. some of the system details are not available from the documentation), the Contractor shall be responsible for studying the custom programs of the ROP System to ensure that all functions of the ROP System are provided by the System.

2.3.2.8 The Contractor shall provide Implementation Services and System Support and Maintenance Services for the System. Details of the services required are stated in Section 17 – "Implementation Services" and Section 18 – "System Support and Maintenance Services" of Part VII, and Sections 9 and 10 of this Annex.

2.3.2.9 For the fingerprint verification with the fingerprint templates stored in the chip of the existing smart identity card and the database, ImmD will provide algorithms of fingerprint template minutiae extraction and verification to the Contractor. The Contractor shall use and integrate these algorithms with the System for fingerprint template minutiae extraction and verification with the fingerprint templates stored in the existing smart identity card. The Contractor shall provide support services to maintain the existing fingerprint template minutiae extraction and fingerprint verification algorithms. More details of the fingerprint template minutiae extraction and verification algorithms will be provided to the Contractor during SA&D stage.

2.3.2.10 As the Systems provided under all Categories and other Integral Systems are inter-related, the Contractor of this Category shall act as the Prime System Integrator for all Categories and other Integral Systems including the ITI and INI to ensure the successful integration of all Integral Systems.

2.3.2.11 The Contractor shall be responsible for supplying all hardware and software, and developing all application programs and systems to implement all of the functional requirements as specified in this Section 2.3 unless it is expressly stated in this Annex and / or in the other Annexes to the Project Specifications that they shall be the responsibilities of the other parties.

2.3.2.12 The Contractor shall be responsible for the design of the interfaces specifications between the System and the Systems of other Categories and other Integral Systems, and shall take on the role of Prime System Integrator for the proper integration of all Integral Systems as a whole comprising the Systems of all Categories and other Integral Systems. Once the design for these interfaces specifications have been developed and proposed by the Contractor, the Contractor shall confirm and seek the agreement of such design with the Government and Contractors of other Categories and contractors of other Integral Systems. Once such the interface specifications have been agreed amongst them, the Contractor of the relevant Category and contractor of other Integrals Systems shall be responsible for the developing of individual Custom Program based on the agreed interface specifications for integration between the System and the system of that relevant Category and other Integral Systems.

2.3.2.13 The Contractor shall be responsible for the design, development and implementation of the common data services for SMARTICS-2 (as more particularly described in Section 2.3.8.22 of this Annex), including the related functions and services, for SMARTICS-2 to be running on ITI Service Layer. The components under ITI Service Layer are described in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII.

2.3.2.14 The Contractor shall implement the functions and services of common data services for SMARTICS-2 listed in the Appendix J – "List of Common Data Services for SMARTICS-2" to Part VII. The list is not meant to be exhaustive and is subject to be further refined and finalised during the SA&D stage. The refinements shall not be System Changes.

2.3.3 Functional Requirements for Business Services

2.3.3.1 General Description

2.3.3.1.1 High-level functional requirements for the Core System are all of those as mentioned in Section 2.3.2.1 above including those described in this Section 2.3.

2.3.3.1.2 The System shall improve the overall efficiency in identity card registration and issuance (including other ROP related application and services) through the introduction of self-service facilities and automated workflow, as well as enhancing the authorised record checking requests made by other Government bureaux and departments ("B/Ds"). The System shall provide user-friendly instructions and user interface to all self-service facilities to be used by general public. The System shall also enhance usage experience with more convenient user / card interfaces in line with the latest smart card technology.

2.3.3.1.3 The Contractor shall ensure the System can handle exceptions and irregularities which may arise in day to day operation.

2.3.3.2 HKIC Application and Issuance

2.3.3.2.1 General Workflow

2.3.3.2.1.1 The System shall make use of the automatic workflow processing approach for various ROP applications (e.g. first registration, card renewal, lost card and damaged card replacement, Certificate of Registered Particulars and Certificate of Exemption application, amendment of registered personal particulars, notification to change of address, etc.) to streamline the application processing at ROP branch offices, SIDCCs and various immigration offices throughout the application life cycle (e.g. from the application processing of identity card at reception desk up to the issuance of identity cards or other related documents). The application data and the necessary image files are passed automatically from one step to another according to the defined workflow.

2.3.3.2.1.2 According to the application status (e.g. ready for assessment, ready for verification) and the application nature (i.e. normal case or difficult case), the System shall perform case allotment automatically to randomly distribute applications to officers of different functional units for further processing.

2.3.3.2.1.3 The workflow processing status of the ROP application must be traceable and reports shall be generated for audit purposes.

2.3.3.2.1.4 The System shall support the compilation and printing of reports for statistical, performance monitoring and audit purposes.

2.3.3.2.2 The System shall provide streamline workflow for handling and monitoring applications for HKIC in the following area:

(a) HKIC renewal in the territory-wide HKIC replacement exercise;

(b) HKIC application for first-registration; and

(c) HKIC replacement application due to various reasons such as Minor to Juvenile, Juvenile to Adult, change in personal particulars, lost, damaged or defaced HKIC.

2.3.3.2.3 HKIC Renewal in the Territory-wide HKIC Replacement Exercise

The System shall provide, but not limited to, functions for HKIC renewal in SIDCCs with details as follows:

(a) online appointment booking and electronic application form pre-filling, riding on the e-Services-2 platform provided under Category E;

(b) Reception Desk functions (as described in Section 2.3.3.2.6 of this Annex) for the reception of applicants with appointment booking and walk-in, as well as indexing of application;

(c) Self-service Registration Kiosk (as described in Section 2.3.3.2.8 of this Annex) for HKIC renewal registration with identity verification, new fingerprints capturing and application form filling and printing and subject to SA&D, integrating the function of photo taking in the kiosks which will be conducted in manned mode;

(d) Registration Desk functions (as described in Section 2.3.3.2.7 of this Annex) for registration process including automated identity verification against historical photo images and fingerprints, new biometric capturing (including fingerprint and photo), registration information recording, printing of forms and record checking;

(e) Assessment Desk functions (as described in Section 2.3.3.2.9 of this Annex) for automatic record checking, fingerprints verification and liveliness check, assessment and issuance of NOC;

(f) Verification Desk functions (as described in Section 2.3.3.2.11 of this Annex) to verify the applicants identities against historical records;

(g) e-Cabinet (to be provided by the Contractor of Category C) for storage and retrieval of personalised new smart identity cards;

(h) Collection Desk functions (as described in Section 2.3.3.2.12 of this Annex) for verification of identity and issuance of new smart identity cards to the cardholders or the proxy; and

(i) Self-service Collection Kiosk (as described in Section 2.3.3.2.13 of this Annex) for automated issuance of new smart identity card to cardholder and collection of existing smart identity cards after identity verification.

2.3.3.2.4 HKIC Application for First-registration and Replacement

The System to be implemented by the Contractor shall provide, but not limited to, functions for HKIC first-registration and replacement application in ROP branch offices with details as follows:

(a) online appointment booking and electronic application form pre-filling by applicant;

(b) Reception Desk functions (as described in Section 2.3.3.2.6 of this Annex) for the reception of applicants with appointment booking and walk-in, as well as application indexing;

(c) Registration Desk functions (as described in Section 2.3.3.2.7 of this Annex) for registration process including identity verification (with automated facial recognition and fingerprint verification with database, if applicable), new biometric capturing (including fingerprint and photo), registration information recording, application form printing and record checking;

(d) Assessment Desk functions (as described in Section 2.3.3.2.9 of this Annex) for automatic record checking, fingerprints verification and liveliness check, assessment and issuance of ROP140 / ROP140A;

(e) Shroff Desk functions (as described in Section 2.3.3.2.10 of this Annex) for revenue collection and issuance of ROP140A;

(f) Verification Desk functions (as described in Section 2.3.3.2.11 of this Annex) to verify the applicants identities against historical records;

(g) e-Cabinet (to be provided by the Contractor of Category C) for storage and retrieval of personalised new smart identity cards;

(h) Collection Desk functions (as described in Section 2.3.3.2.12 of this Annex) for verification of identity and issuance of new smart identity cards to the cardholders or the proxy; and

(i) Self-service Collection Kiosk (as described in Section 2.3.3.2.13 of this Annex) for automated issuance of new smart identity card to cardholder and collection of ROP140 / ROP140A after identity verification.

2.3.3.2.5 Online Appointment and Form Pre-filling

The System shall provide web applications (including applications running on mobile platform and mobile apps) for online appointment booking and application form pre-filling, which shall be running on the e-Services-2 platform to be provided under Category E, with details as follow:

(a) allow applicants to book a time slot at a SIDCC or ROP branch office for HKIC renewal, replacement, first registration and mix application of HKIC-cum-Travel Document on desktop and mobile platform. The application shall be able to allow officer to add new location flexibly without the need to perform system change;

(b) allow applicants (on voluntary basis) to pre-fill the application form by inputting personal data in electronic format for HKIC and mix application of HKIC-cum-Travel Document with address data input function;

(c) support applicants to amend, cancel and enquire the appointment details online by inputting some retrieval keys (such as HKIC number, appointment reference number, etc.), provided that no personal information can be retrieved from database and be displayed to the applicant online;

(d) provide electronic notification (e.g. e-mail or SMS) immediately after successful booking; and

(e) obtain appointment booking records and pre-filled application data through interface with e-Services-2 platform, provide appointment booking records to TAGS-2 (to be provided under Category D) and store all necessary information locally in ROP branch offices and SIDCCs before the appointment date.

2.3.3.2.6 Reception Desk Functions

The System shall provide, but not limited to, the following reception functions for HKIC first and replacement application in ROP branch offices and SIDCCs ("Reception Desk") with details as follows:

(a) for each appointment, match the applicant with the corresponding appointment by inputting certain retrieval keys or scanning the number printed on, or stored in the chip of, the personal document or travel documents, such as HKIC, electronic Exit-Entry Permit for Travelling to and from Hong Kong and Macao ("e-EEP") issued by the Mainland authorities, etc. A tag will be printed to the applicant by TAGS-2;

(b) provide function(s) for the reception officer to make appointments for walk-in applicants through TAGS-2 and retrieve related information from the System for processing of application. Upon the completion of application reception process, the application shall be routed to the Registration Desk or self-service registration kiosk (applicable to the territory-wide HKIC replacement exercise only) for registration;

(c) create an application, indicating the nature of the application; initiating the registration workflow by retrieving related application data and ROP data from local servers (if any); generating unique ARN according to selected application type and section code and pass the information to Registration Desk; and

(d) for "walk-in" application of existing identity cardholders, retrieve ROP data from database; match the application details to the tag number assigned by TAGS-2.

2.3.3.2.7 Registration Desk Functions

The System shall provide, but not limited to, the following registration functions for HKIC first and replacement application in ROP branch offices and SIDCCs ("Registration Desk") with details as follows:

(a) provide function(s) to bring up an application for registration, including but not limited to, inputting retrieval keys or selecting from the list. The System shall also interface with the System of Category D and provide functions to allot an application to an officer by application type and priority of the tag;

(b) provide function(s) for officers to check application details and amend the details if created wrongly, retrieve personal data from ROP database and pre-filled application data from online, mark show up and other special remarks if needed;

(c) perform double registration check by using, but not limited to, biometric matching to reduce suspected multiple record hit;

(d) perform automatic record check according to business rules and to facilitate exception handling of special cases;

(e) provide function(s) for the supervisor to allot cases to the registration officer;

(f) index the application to the guardian's person record for minor and juvenile applications;

(g) allow the registration officer to capture colour facial image during registration and allow both the applicant and officer to view the photo image on two separate monitors for quality check. The System shall provide function(s) for retaking of photo if needed and allow the applicant to choose between two (2) photos. The selected photo shall be stored in the database. The System shall perform automatic facial recognition by checking the newly captured facial image against the historical records. The new photo image shall be captured with resolution and quality according to the updated international standards and align with the latest International Civil Aviation Organization ("ICAO") standard for travel documents. The photo shall contain 1200x1600 pixels with image format according to ISO/IEC 19794-5 format. The System shall also ensure that the photo image captured complies with ICAO Doc 9303 and it shall be ready to be used as a photo image for passport in the e-Passport-2, which will be implemented in early 2019 tentatively. The details will be confirmed during SA&D stage;

(h) provide function(s) to capture the applicant's two live fingerprint images by a fingerprint scanner (enrolment) and convert them to digitised images. The System shall perform automatic verification of the newly captured fingerprint against the historical fingerprint, by ways of, but not limited to, comparing with the existing templates using the current fingerprint matching algorithm. The System shall provide function(s) to display the enrolled fingerprints on screen for officer's confirmation. The officer shall be alerted if the quality of fingerprint images are not up to requirement and the System shall allow re-scanning of fingerprints. The System shall indicate the finger captured and generate templates that facilitate subsequent storage into the new smart identity card chip during card personalisation. The System shall maintain two sets of new fingerprint templates, which shall be generated by the Custom Programs mentioned in Section 2.3.8.5 of this Annex and in the standard format of ANSI-INCITS 378. The System shall link and index the fingerprint images and templates to the application record;

(i) when processing an application, the System shall:

(i) support retrieval of database information (including images) and pre-filled personal data;

(ii) perform field validation;

(iii) read chip information from smart identity cards and travel documents;

(iv) provide function(s) for an officer or applicant to input or update registration information of the application form electronically, including address and contact number, in structural format. The System shall support the input in both English and Chinese (in both traditional and simplified Chinese);

(v) provide function(s) for an officer or applicant to input some specific information, such as occupation, by selecting from the predefined categories;

(vi) retrieve or generate an HKIC number where appropriate;

(vii) allow officer to correct details and other relevant information;

(viii) provide selection of Braille lettering printing;

(ix) provide function(s) for an officer or applicant to input collection place, mode of collection (i.e. in person or by proxy) and indicate voter’s consent, as well as any other information as required by the Government from time to time;

(x) allow officer to make remarks for non-routine cases;

(xi) provide function(s) to scan supporting documents. The System shall provide function(s) for an officer to view the scanned document images for quality assurance. The document scanning function shall be able to automatically locate some essential information on the document separately for subsequent extraction in digital image. It must also allow the officer to refine the scanning position manually;

(xii) provide automatic fingerprint matching with live submitted fingerprint;

(xiii) for replacement cases, provide functions to record the collection of existing smart identity card and provide reconciliation report;

(xiv) update application progress and status for mix application, if required;

(xv) provide function(s) for an applicant to review the filled application form and print out the form for applicant to sign after confirmation;

(xvi) record the applicant's choice on whether to have the non-ImmD application(s) loaded into the new smart identity card;

(xvii) pass application and relevant information for ARC;

(xviii) perform checking on compliance with ICAO Doc 9303 on the photo captured;

(xix) for regular case in SIDCC, print NOC;

(j) provide function(s) for an officer to handle case reverting from assessment officer;

(k) provide special design for the disabled applicants (such as visually impaired persons and wheelchair users) to go through the registration process;

(l) all equipment shall be mounted securely and integrated seamlessly to the Registration Desk; and

(m)the design of the overall workflow and user interface as described in this Section 2.3.3.2.7 shall be user-friendly and facilitate registration officer to complete the registration process within nineteen (19) minutes.

2.3.3.2.8 Self-service Registration Kiosk Functions

The System shall provide applications for registration process, which shall be running on the MSK_REG to be provided under Category C in SIDCCs, with details as follow:

(a) provide functions for applicant, including wheelchair users, to process the registration process by automated means in SIDCCs;

(b) inside the kiosk, allow an interactive screen display with operational guidance by application type and to guide applicants to go through the application process;

(c) the System shall:

(i) perform mutual authentication and read data from the existing smart identity card;

(ii) authenticate applicant by fingerprint verification (i.e. live captured fingerprint against templates in card or historical record in ROP database) and trigger appropriate application process by application type upon successful authentication;

(iii) retrieve necessary information from database;

(iv) bring up the corresponding pre-filled electronic application form data if applicant already performed online application form pre-filling;

(v) if the applicant has not yet performed online application form pre-filling, bring up an electronic form with personal particulars filled by extracting relevant information from the ROP database;

(vi) provide function(s) for an applicant to input other necessary information into the application form electronically and perform validation in textual format. The System shall support the input in both English and Chinese (in both traditional and simplified Chinese);

(vii) provide function(s) for an officer or applicant to input collection place, mode of collection (i.e. in person or by proxy) and voter’s consent;

(viii) capture live fingerprint with liveliness and quality check. The System shall indicate the finger captured and generate fingerprint templates for storage in the chip of the new smart identity card and the database for subsequent identity verification purposes. In case if the fingerprint captured cannot meet the required standard, the System shall allow capturing the fingerprint again;

(ix) perform automatic one-to-one fingerprint matching between new fingerprint images captured and fingerprint images stored in the chip of the new smart identity card or database;

(x) capable of capturing live photo of the applicant by camera installed in the kiosk with capturing function manned by officers;

(xi) index application automatically;

(xii) display notification or other necessary messages;

(xiii) record the applicant's choices of use (if applicable) on the smart identity card;

(xiv) provide function(s) for an applicant to preview and print out the application form for signature after confirmation; and

(xv) redirect applicants to the Registration Desk for further processing and for handling any failure or abnormal cases.

(d) the Contractor shall provide a solution to capture live photo of applicants by camera installed in the kiosk in manned operation, so as to provide a more streamline workflow for applicants during registration process. The final solution for photo taking in SIDCCs shall be subject to any modifications as stipulated and confirmed by the Government in the SA&D stage; and

(e) the design of the self-service registration kiosk workflow and the user interface shall be user-friendly for use by general public and facilitate the general public to complete the self-service workflow within sixteen (16) minutes.

2.3.3.2.9 Assessment Desk Functions

The System shall provide, but not limited to, the following application assessment functions for HKIC first and replacement application in ROP branch offices and SIDCCs (“Assessment Desk”) with details as follows:

(a) provide function(s) for an officer to bring up an application routed from Registration Desk by a number of ways, including but not limited to, automatic case allotment according to tag priority or inputting of retrieval keys, etc;

(b) the System shall:

(i) provide function(s) for an officer to bring up an application case routed from Registration Desk;

(ii) provide automatic case allotment;

(iii) perform identity verification by fingerprint matching with database record and verify the fingerprints (including liveliness) against the fingerprints captured in Registration Desk or the MSK_REG; and

(iv) prompt record check result done by ARC and highlight irregularities found (if any) for officer's attention;

(c) In assessing an application, the System shall:

(i) perform necessary record check and movement record check and alert officer for any irregularities identified;

(ii) refer the case to supervisor or route back to Registration Desk if needed;

(iii) handle change of HKIC number cases and to print special notice to the applicant;

(iv) confirm the applicant's residential status, change application nature in case the applicant's right of abode is lost;

(v) provide function(s) to view and print all documents and images of the application and those related documentation stored in the IMS, zooming and panning of the document images must be allowed. The System shall provide function(s) for an officer to view the scanned document images for quality assurance and printing of the scanned images upon enquiries;

(vi) scan and verify applicant's live fingerprints against the fingerprint images captured at the Registration Desk or self-service registration kiosk, as well as the record in the database. Both images and score / grade shall be shown on screen simultaneously, re-capturing of fingerprints at Registration Desk shall be required for low score / grade;

(vii) amend application data;

(viii) print proxy collection form;

(ix) confirm the selection for inclusion into juror list;

(x) scan additional document(s) to be appended to the application;

(xi) provide online updating of invalid and lost HKIC status in Common Data Repository ("CDR");

(xii) show fingerprints of the new and previous application simultaneously in different colour on one screen;

(xiii) verify new photo image and document images against any previous images in IMS;

(xiv) update assessment result;

(xv) suspend the assessment and bring up cases periodically;

(xvi) for mix application, send personal and relevant information to e-Passport-2, which will be implemented in early 2019 tentatively, upon confirmation of successful assessment by officers;

(xvii) print and reprint Notice of Collection (for applications in SIDCC) or

ROP140 (for applications without payment in ROP branch office) with photo of the applicant and personal data. The ROP140 shall also include a feature which prevent the document from being counterfeited, such as the current 2-dimensional barcode encoding the encrypted photo image of the applicant; and

(xviii) record the serial numbers of the ROP140 being allotted to individual officer and confirm forms being used, unused or voided and maintain the range available information;

(d) provide special design to facilitate disabled applicants, including visually impaired persons and wheelchair users, to perform assessment;

(e) all equipment shall be mounted securely and integrated seamlessly to the Assessment Desk;

(f) provide stock control mechanism and generate daily audit report for ROP140 allotted to and issued by each officer; and

(g) all assessed cases shall be directed to Verification Office instantly or at a time interval specified by the Government for application verification before personalisation. The System shall provide functions for senior officers to perform spot check on the applications assessed by the assessment officers.

2.3.3.2.10 Shroff Desk Functions

The System shall provide, but not limited to, the following shroff functions in ROP branch offices (“Shroff Desk”) with details as follows:

(a) provide function(s) for an officer to bring up the application for collection of necessary fee in cash, cheque or different kinds of e-payment and print an acknowledgement form, i.e. ROP140A for applications with payment in ROP office, with a feature same as the one of ROP140, described in Section 2.3.3.2.9(c)(xvii) of this Annex, after confirmation of payment;

(b) record the serial numbers of the ROP140A being allotted to individual officer and confirm forms being used, unused or voided and maintain the range available information;

(c) provide function(s) to reprint the acknowledgement form or suspension of cases if needed;

(d) provide function(s) for retrieval of application or group of applications from the queue, calculate the total sum payable with pre-defined payable amount of each application type and connect to different payment system (such as EPS) for payment processing and recording;

(e) support the following shroff related functions:

(i) update amount of revenue withdrawn;

(ii) enquire amount of cash on hand;

(iii) update amount payable for application or group of applications;

(iv) accept single and multiple application payment;

(v) accept multiple application payment;

(vi) update manual fee collection information;

(vii) cancel payment; and

(viii) generate shroff online reports;

(f) manage and update cash drawer transactions for reconciliation and record payment;

(g) support enquiry of payment record, cash and cheque on hand and e-payment record and create audit trial report for detail of correction, updating and deletion of payment record and daily report for account reconciliation; and

(h) in case payment of HKIC is required together with other travel document applications, support system interface with other systems (such as e-Passport-2 to be implemented in early 2019 tentatively) to calculate the total sum payable for such mix application and allow total amount to be collected in one go.

2.3.3.2.11 Verification Desk Functions

The System shall provide, but not limited to, the following verification desk functions in Verification Office ("Verification Desk") with details as follows:

(a) all applications shall be directed to the Verification Unit in HQ for verification centrally. The System shall automatically allocate applications to individual officers in Verification Unit for processing;

(b) provide functions at the Verification Desk for officers to perform verification on application data including personal details, photo image, fingerprint images and document images, against previous HKIC application records instantly. Automatic fingerprint matching shall be performed;

(c) support different checking mechanism for different kinds of applications, including but not limited to first registration, applications with fingerprint matching score below or above the pre-defined score and suspected double registration;

(d) alert officers for registrations with suspected irregularities;

(e) retrieve and display all images, including historical images, related to the applications;

(f) provide function(s) for spot checking of records by supervisors;

(g) provide function(s) for double registration check by automatic one-to-one matching between the biometric (fingerprint and facial) of new application and previous records;

(h) the one-to-one fingerprint matching score and the images of the new and historical fingerprints are displayed individually and together on the screen for verification;

(i) extract and highlight fingerprint minutiae of all available fingerprint images and display such fingerprint minutiae for manual comparison;

(j) update verification status and pass the verified application to CPMS (to be provided under Category B) instantly. Spot check mechanism shall be in place; and

(k) provide mechanism to monitor the work efficiency, including but not limited to, number of application verified by individual staff per time period to be defined by ImmD, time taken for individual staff in completing one application verification, etc.

2.3.3.2.12 Collection Desk Functions

The System shall provide, but not limited to, the following card collection functions in ROP branch offices and SIDCCs ("Collection Desk") with details as follows:

(a) retrieve applications by scanning barcode printed on the NOC or ROP140 / ROP140A, HKIC number printed on the HKIC or inputting other reference number;

(b) if the applicant is not able to provide the necessary document for collection of new smart identity card, such as existing smart identity card and ROP140 / ROP140A, generate a form to declare for loss of acknowledgement form / existing smart identity card for the applicant to sign;

(c) inform officer if new smart identity card intended to be collected is not ready;

(d) upon collection by the applicant or the proxy, based on the HKIC number or application number inputted or scanned, send relevant information to CabS under Category C for automatic location and dispensation of the required new smart identity card from the secured storage of the e-Cabinet;

(e) update relevant information in chip for temporary residents and perform records check (e.g. card shall not be issued if the cardholder has overstayed); alert officer if irregularity is detected;

(f) check proper functioning of the chip of the new smart identity card for both contact and contactless interfaces;

(g) support checking of applicant's live fingerprint and facial image against information on the new smart identity card and database, refer unmatched case to supervisor;

(h) provide function(s) for an applicant to verify information on chip and the list of non-ImmD applications;

(i) record collection of existing smart identity card or ROP140 / ROP140A;

(j) update application status after issuance. If the card is rejected by applicant due to quality issue, the System shall resend the case to CPMS (to be provided under Category B) for card re-print without the need to go through registration process again;

(k) an Optical Character Recognition ("OCR") reader shall be installed to read the current feature of 2-D barcode (or equivalent technology with device) for authenticity checking of the ROP140 / ROP140A;

(l) support local and standalone mode of card collection for any prolonged service failure;

(m) support issuance of existing smart identity card, including reading the chip of existing smart identity card and verification of fingerprint through the templates in the chip of the existing smart identity card during the transition period for applicants who have not yet collected their new smart identity cards after the rollout of SMARTICS-2; and

(n) for card inventory management, the System shall also provide the following functions:

(i) receive information from the CPMS (to be provided under Category B) of newly personalised new identity cards which are delivered to various ROP branch offices and SIDCCs, the information shall also be reconciled with the cards which are checked-in into the e-Cabinets and self-service collection kiosks in respective ROP branch offices and SIDCCs, under CabS of Category C, alert officers if irregularity is found;

(ii) record information on cards issued to applicants and reconcile with the inventory list of cards as recorded in CabS, alert officers if irregularity is found;

(iii) provide functions to facilitate reconciliation of smart identity card pending collection;

(iv) for long outstanding uncollected smart identity card, issue instruction to CabS for retrieval of concerned cards from the e-Cabinet and record the follow up actions (such as return to CPO or disposal, update inventory record, etc.); and

(v) provide identity card reconciliation report showing the number of cards issued and cards left in the inventory.

2.3.3.2.13 Self-service Collection Kiosk Functions

The System shall provide applications for running on the SCK to be provided under Category C for self-service collection of new smart identity card, with details as follows:

(a) using devices provided by the Contractor of Category C, read the chip of the existing smart identity card or barcode from the NOC or ROP140 / ROP140A, extract the HKIC number or application number for CabS of Category C to automatically retrieve new smart identity cards from the secured storage;

(b) perform identity verification of the applicant using fingerprint and facial information stored in the existing smart identity card and database;

(c) update relevant information in chip for temporary residents and perform records check (e.g. card shall not be issued if the cardholder has overstayed); alert officer if irregularity is detected;

(d) verify the fingerprint and facial information stored in the chip of the new smart identity card against the applicant before sending instruction to CabS for dispensing out the new smart identity card;

(e) ensure proper functioning of the chip of the new smart identity card for both contact and contactless interfaces;

(f) update the inventory list;

(g) collect existing smart identity card with authentication;

(h) check genuineness and collect ROP140 / ROP140A;

(i) in case of exception, route the application to Collection Desk or supervisors, send instruction to CabS for retrieval of the concerned new smart identity card by supervisors;

(j) retrieve the dispensed card in case if the applicant fails to collect the card within a time period;

(k) for long outstanding uncollected new smart identity card, issue instruction to CabS for retrieval of concerned cards from the self-service collection kiosk and record the follow up actions (such as return to CPO or disposal, update inventory record, etc.);

(l) provide identity card reconciliation report showing the number of cards issued and cards left in the inventory;

(m) support local and standalone mode of card collection for any prolonged service failure; and

(n) the workflow and the user interface design shall be user-friendly and facilitate applicant to perform self-service collection of new smart identity card within three (3) minutes.

2.3.3.2.14 Supervisor Desk Functions

The System shall provide but not limited to, functions for maintenance and monitoring, record enquiry and other application processing management functions ("Supervisor Desk") with details as follows:

(a) provide functions for maintenance of the system security profiles, code tables and quota management (including appointment booking quota, walk-in quota, quota adjustment, etc.) in ROP branch offices and SIDCCs;

(b) provide different enquiry functions such as quota enquiry, appointment and tag enquiry via interface with TAGS-2 and e-Services-2, progress of applications, statistics and audit trail enquiry, as well as to perform maintenance of records, including change of address request submitted by post or e-mail and recording of MPIC issuance together with passport;

(c) provide functions for the compilation of data files on ad hoc and periodic basis;

(d) allow officers to enquire and print ROP record, including data and images as well as to compile data files for interface with other systems;

(e) provide instant batch printing function of some selected data (such as address, telephone number, etc.), which are stored either as image or textual format in the database. Before compiling data for batch printing, the System shall also perform checking such as card validity;

(f) process applications of CRP, EC, CCIC, MPIC, OPIC, perform record enquiry, verification and Jury Unit functions;

(g) for Supervisor Desk in investigation offices, provide function for authorised officers to assign designated officers to operate the handheld smart card readers and to activate the handheld smart card readers before deployment to field operations, the System shall also support uploading of transaction logs stored in the handheld smart card readers to the System after field operations; and

(h) provide functions to check the possible malfunction of smart identity card chip cases reported to the ROP branch office.

2.3.3.2.15 Confidential Registry Unit ("CRU") and Immigration Telephone Enquiry Unit ("ITEU") functions

The System shall provide functions to perform record enquiry and verification, including verification of fingerprint images impressed on paper document against fingerprint image in database, and provide record information to authorised parties, as well as to properly record all processes.

2.3.3.2.16 ROP Certificate Unit functions

The System shall provide, including but not limited to, the following functions for officers to process and monitor the applications as stated below:

(a) Certificate of Registered Particulars (“CRP”)

(i) appointment booking with submission of application data running on the e-Services-2 platform (to be provided under Category E);

(ii) allow inputting and indexing of new cases when the CRP application is submitted in person or by post;

(iii) automatic printing of letter and sending of e-mail to notify applicant or the representative;

(iv) application creation, document scanning, confirmation of requirement with applicant, application indexing and payment in ROP branch office, upon interview date;

(v) automatic routing of application case to Certificate Unit for CRP preparation and production;

(vi) auto filling of information into CRP, which is based on availability of data in textual format;

(vii) creation and maintenance of different templates for CRP;

(viii) application submission to authorised party for necessary actions; and

(ix) transactions logging and reporting for all application processes and keep application statistics and inventory.

(b) Certificate of Exemption ("EC")

(i) EC application submission through online services via e-Services-2 platform (to be provided under Category E), in person submission in ROP offices and by post;

(ii) EC application creation, document scanning, portrait image scanning, confirmation of requirement with applicant (or representative) and application indexing;

(iii) registration and assessment workflow functions for Certificate Unit to process the applications;

(iv) production of personalised EC with portrait image;

(v) transactions logging and reporting of all application processes for audit purpose and keep application statistics; and

(vi) data indexing and migration of historical EC records in image format into the database.

(c) Consular Corps Identity Card ("CCIC")

(i) CCIC record creation, assign a CCIC reference number and scan the applicant's photo into the System;

(ii) application for approval by authorised officers;

(iii) personalised CCICs including check-in / check-out functions and alert officers for long outstanding cards not being collected; and

(iv) maintenance of register of CCIC issued, audit trail and statistical returns.

2.3.3.2.17 Self-service General Application Kiosk Functions

The System shall provide SMARTICS-2 related applications to be running on the MSK_GEN to be provided under Category C and shall provide, but not limited to, the following functions:

(a) mutual authentication with existing and new smart identity cards and read data stored in the chip of the card;

(b) identity verification based on matching of fingerprint templates stored in existing and new smart identity cards;

(c) application for change of registered particulars (such as address, telephone number, nationality claimed, etc);

(d) personal information enquiry and updating of Condition of Stay ("C/S") and Limit of Stay ("L/S") stored in card;

(e) e-Cert checking and change of e-Cert password;

(f) booking details enquiry and booking service for ImmD services;

(g) facilitation of relevant functions for visually impaired persons to go through the kiosk operation; and

(h) interactive voice response capabilities for user interaction through the keypad input.

2.3.3.2.18 Jury Unit Functions

The System shall support selection of eligible HKIC holders as jurors in accordance with the Jury Ordinance. The System shall provide but not limited to, the following functions:

(a) compile list of eligible jurors daily from the following sources:

(i) information submitted by the applicants on applications received, including new application and replacement application, with reference to pre-defined business criteria;

(ii) receipt of notification (i.e. ROP18 and ROP18A) from fresh university graduates;

(iii) receipt of notification (i.e. ROP18 and ROP18A) from existing jurors; and

(iv) receipt of deletion list (i.e. list of permanent exemption from being a juror or the juror is over the age 65) from Judiciary Administrator's Office ("JAO");

(b) provide functions to update address from ROP18 / ROP18A submitted by the public via e-mail automatically to facilitate verification;

(c) according to pre-defined criteria, determine whether a HKIC holder is eligible as juror according to the Jury Ordinance;

(d) update juror status of the ROP records;

(e) assemble a list of newly selected jurors and a list of jurors with updated information; and

(f) allow authorised personnel of the Judiciary to receive / download the list through encrypted electronic means or other secured channel.

2.3.3.2.19 Interface Functions with e-Services-2 platform

2.3.3.2.19.1 The System shall provide applications related to SMARTICS-2 running on e-Services-2 platform (to be provided under Category E) and the system interface between e-Services-2 platform, for integrating the necessary online ROP related functions including appointment booking and pre-filling of electronic application form of application for HKIC, booking quota enquiry, online submission of application for CRP and EC, amendment of registered particulars, etc, as well as transferring online pre-filled application data from e-Services-2 to facilitate registration processing on appointment date.

2.3.3.2.20 Interface Functions with TAGS-2

2.3.3.2.20.1 The System shall interface with the TAGS-2 (to be provided under Category D) for integrating the necessary tag related functions into the ROP application processing functions, including the quota plan, tag issuance and application processing in various desks in ROP offices and SIDCCs, card collection, etc.

The workflow engine of the System shall support dynamic change of priorities for application cases.

2.3.3.2.21 Interface Functions with CPMS

2.3.3.2.21.1 The System shall interface with CPMS (to be provided under Category B) and provide application information, including personal particulars, C/S, L/S, fingerprint templates, photo image which is capable of performing facial recognition and other essential information to CPMS for the production and personalisation of new smart identity cards, as well as the distribution of key and certificate renewal for smart card readers.

2.3.3.2.21.2 On completion of the card personalisation processing, the System shall obtain the card production result from CPMS and initiates subsequent workflow processing.

2.3.3.2.22 Minor Permanent Identity Card (“MPIC”) and Overseas Permanent Identity Card (“OPIC”) Functions

2.3.3.2.22.1 The System shall provide streamline workflow to handle and monitor MPIC / OPIC applications. The processing shall be similar to that of HKIC applications with the following additional features:

(a) provide workflow process with appropriate functions of registration and assessment;

(b) support ARC when performing assessment;

(c) scan relevant documents and input application information for application indexing. Apart from capturing the whole application form, fingerprint images and photo of the applicant shall be extracted from the application form and stored as separate images at 300 dpi, 256 grayscale or better;

(d) extract relevant information from relevant systems of birth registry for record checking and assignment of HKIC number;

(e) automatically fill in guardian’s information and index the application record to the guardian’s record;

(f) after case approval, the related information, including applicant’s photo, shall be passed to CPMS (to be provided under Category B) for card personalisation;

(g) interchange result codes with e-Passport after assessment and issuance of MPIC / OPIC;

(h) after personalisation and quality check in Card Personalisation Office, the MPIC / OPIC shall be packed in a secured box and be transferred to and inserted into the e-Cabinet located in the e-Passport office (TDI Section) to await matching with the corresponding personalised e-Passport before delivery to respective immigration offices, the System shall interface with both the Systems of Categories B and C for inventory management;

(i) upon the implementation of e-Passport-2, support interface from e-Passport-2 for data transfer and automatic creation of ROP application when the applicant applies for HKSAR passport together with MPIC or OPIC application; and

(j) upon the implementation of e-Passport-2, receive application data, including textual data, scanned documents and photo collected in the course of passport application automatically from e-Passport-2 via secured platform.

2.3.3.2.23 Other Functional Requirements

2.3.3.2.23.1 Extracts information of HKIC replacement applications to compile an interface table of invalid and lost HKIC for updating such information to CDR to facilitate invalid and lost HKIC check in control points.

2.3.3.2.23.2 The acknowledgement form (ROP140 / ROP140A) shall contain features for preventing the document from being counterfeited, the current feature is a 2-D barcode encoding with the encrypted black and white photo of the applicant which can be read by 2-D barcode reader connecting to the current system, as well as UV features on the paper of the ROP140 / ROP140A. The System shall provide function(s) to verify the genuineness of the form as well as the rightful holder, e.g. printing of 2-D barcode on the form and reading and decoding the barcode using equipment connecting to workstations, as well as printing of features (such as UV pattern) which can be used to verify the genuineness of the form automatically by dedicated equipment to be installed in the self-service collection kiosk for automatic form collection purpose. In Schedule 1 – “Hardware”, Schedule 2 – “Software” and Schedule 4 – “Technical Proposal and System Configuration” of Part V, Tenderers shall propose and supply ROP140 / ROP140A automatic collecting device which will be installed into the self-service collection kiosk provided under Category C for providing genuineness verification and automatic collection function of a ROP140 / ROP140A upon issuance of new smart identity card. The equipment shall be able to verify the genuineness of the form, return the form to the applicant if genuineness check is failed and send alert to officer if the returned form remains uncollected after a period of time. In proposing the equipment, Tenderers shall provide either one of the following solutions:

(a) provide automatic collection function of the existing ROP140 / ROP140A, such equipment shall be able to verify the genuineness of the form by identifying the printed features on the form by optical means, such as UV pattern. The existing ROP140 and ROP140A are printed on 100gsm paper with sizes of 147mm x 200mm and 147mm x 271mm respectively. The size of the equipment for automatic collection shall not be over 220mm x 510mm x 350mm; or

(b) redesign the paper based ROP140 / ROP140A with considerations on the size and printed features on the form for genuineness check and to supply an equipment which can verify the genuineness of the printed features on the paper based form and to perform automatic collection. The size of the equipment for automatic collection shall not be over 220mm x 510mm x 350mm. The Contractor shall also be responsible to provide a one-time supply of the proposed paper based ROP140 / ROP140A of a quantity of 900,000.

The final solution of feature for the acknowledgement form shall be confirmed by the Government in the SA&D stage.

2.3.3.2.23.3 The Contractor shall design the System with due consideration on enhancing the overall workflow for the registration and assessment process in order to facilitate HKIC registration process at SIDCCs to be completed within 30 minutes and the HKIC application process at ROP branch offices to be completed within 60 minutes.

2.3.3.2.23.4 The System shall display performance statistics of all operations, including but not limited to, identity card registration and issuance and other ROP services, handling of identity verification requests and the healthiness of the system equipment.

2.3.3.2.23.5 The System shall provide staff monitoring statistical functions and operation irregularities.

2.3.3.2.24 Local Mode Functions

2.3.3.2.24.1 The System shall provide high resilience to support continuous ROP service to the public. In addition, as a contingency measure to cater for any prolonged failure in accessing the centralised servers, the Contractor shall provide a set of ROP functions to support application processing functions in local mode operation, including the functions of handling applications through Reception Desk, Registration Desk, Assessment Desk, Shroff Desk, Collection Desk, self-service registration kiosk, self-service collection kiosk and other necessary supporting functions in ROP branch offices and SIDCCs. The corresponding functions shall be performed using locally stored repositories, including local CDR, and the applications details captured will be stored temporarily in the local servers. The essential functions shall be confirmed by the Government during the SA&D stage.

2.3.3.2.24.2 When centralised server service resumes, application data captured by the local mode functions will be uploaded to the centralised database for recovery processing. The applications will be processed, record checking will be performed and the application will be uploaded to centralised servers. The applications will then be merged into normal flow if no irregularity is detected. Otherwise, the System shall alert supervisor for follow up actions.

2.3.3.2.24.3 The Contractor shall provide functions and procedures to switch the operations from normal mode to local mode and vice versa. The Contractor shall perform drill on local mode functions regularly at least once a year.

2.3.3.2.25 Standalone Mode Functions

2.3.3.2.25.1 As another contingency measure to cater for any prolonged failure in running the ROP services in local mode operation, the Contractor shall provide a set of ROP functions to support application processing with essential capabilities, in standalone workstation mode, including the functions of Reception Desk, Registration Desk (with Assessment Desk functions), Shroff Desk, Collection

Desk, self-service registration kiosk, self-service collection kiosk and other necessary supporting functions in ROP branch offices and SIDCCs. The essential functions shall be confirmed by the Government during the SA&D stage.

2.3.3.2.25.2 Some of the workstations and kiosks at ROP branch offices and SIDCCs shall be configured to support the standalone mode functions, including the Reception Desk, Registration Desk (with Assessment Desk functions), Shroff Desk, Collection Desk, MSK_REG, SCK and other necessary supporting functions. These workstations and kiosks shall be configured with all necessary hardware peripherals and software used by these functions, such as document scanner, smart card reader, fingerprint scanner (enrolment) / fingerprint scanner (verification), digital portrait camera, OCR reader, document printer, slip printer, etc.

2.3.3.2.25.3 All the Registration Desk workstations and self-service registration kiosks shall be able to support the functions of registration and assessment (for the case of self-service registration kiosks, assessment can be done by officers through kiosk equipment) for application processing and other necessary supporting functions to operate in standalone mode. The details of the application processing will be confirmed at the SA&D stage.

2.3.3.2.25.4 All the Collection Desk workstations and self-service collection kiosks shall be able to support the Collection Desk and self-service collection of new smart identity cards functions and other necessary supporting functions to operate in standalone mode.

2.3.3.2.25.5 The Contractor shall provide functions and procedures to switch the operations from normal mode or local mode to standalone mode and vice versa. The Contractor shall perform drill on standalone mode functions regularly at least once a year.

2.3.3.2.25.6 To protect data privacy and confidentiality, the Contractor shall provide and implement data encryption and access control solution to the data stored in the standalone workstations and kiosks.

2.3.3.2.25.7 To minimise the risk of losing application data during standalone mode, data in standalone workstations and kiosks shall be saved in mirror copy and protected by uninterruptible power supply (“UPS”).

2.3.3.2.25.8 After the System resumes its normal operation, application data captured by the standalone mode functions shall be uploaded to the centralised database for recovery processing. During recovery processing, the System shall perform record checking for each application to ensure the records are in order without duplication and irregularity. A report of the checking results shall be produced.

2.3.3.2.25.9 The Contractor shall provide the standalone mode solution and any necessary hardware and software for applications running in the self-service registration kiosk and self-service collection kiosk.

2.3.3.2.26 Mobile Registration Unit Functions

2.3.3.2.26.1 The System shall support the provision of the business services via mobile device. The mobile device shall provide the functions of Registration Desk, Assessment Desk, Shroff Desk and Collection Desk ("Mobile Registration / Card Collection Device"). The System shall also support the compilation and printing of reports for statistical, performance monitoring and audit purposes on applications processed through the Mobile Registration / Card Collection Device.

2.3.3.2.26.2 The Contractor shall integrate all required peripherals in order to carrying out the functions as mentioned in Section 2.3.3.2.26.1 above into each mobile device which can be carried by officers.

2.3.3.2.26.3 For data synchronisation, the System shall support secure loading of application data into the mobile device and uploading of data to the System after use via a Supervisor Desk. The System shall be expandable to online mode under which the System would have remote access to data centres for performing online functions as in the Registration Desk, Assessment Desk, Shroff Desk and Collection Desk.

2.3.3.2.26.4 The System shall support contact interface only for reading of data from chip of smart identity card by mobile registration device.

2.3.3.2.26.5 The application and data in the mobile device shall be cryptographically protected against unauthorised access. All data stored in the mobile device and transferred through untrusted network shall be encrypted. The System shall provide application to erase all personal data stored in the mobile device when irregular attempts to log-in the mobile device are detected (such as failure to log-in due to wrong password for a number of times).

2.3.3.2.26.6 The functions of mobile registration unit shall be confirmed by the Government during SA&D stage.

2.3.3.2.27 Handheld Smart Card Reader Functions

2.3.3.2.27.1 The handheld smart card reader shall support authorised officers to view the details of a new smart identity card and check the cardholder's live fingerprint against the template in the chip so as to verify the authenticity of the identity. For security and auditing purposes, the handheld smart card reader and the related supervisor workstation shall also provide functions such as handheld smart card reader activation and audit log upload. The System shall only allow authorised officers to operate the handheld smart card reader. Major functions of the handheld smart card readers shall, including but not limited to:

(a) perform mutual authentication with the new smart identity card;

(b) read data from chip via contact interface only;

(c) authenticate a cardholder using a secure fingerprint scanner (verification);

(d) display the photo image stored in the card;

(e) provide security measures to ensure the handheld smart card reader is properly authorised and authenticated with the authorised officers for device activation before and during field operations;

(f) provide data encryption to protect data stored in the device;

(g) provide audit log information; and

(h) erase all data after uploading of logs to supervisor workstations and deactivate the device.

2.3.3.2.27.2 Security mechanism shall be in place to ensure the handheld smart card reader is properly authorised for activation before deployment to field operation.

2.3.3.2.28 Update of C/S and L/S Functions

2.3.3.2.28.1 The System shall provide functions to obtain the most updated C/S and L/S and provide to CPMS for updating of C/S and L/S in the existing and new smart identity cards.

2.3.3.2.28.2 The System shall provide functions at the Collection Desk, self-service collection kiosk and self-service general application kiosk to retrieve C/S and L/S from the System for updating in the existing and new smart identity cards upon and after card issuance.

2.3.3.2.28.3 The System shall provide functions to update C/S and L/S in the existing and new smart identity cards using workstations at control points and various immigration offices, which are non-ROP offices. Access control, audit control and report printing functions shall also be provided to track and print report for all enquiries and updates performed at these workstations.

2.3.3.2.29 Record Maintenance Functions

2.3.3.2.29.1 The System shall support the batch scanning of documentation and notification forms, such as Notification of Change of Address and Certificate of Registered Particulars. The images shall be indexed with identity card number and stored in the IMS for permanent storage.

2.3.3.2.29.2 The System shall support auto cropping of data image, retrieval, display and printing of the scanned documents or the cropped image, using the identity card number and document type, individually or in batch mode.

2.3.3.2.29.3 The document scanning function shall be able to automatically locate the address information and some other essential information on the Notification of Change of Address form for extraction in digital format. It must also allow the operator to refine the scanning position manually.

2.3.3.2.29.4 The System shall provide functions for officers to update address and other information in textual format upon receipt of change of personal details application.

2.3.3.2.30 Automatic Record Check ("ARC")

2.3.3.2.30.1 The System shall provide function(s) for record checks on different types of

HKIC applications in daily ROP operation. ARC shall be performed based on the pre-defined business criteria and the results shall be returned to registration officer or assessment officer for consideration instantly during registration or assessment workflow.

2.3.3.2.31 Image Management System Functions

2.3.3.2.31.1 The Contractor shall design and implement the IMS (which shall form part of the System). The IMS shall store and index images, including but not limited to, document, fingerprint and photo of applicant, which are captured during registration, assessment and when processing other ROP related applications and record maintenance. To retain the images in perpetuity, IMS shall keep all images in permanent massive storage media, such as disk-based Write Once Read Many ("WORM") storage system. A prompt and efficient retrieval of records from the IMS shall be provided. In designing and implementing the IMS, the Contractor shall ensure the functions compile with all government and departmental guidelines on records management. The System shall provide the following functions:

(a) Image Creation

IMS shall provide functions to create new image record on application and link to identity card record.

(b) Image Compression and Decompression

IMS shall automatically compress images before storage and decompress images upon retrieval.

(c) Image Storage

IMS shall ensure complete set of images is stored in a consistent manner and only write once storage shall be adopted. Images shall be stored at PDC(KC) for permanent massive storage and synchronised to DDC(FL) automatically.

(d) Image Indexing

Automatic indexing function shall be provided in IMS to generate indices for document images, fingerprint images and photo image for each application. The IMS indices shall support the searching and retrieval of images.

(e) Image Retrieval

Round-the-clock online access functions of IMS to retrieve images, including but not limited to, document, photo and fingerprint for viewing, printing and sending out by facsimile via fax server. Images can be enlarged to facilitate viewing on display monitors.

(f) Image Deletion

The IMS shall support logical deletion of image files. Deletion of images and retrieval of deleted images can only be performed by authorised users.

(g) Image Re-instate

The IMS shall support re-instate of deleted images by authorised users.

(h) Image Transfer

The System shall provide functions to transfer images, including but not limited to, document, photo and fingerprint and link them with application record image file throughout the application processing cycle.

(i) Secure Document Delivery Functions

The System shall support functions to send encrypted images to predefined locations. Decryption with direct printing functions shall be supported at the designated locations.

(j) Other Functions

High availability of 7 x 24 hours shall be supported for IMS. All image data throughout transmission shall be encrypted. The System shall provide different management, statistical, audit trail and exception reports for the IMS functions.

2.3.3.2.31.2 The IMS shall support different types of fingerprint archives, including fingerprint images which are produced from the microfilm and paper index cards conversion exercise, some are live-captured by SMARTICS and some will be captured by the System.

2.3.3.2.31.3 The Contractor shall provide functions to support enquiry of images and records relating to identity cards applications made prior to first generation of computerised identity card. The function shall be provided in a way that the concerned images and records can be enquired and retrieved in a single transaction same as other ROP records relating to computerised identity card in order to save the time and efforts of officers.

2.3.3.2.31.4 For contingency and backup purpose, standalone IMS workstation shall be set up to support enquiry of IMS indices in off-line mode during disaster situation of IMS.

2.3.3.2.31.5 Tenderers shall provide in Table 5-4.1(A) of Schedule 4 – “Technical Proposal and System Configuration” of Part V the preliminary design of IMS. The placement of images and the mechanism to file and index images to IMS throughout the application processing cycle (e.g. beginning from image capturing by the Registration Desk until the images are stored in permanent massive storage device) shall be addressed in the preliminary design.

2.3.3.2.31.6 Tenderers shall propose and explain the compression and decompression options and techniques to be used for image processing in the System in Schedule 3 – “Specifications” of Part V.

2.3.3.2.32 Batch Jobs and Reporting Functions

2.3.3.2.32.1 The System shall provide batch jobs for record updating and purging, batch report generation, data consistency check, statistics compilation and interface file generation.

2.3.3.2.32.2 The System shall provide functions for making enquiry and facilities for users to view, print and download reports and statistics, including but not limited to, statistical report related to Mobile Registration / Card Collection Device operation.

2.3.3.2.33 Interface Functions with APPLIES

2.3.3.2.33.1 The System shall interface with APPLIES and through such interface to provide the following existing functions (and all changes to such existing functions until the rollout of SMARTICS-2). These functions include, but not limited to, the following to support accessing of data made available by APPLIES on DSOP, and uploading relevant data by the System to DSOP for APPLIES users to review:

(a) update condition and limit of stay of an applicant using information from APPLIES via DSOP (including pre-mature termination of stay information of certain categories of temporary residents) and provide HKIC application and other relevant information;

(b) receive application information from APPLIES;

(c) provide functions to maintain invalid card indicators (such as deceased indicators) and to update Invalid and Lost Identity Card (“ILIC”);

(d) support provision of digital images to APPLIES; and

(e) provide update to SMARTICS-2 for application merging.

2.3.3.2.34 Interface Functions with Data Warehousing Information System (“DWIS”)

2.3.3.2.34.1 The System shall interface with DWIS and through such interface to provide the following existing functions (and all changes to such existing functions until the rollout of SMARTICS-2). The System shall provide batch jobs to extract different types of statistics to support DWIS. The System shall provide, but not limited to, the interface files for ROP application registration and issuance, application result and statistical information for the HKPIC / HKIC required by the DWIS. The function shall also cater for the transactions during the territory-wide HKIC replacement exercise.

2.3.3.2.35 Interface Functions with Immigration Control System (“ICONS”)

2.3.3.2.35.1 The System shall interface with ICONS and through such interface to provide the following existing functions (and all changes to such existing functions until the rollout of SMARTICS-2), including but not limited to, functions by accessing data made available by ICONS and uploading relevant data by the System for performing the following:

(a) extract certain information from the System for compiling passenger statistics;

(b) enquire movement record information (HKIC or non-HKIC holders) from ICONS to facilitate registration assessment;

(c) allow data matching (including fingerprint template and photo) on information provided by ICONS and return matching results;

(d) obtain One-way Permit (“OWP”) information from ICONS;

(e) allow ICONS users to view the ROP information; and

(f) provide information regarding ILIC.

2.3.3.2.35.2 The System shall receive enrolled Macao e-Channel information from ICONS and send the respective updated date of registration information to ICONS.

2.3.3.2.35.3 For reported lost HKIC cases at control points, the System shall receive e-format memo from ICONS regarding the lost HKIC case and index to the record of the concerned person in the System, the corresponding lost HKIC alert will be passed to CDS for ILIC table update. For identity verification at control points, the System shall support instant auto-verification by comparing the concerned resident’s fingerprint captured by ICONS with that in the System’s database and return matching scores to ICONS. The System shall provide daily audit trail report for the auto-verification.

2.3.3.2.36 Interface Functions with e-Passport

2.3.3.2.36.1 The System shall interface with e-Passport and through such interface, to perform the following existing functions, (and all changes to such existing functions until the rollout of SMARTICS-2), including but not limited to, functions by uploading relevant data to and from e-Passport:

(a) upon receiving request from e-Passport, provide information, including photo and personal details, to e-Passport for facilitating e-Passport application assessment;

(b) pass information to e-Passport regarding the application result of minor PIC and overseas issued PIC application and the completion of card personalisation;

(c) update e-Passport the change of assessment result code after approval of MPIC / OPIC , e.g. application correction;

(d) receive information from e-Passport regarding completion of issuance of minor PIC and overseas issued PIC; and

(e) transfer information related to travel document application to e-Passport for facilitation of the related application processing.

2.3.3.2.37 Interface Functions with e-Passport-2

2.3.3.2.37.1 The System shall support interface with e-Passport-2, which will be implemented in early 2019 tentatively. On top of the existing interface functions with e-Passport as mentioned in Section 2.3.3.2.36 above, the System shall provide, including but not limited to, the following functions:

(a) interface with e-Passport-2 in real time to facilitate verification for passport applications;

(b) receive and provide information from / to e-Passport-2 to process MPIC and OPIC applications;

(c) facilitate ROP photo matching function for auto-assessment in e-Passport-2; and

(d) provide ROP photo for passport application within a designated time.

2.3.3.2.38 Interface Functions with Other Government Departments

2.3.3.2.38.1 The System shall provide External Interfaces (as defined in Section 2.3.8.12.5 of this Annex) with the systems of around ten (10) Government departments (collectively "External Systems") and through such External Interfaces, provide functions in handling requests of verification of personal data for specific authorised purposes. Tenderers shall note that some Government departments have one (1) or more External System(s) each with one (1) or more interface(s) with ImmD.

2.3.3.2.38.2 The System shall provide the following functions via External Interfaces with the External Systems to be developed by the Contractor and subsequently to be migrated from DSOP to the System for necessary data transfer via these interfaces:

(a) authenticate and authorise connection with External Systems and receive files and return files, including card status, residential status, textual data and images, etc., to / from the systems. The interface files shall be transmitted by secure electronic means, e-mail or in a printer file format via the GNET, as well as by dataline or external devices. All interface files requires encryption and the System shall be able to validate the digital signature with e-Cert. The System shall also provide function to update the list of authorised information requesters of the External Systems. The System shall produce online and batch statistics as well as exception report;

(b) initiate compilation of files upon receiving paper requests and return files to the requesting party via designated dataline, workstations or other means. All data requires encryption and access control shall be in place;

(c) perform the handling of ad hoc requests for information of selected HKIC holders;

(d) based on specific business criteria, assemble reports to extract information obtained during the registration process and upon the receipt of notification of change of registered particulars, and send out the reports to requesting departments;

(e) receive e-Cert information from Hongkong Post; and

(f) access Government Financial Management Information System ("GFMIS") of Treasury for transfer of daily collection books regarding the daily revenue received from ROP branch offices.

2.3.3.2.38.3 The System shall interface specifically with a Government department (collectively "Specific External Interface") to receive enquiry regarding validity of an identity card and the System shall give instant response with a code indicating validity of the identity card. Before returning a code to the originating department, record checkings shall be performed which include checking of lost card, invalid and deceased information, as well as the updated condition and limit of stay of the cardholder obtained from other relevant ImmD systems.

2.3.3.2.39 Interface Functions with Other ImmD Applications

2.3.3.2.39.1 The System shall interface with the following systems to enable exchange of data between them.

Systems in ImmD	Brief Description / Information Involved
Pre-checking Enrolment System (“PRES”)	Transfer reported death records to PRES
Online Checking System for Subsidised Public HealthCare Services (“OCSSS”)	Transfer relevant information of HKIC holders and residential status (i.e. unconditional and conditional) to OCSSS
User & Profile Management System (“UPMS”)	All UPMS related functions (e.g. user access control) via ITI
Next Generation Computer Output Management System (“COMS-2”)	Send reports (in text, PDF, etc.) to COMS-2
e-EEP	Send key pairs for authentication with chip on e-EEP

2.3.3.2.39.2 Other than aforesaid, the System shall coordinate information from other existing or future ImmD applications and allow interface for information exchange and provision such that consolidated response is viable within reasonable time.

2.3.3.2.40 Interface Functions with CDR

2.3.3.2.40.1 The System shall provide functions by accessing common data made available by other ImmD systems on CDR, and uploading data by the System to CDR via common data services and functions, including the new services and functions for SMARTICS-2 to be provided by the Contractor. The System shall support interfaces which are real time or by batch periodically. The System shall provide the following, but not limited to, functions to interface with CDR:

(a) provide functions to view application information;
(b) provide functions at the Registration Desk and Assessment Desk to check C/S and L/S and pre-mature termination information to facilitate new smart identity card application;
(c) provide functions at the Collection Desk and self-service collection kiosk to retrieve C/S and L/S for updating to the chip of the HKIC;
(d) use visa reference number or Hong Kong Birth Certificate number to retrieve personal data for indexing at Registration Desk;
(e) retrieve and maintain non-permanent resident records;
(f) provide online update on registration of personal particulars;
(g) provide online update on ILIC;
(h) provide online update upon completion of first registration cases and other

applications involving changes in personal particulars, including re-registration cases; and

(i) provide online enquiry functions for ICONS movement records.

2.3.3.2.41 Interface with Down-sized Open Platform ("DSOP")

2.3.3.2.41.1 The System shall upload and enquire relevant information stored in DSOP to facilitate use of data across ISS-2 systems, e.g. APPLIES, as well as ICONS.

2.3.3.2.42 Receive Common Change of Address File from Office of the Government Chief Information Officer ("OGCIO")

2.3.3.2.42.1 The System shall receive common change of address data file in the form of structured data from OGCIO and update system database.

2.3.3.2.43 Interface for electronic payment systems

2.3.3.2.43.1 The System shall interface with EPS (and other payment means) to facilitate electronic payment services.

2.3.3.2.44 Other Miscellaneous Functions

2.3.3.2.44.1 In addition to the above functions, the System shall also support the following functions:

(a) online report printing;

(b) record matching by online and batch modes;

(c) data synchronisation for records, security profiles and code tables;

(d) 24-hour enquiry access of database and images;

(e) transaction logging;

(f) batch job control and scheduling;

(g) generation of reports for management, monitoring, audit trail and statistical purposes; and

(h) system and data backup / recovery.

2.3.3.2.45 Access Control and System Maintenance

2.3.3.2.45.1 The System shall provide functions for access control and system maintenance as follows:

(a) provide stringent access control measures within different authentication and authorisation levels for controlling any access into the computer system, e.g. by location, post, role, user and workstation, as well as general administration functions;

(b) adopt single terminal approach and single sign-on for accessing the System and other ISS-3 systems. Apart from accessing SMARTICS-2, security measures on accessing other ImmD systems shall also be designed with the support of single sign-on approach;

(c) insert, amend, enquire and delete specific system tables;

(d) able to make use of the system code tables maintained in CDR; and

(e) broadcast messages and show help text for users. The help text shall be editable when required.

2.3.3.2.45.2 The System shall integrate with UPMS provided under ITI to provide system security and access control functions.

2.3.3.2.45.3 The System shall support change mode of operation when there is system failure and when system resumes normal processing to operate in local mode, standalone mode and normal mode.

2.3.3.2.45.4 The System shall support any abnormal scenario, including but not limited to, centralised ITI UPMS service suspension, system failure, etc, in order to provide contingency measures for users to log in the application with appropriate security access control.

2.3.4 Functional Requirements for Infrastructure of Core System

2.3.4.1 The infrastructure of the Core System as listed in Section 2.2.4.9 of this Annex shall provide a secure, high performance, high resilience and easily expandable infrastructure to support the distributed processing and information exchange needs of SMARTICS-2. It shall primarily ride on the ITI MCN, the Extended MCN, the ITI AN, the Local Kiosk Network, the General Kiosk Network and in some cases the INI and ITI connecting among all the Locations as specified in Section 8 – "Location Requirements" of Part VII. Network diagrams are set out in Section 2.2.4 of this Annex for reference.

2.3.4.2 The infrastructure of the Core System, as listed in Section 2.2.4.9 of this Annex, shall comprise of the following components:

(a) network and communication infrastructure;
(b) server and storage infrastructure;
(c) data management infrastructure;
(d) application services infrastructure;
(e) business services provisions;
(f) system management and backup infrastructure;
(g) cryptography and security infrastructure;
(h) development, testing and training environments; and
(i) development and testing tools.

2.3.4.3 All components of the System, which will support ImmD's business functions, and applications in a shared data and distributed computing environment, shall be integrated into the infrastructure of the Core System.

2.3.4.4 The Contractor shall make sure that the design and implementation of the infrastructure of the Core System will not introduce any adverse impact to the existing networks and system service of ImmD. The Contractor shall provide the detailed designs during SA&D stage.

2.3.4.5 The Contractor shall cater for the necessary special arrangements (e.g. housing of equipment, cabling) during site preparation of the LAN for SMARTICS-2 at those locations with existing setup for INI or ITI.

2.3.4.6 ITI maintains the availability of the mission-critical services of ITI and supports the backbone network connectivity for ISS-3 systems at the PDC(KC) and DDC(FL). The DDC(FL) acts as the standby site of the PDC(KC) when system disaster occurs. The high-level conceptual infrastructure topology of the Core System is illustrated in Figure 7A-2.2.4.2 for indication. The Contractor shall implement and establish the infrastructure of the Core System riding on the ITI.

2.3.4.7 The production capacity of the infrastructure of the Core System shall be able to support all the business operation needs at the PDC(KC), the DDC(FL), ROP branch offices, SIDCCs, HQ, control points and immigration offices outside HQ such that all the functions for the System can be performed in compliance with the Overall Specifications, Reliability Levels and Performance Criteria.

2.3.4.8 Tenderers shall provide overall technical design and architecture of the System in Schedule 4 – “Technical Proposal and System Configuration” of Part V, describe how the design can meet the requirements and how the proposed infrastructure of the Core System components can be integrated with the ITI MCN and ITI AN at PDC(KC) and DDC(FL) including but not limited to, network connection, ITI services (including UPMS, CDR and CDS), system management and monitoring, backup and other components of SMARTICS-2 as a whole.

2.3.4.9 All network diagrams in this Annex only illustrate the high-level concept from FSR. Tenderers can propose better design where appropriate.

2.3.5 Functional Requirements for Network and Communication Infrastructure

2.3.5.1 General Requirements

2.3.5.1.1 The network and communication infrastructure to be implemented by the Contractor shall support the following:

(a) workstations of SMARTICS-2, self-service collection kiosks, e-Cabinets, self-service general application kiosks, self-service tag issuing kiosks and information display units at ROP branch offices and SIDCCs to access the System functions;

(b) self-service registration kiosks at SIDCCs to access the System functions;

(c) workstations of existing ISS-2 systems (e.g. e-Passport, APPLIES, etc.) or ISS-3 systems (e.g. ICONS, UPMS, etc.) at ROP branch offices and SIDCCs to access respective ISS-2 or ISS-3 systems which are riding on the INI or ITI; and

(d) workstations of SMARTICS-2 and self-service general application kiosks to be provided under SMARTICS-2 at control points and immigration offices at and outside HQ, via INI or ITI, to access the System functions.

2.3.5.1.2 The network and communication infrastructure of the Core System (or “network”) to enable the above-mentioned functions (viz. including all network architecture to be established by the Contractor for establishing the Extended MCN, the Local Kiosk Network, the General Kiosk Network, and for connecting the System to ITI and INI) shall be of high security, high performance and high availability to support the data exchange and transfer of images among all locations of the System.

2.3.5.1.3 The network shall be scalable, modular, reliable and easy to maintain. The network shall be compatible and fully integrated with ITI.

2.3.5.1.4 All network equipment, including firewalls, routers and server switches, shall support high availability features to ensure system resilience, minimise service downtime and prevent any single point of failure for the network infrastructure.

2.3.5.1.5 The network shall use prevalent industry standards-based network equipment and protocols.

2.3.5.1.6 The Contractor shall make recommendations on the Internet Protocol (“IP”) address and Virtual Local Area Network (“VLAN”) assignment strategy to ImmD for consideration and endorsement.

2.3.5.1.7 The network (viz. such part of the network to be set up by the Contractor for integrating the System with the AN) shall support secure and controlled connectivity to external networks for data exchange with external parties.

2.3.5.1.8 The network shall follow a homogeneous Transmission Control Protocol / Internet Protocol (“TCP/IP”) based network architecture.

2.3.5.1.9 The network shall have IPv6 support capability to support other potential ISS-3 applications and other future ImmD systems that have explicit requirement with IPv6.

2.3.5.1.10 Upon switch or network failure, recovery procedures shall be initiated transparently and completed quickly.

2.3.5.1.11 All switches and routers for the network shall be configured to support Dynamic Host Configuration Protocol (“DHCP”) forwarding and dynamic IP address assignment. They shall be configured to ensure that workstations continue to get IP addresses even if one of the DHCP servers fails.

2.3.5.1.12 All server and network switches shall be gigabit switches and shall have spare ports for further expansion of servers, workstations and kiosks at the locations.

2.3.5.1.13 The network shall be capable of implementing multiple VLANs on the same floor or across floors.

2.3.5.1.14 Network error due to any misconfigured or malfunctioning workstation shall not affect serviceability and performance of other workstations.

2.3.5.1.15 Resilience shall be provided for connection to server farm layer against switch failure.

2.3.5.1.16 The network shall have workload sharing and balancing capability.

2.3.5.1.17 The edge routers shall be interoperable with the network infrastructure in ITI and interoperable with the existing INI implemented at ROP branch offices and immigration offices within and outside HQ.

2.3.5.1.18 Tenderers shall provide reference(s) of the proposed network design in Schedule 4 – "Technical Proposal and System Configuration" of Part V.

2.3.5.1.19 The Contractor shall set up the network infrastructure of the proposed design during SA&D stage to demonstrate its interoperability with ITI and INI.

2.3.5.1.20 The Contractor shall provide network management system comprising network management software and relevant equipment to manage all the network equipment provided by the Contractor.

2.3.5.2 Wide Area Network ("WAN") Architecture

2.3.5.2.1 WAN for MCN

2.3.5.2.1.1 The WAN architecture for the both MCN and Extended MCN shall be of high security, high performance and high availability to inter-connect all ROP branch offices, SIDCCs, control points, immigration offices within and outside HQ, PDC(KC) and DDC(FL) for SMARTICS-2 applications.

2.3.5.2.1.2 The WAN architecture for the both MCN and Extended MCN to be implemented by the Contractor shall be able to support Metro-Ethernet technologies and able to integrate with the ITI MCN at PDC(KC) and DDC(FL) as well as the INI at HQ and RC.

2.3.5.2.1.3 MCN WAN links will be provided by the Government. The Contractor shall make use of these WAN links for the connection among the PDC(KC), DDC(FL), ROP branch offices, SIDCCs, control points and immigration offices within and outside HQ. Tenderers shall provide the sizing details for the requirement of the System with respect to these MCN WAN links in Table 5-3.4(A) of Schedule 3 – "Specifications" of Part V.

2.3.5.2.1.4 Dual WAN links will be provided by the Government for each ROP branch office and SIDCC for WAN resilience. Two edge routers shall be provided and installed by the Contractor at each location of ROP branch offices and SIDCCs for the MCN. The Contractor shall provide a solution (e.g. by creating additional logical circuits / VLANs) to establish direct link between ROP branch offices, together with SIDCCs, and PDC(KC) as well as DDC(FL) (viz. the Extended MCN). The solution shall also allow the existing INI switches installed at ROP branch offices to connect to the network equipment so that the existing ISS-2 workstations at ROP branch offices can access INI at HQ and RC before these ISS-2 workstations at ROP branch offices are completely migrated and connected to the Extended MCN at ROP branch offices. The solution shall also allow other ISS-3 workstations (e.g. ICONS) at ROP branch offices and SIDCCs can access the respective ISS-3 system and ITI at PDC(KC) and DDC(FL).

2.3.5.2.2 WAN for General Kiosk Network

2.3.5.2.2.1 The WAN architecture for the General Kiosk Network shall be of high security and high performance to inter-connect all ROP branch offices, SIDCCs, HQ, control points, immigration offices outside HQ, PDC(KC) and DDC(FL) for the network communication of MSK_GEN. It shall be able to support Metro-Ethernet technologies and integrate with the ITI AN at PDC(KC) and DDC(FL).

2.3.5.2.2.2 AN WAN links will be provided by the Government. The Contractor shall make use of these WAN links for the connection among PDC(KC), DDC(FL), ROP branch offices, SIDCCs, HQ, control points and immigration offices outside HQ of the General Kiosk Network for MSK_GEN. Tenderers shall provide the sizing details for the requirement of the System with respect to these AN WAN links in Table 5-3.4(A) of Schedule 3 – “Specifications” of Part V.

2.3.5.2.2.3 Edge routers shall be provided and installed by the Contractor at the Untrusted Zone of PDC(KC), DDC(FL), ROP branch offices, SIDCCs, HQ, control points and immigration offices outside HQ, as the locations specified in Sections 6.2.2.5.1 to 6.2.2.5.4 of this Annex for the network communication of self-service general application kiosks.

2.3.5.2.3 External Interface Services for Other Government Departments

2.3.5.2.3.1 An external perimeter security solution is provided by the ITI AN to protect the security of ImmD production environment while linking production system with other external government systems via the GNET.

2.3.5.2.3.2 The network at ImmD is divided into multiple security zones which are delimited by security gateways provided by ITI. If necessary, the Contractor shall upgrade these security gateways to accommodate the workload for the System.

2.3.5.2.3.3 The Contractor shall integrate the System with the ITI AN so that the System will have the network connection for the External Interfaces with the External Systems as described in Section 2.3.3.2.38 of this Annex. The Contractor shall cater for the necessary configuration updates of the network equipment in ITI AN.

2.3.5.2.3.4 Intrusion prevention services (“IPS”) and intrusion detection services (“IDS”) are provided at the network level in the AN. The Contractor shall provide and install host-based IDS on servers connected to external parties, in order to protect and alert when an attack event is detected.

2.3.5.2.3.5 The Contractor shall provide any necessary hardware, software, tools and services for establishing the External Interfaces between the External Systems and the System. Appendix C – "Description of IT Infrastructure of ImmD" to Part VII sets out the network architecture of AN setup by ITI.

2.3.5.2.4 The System shall be able to recover from network problem within reasonable time such that it can function continuously and normally.

2.3.5.2.5 Network recovery from link failure shall be transparent to end-users.

2.3.5.2.6 Data encryption technology shall be deployed so that all traffic travelling across all WANs of the System are encrypted. The encryption standard shall be compatible with the data encryption technology implemented by ITI. Details of WAN encryption and security of ITI are set out in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII.

2.3.5.2.7 Quality of Service ("QoS") shall be implemented for supporting time critical applications.

2.3.5.3 Local Area Network ("LAN") Architecture

2.3.5.3.1 Similar to the current INI MCN in HQ, Restricted Zone and Secured Zone are built in the ITI MCN. As security requirement, the Core System shall ride on the server farm layer in the Secured Zone in PDC(KC) and DDC(FL), ROP branch offices and SIDCCs.

2.3.5.3.2 The three-tier network infrastructure, i.e. core layer, distribution layer and access layer, is adopted in the LANs of MCN at data centres. The core layer switches with high throughput performance provide network stability. The distribution layer is used as the communication point between the access layer and the core layer. The functions of the distribution layer are to provide routing and filtering, and determine the fastest way that user requests are serviced. The access layer switches provide network access ports to servers and workstations.

2.3.5.3.3 Two-tier network infrastructure for the LANs of AN is adopted, namely distribution and access layers, at data centres. Similar to the INI AN in HQ, Untrusted Zone ("UTZ"), Demilitarised Zone ("DMZ" or "DM Zone") and Trusted Zone ("TZ") are built in the ITI AN at data centres.

2.3.5.3.4 Two-tier network layers, namely distribution and access layers, shall be adopted for the LANs at ROP branch offices and SIDCCs. Distribution layer switches are used to provide LAN connection for access layer switches and edge routers for WAN, while access layer switches are used to provide LAN connections for servers, workstations, kiosks and printers. The Contractor shall implement the two-tier network infrastructure for the LANs of MCN and AN in ROP branch offices and SIDCCs.

2.3.5.3.5 The allocation of workstations and kiosks shall be evenly distributed into access layer switches in order to minimise the impact to the operation when any hardware failure occurs.

2.3.5.3.6 The network of the infrastructure of the System shall possess the following LAN :

(a) LANs at PDC(KC) and DDC(FL);

(b) LANs at ROP branch offices and SIDCCs;

(c) LANs at the immigration offices at HQ; and

(d) LANs at control points and other immigration offices outside HQ.

2.3.5.3.7 LANs at PDC(KC) and DDC(FL)

2.3.5.3.7.1 The Contractor shall provide the LAN of Central Service Layer for the System, which shall be set up and ride on the ITI MCN and ITI AN in PDC(KC) and DDC(FL).

2.3.5.3.7.2 The Contractor shall provide all equipment, including network appliances, in dual as network resilience to the System for the production environment in the PDC(KC), and all network equipment for the production resilience environment in the DDC(FL).

2.3.5.3.7.3 The three-tier network infrastructure for the LANs of MCN shall be adopted in data centres. The Contractor shall provide at least two distribution layer switches and sufficient number of access layer switches in pairs for connecting the System infrastructure servers to the distribution layer switches at the Restricted Zone. Two distribution layer switches in the Secured Zone are provided by ITI and the switches will be shared with the System of Category B. The Contractor shall provide sufficient number of access layer switches in pairs for connecting the server farm of the System in Secured Zone and Restricted Zone of data centres.

2.3.5.3.7.4 The network infrastructure of the System shall be able to configure with load balancing and resilience capabilities.

2.3.5.3.7.5 For the LANs of AN in data centres, the Contractor shall provide sufficient number of access layer switches in Trusted Zone and DM Zone for connecting the System servers to the distribution layer switches. For the access switch in Trusted Zone and DM Zone, the access switches provided by the Contractor shall support stacking technology and stackable with ITI distribution and access layer switches set out in Section 3.6 (a) and (b) of Appendix C - “Description of IT Infrastructure of ImmD” to Part VII.

2.3.5.3.7.6 The distribution layer switches in Trusted Zone, DM Zone and Untrusted Zone in AN are provided by the ITI. The design of the network infrastructure of ITI is set out in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII.

2.3.5.3.7.7 The Contractor shall provide staging and interface servers, web and application servers and other equipment for data exchange and file transfer with external parties and the Core System web application running on self-service general application kiosks via ITI AN in PDC(KC) and DDC(FL).

2.3.5.3.7.8 Tenderers shall review and provide any additional equipment or components for the connection of the Core System servers and equipment to ITI switches and network equipment in Schedule 1 – “Hardware” and Schedule 2 – “Software” of Part V. Network infrastructure of ITI is set out in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII.

2.3.5.3.7.9 The Contractor shall be responsible to provide necessary hardware, software and services to set up the LANs infrastructure of MCN and AN for the infrastructure of the Core System at PDC(KC) and DDC(FL).

2.3.5.3.8 LANs at ROP branch offices and SIDCCs

2.3.5.3.8.1 Local Service Layer for SMARTICS-2 rides on the LANs of the Extended MCN and Local Kiosk Network in ROP branch offices and SIDCCs. The Contractor shall provide and implement all equipment, including network appliances, in dual as network resilience to SMARTICS-2 in each location of ROP branch offices and SIDCCs.

2.3.5.3.8.2 The Contractor shall provide and implement the double firewalls, in different brands to minimise risk of vulnerability, in dual for segregating the Extended MCN and Local Kiosk Network for allowing only authorised data traffic passing through.

2.3.5.3.8.3 The Contractor shall provide and implement the firewalls in dual for segregating the Restricted Zone and Secured Zone in the Extended MCN for each location of ROP branch offices and SIDCCs. The System shall ride on the server farm in the Secured Zone and Restricted Zone in the Extended MCN of ROP branch offices and SIDCCs.

2.3.5.3.8.4 The Contractor shall provide and implement the firewalls in dual for segregating the Kiosk DM Zone and Untrusted Zone in AN for the Local Kiosk Network in ROP branch offices and SIDCCs.

2.3.5.3.8.5 The LANs of the Extended MCN and the Local Kiosk Network at ROP branch offices and SIDCCs shall be of high availability, high performance, scalable, and with sufficient network security. The LANs shall provide network support services, including time synchronisation, DHCP, domain name system (“DNS”) and other necessary services, for the System and the Systems of Categories C and D at ROP branch offices and SIDCCs.

2.3.5.3.8.6 At least two (2) distribution layer switches shall be provided by the Contractor and shall be installed for the distribution layer for the LANs of Extended MCN of each location of ROP branch offices and SIDCCs. Network-level resilience shall be implemented at this layer.

2.3.5.3.8.7 The distribution layer at ROP branch offices and SIDCCs shall connect to the edge routers so that data traffic, not only SMARTICS-2, but also other ISS-3 applications, can be routed to / from other locations of ITI MCN. The distribution layer at ROP branch offices and SIDCCs shall have multiple-paths connected to the core layer of ITI at data centres.

2.3.5.3.8.8 The Contractor shall provide and deploy sufficient access layer switches, with at least two (2) for connecting SMARTICS-2 server equipment in Secured Zone and at least four (4) for connecting infrastructure servers and Front-end Service Layer in Restricted Zone, at the Extended MCN for each location of ROP branch offices and SIDCCs. SMARTICS-2 workstations (to be supplied by the Government), e-Cabinets (to be provided under Category C) and other ISS-3 application workstations shall be connected as the Front-end Service Layer to the access layer switches in the Extended MCN at ROP branch offices and SIDCCs.

2.3.5.3.8.9 The Contractor shall provide and deploy sufficient access layer switches, with at least two (2) for connecting server equipment in Kiosk DM Zone and at least two (2) for connecting kiosks of Front-end Service Layer in Untrusted Zone, for each location of ROP branch offices and SIDCCs. The Contractor shall provide and deploy sufficient equipment for the connection of self-service registration kiosks, self-service collection kiosks and self-service tag issuing kiosks (to be provided under Category C and Category D) in Untrusted Zone of the Local Kiosk Network and self-service general application kiosks (to be provided under Category C) in Untrusted Zone of the General Kiosk Network.

2.3.5.3.8.10 The access layer switches shall filter out unauthorised packets at Media Access Control (“MAC”) or IP layer.

2.3.5.3.8.11 Besides the distribution layer and access layer switches, the Contractor shall provide all other necessary network equipment for SMARTICS-2 to build the LANs in ROP branch offices and SIDCCs.

2.3.5.3.8.12 Switches in the access layer of MCN shall be installed and configured with physically separated fibre-optic cables connecting to distribution layer switches. For the access layer switch of Untrusted Zone in AN, the uplink shall be connected to the edge router directly. Restricted access shall be implemented for authorised traffic.

2.3.5.3.8.13 ImmD is currently using both Unshielded Twisted Pair (“UTP”) and fibre-optic cables at ROP branch offices. The Contractor shall perform site visits to various ROP branch offices to get the latest information for planning and implementation.

2.3.5.3.8.14 Fibre-optic cables shall be used for inter-floor and outdoor connections as well as the connection over 100 meters.

2.3.5.3.8.15 The Contractor shall provide Enhanced Category 5 / Category 6 or above UTP cables and fibre-optic cables for connecting the front-end equipment, such as SMARTICS-2 workstations, self-service registration kiosks, self-service collection kiosks, e-Cabinets and self-service general application kiosks, to the access layer switches at ROP branch offices and SIDCCs.

2.3.5.3.8.16 The Contractor shall be responsible for setting up and configuring the trunk port for connecting the switches in ROP branch offices and SIDCCs.

2.3.5.3.8.17 The Contractor shall be responsible for the cabling services including the necessary material for all workstations, kiosks, servers, and computer equipment, connecting to SMARTICS-2, including the workstations and kiosks which will be provided by other contractors. The Contractor shall lay all the uplinks fibre-optic cables between all the network equipment including edge routers, distribution layer and access layer switches in the Extended MCN, Local Kiosk Network and General Kiosk Network.

2.3.5.3.8.18 The Contractor shall be responsible to test all the cables so as to ensure the cables adhere to the cable standard for the network technology.

2.3.5.3.8.19 The Contractor shall provide cabling service and the supply of materials for cabling for the System.

2.3.5.3.8.20 The Contractor shall provide cabling services and materials required for the installation of SMARTICS-2 network at ROP branch offices and SIDCCs. The required cabling services and materials shall include, but not limited to:

(a) equipment cabinets for housing network equipment and patch panels;

(b) enhanced Category 5 / Category 6 or above UTP cables from workstations, kiosks and / or printers to the data port at back offices;

(c) patch cables from routers / switches to the patch panel; and

(d) all cabling works within the computer room up to the patch panel.

2.3.5.3.8.21 For the spare switch ports available on the switches provided by the Contractor, the Contractor shall provide corresponding network configuration and support upon ImmD request for both SMARTICS-2 and other projects.

2.3.5.3.8.22 The high-level infrastructures of the LANs at ROP branch offices are briefly illustrated as below:

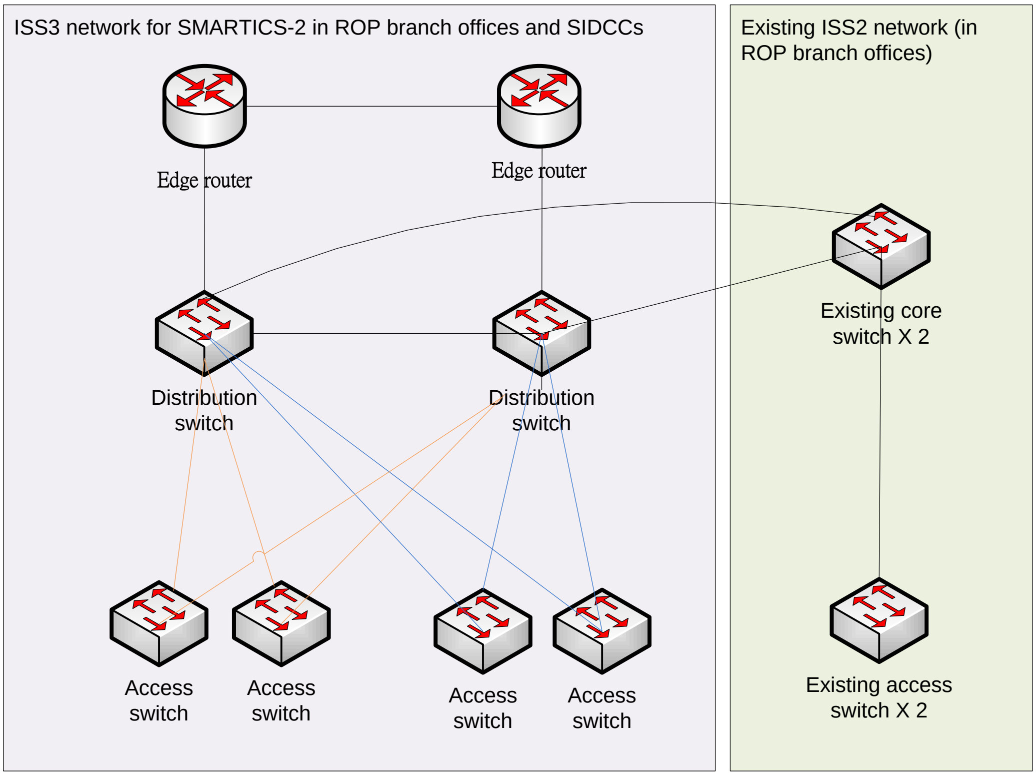


Figure 7A-2.3.5.3.8.22 High-level Infrastructures of LANs at ROP Branch Offices

2.3.5.3.8.23 Some ISS-2 systems are installed at ROP branch offices and shall continue to be used after the rollout of the System. The Contractor shall provide a solution for migrating the followings from INI to the Extended MCN:

(a) existing ISS-2 workstations of other ImmD systems;

(b) existing ISS-2 network equipment of other ImmD systems;

(c) existing ISS-2 servers of other ImmD systems; and

(d) existing ISS-3 workstations of other ImmD systems (e.g. ICONS).

2.3.5.3.8.24 The solution for Section 2.3.5.3.8.23 of this Annex shall not require any modification of other ImmD systems at ROP branch offices. The Contractor shall provide all the necessary hardware, software and related services, including but not limited to, the network configuration and cabling services.

2.3.5.3.8.25 About five (5) workstations of some existing ISS-2 systems (e.g. APPLIES) and ISS-3 systems (e.g. ICONS) shall be installed at each SIDCC and the Contractor shall provide a solution for the installation of those systems to be run at SIDCCs. The Contractor shall provide all the necessary hardware, software and related services, including but not limited to, the network configuration and cabling services for the connection of workstations of existing ISS-2 and ISS-3 systems at SIDCCs.

2.3.5.3.8.26 The Contractor shall be responsible to provide all necessary hardware, software and services to set up the LANs infrastructure of the Extended MCN, Local Kiosk Network and General Kiosk Network, for the connection of the servers and equipment provided by the Contractor, and also the equipment to be provided by the Government, the Contractors of Category C and Category D, including but not limited to, TAGS-2 servers and equipment, SMARTICS-2 workstations, e-Cabinets, self-service registration kiosks, self-service collection kiosks, self-service general application kiosks, TAGS-2 workstations, self-service tag issuing kiosks and information display units of Local Service Layer and Front-end Service Layer in ROP branch offices and SIDCCs.

2.3.5.3.9 LANs at the immigration offices at HQ

2.3.5.3.9.1 Two-tier network infrastructure for the LANs of ITI MCN was implemented in HQ. The Contractor shall provide the equipment to support the LANs of ROP-HK, which is one of the ROP branch offices to be set up and provided by the Contractor as mentioned in Section 2.3.5.3.8 of this Annex, and the LANs of ROP offices at different floors in HQ, including the Card Personalisation Office, which servers and equipment will be provided by the Contractor of Category B.

2.3.5.3.9.2 The Contractor shall provide at least two (2) distribution switches for consolidating all infrastructure servers, equipment and workstations for SMARTICS-2 at different floors and connecting to the distribution switches which are provided by ITI in HQ.

2.3.5.3.9.3 The Contractor shall provide at least two (2) network module devices and any necessary equipment to be installed into the module card slots of the existing ITI MCN distribution switches in HQ for the connection of servers and equipment of SMARTICS-2 to the ITI distribution switches in HQ. The Contractor shall implement a solution that requires no more than four (4) 10 GE ports in each network module devices and at least eight (8) 10 GE ports in each network module devices can be reserved for future expansion in ImmD. Details of the existing network equipment of ITI in HQ are depicted in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII.

2.3.5.3.9.4 The Contractor shall provide Enhanced Category 5 / Category 6 or above UTP cables and fibre-optic cables and cabling services for the network ports for SMARTICS-2 users in HQ.

2.3.5.3.9.5 The Contractor shall provide and deploy sufficient access layer switches and floor level access switches for connecting servers, equipment and workstations for SMARTICS-2 at different floors in HQ, including the equipment provided by the Contractor of Category B in Card Personalisation Office, to the ITI distribution switches. The uplinks of the added access switches shall be connected to the INI core switches or the ITI distribution switches at computer rooms at 9/F and 18/F by fibre-optic cables. The locations of ROP offices and immigration offices at HQ are described in Section 8 – "Location Requirements" of Part VII.

2.3.5.3.10 LANs at control points and other immigration offices outside HQ

2.3.5.3.10.1 Tenderers shall consider reusing the existing LAN cables, where appropriate. The Contractor shall provide cabling services for the network ports required by SMARTICS-2 users and shall be responsible for the on-going maintenance of the cables.

2.3.5.3.10.2 The Contractor shall make use of the existing access switches and deploy additional access switches if the existing access switches cannot support the network port requirement of SMARTICS-2. The uplinks of the added access switches shall be connected to the INI / ITI distribution switches or INI / ITI core switches.

2.3.5.3.10.3 The location of other offices outside HQ, number of user floors and number of network ports required are subject to change. The Contractor shall cater for any change of these as required by the Government.

2.3.5.3.10.4 The Contractor shall provide sufficient access layer switches and network equipment, including routers, for connecting self-service general application kiosks in Untrusted Zone at the General Kiosk Network for each location of control points and other immigration offices outside HQ.

2.3.5.4 Structured Cabling

2.3.5.4.1 The Contractors shall be responsible for the structured cabling in PDC(KC), DDC(FL), HQ, ROP branch offices, SIDCCs, control points and other immigration offices that are required to house the Core System and related equipment, including SMARTICS-2 workstations, self-service registration kiosks, self-service collection kiosks, e-Cabinets, self-service general application kiosks, self-service tag issuing kiosks, etc. which will be provided by the Contractor, the Government or the Contractors of other Categories. The cabling design shall match the physical environment of the data centres and computer rooms in Locations.

2.3.5.4.2 The structured cabling shall support the connectivity for the equipment of the System and the equipment and kiosks, which will be provided by the Contractors of Category C and Category D, to the IP network and Storage Area Network (“SAN”) fabrics.

2.3.5.4.3 The console monitoring room in HQ, PDC(KC) and DDC(FL) may be located in separated area / separated floor. The Contractor shall be responsible for the cabling, including necessary trunking, or connecting between the console monitoring room and the data centres.

2.3.5.4.4 For the special equipment area in PDC(KC) and DDC(FL), the Contractor shall be responsible for the uplink cabling, including necessary trunking, or connecting between the special equipment area and ITI network equipment in Secured Zone.

2.3.5.4.5 The design shall cater for the future expansion on the cables connected to major network devices.

2.3.5.4.6 The Contractor shall prepare cabling design layout with schematic drawings.

2.3.5.4.7 The Contractor shall provide labeling scheme document.

2.3.5.4.8 The Contractor shall supply and install, which includes but not limited to, cable laying, termination and connectivity testing for fibre and copper cable, the required materials for the designed location.

2.3.5.4.9 The Contractor shall provide labeling on patch panel and patch cord including fibre cable and copper cable.

2.3.5.4.10 The Contractor shall provide labeling on power cords and UTP cables connected to servers for SMARTICS-2 in data centres, ROP branch offices and SIDCCs.

2.3.5.4.11 The Contractor shall provide testing report upon finishing the testing and commissioning.

2.3.5.4.12 The Contractor shall supply sufficient number of patch panels, including but not limited to, UTP and fibre-optic patch panels / termination boxes.

2.3.6 Functional Requirements for Server and Storage Infrastructure

2.3.6.1 General Requirements

2.3.6.1.1 The server and storage infrastructure for the System shall have high availability and no single point of failure. The infrastructure shall be expandable and reliable.

2.3.6.1.2 In the production environment, each type of servers shall have at least two (2) machines running in either active-active or active-passive mode for the System at ROP branch offices, SIDCCs and PDC(KC).

2.3.6.1.3 The Contractor shall implement either active-active or active-passive server clusters design for the servers of Central Service Layer and Local Service Layer. One (1) single server cluster shall be capable of handling all transactions without any service level degradation. For the active-active mode, all requests to the clusters shall be distributed by load balancers or handled by software or operating system, both web and application servers shall handle transactions in the same manner. In case there is any service outage of one member of the cluster, all transactions will be redirected to the remaining members of the cluster. For the active-passive mode, all requests shall be handled by one cluster member, while the other cluster members shall be in standby mode. If the primary member fails, the other cluster member shall pick up the primary role automatically less than three (3) minutes.

2.3.6.1.4 Pairs of SAN switches shall be supplied and each server requiring access to the SAN storage shall be multi-path connected to the SAN switches. Each SAN switch shall be multi-path connected to the SAN storage.

2.3.6.1.5 The Contractor shall implement the SAN storage for the server farms at PDC(KC), DDC(FL), ROP branch offices and SIDCCs. The design of storage solution shall support data encryption according to the user requirements and relevant security guidelines and regulations.

2.3.6.1.6 The server and storage infrastructure shall be able to support continuous business operations of SMARTICS-2. High resilience facilities shall be provided at network and system hardware levels to minimise the impact of individual component failure on the System.

(a) Local resilience – equipment redundancy shall be implemented for each individual hardware component of the Central Service Layer and Local Service Layer at the production environment, so that the takeover of a failed component can be performed automatically to ensure minimum interruption to SMARTICS-2 business operations and minimise the impact of the failure on the System.

(b) Site resilience for Central Service Layer – resilient server and storage infrastructure shall be set up at DDC(FL) to support continuous operations when the Central Service Layer at PDC(KC) is unable to provide services.

2.3.6.1.7 The System shall be able to expand to meet the demand of increasing utilisation. The Contractor shall reserve at least 50% of the server capacity for all servers in the production environment so as to cater for vertical transaction growth as well as workload surge. The Contractor shall reserve at least 50% of all storage devices for future growth.

2.3.6.1.8 The servers and storage shall have redundant power supplies, which connect to different power source. If one of power supplies fails, the other power supply will continue to support the server operation without interruption.

2.3.6.1.9 The servers and storage shall equip with hot swappable power supplies and hot swappable hard disks such that no interruption during replacement of the damaged unit.

2.3.6.1.10 The Contractor shall ensure secure deletion of information before the faulty parts can be returned to the vendor.

2.3.6.1.11 The Contractor shall provide sufficient rack-mountable Keyboard-Video-Mouse (“KVM”) switches through which the operators of computer suites and supporting project teams can access the console display of all servers to manage the hardware for the physical servers or server partitions.

2.3.6.1.12 All physical servers shall include basic Input / Output (“I/O”) devices, such as DVD drive, to load or install the associated system software.

2.3.6.2 SMARTICS-2 Server Farm

2.3.6.2.1 The Contractor shall implement the SMARTICS-2 server farms at PDC(KC), DDC(FL), all of the ROP branch offices and SIDCCs to support the business operations at all Locations, including PDC(KC), DDC(FL), ROP offices, SIDCCs, control points, immigration offices within and outside HQ. Hybrid system model shall be adopted for the SMARTICS-2 server farms.

2.3.6.2.2 The servers shall include midrange and PC servers to support the business services of SMARTICS-2.

2.3.6.2.3 Tenderers shall provide sizing details to support their technical proposals for the hardware, software and communication lines. Tenderers shall also provide the justifications for the proposal in Schedule 21 – "Information Summary" of Part V.

2.3.6.2.4 The midrange system shall support clustering for high availability, and shall provide automatic switchover capability if one of the cluster node fails. The switchover shall meet the resilience and disaster recovery requirement specified in Section 8 – "Resilience and Disaster Recovery Requirements" of this Annex.

2.3.6.2.5 The network connectivity of all servers shall be designed in such a way that there is no single point of failure.

2.3.6.2.6 Servers shall be directly connected to server switches in ROP branch offices, SIDCCs, PDC(KC) or DDC(FL). The server switches shall provide sufficient switch ports for connecting the servers and equipment of the System as well as the servers of other existing systems in ROP branch offices, if any. Each server switch shall have multiple-uplinks to different distribution switches.

2.3.6.2.7 The server and storage infrastructure shall be equipped with the state-of-the-art technology, employing servers which support open connectivity.

2.3.6.2.8 Local Service Layer, which provides local computing facilities at branches, shall be set up in the computer rooms at ROP branch offices and SIDCCs.

2.3.6.2.9 Central Service Layer, which mainly provides services requiring centralised processing, shall be set up at PDC(KC) and DDC(FL).

2.3.6.2.10 Servers and equipment shall be set up in the Extended MCN, Local Kiosk Network and ITI MCN at ROP branch offices, SIDCCs, HQ, PDC(KC) and DDC(FL) to support the core business operations, application processing, kiosk registration and card cabinet services for SMARTICS-2.

2.3.6.2.11 Servers and equipment shall be set up in the General Kiosk Network and ITI AN at ROP branch offices, SIDCCs, HQ, control points, other immigration offices, PDC(KC) and DDC(FL) for supporting general application kiosk services for SMARTICS-2.

2.3.6.2.12 Servers and other necessary equipment shall be set up in ITI AN at PDC(KC) and DDC(FL) to support data exchange with other Government B/Ds.

2.3.6.2.13 The server farm of the Local Service Layer of the System at each location of ROP branch offices and SIDCCs shall consist of the following basic server and storage components to support ROP business functions:

(a) web and application servers for providing user interface, performing ROP business functions and providing CDS functions as contingency during local mode operation;

(b) workflow servers for performing automatic workflow processing;

(c) database servers for storing local ROP application data and local CDR records for contingency operation;

(d) report servers;

(e) backup servers and equipment;

(f) UPMS servers for providing services for user authentication;

(g) infrastructure servers for providing infrastructure services;

(h) TAGS-2 servers and equipment for TAGS-2$^{(\text{Note 1})}$;

(i) firewalls for protecting the server farms and controlling the traffic from WAN and authorised equipment;

(j) SAN storage and encryption appliance for SAN, if applicable;

(k) hardware security module (“HSM”);

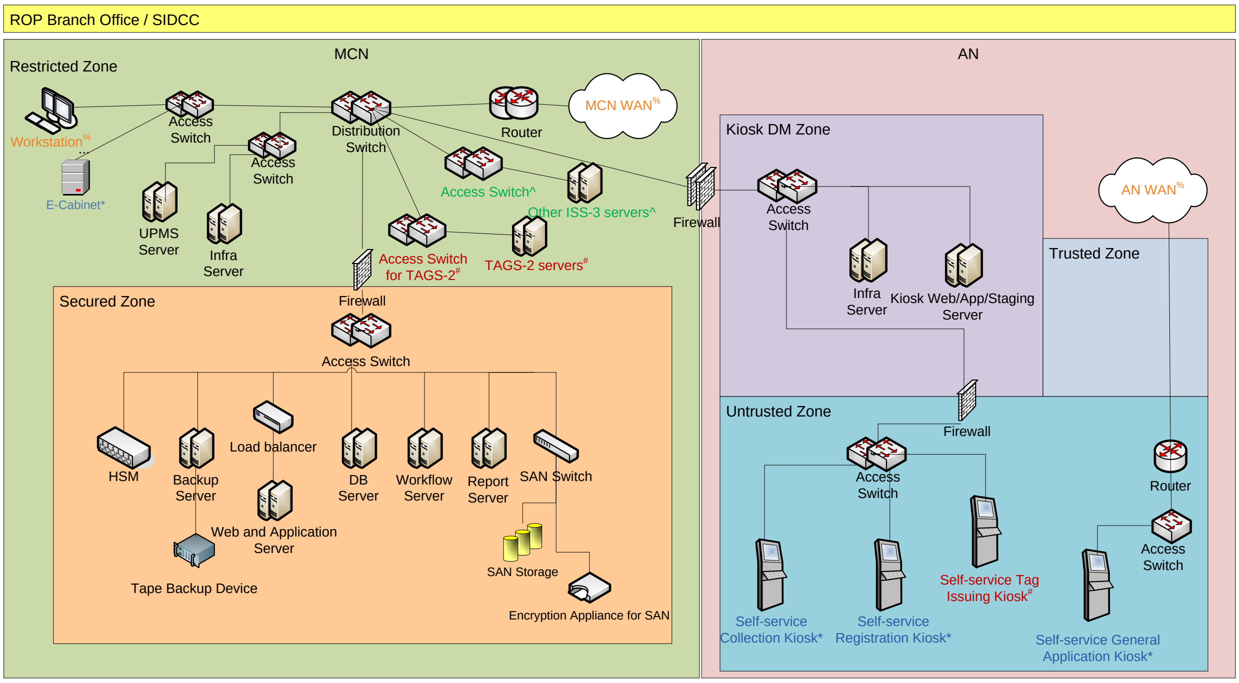
(l) load balancers for load balancing function on web and application servers; and

(m) kiosk web / application / staging servers for providing user interface, performing business functions and storing transient data in AN Kiosk DM Zone for supporting self-service registration kiosks$^{(\text{Note 2})}$, self-service collection kiosks$^{(\text{Note 2})}$ and self-service tag issuing kiosks$^{(\text{Note 1})}$ in Local Kiosk Network.

Note 1: TAGS-2 servers and equipment, self-service tag issuing kiosks and tag services will be provided by the Contractor of Category D. The infrastructure of the Core System shall support the connection of TAGS-2 servers in the Local Service Layer, and the System shall provide staging area for storing transient data for TAGS-2.

Note 2: Kiosks will be provided by the Contractor of Category C. The infrastructure of the Core System shall support all servers and network equipment for the connection of kiosks and the Contractor shall provide the SMARTICS-2 applications running on the kiosks.

The following diagram, for indication only, illustrates the high-level logical infrastructure of the Local Service Layer at ROP branch offices and SIDCCs:



Notes: * MSKS and CabS
TAGS-2
^ Other ISS-3 systems
% Acquired by the Government separately
(without symbol) Core System

Figure 7A-2.3.6.2.13 High-level Infrastructure of Local Service Layer at ROP Branch Offices and SIDCCs

2.3.6.2.14 The server farm of the Central Service Layer of the System at PDC(KC) and DDC(FL) shall consist of the following components to support ROP centralised processing functions, including SMARTICS-2 application on self-service general application kiosks, and data exchange with other Government B/Ds:

(a) web and application servers for providing user interface and performing ROP business functions;

(b) workflow servers for performing automatic workflow process;

(c) database servers for storing centralised ROP application data and CDR records to be replicated to ROP branch offices and SIDCCs;

(d) IMS servers for managing ROP document and biometric images, which shall be stored in disk-based WORM device;

(e) disk-based WORM device for storing document and biometric images;

(f) report servers;

(g) backup servers and equipment;

(h) batch processing servers;

(i) infrastructure servers for providing infrastructure services;

(j) SAN storage and encryption appliance for SAN, if applicable;

(k) hardware security module;

(l) disk-based backup system;

(m) load balancers for load balancing function on web and application servers;

(n) AN web and interface servers for providing system interfaces, file transfer and record enquiry services with other Government B/Ds and user interface of SMARTICS-2 applications on self-service general application kiosks(Note 1);

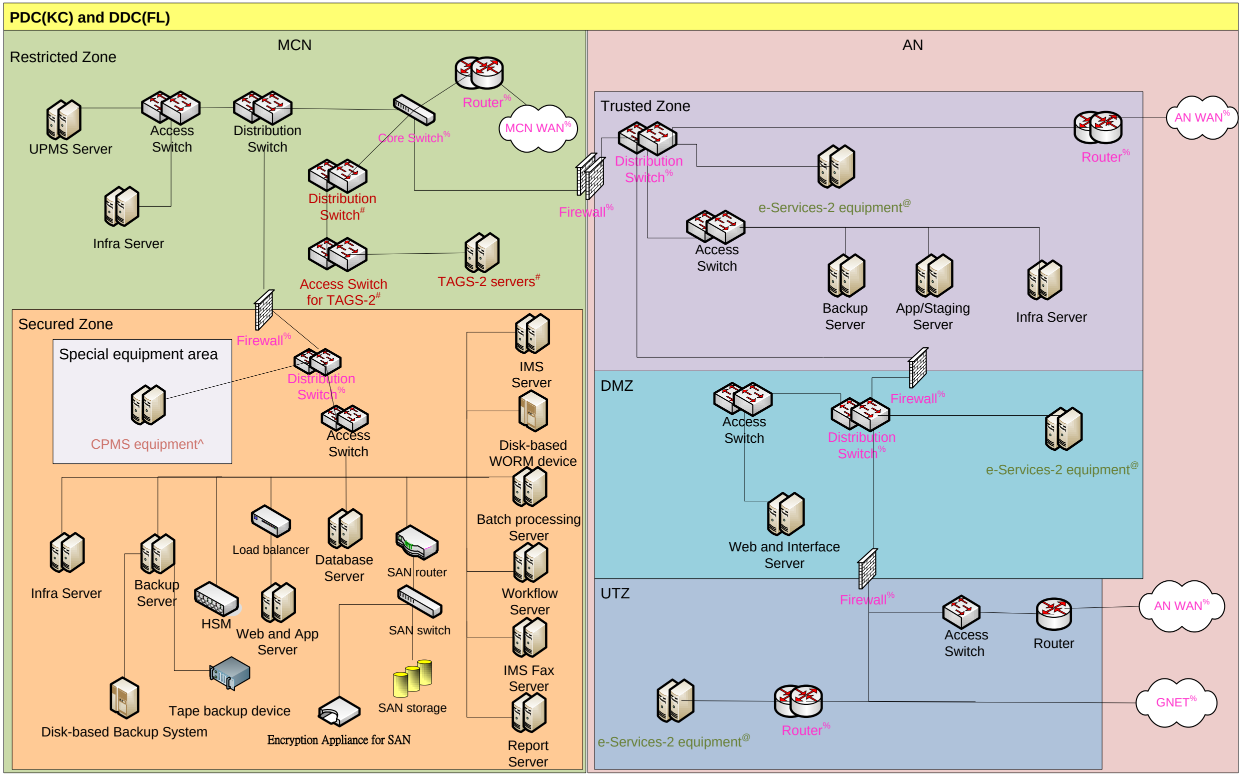
(o) AN application and staging servers for performing business functions and storing transient data between MCN and AN;

(p) IMS fax servers for providing fax service; and

(q) other services, including but not limited to, host-based IDS, proxy, radius, anti-virus, system management and monitoring services.

Note 1: Kiosk will be provided by the Contractor of Category C. The infrastructure of the Core System shall support all servers and network equipment for the connection of the kiosks and the Contractor shall provide the SMARTICS-2 applications running on the kiosks.

The following diagram, for indication only, illustrates the high-level logical infrastructure of the Central Service Layer at PDC(KC) and DDC(FL):



Notes: ^ CPMS
% ITI
TAGS-2
@ e-Service 2
(without symbol) Core System

Figure 7A-2.3.6.2.14 High-level Infrastructure of Central Service Layer at PDC(KC) and DDC(FL)

2.3.6.2.15 Host-based IDS shall be installed at each AN web and interface server. The Contractor shall provide solution for updating signature and for incident management. The Contractor shall work with ITI project team on the solution such that it can be integrated with ITI infrastructure.

2.3.6.2.16 Tenderers can propose any other equipment other than the above according to their proposed solution in Table 5-4.1(A) of Schedule 4 – “Technical Proposal and System Configuration” of Part V.

2.3.6.3 Server

2.3.6.3.1 Midrange Server

2.3.6.3.1.1 Midrange servers shall be deployed for the System to provide high availability features to minimise interruption or outage caused by processor and hard disk failure, prevent single point of failure, and provide automatic switchover to the redundant system / disk within allowable downtime. Besides, the midrange servers shall be of UNIX based architecture and shall support virtualisation technology to enable automatic, dynamic and effective sharing and allocation of computing resources between various functionalities and environments according to the actual workload.

2.3.6.3.1.2 In PDC(KC) and DDC(FL), there shall be a group of production midrange servers to support the Central Service Layer. At least the following midrange servers shall be deployed for the System:

(a) Web and application servers at MCN of PDC(KC) and DDC(FL)
  (i) provide web interface to serve SMARTICS-2 users, excluding users of ROP branch offices and SIDCCs; and
  (ii) provide application services for the following application servers:
    (i) application server for ROP back offices business logic;
    (ii) address data infrastructure server;
    (iii) data matching server for monitoring data requests in AN Trusted Zone staging server of any data matching requests received from other Government B/Ds; and
    (iv) staging server for storing temporary data for authorised parties.

(b) Workflow servers at MCN of PDC(KC) and DDC(FL)
  (i) provide automatic workflow to streamline application processing between ROP offices and / or SIDCCs.

(c) Report servers at MCN of PDC(KC) and DDC(FL)
  (i) provide report generating services to ROP offices, excluding the branch offices.

(d) Batch processing servers at MCN of PDC(KC) and DDC(FL)
  (i) provide batch job scheduling and running process.

(e) Database servers at MCN of PDC(KC) and DDC(FL)
  (i) provide relational database management system (“RDBMS”) to store all application data of ROP offices processes; and

(ii) provide database synchronisation services to replicate data from CDR and act as a CDR replica and to distribute to ROP branch offices and SIDCCs and act as a CDR distributor.

(f) IMS servers at MCN of PDC(KC) and DDC(FL)

(i) provide content management services for managing ROP document and biometric images to be stored in disk-based WORM device; and

(ii) provide file integrity check for files stored in the device to assure the files have not been modified and a signature file of file information, including but not limited to, name and size of file, digest of file content, timestamp of signature, etc., shall be generated when files are being stored.

(g) Backup servers at MCN of PDC(KC) and DDC(FL)

(i) provide both system and data backup services for servers in data centres.

2.3.6.3.2 PC Server

2.3.6.3.2.1 The PC servers for the System shall be of x86-based architecture for supporting business operations at ROP branch offices, SIDCCs, HQ, PDC(KC) and DDC(FL). They shall support high availability features to minimise interruption or outage caused by processor and hard disk failure, prevent single point of failure, and provide automatic switchover to the redundant system / disk within allowable downtime. The PC servers shall support virtualisation or partitioning technology to enable automatic, dynamic and effective sharing and allocation of computing resources between various functionalities and environments according to the actual workload.

2.3.6.3.2.2 The following PC servers shall be deployed for the System:

(a) AN web and interface servers at AN DM Zone of PDC(KC) and DDC(FL)

(i) provide web interface, file transfer and record enquiry services to serve other Government B/Ds;

(ii) provide web interface for SMARTICS-2 applications running on MSK_GEN$^{(Note\ 1)}$; and

(iii) provide secure file transfer interface with other Government B/Ds.

(b) AN application and staging server at AN Trusted Zone of PDC(KC) and DDC(FL)

(i) provide application and staging services to handle data exchange with other Government B/Ds; and

(ii) provide application and staging services for SMARTICS-2 applications running on MSK_GEN$^{(Note\ 1)}$.

(c) IMS fax servers at MCN of PDC(KC) and DDC(FL)

(i) provide fax service to IMS server for sending IMS record / file.

(d) Infrastructure servers at AN and MCN of PDC(KC), DDC(FL), ROP branch offices and SIDCCs

(i) provide domain name system (“DNS”) services;

(ii) provide Network Time Protocol (“NTP”)services;

(iii) provide domain controller services;

(iv) provide system and network monitoring services;

(v) provide system management and anti-virus services;

(vi) provide gateway services for Enterprise System Management ("ESM") of ITI; and

(vii) provide software distribution services.

(e) Kiosk web / application / staging servers at AN Kiosk DM Zone of ROP branch offices and SIDCCs

(i) provide web interface, application and staging services for SMARTICS-2 application running on self-service registration kiosks^(Note 1)^, self-service collection kiosks^(Note 1)^, and self-service tag issuing kiosks^(Note 2)^.

(f) Web and application servers at MCN of ROP branch offices and SIDCCs

(i) provide web interface and application services for SMARTICS-2 users at ROP branch offices and SIDCCs; and

(ii) provide CDS to SMARTICS-2 users at ROP branch offices and SIDCCs during local mode operation.

(g) Workflow servers at MCN of ROP branch offices and SIDCCs

(i) provide automatic workflow to streamline application processing in ROP branch offices and SIDCCs.

(h) Database servers at MCN of ROP branch offices and SIDCCs

(i) provide RDBMS to store all application data of that ROP branch office or SIDCC; and

(ii) provide RDBMS to store CDR records for supporting local mode operation in the office.

(i) Report servers at MCN of ROP branch offices and SIDCCs

(i) provide report generating services in ROP branch offices and SIDCCs.

(j) UPMS servers at MCN of ROP branch offices and SIDCCs

(i) provide UPMS services for user authentication in ROP branch offices and SIDCCs.

(k) Backup servers at ROP branch offices and SIDCCs

(i) provide both system and data backup services for servers in ROP branch offices and SIDCCs.

Note 1: Kiosk will be provided by the Contractor of Category C. The infrastructure of the Core System shall support all servers and network equipment for the connection of kiosks and the Contractor shall provide the SMARTICS-2 applications running on the kiosks.

Note 2: TAGS-2 servers, equipment, self-service tag issuing kiosks and tag services will be provided by the Contractor of Category D. The infrastructure of the Core System shall support the connection of self-service tag issuing kiosks and the System shall provide staging area for storing transient data for TAGS-2.

2.3.6.3.2.3 In each location of ROP branch office, SIDCC and HQ, infrastructure servers and UPMS servers shall be deployed to provide and support the infrastructure and UPMS services at that office, which include the Contractors of other Categories and other ISS-3 systems at that location.

2.3.6.3.2.4 In PDC(KC) and DDC(FL), infrastructure servers shall be deployed to provide local infrastructure services, which will be centrally supported by ITI, for supporting the Central Service Layer for the System and the system to be provided under Category B in the special equipment area of the data centres and the Local Service Layer in ROP branch offices and SIDCCs.

2.3.6.4 Server Virtualisation

2.3.6.4.1 A virtualised server infrastructure shall be implemented, which shall run on server farms / clusters supporting multiple virtualised server partitions inside. Functions shall be designed and implemented under a multi-tier architecture (e.g. an application tier for business logic processing, a database tier for storing of application and system data, etc.) with load sharing and dispatch capability among the virtualised server partitions of the server farms / clusters. A common pool of resources shall be available for efficient sharing and flexible dynamic allocation to handle the actual workload by using the virtualisation technology.

2.3.6.4.2 At PDC(KC) and DDC(FL), ITI built a virtualised server platform to implement ITI services in supporting ISS-3 projects. SMARTICS-2 shall also adopt server virtualisation technology in order to save equipment rack space in PDC(KC), DDC(FL), ROP branch offices and SIDCCs and take advantages of server virtualisation like allocating dynamically in response to transaction loading, reducing the dependency of operation systems on physical hardware and increasing the flexibility of future system refreshment.

2.3.6.4.3 The Contractor shall provide necessary quantities of physical servers with the following features, in order to support sufficient server partitions or instances to be formed within the virtualised server infrastructure:

(a) built-in redundancy hypervisors within a physical server or redundancy hypervisors across multiple physical servers supporting high level of security and reliability to control the provisioning of computing resources to the server partitions or instances;

(b) hardware redundancy on major server partitions or instances, such as dual network interfaces, dual power supplies, etc., to support higher resilience;

(c) vertical growth capability to facilitate capacity upgrade for high scalability; and

(d) local resilience of clustering.

2.3.6.4.4 The virtualised server partitions or instances shall have the following features:

(a) each virtualised server partition or instance shall have its own operating system, and the level or type of the operating system shall be independent of the operating systems running in other partitions or instances;

(b) failure of the operating system and applications inside a partition or instance shall not affect the normal operation of the others;

(c) partitions or instances shall be dynamically created, modified and deleted with no interruption to other existing partitions or instances;

(d) power-on / activate, power-off / deactivate, reboot and maintenance of individual partition or instance shall not affect the others; and

(e) support mobility feature to ease regular maintenance or resource scale-up.

2.3.6.4.5 For the virtualised server infrastructure to be placed in the DDC(FL), server partitions or instances shall be created to support various system environments for development and testing purposes of the System. The physical servers shall have sufficient capacity of processor cores, memory, I/O adapters and the capacity to create the required number of server partitions or instances to meet this requirement.

2.3.6.4.6 The disaster recovery ("DR") drill environment shall be set up at DDC(FL) to regularly simulate the disaster situation at PDC(KC) and practise the disaster recovery procedures at DDC(FL). The Contractor shall set up the DR drill environment with the production equipment. The DR drill environment shall be co-existed with the production environment using virtualisation technology.

2.3.6.4.7 Each component of database, application, and any necessary middleware shall be hosted in server partitions or virtualised instances with certain amount of computing resources such as central processing unit ("CPU") and memory being allocated, according to proposed design with consideration of factors such as the required serviceability level, better performance, ease of maintenance, etc. Resources shall be able to be dynamically re-allocated to any server partition or instance without any service interruption through the hypervisor(s). The Contractor shall provide necessary system management solution and consoles to manage the virtualised server infrastructure.

2.3.6.4.8 The Contractor shall provide necessary equipment to effectively support the high availability ("HA"), local resilience and site resilience requirements, and with applicable load balancing features to distribute the actual transaction workload among cooperating virtualised server partitions or instances within a server farm or cluster. The local resilience solution shall also cater for the server failure scenario, in order to sustain the production service in case one of the physical servers in a local resilience configuration fails.

2.3.6.4.9 Apart from virtualised servers, some applications and middleware may be required to be hosted in dedicated physical servers to achieve better performance or ease of maintenance. In such cases, the Contractor shall provide additional dedicated physical servers, if necessary, to support the System.

2.3.6.4.10 The Contractor shall review the detailed requirements and approaches for handling the local resilience and site resilience under different scenarios during the SA&D stage.

2.3.6.4.11 All virtualised servers within the server farm(s) and dedicated servers shall support Simple Network Management Protocol ("SNMP") management and capable of sending alerts to the ESM infrastructure to be supplied by ITI for notifications and centralised monitoring.

2.3.6.4.12 The System shall be automatically and continually adjust the amount of processing capacity allocated to each logical partition based on the workload demand.

2.3.6.4.13 UNIX and other application software shall be installed on the logical partition according to the functional needs.

2.3.6.5 Storage

2.3.6.5.1 The Contractor shall provide SAN storage as the enterprise storage solution for all servers and databases in the PDC(KC) and in the DDC(FL), as resilience and disaster recovery purposes. The storage shall be used to store at least the following data:

(a) SMARTICS-2 ROP database and file system;

(b) biometric data and images;

(c) CDR replica and CDR distributor for local mode operation;

(d) a separate storage for data in non-production environments (such as development, testing and training environments) in DDC(FL); and

(e) a separate storage for set up the DR drill environment, without affect any production activities, in DDC(FL).

2.3.6.5.2 The Contractor shall also provide local SAN storage at each location of ROP branch offices and SIDCCs and the storage shall be used to store at least the following data:

(a) SMARTICS-2 ROP database for ROP branch office functions;

(b) file system storing SMARTICS-2 data files (e.g. fingerprint images, photo images, supporting document images);

(c) local copy of CDR for supporting local mode operation;

(d) data backup; and

(e) virtualised servers operating systems.

2.3.6.5.3 The Contractor shall estimate and provide necessary quantities of SAN storage equipment to cater for the storage requirements of the System.

2.3.6.5.4 The Contractor shall also provide sufficient SAN storage, including the overhead on storage and data backup, and sufficient number of database instances to cater for the minimum storage requirements of the System as follows:

SMARTICS-2 Server Farms	**Provisioning**	**Minimum Storage Requirements**
Central Service Layer (at PDC(KC) and DDC(FL))	SMARTICS-2 ROP database, IMS database, CDR replica and CDR distributor	4TB raw data
Local Service Layer (at each ROP branch office and SIDCC)	SMARTICS-2 ROP database (for each ROP branch office and SIDCC) and local copy of CDR	1.2TB raw data

2.3.6.5.5 The Contractor shall estimate and provide the sizing details for the storage capacity of SAN storage which meet the workload requirement specified in Section 5 – “Workload Requirements” of Part VII.

2.3.6.5.6 The Contractor shall implement data encryption, to be performed at SAN switch or SAN enclosure level, to store the ROP data for the System, which involves confidential data. The encryption keys shall be stored separately from the SAN storage. The encryption, decryption and key protection standard shall fully comply with security policies, standards and guidelines of the Government. Details of the data encryption requirements are depicted in Section 12 – “Security Requirements” of Part VII.

2.3.6.5.7 Sufficient spare disk space shall be provided so that the SAN can rebuild the data using the spare disk space automatically and immediately at the time a hard disk failure is detected.

2.3.6.5.8 The SAN storage shall support high volume of I/O demand, prevent single point of failure and be expandable. The Contractor shall implement Redundant Array of Independent Disks (“RAID”) solution, such as RAID 1, RAID 5 or RAID 6, depends on the level of redundancy and performance required.

2.3.6.5.9 The Contractor shall provide a central monitoring solution to centrally monitor the healthiness of the storage system in PDC(KC), DDC(FL), ROP branch offices and SIDCCs. Alert mechanism shall be required to alert support staff and Computer Operations Section (“COS”) whenever there is any component failure or exceeds the predefined thresholds.

2.3.6.5.10 The Contractor shall provide sufficient quantity of SAN switches, WAN encryptors, SAN routers and any necessary device for data synchronisation of SAN storage at PDC(KC) and DDC(FL) via SAN replication WAN connection. The Contractor shall provide any additional devices for the connection of the proposed SAN storage infrastructure.

2.3.6.5.11 It is desirable for the SAN storage at data centres to share spare storage with other ImmD projects via ITI Virtualisation Layer to allow more flexibility for resources sharing. The details of storage infrastructure of ITI are set out in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII. Tenderers can propose any necessary hardware and software in Schedule 1 – “Hardware” and Schedule 2 – “Software” of Part V.

2.3.6.6 Disk-based Write Once Read Many Storage Device

2.3.6.6.1 The Contractor shall provide at least one disk-based WORM storage device at each data centre to store document images and biometric images in an unaltered format. Data written to the disk-based WORM device at PDC(KC) shall be replicated to the disk-based WORM device at DDC(FL) as resilience. The Contractor shall provide all necessary hardware, software and related services for the replication solution of the disk-based WORM devices between data centres.

2.3.6.6.2 The Contractor shall provide all necessary hardware, software, tools and related services for the migration solution of image files from current Optical Library

Dataserver (Jukeboxes) of SMARTICS, which are stored in around 2200 optical disks, to the disk-based WORM devices of the System.

2.3.6.6.3 The Contractor shall provide sufficient storage size for the disk-based WORM devices to accommodate all images, including images stored in current SMARTICS Jukeboxes and the new images created in the System, as follows:

SMARTICS-2	**Provisioning**	**Minimum Storage Requirements**
Central Service Layer (at PDC(KC) and DDC(FL))	SMARTICS-2 IMS Image	25TB images

2.3.6.6.4 The Contractor shall estimate and provide the sizing details for the storage capacity of the disk-based WORM devices which meet the workload requirement specified in Section 5 – “Workload Requirements” of Part VII.

2.3.6.6.5 The Contractor shall provide all necessary hardware, software and related services for implementing encryption solution to the document images stored in the disk-based WORM devices of the System, according to the relevant security guidelines and regulations.

2.3.6.6.6 The disk-based WORM devices shall have the following features:

(a) preserve the data exclusively in a non-rewriteable and non-erasable format;

(b) verify automatically the quality and accuracy of the storage media recording process;

(c) retrieve the data in original format; and

(d) provide internal resilience and data protection against single point of disk failure.

2.3.6.7 System Resilience and Failover

2.3.6.7.1 The Contractor shall design and develop system resilience and failover features for the System as specified in Section 8 – “Resilience and Disaster Recovery Requirements” of this Annex.

2.3.6.8 UPMS Servers and Infrastructure Servers at Data Centres, HQ, ROP Branch Offices and SIDCCs

2.3.6.8.1 To provide better performance and reduce the dependency of ITI, UPMS and infrastructure services shall be deployed at data centres for connection to the services provided by ITI. The Contractor shall provide all necessary hardware and software for the implementation of UPMS and infrastructure services at data centres with the centralised support provided by ITI.

2.3.6.8.2 To avoid interruption on UPMS and infrastructure service, a set of local UPMS and infrastructure services shall be deployed at HQ, ROP branch offices and SIDCCs to support local mode operations. The Contractor shall provide all necessary hardware and software for the implementation of local UPMS and infrastructure services at HQ, ROP branch offices and SIDCCs. The Contractor shall provide local storage and backup solution for the UPMS and infrastructure services.

2.3.6.8.3 The local UPMS and infrastructure services shall be provided to the Systems of other Categories and other ISS-3 systems, including the CPMS at HQ, MSKS, CabS and TAGS-2 at ROP branch offices and SIDCCs. The Contractor shall work with the ITI project team and be responsible for liaising directly with the Contractors of other Categories, other contractors of the Government and ImmD project teams.

2.3.6.8.4 The Contractor shall be responsible to set up the local UPMS and infrastructure services at HQ, ROP branch offices and SIDCCs. Details of UPMS and infrastructure management services are set out in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII.

2.3.6.8.5 In addition to the shared storage resources, the Contractor shall provide sufficient network ports at server switches at HQ and each location of ROP branch offices and SIDCCs for UPMS servers and infrastructure servers.

2.3.6.9 Integration with ITI

2.3.6.9.1 ITI will be able to make use of the server and storage infrastructure of the System through appropriate integration between ITI and such infrastructure to be implemented by the Contractor. The virtualised server farms and storage of the System at PDC(KC) and DDC(FL) shall be capable to allow the processing capacity to be shared for use by ITI and other ImmD systems as and when required. Whilst the Contractor shall be primarily responsible, the Contractor shall work with ITI project team on the integration of the System with ITI.

2.3.7 Functional Requirements for Data Management Infrastructure

2.3.7.1 The following categories of data repository are required to support the application functions:

(a) SMARTICS-2 ROP database in the Local Service Layer at ROP branch offices and SIDCCs;

(b) SMARTICS-2 ROP database in the Central Service Layer at PDC(KC) and DDC(FL);

(c) CDR replica and CDR distributor at PDC(KC) and DDC(FL), which shall synchronise data from ITI CDR and further update for the distribution of local copy of CDR; and

(d) local copy of CDR at ROP branch offices and SIDCCs.

Tenderers shall propose the design of the SMARTICS-2 ROP database for Local Service Layer, including the local data repository for CDR at ROP branch offices and SIDCCs, and the SMARTICS-2 ROP database for Central Service Layer, including the CDR replica and CDR distributor for the distribution of local copy of CDR, as well as its interactions with other data repositories developed under the ITI project (i.e. DSOP and CDR) in Schedule 4 – "Technical Proposal and System Configuration" of Part V.

2.3.7.2 Resilience

2.3.7.2.1 The database management design shall provide high resilience with features supporting:

(a) active-active or active-passive clustering (within the same database cluster) in ROP branch offices, SIDCCs and data centres; and

(b) failover operation at PDC(KC) and DDC(FL).

2.3.7.2.2 A high availability design is required for SMARTICS-2. In general, active-active server clustering shall be used for mission-critical servers such as web and application servers. Load balancers shall be in place to balance workload of the active-active server cluster.

2.3.7.2.3 Active-passive or active-active clustering for database servers at the Local Service Layer and Central Service Layer shall be implemented. Database transactions shall be handled by the database servers in clustering or load balancing mechanism. SAN controllers shall be implemented as storage resilience for the Local Service Layer in each location of ROP branch offices and SIDCCs and the Central Service Layer at data centres.

2.3.7.2.4 Data at PDC(KC) shall be replicated to DDC(FL) for resilience purposes. The replication shall be done at SAN level or database level. Data replication (one-way) and synchronisation (two-way) shall be supported by the RDBMS software.

2.3.7.2.5 It is desirable for providing a solution that can support a standby Local Service Layer at PDC(KC), i.e. servers at Central Service Layer can provide same functionalities and have enough capacity to handle same workload and support servers at Local Service Layer of at least two ROP branch offices or SIDCCs for serving as a resilience arrangement, in case of total server failure occurs at that ROP branch office or SIDCC. Tenderers may propose the design of the solution in Table 5-4.2(A) of Schedule 4 – "Technical Proposal and System Configuration" of Part V.

2.3.7.3 Security

2.3.7.3.1 The database server shall support all the following security features:

(a) encryption of data in the database or on the file system shall be used to protect sensitive and confidential data. Encryption keys shall be stored in a security module external to the database; and

(b) separation of duties of account management, security administration and database administration shall be implemented. Security features shall be in place to prevent privileged users from accessing application databases and to enforce controls over how, when and where application data can be accessed transparently.

2.3.7.4 SMARTICS-2 ROP Database in the Local Service Layer at ROP Branch Offices and SIDCCs

2.3.7.4.1 A resilient pair of database servers shall be set up at each location of ROP branch offices and SIDCCs to provide high availability. The RDBMS shall house ROP application data for the office operation at the Local Service Layer, covering at least the following major types of data:

(a) ROP appointment and application records, including HKIC and CRP;
(b) workflow data of office operations; and
(c) CDR for supporting of local mode operation.

2.3.7.4.2 The RDBMS shall support data clustering features with active-active or active-passive configuration.

2.3.7.4.3 Completed assessment applications in ROP branch offices and SIDCCs shall be uploaded to the SMARTICS-2 ROP database at the Central Service Layer for subsequent operations.

2.3.7.5 SMARTICS-2 ROP Database in the Central Service Layer at Data Centres

2.3.7.5.1 The Contractor shall set up two dedicated database servers at data centres. The System shall maintain SMARTICS-2 ROP database of the Central Service Layer at PDC(KC) and it shall be replicated to DDC(FL) to further increase resilience level and data availability. The Contractor shall ensure the data at PDC(KC) is replicated at real-time to DDC(FL).

2.3.7.5.2 Under normal operation, data replication shall be unidirectional. The RDBMS shall support data replication and synchronisation features for replicating the databases for the System from PDC(KC) to DDC(FL).

2.3.7.5.3 The Contractor shall implement the alert mechanism to alert support staff and / or COS whenever there is any synchronisation problem between the data repository at PDC(KC) and the data repository at DDC(FL).

2.3.7.5.4 The RDBMS shall house application data to support the ROP operations at the Central Service Layer at data centres, covering at least the following major types of data:

(a) ROP application and registration records;
(b) IMS including document images and biometric images; and
(c) CDR to be replicated from ITI CDR and distributed to ROP branch offices and SIDCCs for supporting of local mode operation.

2.3.7.5.5 The System shall maintain its image data under IMS at PDC(KC) and DDC(FL). The image data will be used for legal evidence and therefore their content shall be kept from modification. Under normal operation, data written to the disk-based WORM device at PDC(KC) shall be replicated or written to the disk-based WORM device at DDC(FL) as resilience. The Contractor shall implement a solution to ensure the integrity and replication of images stored in the disk-based WORM devices in data centres.

2.3.7.6 Common Data Repository

2.3.7.6.1 The System shall access common data contributed by other ImmD systems, including SMARTICS-2, via common services. All data in CDR can only be accessed and updated through CDS in data centres.

2.3.7.6.2 The System shall contribute the common data (e.g. valid HKIC range), which will be accessed by other ImmD systems, to CDR via the common services.

2.3.7.6.3 To support the normal operation mode, the System shall access the CDR in data centres via CDS. The Contractor shall design and develop the common services for SMARTICS-2 to access the CDR in ITI Service Layer.

2.3.7.6.4 The Contractor shall provide solution to access, retrieve and update data in CDR, which is stored in SAN storage of ITI at PDC(KC) and DDC(FL).

2.3.7.6.5 To support the local operation mode at ROP branch offices and SIDCCs, a subset of CDR, i.e. local copy of CDR, with relevant services shall be replicated and deployed at ROP branch offices and SIDCCs. A separate partition of the database server shall be reserved to hold the CDR subset. The Contractor shall be responsible to implement the function for storing the CDR subset in database servers. The local CDR data shall be accessed for read only. The Contractor shall be responsible to make available the data in the CDR for the local platform at ROP branch offices and SIDCCs, and make use of the CDS developed under ITI and the CDS for SMARTICS-2 for the access to and update of CDR to support the business requirements and the local mode operation under SMARTICS-2 in ROP branch offices and SIDCCs.

2.3.7.6.6 The Contractor shall be responsible to provide solution to maintain the critical business operations in ROP branch offices and SIDCCs, even if there is any service interruption occurred at the common data services or CDR in ITI Service Layer. The System shall be able to operate and provide the business operations without the dependency of the ITI Service Layer or the Central Service Layer.

2.3.7.6.7 Tenderers shall provide the proposal and solution for the local copy of CDR at ROP branch offices and SIDCCs in Table 5-4.1(A) of Schedule 4 – “Technical Proposal and System Configuration” of Part V.

2.3.7.7 Data Synchronisation

2.3.7.7.1 The System shall perform data synchronisation within the Core System, including but not limited to:

(a) between Central Service Layer and ITI CDR, including CDR records;

(b) between Local Service Layer and Central Service Layer, including appointment, application and registration records, document and biometric images and replicated CDR records for local mode; and

(c) between standalone mode workstations and Local Service Layer, including appointment records and data supporting standalone mode.

2.3.7.7.2 Data synchronisation can be done by data synchronisation tools or via customised programs built on standard interface protocols such as web services. Similar data synchronisation shall be required for the user profiles information in UPMS from data centres to ROP branch offices and SIDCCs.

2.3.7.7.3 The System shall adopt standard protocol for data synchronisation process. If any failure of connectivity or server availability happens during synchronisation, the original data source shall be retained until service is resumed. The Contractor shall design and develop a robust recovery mechanism for the data synchronisation process to assure the data consistency and integrity across different data repositories.

2.3.7.7.4 To support the local mode operation in ROP branch offices and SIDCCs, certain CDR data shall be stored in local database servers. The Contractor shall be responsible for not only the data synchronisation of CDR data to Central Service Layer and Local Service Layer, but also the application solution and the implementation of the CDS functions supported under local mode operations in ROP branch offices and SIDCCs.

2.3.7.7.5 Data shall be replicated from ITI CDR to identified tables in CDR replica in Central Service Layer, which shall have the same table schema as CDR. It will further update to CDR distributor and distribute to local copy of CDR in Local Service Layer in ROP branch offices and SIDCCs. To reduce the data to be distributed to ROP branch offices and SIDCCs, the CDR distributor may have different table schema from CDR, and it will not be accessed by CDS program. It is subject to any modifications as approved or stipulated by the Government in the SA&D stage.

2.3.7.7.6 The Contractor shall provide necessary software licence if the database synchronisation solution is adopted by the Contractor. The Contractor shall implement the data synchronisation solution of CDR for the System either using the database synchronisation tool or the application solution. The Contractor shall provide relevant programs / scripts and reports to facilitate the data reconciliation and user verification to ensure that the data are being migrated and synchronised correctly to the target database.

2.3.7.8 The Contractor shall provide database administration services for the System, local mode of CDR and local mode of UPMS.

2.3.7.9 The Contractor shall provide the monitoring tools for the proposed data synchronisation solution to closely monitor the synchronisation status and performance in real time. In case the data synchronisation time lag reaches the predefined threshold, the proposed solution shall generate and display alert messages on ESM of ImmD to alert relevant support personnel to take appropriate actions. Both acknowledgement and unsuccessful synchronisation shall be tracked down by the System. Also, the replication frequency shall be adjustable to minimise the impact on the availability and performance of the database service.

2.3.7.10 Down-sized Open Platform

2.3.7.10.1 The Down-sized Open Platform hosts the applications and data for ISS-2 systems and maintains system interfaces shared among ISS-2 systems. The applications and data will be progressively migrated to the CDR. The Contractor shall provide and maintain existing means of message-oriented communication and system interface files to DSOP that currently provided and supported by SMARTICS, in order to minimise the consequential changes to ISS-2 systems.

2.3.7.10.2 To minimise data migration risk and effort, the data management design of SMARTICS-2 shall take consideration for the ROP records maintained in Down-sized Open Platform and the CDR.

2.3.8 Functional Requirements for Application Services Infrastructure

2.3.8.1 Application Services Architecture

2.3.8.1.1 The application services architecture for the System shall support the application processing in a distributed computing environment between different platforms and layers, including Central Service Layer, Local Service Layer, Front-end Service Layer and ITI Service Layer. The application architecture shall be a multi-tier architecture and service-oriented with high adaptability to cope with future business and technology changes.

2.3.8.1.2 The application services architecture for the System shall be efficient, flexible, scalable and easy to manage.

2.3.8.1.3 The design of the application services architecture for the System shall be compliant with Java^{TM} Enterprise Edition (“Java EE”) architecture. The Java EE architecture shall provide an integration hub that interfaces with the components of SMARTICS-2 through open standards in web services or Java Message Service (“JMS”).

2.3.8.1.4 The System shall be able to interact with various components in the SMARTICS-2, including but not limited to, database services, directory services, CDS and System Management Services, in an integrated manner.

2.3.8.1.5 Without prejudice to the recommendations set out in Appendix B which have been incorporated in this Annex as essential requirements, the selected technical options described in Section 5 in Appendix B – “Extract of the Feasibility Study Report on the Implementation of SMARTICS-2” and Appendix C – “Description of IT Infrastructure of ImmD” to Part VII shall be complied with in the design and implementation of the System.

2.3.8.2 Application System Integration

2.3.8.2.1 The Contractor shall provide the system integration services in relation to all application components for the implementation of SMARTICS-2, including but not limited to, the following:

(a) Card Personalisation and Management Services (to be implemented under Category B);

(b) Cabinet Services (to be implemented under Category C);

(c) Tag Services (to be implemented under Category D);

(d) e-Services-2 platform (to be implemented under Category E);

(e) Down-sized Open Platform Application;

(f) CDR and CDS; and

(g) Government Supplied Hardware and Software.

2.3.8.2.2 Card Personalisation and Management Services

2.3.8.2.2.1 The System shall integrate and interface with the System of Category B (or “CPMS”), in order to, inter alia, enable the necessary transmission of all necessary data between the two Systems so as to further enable the System of Category B to perform its business functions in smart card personalisation services as more particularly specified in Annex B to Part VII.

2.3.8.2.2.2 After the collection and verification of application data at ROP offices, the System shall provide HKIC registration details, including registration and collection information, portrait images and fingerprints templates, to CPMS for card production and personalisation.

2.3.8.2.2.3 The System shall via interfaces with CPMS provide the necessary details for the update of card production, card status and any update information on chip of HKIC.

2.3.8.2.2.4 The Contractor shall produce the detailed specifications and design of the system interface between the System and CPMS during the SA&D stage. The Contractor shall seek the agreement of the Contractor of Category B and the Government concerning the specifications and design in accordance with the co-operation arrangement specified in Section 1.4 of Part VII. The Contractor shall subsequently implement the interface based on such specifications and design endorsed by all necessary parties in accordance with the arrangement specified in Section 1.4 of Part VII.

2.3.8.2.2.5 The Contractor shall work and coordinate with the Contractor of Category B and other contractors of the Government to ensure the smooth integration and rollout of SMARTICS-2 and the implementation of CPMS.

2.3.8.2.3 Cabinet Services

2.3.8.2.3.1 The System shall integrate and interface with the System of Category C (or "CabS"), in order to, inter alia, enable the necessary transmission of all necessary data between the two Systems so as to further enable the System of Category C to perform its functions to provide secure storage and automatic card dispensation functions of new smart identity cards at SCKs and e-Cabinets in ROP branch offices and SIDCCs as more particularly specified in Annex C to Part VII.

2.3.8.2.3.2 The System shall via system interfaces with the System of Category C, exchange data including but not limited to the following: retrieval of new smart identity cards from CabS, check-out of expired new smart identity cards, check-in new smart identity cards inventory into CabS, exchange of card key text information, new smart identity cards stock-taking and management information, new smart identity card status and error notification, etc.

2.3.8.2.3.3 Upon receiving the card personalised status information from the System of Category B after the new smart identity card is personalised in Card Personalisation Office, the System shall perform reconciliation check of new smart identity card inventory in cabinets when the new smart identity cards are checked-in into the cabinets to ensure the successful delivery of new smart identity cards to ROP branch offices and SIDCCs. The System shall provide error report and alert officer for any discrepancy.

2.3.8.2.3.4 The System shall provide central management functions, with the support of card inventory report and inventory discrepancy report, etc., for indicating the locations and status of personalised new smart identity cards, such as in self-service collection kiosk, e-Cabinet or already collected, to support inventory management and handle abnormal scenarios, in case of power outage or malfunction of kiosk or cabinet.

2.3.8.2.3.5 The System shall maintain the new smart identity card inventory information in each e-Cabinet and self-service collection kiosk. The System shall be able to manage and provide information for the e-Cabinet and self-service collection kiosk to check-out those expired new smart identity cards and free spare available slots for subsequent check-in processes.

2.3.8.2.3.6 The Contractor shall produce the detailed specifications and design for the interface between the System of this Category and the System of Category C during the SA&D stage. The Contractor shall seek the agreement of the Contractor of Category C and the Government concerning the specifications and design in accordance with the co-operation arrangement specified in Section 1.4 of Part VII. The Contractor shall subsequently implement the interface based on such specifications and design endorsed by all necessary parties in accordance with the arrangement specified in Section 1.4 of Part VII.

2.3.8.2.3.7 The Contractor shall provide, including but not limited to, network equipment, system monitoring tools, etc. for setting up in ROP branch offices and SIDCCs to support the System of Category C for delivery of services of the System of Category C. Tenderers shall propose the hardware and software in Schedules 1 and 2 – “Hardware” and “Software” of Part V respectively and the price in Schedule 23 – “Price Schedule” of Part V.

2.3.8.2.3.8 The Contractor shall work and coordinate with the Contractors of Categories B and C and other contractors to ensure the smooth integration with CabS and maintain the centralised new smart identity card inventory information for SMARTICS-2.

2.3.8.2.4 Tag Services

2.3.8.2.4.1 The System shall integrate and interface with the System of Category D (or “TAGS-2”), in order to, inter alia, to enable the necessary transmission of all necessary data between the two Systems so as to further enable the System of Category D to perform the business operations related to tag services in ROP branch offices and SIDCCs as more particularly specified in Annex D to Part VII.

2.3.8.2.4.2 At the time an applicant arrives at a ROP branch office or SIDCC, the applicant will present a document, e.g. identity card, travel document, e-EEP, birth certificate, etc., at Reception Desk and the System shall integrate to the System of Category D to generate an appointment tag or a walk-in tag to the applicant. The System shall support similar processing at self-service tag issuing kiosks, which will be provided by the Contractor of Category D.

2.3.8.2.4.3 At the Registration Desk, Assessment Desk and Shroff Desk, the System shall integrate with TAGS-2 to display the tag and booth number on the display unit, to notify the next applicant. The System shall notify TAGS-2 once the applicant show up for application processing or no show after a certain period.

2.3.8.2.4.4 For collection process of new smart identity card, the System shall integrate with TAGS-2 for the status and location of the new smart identity card stored, e.g. self-service collection kiosk or e-Cabinet at Collection Desk, when the applicant or proxy presents the ROP140 / ROP140A or the existing smart identity card at self-service tag issuing kiosk or Collection Desk.

2.3.8.2.4.5 The System shall exchange data with TAGS-2, via interface, including but not limited to the following data: the appointment booking and quota information of ROP application, next tag and applicant show up details, identity card status and location, etc.

2.3.8.2.4.6 As a contingency measure to cater for any prolonged failure of tag service, the System shall support the application processing of ROP functions running under no tag mode, i.e. without tag service of TAGS-2, in ROP branch offices and SIDCCs.

2.3.8.2.4.7 The Contractor shall produce the detailed specifications and design for the interface between the System and the System of Category D during the SA&D stage. The Contractor shall seek the agreement of the Contractor of Category D and the Government concerning the specifications and design in accordance with the co-operation arrangement specified in Section 1.4 of Part VII. The Contractor shall subsequently implement the interface based on such specifications and design endorsed by all necessary parties in accordance with the arrangement specified in Section 1.4 of Part VII.

.

2.3.8.2.4.8 The Contractor shall work and coordinate with the Contractor of Category D and other contractors to ensure the smooth integration and rollout of SMARTICS-2 and the implementation of TAGS-2.

2.3.8.2.5 e-Services-2 platform

2.3.8.2.5.1 The System shall integrate and interface with the System of Category E (or "e-Services-2 platform"), in order to, inter alia, enable the necessary transmission of all necessary data between the two Systems so as to further enable the System of Category E to perform the functions more particularly described in Annex E to Part VII.

2.3.8.2.5.2 The appointment bookings and application pre-filling information shall be maintained on e-Services-2 platform when applicants perform booking in the Internet. The booking and application information relating to SMARTICS-2 applications shall be interfaced to the System before the appointment day and the appointment quota plan information shall be integrated to the e-Services-2 platform for appointment booking.

2.3.8.2.5.3 The Contractor shall deliver the detailed specifications and design for the interface between the System and the System of Category E during the SA&D stage. The Contractor shall seek the agreement of the Contractor of Category E and the Government concerning the specifications and design in accordance with the co-operation arrangement specified in Section 1.4 of Part VII. The Contractor shall subsequently implement the interface based on such specifications and design endorsed by all necessary parties in accordance with the arrangement specified in Section 1.4 of Part VII.

2.3.8.2.5.4 The Contractor shall work and coordinate with the Contractor of Category E and other contractors to ensure the smooth integration and rollout of SMARTICS-2 and the implementation of SMARTICS-2 applications on e-Services-2 platform.

2.3.8.2.6 Down-sized Open Platform Application

2.3.8.2.6.1 The DSOP is the midrange platform which was downsized from the mainframe system by the contractors of ITI project. DSOP holds all mainframe data, functions, programs, processes, jobs, modules and interfaces, it is used as the central data repository for communication among ISS-2 systems, including SMARTICS. Detailed description of the Down-sized Open Platform is set up in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII.

2.3.8.2.6.2 Currently, the Message Oriented Middleware ("MOM") architecture is used by the existing ISS-2 systems to communicate with the DSOP. In order to minimise consequential changes to ISS-2 systems and maintain the existing external system interface with each Government department, the existing means of message-oriented communication to the DSOP shall be retained.

2.3.8.2.6.3 For the Specific External Interface described in Section 2.3.3.2.38.3 of this Annex, the Message Queue ("MQ") gateway servers is currently placed in MCN and / or AN of ImmD with the MQ software, to set up a secured external system connection with the MQ servers of the Government department to receive and reply online requests by MQ protocol. The information is extracted from DSOP in MCN by the system interface programs in DSOP to serve the online requests received from that Government department. Currently, there are nine (9) control programs maintained by the contractors of ITI project and two (2) SMARTICS interface programs maintained by the project team of SMARTICS in DSOP for performing data retrieval of online requests from the Government department. The detailed design and requirements for the External Interfaces on SMARTICS-2 platform shall be confirmed at the SA&D stage. The Contractor shall provide the System Support Services for the aforementioned two (2) SMARTICS interface programs maintained in DSOP if it is confirmed to maintain for SMARTICS-2 as an interim solution.

2.3.8.2.6.4 To cater for enhancement of the Specific External Interface as described in Section 2.3.8.2.6.3 of this Annex, the Contractor shall provide hardware, software and related services to migrate the Specific External Interface with the External System described in Section 2.3.3.2.38.3 of this Annex from DSOP to SMARTICS-2 platform with the adoption of web services approach. The Contractor shall be responsible to implement the services and functions of record check to that department and re-develop the application program logic, including the nine (9) control programs currently maintained by the contractors of ITI project and the two (2) interface programs to be maintained and supported by the Contractor, on SMARTICS-2 platform. The detailed design and requirements for the External Interfaces on SMARTICS-2 platform shall be confirmed at the SA&D stage. The Contractor shall be responsible to provide System Support Services for the aforementioned interface programs.

2.3.8.2.6.5 Data exchange for existing system interfaces with SMARTICS and ISS-2 systems, including APPLIES and e-Passport, are using MQ. The Contractor shall implement the backward compatible solution in SMARTICS-2 to provide same system interfaces with each of these existing ISS-2 systems until they are revamped to ISS-3 systems.

2.3.8.2.6.6 The Contractor shall demonstrate as part of the System Acceptance Tests and User Acceptance Tests that the performance of the DSOP through its interface with the System shall provide at least the same or even better performance for all the functionalities and interfaces of the SMARTICS currently operating on the DSOP. If the Contractor fails to do so, the System Acceptance Tests and User Acceptance Tests will not be considered as passed. Without prejudice to other rights and claims of the Government, it shall have to implement such modification to the DSOP or other relevant parts of the System to ensure that the same or even better performance can be achieved.

2.3.8.2.6.7 Details in relation to the functions of SMARTICS in the DSOP are set out in Appendix A – "Description of Existing Systems" to Part VII.

2.3.8.2.6.8 The Contractor shall work and coordinate with other contractors of the Government and ImmD project teams to ensure the smooth integration and rollout of SMARTICS-2 and the system interfaces on DSOP.

2.3.8.2.7 Common Data Repository and Common Data Services

2.3.8.2.7.1 A CDR is provided by ITI as a centralised repository for storing the data and image commonly used by ISS-3 systems of ImmD. The associated CDS will also be provided to access and update the data in CDR at data centres. The System shall provide common data to CDR and make use of common data shared in CDR via web services by CDS. The CDR and CDS will be built up and established progressively together with the application of ISS-3 systems. The Contractor shall work with ITI project team for the establishment of CDR and CDS and be responsible for any necessary services related to SMARTICS-2. The Contractor shall also be responsible for the implementation of CDS for SMARTICS-2 as described in Section 2.3.8.22 of this Annex. The detailed design will be confirmed together with ITI project team and SMARTICS-2 project team in the SA&D stage.

2.3.8.2.7.2 The master copy of CDR is maintained in the PDC(KC) and the DDC(FL) as resilience purpose. To facilitate the operation efficiency and support the minimal services when there is interruption in WAN connection, the Contractor shall provide all the necessary hardware, software and related services and be responsible for the implementation of local mode operation of web services to meet the business requirement of SMARTICS-2. The local CDR shall be maintained in read only for any contingency operation and the CDS provided by ITI will not support for any change to CDR schema.

2.3.8.2.7.3 The Contractor shall be responsible to make available the local CDR to Local Service Layer and make use of the CDS for the access to local CDR to support the business requirement of SMARTICS-2. Tenderers shall propose all hardware, software and related services in Schedule 1 – "Hardware", Schedule 2 – "Software" and Schedule 4 – "Technical Proposal and System Configuration" of Part V for the setup of local CDR and CDS at ROP branch offices and SIDCCs to support the contingency operations in case of WAN is not available. The Contractor shall implement and be fully responsible for the local CDR and CDS, including the data synchronisation, business operations and workflows during contingency and recovered period, at ROP branch offices and SIDCCs. The Contractor shall be responsible for the implementation of the CDS in local mode operation under SMARTICS-2 at ROP branch offices and SIDCCs. The detailed requirement and design for the local CDR and CDS will be confirmed in the SA&D stage.

2.3.8.2.7.4 Details of CDR and CDS are depicted in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII.

2.3.8.2.8 Government Supplied Hardware and Software

2.3.8.2.8.1 Tenderers shall propose all hardware, software and related services for the implementation of the System, except the following items which will be provided by the Government or except as elsewhere expressly provided to the contrary:

(a) desktop workstations and some peripherals as stated in Section 6.2.2.5.7 of this Annex;

(b) Chinese Fonts file;

(c) CPMS and new smart identity cards, which will be provided under Category B;

(d) self-service registration kiosk, self-service general application kiosk, self-service collection kiosk and e-Cabinet, which will be provided under Category C (see Section 6.2.2.5.13 of this Annex);

(e) TAGS-2, which will be provided under Category D;

(f) e-Services-2 platform, which will be provided under Category E; and

(g) hardware and software provided by ITI as set out in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII.

2.3.8.2.8.2 The Contractor shall make use of the Government Supplied Hardware and Software for the implementation of the System.

2.3.8.2.8.3 The Contractor shall provide necessary software and sufficient licences for the system management and monitoring, virus protection and backup of the System.

2.3.8.2.8.4 The Contractor shall ensure that the hardware, software and Custom Programs can be fully compatible and interoperable with the Government Supplied Hardware and Software. Items of the Government Supplied Hardware and Software are set out in Appendix G – "List of Government Supplied Hardware and Software" to Part VII.

2.3.8.2.8.5 The Contractor shall work and directly liaise with the contractors of the Government Supplied Hardware and Software for the successful integration with the System.

2.3.8.3 Workflow Processing Services

2.3.8.3.1 Tenderers shall propose a workflow processing solution to support the ROP application processing, including but not limited to, application creation, registration, assessment, acknowledgement, verification, approval, monitoring, personalisation, issuance and finalisation as well as other ROP related applications in Table 5-4.1(A) of Schedule 4 – "Technical Proposal and System Configuration" of Part V.

2.3.8.3.2 The Contractor shall provide workflow application to support the automated electronic application flow, dynamic allocation and workflow management of the large volume of ROP applications under the distributed processing environment of SMARTICS-2 in a secure, accurate and efficient manner.

2.3.8.3.3 The Contractor shall provide the workflow engine which support high availability, resilience, fault tolerance and effective exception handling features.

2.3.8.3.4 The workflow engine shall be able to cater for the integrated document handling and imaging capabilities.

2.3.8.3.5 The workflow shall provide interfacing function to access the profiles stored in the Lightweight Directory Access Protocol ("LDAP") directory of the UPMS.

2.3.8.3.6 The workflow engine shall provide reporting, tracking and deadlining functionalities for monitoring of the case works.

2.3.8.3.7 The workflow engine shall be able to interface with the System.

2.3.8.4 Imaging Services

2.3.8.4.1 The Contractor shall provide a central image storage system, which shall be the repository of all images for SMARTICS-2 and shall consist of:

(a) images of documents, i.e. application forms and supporting documents;

(b) applicant photo images; and

(c) applicant fingerprints images.

2.3.8.4.2 These images originate either from the conversion of existing SMARTICS IMS records or from scanning of new images, mainly at ROP branch offices and SIDCCs, by the System. The retrieval of images mainly takes place at ROP offices, including ROP branch offices, HQ offices and SIDCCs, for ROP application processing, as well as in control points for record checks, or any authorised record enquiry.

2.3.8.4.3 The imaging services shall provide all the functionalities which are currently provided by existing IMS functions and the function as specified in Section 2.3.3.2.31 of this Annex.

2.3.8.4.4 The Contractor shall provide hardware, software and related services for the implementation of existing IMS functions.

2.3.8.4.5 The Contractor shall provide imaging servers at PDC(KC) to manage the retrieval and storage of existing images and newly captured images. The imaging servers shall be equipped with permanent massive storage device, namely as Write Once Read Many device.

2.3.8.4.6 For resilience purpose, the Contractor shall provide another set of imaging servers with permanent massive storage device at DDC(FL). Data in the imaging servers at PDC(KC) shall be copied to the imaging servers at DDC(FL) periodically for online synchronisation.

2.3.8.4.7 The Contractor shall provide all the hardware, software and related services for retrieval of images at ROP branch offices, SIDCCs and HQ offices from

DDC(FL), in case of any service suspension at PDC(KC), as contingency measure.

2.3.8.4.8 In order to minimise the impact on the critical ROP application processing when there is problem with the IMS, the image files for the applications in progress shall be stored temporarily in the file system of imaging server. After the application processing is completed, all these image files shall be imported and indexed in the IMS for permanent storage. The Contractor shall include the size of disk storage required for the temporary storage of image in imaging server.

2.3.8.4.9 The Contractor shall provide all necessary hardware, software and related services to implement secure backup, including offsite storage without any manual logistics arrangement. The imaging servers shall of high availability and be available 7 x 24 hours. The System shall provide resilient servers and mirror disks to maintain reliable services.

2.3.8.5 Fingerprint Enrolment and Verification Services

2.3.8.5.1 The System shall provide fingerprint enrolment services at Registration Desk and self-service registration kiosks at SIDCCs. The System shall capture applicants' fingerprints, check the liveliness of fingerprints and perform fingerprint verification with historical fingerprints using fingerprint matching algorithms. Re-capturing of fingerprints is required if the quality of fingerprint image is lower than a pre-set threshold, to ensure the fingerprints captured can be effectively verified in verification process.

2.3.8.5.2 The System shall provide fingerprint verification services at Assessment Desk to verify the fingerprints captured at registration process and historical record.

2.3.8.5.3 The System shall be able to tune and set the threshold of the fingerprint matching algorithm to the false acceptance rate ("FAR") and the false rejection rate ("FRR") as required by the Government. The details of the fingerprint template minutiae extraction and verification will be confirmed during the SA&D stage.

2.3.8.5.4 During the enrolment and verification process, the System shall provide and support fingerprint one-to-one matching and correctly determine the fingerprint belongs to the same individual.

2.3.8.5.5 The System shall store two captured fingerprint images to the database, which shall be maintained in the disk-based WORM device for permanent storage. The System shall generate and store two sets of fingerprint templates, including a format provided by the Contractor and standard format of ANSI-INCITS 378[1], to the captured fingerprint images for fingerprint matching, in order to achieve high fingerprint matching accuracy and pave the way for the adoption of standard templates for facilitating interoperability among different matching algorithms. The Contractor shall provide and implement the fingerprint matching algorithm on fingerprints minutiae extraction and verification to the Contractor provided

[1] ANSI-INCITS 378, American National Standard for Information Technology – Fingerprint Minutiae Format for Data Interchange Format, defines the placement of minutiae on a fingerprint and record format for containing minutiae data.

format and standard format. The fingerprint templates, in both formats, shall be sets of figures which cannot be used to reconstruct the fingerprints.

2.3.8.5.6 The Contractor shall provide additional customisation on the fingerprint matching algorithms, which shall be exclusively provided to the Government, for both types of fingerprint template format. The customisation algorithms shall be performed in a secure way that the matching process is restricted to authorised parties.

2.3.8.5.7 The System shall provide fingerprint verification services by authenticating the cardholder with the fingerprint templates stored in the chips of existing and new smart identity cards for the use at Registration Desks, Assessment Desks, Collection Desks, self-service registration kiosks, self-service collection kiosks, self-service general application kiosks, the Mobile Registration / Card Collection Device, handheld smart card readers, etc.

2.3.8.5.8 The Contractor shall provide all the hardware, software and related services for the implementation of fingerprint enrolment and verification services as specified in this Section 2.3.8.5 and the existing enrolment and verification functions in SMARTICS.

2.3.8.5.9 The Contractor shall develop Custom Programs and provide the fingerprint template minutiae extraction and verification algorithm services to the Government for authentication of HKIC cardholder, including but not limited to the business services provided by the ImmD: e-Channel, self-service kiosks for passport application submission and Macao automated passenger clearance enrolment. The Contractor shall work with and provide assistance to other contractors and Government project teams.

2.3.8.5.10 The proposed fingerprint verification solution provided by the System shall be compatible with the existing fingerprint scanners used by ImmD in other systems such as the e-Channel, self-service kiosks for passport application submission and Macao automated passenger clearance enrolment for performing identity authentication.

2.3.8.5.11 The Contractor shall provide all software licences for ImmD applications required to perform fingerprint capturing and verification of HKIC cardholder, including Registration Desks, Assessment Desks, Collection Desks, Mobile Registration / Card Collection Device, handheld smart card reader, MSK_REG, SCK, MSK_GEN, e-Channel, self-service kiosks for passport application submission and Macao automated passenger clearance enrolment. In addition to the quantity of fingerprint verification licence required to verify new templates using fingerprint scanners installed in the function desks and kiosks as specified in Section 6.2.2.5.6 of this Annex, the Contractor shall also provide an additional of 1,600 of fingerprint verification licences to the Government for the usage at e-Channel, self-service kiosks for passport application submission and Macao automated passenger clearance enrolment.

2.3.8.5.12 To support the authentication to cardholders of existing smart identity card, the System shall provide fingerprint verification services of the existing fingerprint templates stored in the chip of existing smart identity card at designated registration desks, self-service registration kiosks, self-service collection kiosks and self-service general application kiosks. The licences of the existing fingerprint template extraction and verification algorithm will be provided by the Government and the said algorithm will be provided to the Contractor during SA&D stage. The Contractor shall be responsible for the system support services of the fingerprint verification algorithm for the existing fingerprint templates stored in the chip of existing smart identity cards. The Contractor shall provide any necessary hardware, software and related services to perform the fingerprint verification services to verify the live captured fingerprint against the templates stored in existing smart identity card and new smart identity card and the historical fingerprint images stored in IMS.

2.3.8.5.13 The Contractor shall be responsible for ensuring the compatibility and interoperability between the System and the Government supplied algorithms for a complete and total solution.

2.3.8.5.14 The System shall also provide fingerprint verification functions at verification desk at HQ to verify newly submitted fingerprint images and historical fingerprint images or any fingerprint images comparison. The function shall be able to extract minutiae points or ridge lines on fingerprint images to facilitate verification process.

2.3.8.5.15 The Contractor shall provide hardware, software, services and Custom Programs to support identity verification on matching of fingerprint images stored in the System against scanned copy of thumbprint impressions of a cardholder.

2.3.8.5.16 The Contractor shall work and coordinate with the Contractors of Other Categories and other contractors of the Government for the successful integration and implementation of fingerprint enrolment and verification services.

2.3.8.6 Portrait Image Capturing and Verification Services

2.3.8.6.1 The System shall provide portrait image capturing services to capture live images of applicants by portrait cameras, which shall be provided by the Contractor at Registration Desk and self-service registration kiosks at SIDCCs.

2.3.8.6.2 The Contractor shall be responsible to propose the background environment for capturing portrait image to achieve high quality of images.

2.3.8.6.3 The portrait image capturing service shall have the capability to enhance the captured image.

2.3.8.6.4 The portrait image capture module shall provide function(s) for various manipulation such as live view, automatic face alignment, sizing, brightness, zoom, rotate, crop, panning, capture and re-capture. The image capturing function shall be equipped with face detection function and liveliness detection to prevent forged biometric intervention.

2.3.8.6.5 The Contractor shall ensure the captured portrait image quality is sufficient to maintain the effectiveness in identity verification by visual means. The captured images shall be conformed to the International Civil Aviation Organization (“ICAO”) Doc 9303 standard for identity document and the image shall be interoperable and have sufficient resolution to support face recognition as supplementary authentication method, which can be used in automated clearance and other self-service applications.

2.3.8.6.6 The Contractor shall ensure the captured portrait image, in a colour photo format (e.g. JPEG, JPEG2000) of at least 1200 x 1600 pixels with image size of around 600 KB and in accordance with the ISO/IEC 19794-5 format, which not only defined the data format, but also with additional requirements, such as digital images attributes, scene constraints and photographic properties, to improve the accuracy of facial recognition. The System shall provide functions to check the portrait images that conform to the standard with the following, but not limited to: position of applicant, background, pose, colours and lighting, lighting on applicant and background, hair style and expression, eye glasses, head coverings, quality of image, etc. The photo image to be provided to CPMS for card personalisation and storage in the chip of the new smart identity card shall not be less than 640 x 480 pixels with optimal image size of 16-20 KB.

2.3.8.6.7 The Contractor shall provide hardware, software and related services to perform the portrait image verification services of one-to-one matching to verify the live captured image against the historical portrait images of the HKIC cardholder stored in IMS.

2.3.8.6.8 The Contractor shall provide any necessary hardware, software and related services, including installation, design, implementation and testing the software and algorithm to capture and verify the facial images for the Registration Desks, self-service registration kiosks and mobile registration devices.

2.3.8.6.9 The Contractor shall provide any necessary software and related services, including design, implementation and testing the software and algorithm to verify the facial images captured from self-service collection kiosks.

2.3.8.6.10 The System shall be able to tune and set the facial verification threshold of FAR and the FRR as required by the Government.

2.3.8.6.11 The System shall be able to provide portrait image capturing and verification services with undegraded performance under different environmental conditions in lighting, humidity and temperature at Registration Desk at ROP branch offices and SIDCCs, the Mobile Registration / Card Collection Device and self-service registration kiosks at SIDCCs.

2.3.8.6.12 The System shall be able to provide portrait image verification services with undegraded performance under different environmental conditions in lighting, humidity and temperature at self-service collection kiosks in ROP branch offices and SIDCCs.

2.3.8.6.13 The Contractor shall be responsible to provide the portrait cameras and any necessary facilities, including but not limited to, flash light, for capturing high quality of portrait images at Registration Desks, self-service registration kiosks and the Mobile Registration / Card Collection Device.

2.3.8.6.14 The Contractor shall provide any necessary mounting equipment and services for holding the portrait camera, flash light and any other facilities to be securely installed at Registration Desks with proper protection.

2.3.8.6.15 The Contractor shall work and coordinate with the Contractor of Category C to ensure the portrait camera, flash light and any other facilities to be securely mounted and installed at self-service registration kiosks.

2.3.8.6.16 The Contractor shall work and coordinate with the Contractors of Other Categories and other contractors of the Government for the successful integration and implementation of portrait image capturing and verification services.

2.3.8.7 Self-service Registration Kiosk Application Services

2.3.8.7.1 The Contractor shall be responsible to design and develop application for self-service registration kiosks in SIDCCs to facilitate applicants in preparing and submitting applications for ROP registration process in the territory-wide HKIC replacement exercise via such self-service registration kiosks.

2.3.8.7.2 The self-service registration kiosk application shall be running on the MSK application framework, which will be provided by the Contractor of Category C, on the kiosk, such that any change or replacement of peripherals will minimise the chance for the application running on kiosks from being affected. Section 2.3.3.2 of Annex C to Part VII sets out the details of MSK application framework, which will be provided by the Contractor of Category C.

2.3.8.7.3 The Contractor shall provide the fingerprint scanner (enrolment), portrait camera and related software licences and facilities at self-service registration kiosks.

2.3.8.7.4 Apart from the devices and equipment stated in Section 2.3.8.7.3 of this Annex, self-service registration kiosk will be equipped with peripherals, including but not limited to, personal computers with UPS, touch screen monitor, keyboard, smart card reader for existing smart identity card, handwriting recognition device, document scanner, document printer, stereo speakers, etc. The physical kiosk design and the peripherals, except those stated in Section 2.3.8.7.3 of this Annex, of the self-service registration kiosks will be provided by the Contractor of Category C. The Contractor shall work with the Contractor of Category C to ensure the design of the self-service registration kiosk can protect confidentiality and privacy of applicants while performing application registration at the kiosk. The Contractor shall make use of the peripherals provided by the Contractor of Category C to implement the application running on self-service registration kiosks.

2.3.8.7.5 The Contractor shall provide applications running on self-service registration kiosks with bilingual (Chinese (both Traditional and Simplified Chinese) and English) features for input, display and instruction. Self-service registration kiosk shall be customised with automatic login to provide application registration functions in Local Kiosk Network.

2.3.8.7.6 Tenderers shall propose a solution for applications running on self-service registration kiosk, such that applications, software maintenance, software upgrade and transfer of application data can be maintained securely in the System in Schedule 4 – “Technical Proposal and System Configuration” of Part V.

2.3.8.7.7 The System shall make use of the self-service registration kiosk and peripherals provided by the Contractor of Category C to provide, but not limited to, the functions described in Section 2.3.3.2.8 of this Annex through the design and development of the application running on the self-service registration kiosk.

2.3.8.7.8 The System shall provide function(s) for passing completed cases or failed cases, e.g. failed in identity verification, fingerprints capturing, etc., to subsequent registration process at Registration Desks and Assessment Desks during normal mode and local mode operations in SIDCCs.

2.3.8.7.9 The Contractor shall provide servers and equipment for supporting the self-service registration kiosk functions mentioned above, and any staging servers for the store-and-forward of self-service registration kiosk traffic between the Extended MCN and Local Kiosk Network.

2.3.8.7.10 The System shall support standalone mode operations for all self-service registration kiosks in SIDCCs. Application registration functions shall be provided at self-service registration kiosks as described in Section 2.3.3.2.8 of this Annex. Storage encryption facilities shall be provided to data stored in the kiosks.

2.3.8.7.11 The Contractor shall provide any necessary hardware, software, related services and Custom Programs to support the applications running at the self-service registration kiosks under standalone mode and the recovery process to upload the captured data and images after services resume. The System shall provide any necessary checking and validation against the centralised database with minimal user involvement upon performing recovery operation. The detailed design shall be confirmed at SA&D stage. Details of the hardware requirements for self-service registration kiosks are depicted in Section 6.4.3 of Annex C to Part VII.

2.3.8.7.12 Subject to Section 2.3.8.7.3 of this Annex, the Contractor shall provide hardware abstraction layer for the portrait camera and fingerprint scanner (enrolment) for self-service registration kiosk. Section 2.3.3.2.3 of Annex C to Part VII sets out the details of hardware abstraction layer.

2.3.8.7.13 Subject to Section 2.3.8.7.4 of this Annex, the Contractor shall provide all other related hardware and software for the proposed solution of self-service registration kiosk, including but not limited to, servers, storage encryption facilities, network equipment, monitoring and distribution software tools, etc. Tenderers shall propose the hardware and software in Schedules 1 and 2 – “Hardware” and “Software” of Part V respectively and the price in Schedule 23 – “Price Schedule” of Part V.

2.3.8.7.14 The Contractor shall work and coordinate with the Contractors of Other Categories and other contractors of the Government for the successful integration and implementation of self-service registration kiosk application services.

2.3.8.8 Self-service Collection Kiosk Application and e-Cabinet Services

2.3.8.8.1 The Contractor shall be responsible to design and develop application for self-service collection kiosks at ROP branch offices and SIDCCs to facilitate applicants to collect new personalised smart identity card in a self-service manner from the self-service collection kiosks.

2.3.8.8.2 The Contractor shall provide the software for fingerprint verification licences for performing fingerprint verification with the new fingerprint template, which is provided by the Contractor. The Contractor shall also provide facial recognition tools and licences for the facial recognition to be used in self-service collection kiosks. Self-service collection kiosk will be equipped with peripherals, including but not limited to, personal computers, touch screen monitor, fingerprint scanner (verification), portrait camera, smart card reader for existing smart identity card in SIDCCs, ROP140 / ROP140A automatic collecting device for collection of ROP140 / ROP140A in ROP branch offices, etc. Except the ROP140 / ROP140A automatic collecting device which shall be provided by the Contractor as stated in Section 2.3.3.2.23.2 of this Annex, the physical kiosk design of the self-service collection kiosks and other peripherals will be provided by the Contractor of Category C. The Contractor shall work with the Contractor of Category C to ensure the design of the self-service collection kiosk can cater for the installation of the ROP140 / ROP140A automatic collecting device provided and can protect confidentiality and privacy of applicants while collecting existing smart identity card at the kiosk. The Contractor shall make use of the peripherals provided by the Contractor of Category C to implement the application running on self-service collection kiosks.

2.3.8.8.3 The Contractor shall provide applications running on self-service collection kiosks with bilingual (Chinese (both Traditional and Simplified Chinese) and English) features for display and instruction. Self-service collection kiosk shall be customised with automatic login to provide existing smart identity card collection functions in Local Kiosk Network.

2.3.8.8.4 Tenderers shall propose a solution for applications running on self-service collection kiosk, such that applications, software maintenance, software upgrade and kiosk inventory and management information can be maintained securely in the System in Schedule 4 – “Technical Proposal and System Configuration” of Part V.

2.3.8.8.5 The System shall make use of the self-service collection kiosk and peripherals provided by the Contractor of Category C to provide at least, but not limited to, the functions described in Section 2.3.3.2.13 of this Annex to the application running on the self-service collection kiosk.

2.3.8.8.6 The System shall ensure that all personalised new smart identity cards are verified that no unique serial number or identifier can be read via contactless interface without performing mutual authentication by authorised smart card readers.

2.3.8.8.7 The System shall make use of the devices and functions provided by the Contractor of Category C and the Custom Programs provided by the Contractor of Category B on mutual authentication and data retrieval from the chip of new smart identity cards to perform verification of cardholder's live fingerprints and facial image with the templates and images stored in the chip of new smart identity cards before issuing to cardholders.

2.3.8.8.8 The System shall update the card inventory in the System and notify the CPMS, which will be provided by the Contractor of Category B, via system interface for successful collection cases.

2.3.8.8.9 The System shall allow any abnormal case, e.g. failed in document or identity verification, retrieved a wrong new smart identity card, missing of masking unique serial number or identifier, cardholder overstayed, etc., to be routed to Collection Desks without issuing the new smart identity card.

2.3.8.8.10 The System shall support retrieval of a new smart identity card in self-service collection kiosk by officers with appropriate security measures, in case of collecting the new smart identity card by proxy without advanced notice or failed in identity authentication.

2.3.8.8.11 The Contractor shall provide servers and equipment for supporting the self-service collection kiosk functions mentioned above, and any staging servers for the store-and-forward of self-service collection kiosk traffic between the Extended MCN and Local Kiosk Network.

2.3.8.8.12 The Contractor shall provide equipment for supporting the e-Cabinet function, including but not limited to, staging servers and network equipment.

2.3.8.8.13 Functions of automatic check-in, check-out, retrieval, stock-taking, storage and inventory control of new smart identity cards will be available in kiosk and they are provided by the Contractor of Category C. While integrating with the self-service collection kiosk, the System shall also maintain the smart card inventory information in each kiosk after check-in and check-out. The System shall be able to manage and operate the kiosk to check-out those expired smart cards and spare available slots for subsequent check-in processes.

2.3.8.8.14 In addition to normal mode, the application for self-service collection kiosk and e-Cabinet shall support local mode and standalone mode operation in ROP branch offices and SIDCCs. Cardholders can retrieve and collect their new smart identity cards in self-service collection kiosks, even though any prolonged failure in accessing servers at Central Service Layer and / or Local Service Layer, after performing successful identity verification. ROP staff of card issuance can continue to issue new smart identity cards through ROP application in collection desk and using cabinet application in e-Cabinet provided by the Contractor of Category C. Upon resumption of normal operation, all the updated information shall be synchronised with the System. Storage encryption facilities shall be provided to data stored in the kiosks.

2.3.8.8.15 In case to handle any abnormal scenario, such as power outage and malfunction of kiosk, the self-service collection kiosks and e-Cabinet will support manual retrieval of new smart identity cards. The System shall make use of the functions provided by the Contractor of Category C to perform inventory check, produce inventory report, alert officers, provide discrepancy report and provide functions to synchronise the inventory with the System.

2.3.8.8.16 Subject to Section 2.3.8.8.2 of this Annex, the Contractor shall provide all other related hardware and software for the proposed solution of self-service collection kiosk, including but not limited to, servers, storage encryption facilities, network equipment, monitoring and distribution software tools, etc. Tenderers shall propose the hardware and software in Schedules 1 and 2 – “Hardware” and “Software” of Part V respectively and the price in Schedule 23 – “Price Schedule” of Part V.

2.3.8.8.17 The Contractor shall work and coordinate with the Contractors of Other Categories and other contractors of the Government for the successful integration and implementation of self-service collection kiosk application services.

2.3.8.8.18 The Contractor shall work and coordinate with the Contractors of Other Categories and other contractors of the Government for the successful integration with the cabinet application services provided by Contractor of Category C.

2.3.8.9 SMARTICS-2 Application Services for Self-service General Application Kiosk

2.3.8.9.1 The Contractor shall be responsible to design and develop SMARTICS-2 related applications for self-service general application kiosks installed at ROP branch offices, SIDCCs, control points, HQ and other immigration offices.

2.3.8.9.2 The SMARTICS-2 applications for MSK_GEN shall be running on the MSK application framework, which will be provided by the Contractor of Category C, on the kiosk, such that any change or replacement of peripherals will minimise the chance for the application running on kiosks from being affected. Section 2.3.3.2.1 of Annex C to Part VII sets out the details of MSK application framework, which will be provided by the Contractor of Category C.

2.3.8.9.3 The Contractor shall provide the software for fingerprint verification licences of the new fingerprint template to be used at MSK_GEN. The kiosks will be equipped with peripherals, including but not limited to, personal computers, touch screen monitor, keyboard, slip printer, smart card reader for existing smart identity card, OCR and Radio Frequency Identification (“RFID”) readers for reading new smart identity card, passport and e-EEP, fingerprint scanner(verification), handwriting recognition device, stereo speakers, etc. The physical kiosk design and all peripherals of the MSK_GEN will be provided by the Contractor of Category C. The Contractor shall work with the Contractor of Category C to ensure the design of the MSK_GEN can protect confidentiality and privacy of cardholders while performing SMARTICS-2 related functions at the kiosk. The Contractor shall make use of the peripherals provided by the Contractor of Category C to implement the application running on MSK_GEN.

2.3.8.9.4 The Contractor shall provide SMARTICS-2 application running on MSK_GEN with bilingual (Chinese and English) features for input, display and instruction.

2.3.8.9.5 Tenderers shall propose a solution for SMARTICS-2 applications running on MSK_GEN, such that SMARTICS-2 applications, software maintenance, software upgrade and transfer of the application data can be maintained securely in the System in Schedule 4 – “Technical Proposal and System Configuration” of Part V.

2.3.8.9.6 The System shall make use of the MSK_GEN and peripherals provided by the Contractor of Category C to provide at least, but not limited to, the SMARTICS-2 related functions described in Section 2.3.3.2.17 of this Annex to the application running on the MSK_GEN.

2.3.8.9.7 The Contractor shall provide servers and equipment for supporting the SMARTICS-2 related functions for MSK_GEN as mentioned above, and any staging servers for the store-and-forward of MSK_GEN traffic between the MCN, AN at data centres and General Kiosk Network at ROP branch offices, SIDCCs, control points and other immigration offices.

2.3.8.9.8 Subject to Section 2.3.8.9.3 of this Annex, the Contractor shall provide all other related hardware and software for the SMARTICS-2 applications running on MSK_GEN, including but not limited to servers, network equipment, monitoring and distribution software tools, etc. Tenderers shall propose the hardware and software in Schedules 1 and 2 – “Hardware” and “Software” of Part V respectively and the price in Schedule 23 – “Price Schedule” of Part V.

2.3.8.9.9 The Contractor shall work and coordinate with the Contractors of Other Categories and other contractors of the Government for the successful integration and implementation of SMARTICS-2 application services for MSK_GEN.

2.3.8.10 Electronic Services for SMARTICS-2 Applications (including web applications and mobile apps)

2.3.8.10.1 The Contractor shall be responsible to design and develop SMARTICS-2 related applications on the e-Services-2 platform, which platform will be implemented by the Contractor of Category E.

2.3.8.10.2 The Contractor shall be responsible to develop web applications and mobile apps for SMARTICS-2 to provide, including but not limited to the following online services:

(a) HKIC online appointment booking and application form pre-filling;

(b) Territory-wide HKIC replacement exercise appointment booking and application form pre-filling;

(c) CRP online appointing booking and application submission;

(d) EC online application submission;

(e) online functions for amendment of Registered Particulars application; and

(f) online application status enquiry.

2.3.8.10.3 The Contractor shall make use of the shared web application hosting environment of e-Services-2 Infrastructure, which will be provided under Category E, to develop and implement SMARTICS-2 web applications and mobile apps for the functions specified in Section 2.3.8.10.2 of this Annex.

2.3.8.10.4 The Contractor shall observe the requirements of e-Services-2 Infrastructure in Category E and shall be aware that multiple ImmD electronic services applications shall be running under sharing resources environment of the e-Services-2 platform. The details of resources allocated to the System on the e-Services-2 platform shall be provided and confirmed during the SA&D stage, and the Contractor shall be responsible to implement and tune the web applications and mobile apps services under the restricted resources to fulfil the government requirements, including but not limited to functional, workload, performance, security and privacy requirements.

2.3.8.10.5 The Contractor shall develop and implement the web applications, which shall meet at least the following requirements:

(a) integrate with GovHK of the Government for the provision of online services to the public;

(b) support the most popular operating systems and browsers in the market. The supported combinations of popular operating systems and browsers shall align with the supported system requirements for GovHK online services, which are published at GovHK website for reference;

(c) support at least the two most popular and recent major versions of mobile OS platforms, including iOS and Android, and shall support the most popular browsers for each mobile OS platform;

(d) support the IPv6 network;

(e) be capable of detecting the system platforms used by the public users and inform the public users of any incompatible platforms or issues;

(f) conform to the World Wide Web Consortium (“W3C”) Web Content Accessibility Guidelines (“WCAG”) Version 2.0 Double-A standard or the latest;

(g) support in three versions: Traditional Chinese version, Simplified Chinese version and English version;

(h) adopt the latest version of ISO/IEC 10646, an international coding standard developed by the International Organization for Standardization (“ISO”), for data input, storage and exchange;

(i) support the ImmD specific Chinese characters for data input and display;

(j) verify all input data before acceptance by the System;

(k) support the use of Address Data Infrastructure (“ADI”) service and structured format for data validation;

(l) support file attachment, with file formats specified under Electronic Transactions Ordinance (Chapter 553 of the Laws of Hong Kong) (“ETO”), for online application submission, if any;

(m) validate all attached files and accept only those files meeting the specified file requirements and verify all submitted file attachments to ensure that they are virus free before acceptance by the System; and

(n) prevent repeated invocation abuses by programmed computers and adopt challenge-response test such as Completely Automated Public Turing test to tell Computers and Humans Apart ("CAPTCHA") authentication or other equivalent technique for the prevention.

2.3.8.10.6 The System shall be capable of avoiding overload conditions due to continuing to accept requests from the public when approaching capacity limit. The System shall inform the public to access the service at a later time. The threshold shall be parameter driven and adjustable.

2.3.8.10.7 The System shall support system resource control for individual web applications. The minimum and maximum number of concurrent access for individual web applications shall be adjustable according to business needs.

2.3.8.10.8 The final requirements shall be subject to the further refinement and elaboration during the SA&D stage as and when the design for the System is being worked out.

2.3.8.10.9 The Contractor shall adopt responsive web design, adaptive web design or other equivalent technique to maintain the accessibility to the web applications via desktop / laptop computers, smart phones and tablets.

2.3.8.10.10 The Contractor shall follow the "Guide to Developing Online Services on GovHK" of OGCIO for developing the web applications. Tenderers may refer to the existing online services of ImmD on GovHK for the look and feel advised by the guideline for reference.

2.3.8.10.11 The Contractor shall develop and implement the mobile apps, which shall meet at least the following requirements:

(a) support iOS and Android, and shall support the most popular browsers for each mobile OS platform;

(b) be capable of detecting the system platforms used by the public users and inform the public users of any incompatible platforms or issues;

(c) fulfil the legal responsibility according to the Disability Discrimination Ordinance (Cap 487 of the Laws of Hong Kong) to ensure the services are available to everyone regardless of disability. Relevant guidelines are issued by corresponding mobile OS (such as iOS, Android) to enhance the accessibility of the apps and the Mobile Application Accessibility Handbook (http://www.ogcio.gov.hk/en/community/web_accessibility/maahandbook/) is issued by OGCIO for reference;

(d) support in three versions: Traditional Chinese version, Simplified Chinese version and English version;

(e) adopt the latest version of ISO/IEC 10646, an international coding standard developed by the International Organization for Standardization, for data input, storage and exchange;

(f) support the ImmD specific Chinese characters for data input and display;

(g) verify all input data before acceptance by the System;

(h) support the use of Address Data Infrastructure service and structured format for data validation;

(i) support file attachment, with file formats specified under Electronic Transactions Ordinance (Chapter 553 of the Laws of Hong Kong), for online application submission, if any;

(j) validate all attached files and accept only those files meeting the specified file requirements and verify all submitted file attachments to ensure that they are virus free before acceptance by the System; and

(k) fully utilise relevant features such as camera, Global Positioning System ("GPS"), etc. of smart phones and tablets where applicable.

2.3.8.10.12 The System shall make use of the shared services in e-Services-2 platform and implement the shared services, including but not limited to the Short Message Service ("SMS") services, e-mail services, etc.

2.3.8.10.13 The Interactive Voice Response ("IVR") applications for ImmD, including IVR applications for SMARTICS-2 (e.g. HKIC appointment booking, territory-wide HKIC replacement exercise appointment booking, etc.), will be implemented by the Contractor of Category E. The Contractor shall work with the Contractor of Category E and be responsible to provide functions to facilitate data access by the IVR applications.

2.3.8.10.14 The Contractor shall be responsible to provide initial and regular subsequent updates of technical assistance guidelines, frequently asked questions, trouble shootings, etc. related to the electronic services applications of SMARTICS-2 to the Contractor of Category E for the telephone helpdesk service to public.

2.3.8.10.15 The Contractor shall be responsible to implement the system interface between SMARTICS-2 and the ROP related details, including appointment booking, application form pre-filling details, etc., in e-Services-2 platform.

2.3.8.10.16 The Contractor shall work and coordinate with the Contractors of Other Categories and other contractors of the Government for the successful integration and implementation of electronic services for SMARTICS-2 applications.

2.3.8.11 Smart Identity Card Chip Data Reading and Updating Services

2.3.8.11.1 The System shall provide functions in reading, accessing and / or updating data stored in existing and new smart identity card chip services with mutual authentication at different functional desks, self-service registration kiosks, self-service collection kiosks, self-service general application kiosks, mobile registration devices, as described in this Annex.

2.3.8.11.2 The System shall make use of the program or Custom Program provided by the Contractor of Category B to perform the mutual authentication, retrieval and update of data stored in the chip of existing smart identity card via contact interface and the chip of the new smart identity card via contactless and contact interface. To access via contactless interface, the System shall capture the key text string on card face from authorised reader to activate the wireless data transmission. Details of the terminal access applications are described in Section 2.3.3.4.1 of Annex B to Part VII.

2.3.8.11.3 The Contractor shall work and coordinate with the Contractor of Category B to ensure the mutual authentication solution and the mechanism of Secure Access Module ("SAM") of both existing and new smart identity cards are supported in normal, local and standalone modes of operations.

2.3.8.11.4 The Contractor shall work and coordinate with the Contractor of Category B to support the storage, distribution and update of the secure access module, cryptographic keys and certificates for both existing and new smart identity cards.

2.3.8.11.5 The System shall support to read, access and authenticate existing and new smart identity cards at handheld smart card reader and mobile registration device via contact interface only for data transmission.

2.3.8.12 External Interfaces

2.3.8.12.1 The Contractor shall provide all necessary hardware, software, Custom Programs, Implementation Services and System Support and Maintenance Services for the External Interfaces with the External Systems of other Government B/Ds.

2.3.8.12.2 Tenderers shall propose a preliminary design and specifications of the External Interfaces with External Systems in Table 5-4.1(A) of Schedule 4 – "Technical Proposal and System Configuration" of Part V.

2.3.8.12.3 The System shall automate the processing of requests received via the External Interfaces with the External Systems, including but not limited to, data decryption, content validation, data conversion, authentication of originator and request processing. These processes shall not require human operation and shall be transparent to users.

2.3.8.12.4 The System shall be easily configured to cover the automatic acknowledgements to the originator as well as at different stages of external data processing, including but not limited to, upon receipt of data, after content conversion, etc.

2.3.8.12.5 The Contractor shall design and develop external interfaces for the data transmission between the System and each of the External Systems, including the interfaces currently supported by SMARTICS and those from time to time designated by the Government (collectively, "Interfaces with the External Systems" or "External Interfaces"). The Government will elaborate further on the scope of work to be performed by the Contractor including the requirements concerning the Interfaces with External Systems to the Contractor during SA&D stage but none of such work shall be considered as System Changes.

2.3.8.12.6 The System shall handle the data exchange at least in the following ways.

(a) data exchange in batch mode, such as SSH File Transfer Protocol (also Secure File Transfer Protocol ("SFTP"));

(b) data exchange in online mode. The external users will direct operation through the AN web and interface servers in the DM Zone of ITI AN;

(c) data exchange in web services via Departmental Portal ("DP");

(d) data exchange via mail services.

2.3.8.12.7 The Interfaces with the External Systems shall include external web services as follows:

(a) the external web services shall fully comply with security policies, standards and guidelines of ImmD. Details are provided in Section 12 – "Security Requirements" of Part VII;

(b) the Contractor shall provide solution to extract data from the entry forms uploaded by external parties. The entry forms shall include Microsoft Excel and XML documents; and

(c) the System shall provide audit trail and logical access control software to track activities performed in the AN web and interface servers.

2.3.8.12.8 The Interfaces with the External Systems shall include mail services as follows:

(a) the e-mail solution shall be able to exchange Internet and Intranet e-mails;

(b) the Contractor shall deploy the mail servers in the ITI AN and integrate with ImmD mail system for the communication within ImmD and with external parties; and

(c) the System shall be able to process the e-mails which will finally be transmitted to Central Service Layer and handle the information contained in the e-mails. The solution shall be designed with minimal user intervention.

2.3.8.12.9 The design of Interfaces with the External Systems shall have no single point of failure and fully comply with security policies, standards and guidelines of ImmD. Details are provided in Section 12 – "Security Requirements" of Part VII.

2.3.8.13 Internal Interfaces with ImmD Systems

2.3.8.13.1 The System shall provide internal interfaces with other ImmD systems, including but not limited to APPLIES, ICONS, e-Passport, DWIS, COMS-2, PRES, OCSSS and UPMS.

2.3.8.13.2 The Contractor shall design and develop interfaces for data transmission between the System and other ImmD systems as specified above and those from time to time designated by the Government ("Interfaces with Internal Systems"). The Government will provide and confirm the details of the Interfaces with Internal Systems to the Contractor during SA&D stage but none of such work shall be considered as System Changes.

2.3.8.13.3 The System shall be designed to support the following interface processing:

(a) batch mode;

(b) online mode;

(c) use of different protocols including SFTP;

(d) direct database access or MQ; and

(e) open interface standard including web services.

2.3.8.13.4 The Contractor shall provide middleware for the communication of SMARTICS-2 with other ImmD systems, including but not limited to the Down-sized Open Platform. The System shall maintain existing data exchange approach between SMARTICS and ImmD systems in order to minimise the impact to ISS-2 and ISS-3 systems.

2.3.8.13.5 Interface with DWIS

2.3.8.13.5.1 The System shall provide data to DWIS for generating management statistics.

2.3.8.13.5.2 The Contractor shall be responsible to extract the source data from the System and generate the interfaces files in standard format, which will be confirmed by the Government in the SA&D stage.

2.3.8.14 Database Services

2.3.8.14.1 The application data for SMARTICS-2 shall be stored in RDBMS in database servers of the System. The database in Central Service Layer shall serve as a central data repository and the centralised data shall be maintained in CDR and Down-side Open Platform for access by other major ImmD ISS-3 and ISS-2 applications respectively. The databases in Local Service Layer at ROP branch offices and SIDCCs shall serve as local data repositories.

2.3.8.14.2 The RDBMS shall run on the database servers to manage data storage, structure, access and security.

2.3.8.14.3 The RDBMS shall provide centralised control of data for efficient and secure database access. The data must be organised and managed through the RDBMS, which shall be capable of running on various midrange platforms.

2.3.8.14.4 The RDBMS shall support data replication to synchronise data between homogenous databases among ROP branch offices, SIDCCs, PDC(KC) and DDC(FL). Data shall be able to replicate in both directions. The replication frequency shall be adjustable to minimise the impact on the availability and performance of the database service.

2.3.8.15 Directory Services

2.3.8.15.1 User and Profile Management System replaces the existing Central User Profile Management System (“CUPM”) and it is provided by ITI. UPMS maintains all user profiles, terminal profiles, location profiles as well as role and post related data kept centrally under CDR in the PDC(KC) and the DDC(FL) for resilience purpose. The UPMS provides common authentication services for the sign-on and authentication process of ISS-3 systems, including SMARTICS-2.

2.3.8.15.2 SMARTICS-2 shall maintain its own authorisation repository using a role-based control for all functions of SMARTICS-2.

2.3.8.15.3 To support user authentication process at ROP branch offices and SIDCCs, local UPMS and LDAP servers at ROP branch offices and SIDCCs shall be required and user credentials on the centralised UPMS at PDC(KC) and DDC(FL) shall be synchronised to the local UPMS and LDAP servers. When user authenticates to SMARTICS-2 at a local office, the user’s credentials will be checked against the local UPMS services. Once the user credentials are authenticated successfully, the SMARTICS-2 application server will proceed to the role-based authorisation checking. The local UPMS shall maintain the user sign-on status, which will also be synchronised to the centralised UPMS at PDC(KC) and DDC(FL) to facilitate centralised monitoring and tracking.

2.3.8.15.4 Under local mode operation, any changes performed in local UPMS shall be able to synchronise back to central repository after recovery of WAN connections.

2.3.8.15.5 The local UPMS service at ROP branch offices and SIDCCs shall support not only limited to the users of SMARTICS-2, but also the users of other ISS-3 systems at that location.

2.3.8.15.6 The Contractor shall provide all the necessary hardware, software, Custom Programs, Implementation Services and System Support and Maintenance Services for the implementation of local UPMS at ROP branch offices and SIDCCs, which shall be shared for the users of other ISS-3 systems at that location.

2.3.8.15.7 The Contractor shall be responsible to deploy the local UPMS and LDAP server to Local Service Layer in ROP branch offices, SIDCCs and HQ and make use of the common authentication services to perform the user authentication and support the application / user sign-on / off in SMARTICS-2. Although the Contractor shall be primarily responsible, it shall seek the input from the ITI project team for the implementation of the common authentication services in local mode operation.

2.3.8.15.8 Details of requirement and design of UPMS are set out in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII.

2.3.8.16 Infrastructure Services

2.3.8.16.1 Basic infrastructure services, including Domain Name System (“DNS”) service, Dynamic Host Configuration Protocol (“DHCP”) service, Network Time Protocol (“NTP”) service, Active Directory / domain controller service, system and network monitoring service and system management, anti-virus service and other auxiliary services, at PDC(KC) and DDC(FL) are provided by ITI for ISS-3 systems. The System shall make use of the Enterprise System Management system from ITI to manage the System within a common infrastructure management framework. Details are depicted in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII.

2.3.8.16.2 The Contractor shall provide the hardware, software and related services, including configuration services, to all servers and equipment of the System, the Systems provided by the Contractor of Category B, the Contractor of Category C and the Contractor of Category D located at PDC(KC), DDC(FL), HQ, ROP branch offices and SIDCCs to enable SMARTICS-2 for implementing the infrastructure services specified in Section 2.3.8.16.1 of this Annex.

2.3.8.16.3 Without prejudice to the recommendations set out in Appendix B to Part VII which have been incorporated in this Annex as essential requirements, the selected technical options described in Section 5 in Appendix B – "Extract of the Feasibility Study Report on the Implementation of SMARTICS-2" and Appendix C – "Description of IT Infrastructure of ImmD" to Part VII shall be complied with in the design and implementation of the System.

2.3.8.16.4 The Contractor shall work and coordinate with the Contractors of Other Categories, ITI project team and other contractors of the Government for the implementation of infrastructure services for SMARTICS-2.

2.3.8.17 Fax Services

2.3.8.17.1 The Contractor shall provide fax server to handle enquiry functions of the System via facsimile. The fax software shall support the following business operations of SMARTICS-2:

(a) support both in-bound and out-bound facsimile messages;

(b) provide control on the set of destinations permissible for out-bound messages;

(c) support multiple client workstations to receive in-bound requests and send out-bound responses to pre-defined destinations; and

(d) support supervisor to monitor and follow up for unsuccessful transmissions.

2.3.8.18 Printing Service

2.3.8.18.1 The System shall support printing both online and batch reports. The System shall support reports generated by report servers and reports shall be sent to COMS-2 or stored in the System during the retention period. The System shall provide facilities to view reports on user's workstation or download the report to user's workstation and allow users to print the report at local printer or network printer.

2.3.8.18.2 The printing solution shall support secured printing for the reports with sensitive or confidential data, which shall comply fully with the security regulation and guidelines of the Government.

2.3.8.18.3 The printing solution shall integrate with COMS-2 of ImmD so that the reports are generated and sent to COMS-2 repository for online viewing and print only when users prefer to.

2.3.8.19 Chinese Language Support

2.3.8.19.1 The Contractor shall integrate the System with the Chinese Language Support Solution ("CLS Solution") to be implemented in ImmD so that the System shall be capable of supporting the input, storage, display and printing of a mix of English and Chinese (Traditional and Simplified Chinese) characters.

2.3.8.19.2 The Government will procure the services to develop and maintain the CLS Solution for ImmD under another tender. The CLS Solution will adopt the latest version of ISO/IEC 10646, an international coding standard developed by the International Organisation for Standardisation ("ISO"), for data input, storage, display and exchange.

2.3.8.19.3 The System shall also adopt the latest version of ISO/IEC 10646 for data input, storage, display and exchange and the details will be confirmed during SA&D stage.

2.3.8.19.4 The CLS Solution will support the ImmD specific Chinese characters, which are Chinese characters created by ImmD to handle different glyphs of characters. The CLS Solution will disseminate, from time to time, the font files (including, but not limited to, the ImmD specific Chinese characters, input methods and Chinese characters mapping tables) to the SMARTICS-2 servers and workstations, including the System and the Systems of Category B, Category C, Category D and Category E.

2.3.8.19.5 The System shall make use of the font files provided by the CLS Solution to allow applicant to input and display the Chinese characters (including the ImmD specific Chinese characters) for applications, not only on the workstations of the System, but also on e-Services-2 platform and self-service kiosks. The System shall be able to integrate with the CLS Solution in a seamlessly manner.

2.3.8.19.6 Information for the Chinese processing details in SMARTICS-2 is described in Appendix B – "Extract of the Feasibility Study Report on the Implementation of SMARTICS-2" to Part VII.

2.3.8.19.7 The Contractor shall work and coordinate with the contractor of the CLS Solution and other contractors of the Government for the implementation of Chinese processing for SMARTICS-2.

2.3.8.20 Batch Job Scheduling

2.3.8.20.1 The Contractor shall provide the batch server software with batch job management capabilities to control the initiation time, frequency, execution sequence, exception handling, job priority and dependency assignment of back-end jobs. Function(s) shall be provided to allow authorised users to add, change, delete, enquire and print the job information, execution condition, dependency, schedules and action to be triggered for various result codes. Once the control parameters are set, the job scheduler shall initiate back-end jobs automatically without human intervention. The batch server software shall be compatible with the Contractor Supplied Hardware.

2.3.8.21 Anti-virus Services

2.3.8.21.1 The System shall be protected from virus or malicious attacks. Virus checking programs shall always be enabled on all midrange servers, PC servers, workstations, all self-service kiosks, mobile devices and handheld smart card readers.

2.3.8.21.2 The anti-virus services shall protect both physical and virtualised servers including UNIX and x86 platforms.

2.3.8.21.3 Centralised and automated updating of the latest version of virus control files shall be implemented.

2.3.8.21.4 ITI implements an anti-virus infrastructure at ITI MCN and ITI AN at ROP branch offices and SIDCCs, PDC(KC) and DDC(FL). The Contractor shall make use of the ITI anti-virus infrastructure in the first choice to implement the anti-virus solution for the System. Details of the ITI anti-virus infrastructure are set out in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII. The Contractor shall provide another anti-virus infrastructure in the case that the current ITI anti-virus infrastructure cannot support the proposed devices.

2.3.8.21.5 To minimise the WAN traffic, the Contractor shall implement the anti-virus infrastructure so that the anti-virus control files are stored in the distribution gateway of remote offices including HQ, ROP branch offices and SIDCCs. The distribution gateway shall then be responsible to distribute the anti-virus control files to the Local Service Layer and Front-end Service Layer in that remote office. The System shall also provide support to share the anti-virus control files to other servers at the remote offices upon the Government’s request.

2.3.8.21.6 The Contractor shall ensure that all servers in Central Service Layer, Local Service Layer and all workstations and kiosks in Front-end Service Layer shall be supported under the anti-virus infrastructure, including all servers, self-service kiosks, cabinets, workstations, mobile devices and handheld smart card readers to be connected in Extended MCN, Local Kiosk Network and General Kiosk Network.

2.3.8.21.7 The Contractor shall ensure scheduled scanning and signature updates to SMARTICS-2 components including servers and workstations of the System, servers, kiosks, e-cabinets and workstations of the Systems under the Contractor of Category B, the Contractor of Category C and the Contractor of Category D.

The Contractor shall ensure that the scanning and signature updates shall not affect the normal daily business operations.

2.3.8.21.8 The Contractor shall have routine procedures to update the anti-virus signature to all servers and clients of SMARTICS-2.

2.3.8.21.9 The Contractor shall work and coordinate with the Contractors of Other Categories, ITI project team and other contractors of the Government for the implementation of anti-virus infrastructure for SMARTICS-2.

2.3.8.22 Common Data Services for SMARTICS-2 (“CDS for SMARTICS-2”)

2.3.8.22.1 Design for CDS for SMARTICS-2

2.3.8.22.1.1 Following the recommendations of ISS-3 Review and the technical study for ITI, a set of common data services and related functions and services will be established on top of the Service-oriented Architecture (“SOA”) application framework platform of the ITI Technology Layer in supporting the implementation of ISS-3 initiatives, and in facilitating the interfacing between SMARTICS-2 with existing ImmD systems.

2.3.8.22.1.2 The Contractor shall be responsible for the design, program development, Functional Test, quality assurance, Training, installation, project deployment, Documentation, system tuning and System Support Services for the CDS for SMARTICS-2 as more particularly specified in the Appendix J – “List of Common Data Services for SMARTICS-2” to Part VII. The list of preliminary specifications for CDS for SMARTICS-2 in Appendix J to Part VII is not meant to be exhaustive and is subject to be further reviewed and confirmed with ImmD during the SA&D stage. No work required concerning such CDS for SMARTICS-2 shall be treated as System Changes. The Contractor shall be the service provider of CDS for SMARTICS-2 and shall implement the CDS for SMARTICS-2 in accordance with the finalised detailed design specifications of the System delivered in the SA&D stage and approved by the Government.

2.3.8.22.1.3 The proposed design of CDS for SMARTICS-2 to be implemented to operate on the SOA application framework platform of the ITI Technology Layer shall meet the following objectives:

(a) to support the application reusability by following the common SOA application framework and standards for systematic generation and reuse of the common data services among ISS-3 systems, in order to reduce duplicated efforts and time for application development, integration, testing and maintenance of similar services, and be more responsive to business requirements;

(b) to facilitate efficient information sharing and to ensure consistent access and processing of ImmD information on a high performance, stable and reliable SOA foundation; and

(c) to adopt the flexibility and maintainability of the common data services based on a consistent set of SOA infrastructure components.

2.3.8.22.1.4 The Contractor shall provide the relevant Implementation Services for CDS for SMARTICS-2. Besides, the Contractor shall be responsible for the setup and configuration of CDS for SMARTICS-2 to run in servers in ROP branch offices and SIDCCs to support the local mode operation.

2.3.8.22.1.5 The proposed CDS for SMARTICS-2 shall fulfil, but not limited to, the following design principles:

(a) compliant with Java EE architecture;

(b) support ISO10646 encoding;

(c) support local mode operation (for specific services);

(d) log all transaction details and provide function to retrieve logged transaction details;

(e) capable to generate application alert messages to ESM of ImmD;

(f) capable to be reused by or integrated into other ISS-3 systems, when required by the Government;

(g) back-end data services to be called by other ImmD systems shall be implemented on SOA application framework platform; and

(h) front-end functions shall maintain uniformities and standards of user interfaces, including but not limited to screen layouts, function keys and event buttons.

2.3.8.22.1.6 When implementing the CDS for SMARTICS-2, the Contractor shall adhere to the development standards, programming standards, naming conventions and other standards and guidelines based on the established SOA application framework delivered under the SOA governance by ImmD from time to time on application design and program coding to achieve the required objectives and design principles. The SOA governance framework, which includes the detailed control mechanism and procedures, such as new service registration, change control, deployment procedures, configuration management, etc., provides governance across the entire SOA service life cycle to ensure the effective and efficient use of SOA in enabling ImmD to simplify how developers publish, discover, reuse and change services during the design-time and run-time. The design of CDS for SMARTICS-2 shall be subject to modifications as approved by the Government in the SA&D stage.

2.3.8.22.1.7 The Contractor shall take the advice from the Government when designing CDS for SMARTICS-2 and when making necessary changes to the program codes for sustaining the maintainability of the codes with a view to facilitate sharing the common data services (as web services) so developed for use by other ImmD systems as deemed necessary at the sole discretion of ImmD.

2.3.8.22.1.8 The Contractor shall be responsible to provide technical support for other ImmD project teams and contractors of the Government to utilise the developed CDS for SMARTICS-2 for shared use if required.

2.3.8.22.1.9 The CDS for SMARTICS-2 shall be interoperable with and manageable and governed by the SOA infrastructure components under the SOA application framework.

2.3.8.22.2 Development for CDS for SMARTICS-2

2.3.8.22.2.1 CDS for SMARTICS-2 shall include back-end services, front-end functions and other supporting utilities (e.g. data synchronisation, report generation, etc). Back-end services include batch processes, background processes and services to be called by SMARTICS-2 or other ISS-3 systems if they are to be shared. Front-end functions are functions with online user interfaces.

2.3.8.22.2.2 CDS for SMARTICS-2 shall be run on the SOA application framework platform, and part of which will be selected to be run in the local application / database servers in ROP branch offices and SIDCCs to support the local mode operation.

2.3.8.22.2.3 For the purpose of maintaining uniformities and standards among common data services, the Contractor shall follow the standards and guidelines of the SOA application framework when performing the following:

(a) audit trail logging;

(b) database access and updating;

(c) data item validation;

(d) access control (on data level and service level); and

(e) ESM alert messages generation.

2.3.8.22.2.4 The Contractor shall ensure the successful completion of the Overall SMARTICS-2 System Integration Tests for CDS for SMARTICS-2 with Other Contractors under the cooperation arrangement specified in Section 17.15 of Part VII. The Contractor shall take lead to formulate the test plan and conduct the tests by working closely with other project teams / contractors of the Government.

2.3.8.22.2.5 The Contractor shall be responsible for rectifying any problem encountered in application integration test for CDS for SMARTICS-2 and where necessary seek the cooperation and input from Other Contractors to complete the problem rectification.

2.3.8.22.2.6 To support the local mode operation requirements of provision of essential common data services to run under different local application servers and database servers in ROP branch offices and SIDCCs / other ISS-3 systems, the Contractor shall ensure the CDS for SMARTICS-2 be developed based on open standards and the SOA governance framework, and are capable to deploy to ROP branch offices and SIDCCs without program modification.

2.3.8.22.3 Data Access Control

2.3.8.22.3.1 Most of the CDS for SMARTICS-2 will access the common data in the CDR of ITI, however, the Contractor shall implement certain specified services which require access to the database of DSOP or interfaces with ISS-2 systems when necessary. The Contractor shall confirm with the Government before implementation for the proposed data accesses from these data sources, in particular the data and images from the CDR / DSOP as these common data are under stringent data governance and access control by ImmD. Prior approval from the Government shall be required for any change of data accesses for the implementation of the CDS for SMARTICS-2.

2.3.8.22.3.2 To support the local operation mode operation at ROP branch offices and SIDCCs, local CDR shall be implemented at ROP branch offices and SIDCCs to support the data access needs from the CDS for SMARTICS-2 running locally.

2.3.8.22.3.3 The Contractor shall design with the advice from the Government and provide different authentication and authorisation levels for controlling the access of common data services by following the security policy under the ImmD SOA application framework.

2.3.8.22.3.4 User authorisation shall adopt the role-based access control design in UPMS, which was recommended in the ISS-3 study report, and ride on the common user authentication services of UPMS. The Contractor shall review and design the role-based access control framework during the SA&D stage, and coordinate with project teams and users to define the mapping of business roles and user privileges on both service level and data level.

2.3.8.22.4 Report for CDS for SMARTICS-2

2.3.8.22.4.1 The Contractor shall provide solution to generate reports for CDS for SMARTICS-2 supporting English, Chinese or both. The proposed solution shall be capable to generate reports by retrieving data from database, such as from the CDR. The information and format of reports are subject to be defined during SA&D stage.

2.3.8.22.4.2 The Contractor shall upload report generated in CDS for SMARTICS-2 to coming COMS-2 architecture of ImmD for user to view. Those reports shall be retained and removed periodically.

2.3.9 **Functional Requirements for Business Services Provisions**

2.3.9.1 Workstations and Kiosks

2.3.9.1.1 The System shall support the functional desks and kiosks in ROP branch offices, SIDCCs, immigration offices at and outside HQ and control points for SMARTICS-2 as described in Section 6.2.2.5 of this Annex.

2.3.9.1.2 The Contractor shall provide smart card readers for reading chips of existing and new smart identity cards, fingerprint scanners (enrolment) and fingerprint scanners (verification), portrait cameras and ROP140 / ROP140A automatic collecting devices to support the functional desks and kiosks as specified in Section 6.2.2.5.5 of this Annex.

2.3.9.1.3 The Contractor shall provide the minimum quantities of workstations, equipment and peripherals as specified in Sections 6.2.2.5.6 and 6.2.2.5.9 of this Annex for production, training and UAT purposes; whereas other workstations, kiosks, equipment and peripherals will be provided by the Government or the Contractors of other Categories. The Contractor shall integrate all these workstations, kiosks, equipment and peripherals, including those provided by the Government, the Contractors of other Categories and other contractors of the Government, into the System.

2.3.9.1.4 The Contractor shall work out solution together with the Contractor of Category B for tuning and integration of smart card reader for existing smart identity card and smart card reader for new smart identity card, the Contractor of Category C for setting, tuning and integration of equipment and peripherals with kiosks and cabinets and the Contractor of Category D for integration of tag printer at Reception Desk.

2.3.9.1.5 The Contractor shall provide and confirm with the Government the detailed specifications of the equipment and peripherals to be provided by the Government at the SA&D stage.

2.3.9.1.6 The Contractor shall implement the workstation security measures for SMARTICS-2 which shall include but not limited to:

(a) users shall be prevented from changing the system configuration on hardware, software and application;

(b) use of local administrator account shall be minimised for on-going maintenance of the workstations;

(c) browser cache or transaction data on the workstations must be deleted permanently whenever they are no longer required; and

(d) ensure the secure deletion of information before the faulty parts can be returned to the vendor.

2.3.9.1.7 The Contractor shall design and develop SMARTICS-2 application running on different types of SMARTICS-2 workstations which meet the business and performance requirements.

2.3.9.1.8 The standalone registration workstations shall be able to operate in standalone mode when they are isolated from the network. The Contractor shall provide data encryption solution to encrypt and decrypt data captured by workstations of functional desks, self-service registration kiosks and self-service collection kiosks during standalone mode operations for data privacy and confidentiality. The encryption, decryption and key protection standard shall fully comply with security policies, standards and guidelines of ImmD. Details are provided in Section 12 – “Security Requirements” of Part VII. The standalone mode operations for workstations, self-service registration kiosks and self-service collection kiosks shall be capable to support daily application workload in the ROP branch office and SIDCC. The Contractor shall provide corresponding facility for uploading of the data stored in the workstations and kiosks to the servers at Local Service Layer when the workstations and kiosks are able to reconnect to the servers at Local Service Layer.

2.3.9.1.9 The Contractor shall make sure clear and same quality fingerprint images can be captured by the registration desks and self-service registration kiosks.

2.3.9.1.10 The Contractor shall make sure dual-factor authentication in combination with fingerprint verification and facial recognition to strengthen the security and accuracy for self-service collection kiosks before confirmation of releasing the new smart identity card in the self-service collection kiosks. The Contractor shall provide function to verify the to-be released new smart identity card and to ensure that no information and no identifier (e.g. unique identifier, etc.) can be read by any smart card reader without mutual authentication before releasing the new smart identity card in the self-service collection kiosks.

2.3.9.1.11 The Contractor shall design and develop SMARTICS-2 application running on self-service registration kiosks, self-service general application kiosks and self-service collection kiosks which meet the business and performance requirements.

2.3.9.2 Handheld Smart Card Readers

2.3.9.2.1 The Contractor shall provide the handheld smart card readers to facilitate investigation operations in the quantities specified in Sections 6.2.2.5.6 and 6.2.2.5.9 of this Annex, and the required hardware and software to implement the checking of the validity of smart identity card via contact interface, authenticate cardholder with a fingerprint scanner (verification) and display the photo image stored in the card.

2.3.9.2.2 The Contractor shall provide solutions for operators to validate themselves before using the handheld smart card readers for the checking of cardholders.

2.3.9.2.3 The Contractor shall provide solutions to activate the handheld smart card reader before using, to restrict the checking limit and to upload the checked smart identity card information to the System via the supervisor workstations in investigation offices.

2.3.9.2.4 The Contractor shall work out solution together with the Contractor of Category B for reading the chip of existing and new smart card via contact interface.

2.3.9.2.5 Tenderers shall propose the handheld smart card reader solutions in Schedule 4 – “Technical Proposal and System Configuration” of Part V, hardware and software in Schedule 1 – “Hardware”, Schedule 2 – “Software” of Part V respectively and the price in Schedule 23 – “Price Schedule” of Part V.

2.3.9.3 Mobile Registration / Card Collection Device

2.3.9.3.1 The Contractor shall provide the mobile device with appropriate equipment to facilitate the registration, assessment, shroff and collection functions in the quantities specified in Sections 6.2.2.5.6 and 6.2.2.5.9 of this Annex. The mobile device with the associated equipment shall be compact in size and portable so that it can be easily carried by officers.

2.3.9.3.2 The mobile device shall be able to perform the functions as in the Registration Desk, Assessment Desk, Shroff Desk and Collection Desk, with same quality of fingerprint images and portrait images captured by the registration desks.

2.3.9.3.3 The Contractor shall provide solutions for loading the application data to the device and uploading to the System. The Contractor shall provide encryption solution to all application data to be stored in the mobile devices.

2.3.9.3.4 The Contractor shall work out solution together with the Contractor of Category B for reading and updating the chip of existing and new smart card via contact interface.

2.3.9.3.5 Tenderers may consider integrating mobile device with peripherals into one device. The integrated peripherals shall meet the respective specifications set out in this Annex.

2.3.9.3.6 The Contractor shall provide a single portable carrying case to put inside mobile device and all the peripherals for each set of mobile device. The carrying case shall be ruggedised for transportation, with cushion inside to protect the equipment from shock and able to be set up by non-technical staff.

2.3.9.3.7 Tenderers shall propose the mobile device solutions in Schedule 4 – “Technical Proposal and System Configuration” of Part V, hardware and software in Schedule 1 – “Hardware”, Schedule 2 – “Software” of Part V respectively and the price in Schedule 23 – “Price Schedule” of Part V.

2.3.9.4 Other Requirements

2.3.9.4.1 The Contractor shall design and develop the following functions for SMARTICS-2 Local Service Layer and Front-end Service Layer:

(a) workstation level security;

(b) single terminal approach and single sign-on;

(c) centralised and automated updating of the latest version of Chinese fonts and mapping tables;

(d) centralised and automated updating of latest version of virus control files;

(e) centralised and automated updating of the latest security patches including both Microsoft Windows and non-Microsoft Windows software;

(f) centralised and automated updating of the latest version of application programs;

(g) centralised and automated updating of system and application configurations of the System; and

(h) centralised and automated updating of other application and configurations including software and custom programs to be provided by the Contractor of Category C as well as the Government Supplied Software.

2.3.9.4.2 The design of the System shall minimise the impact of the above-mentioned updating functions (c) to (h) on workstation boot up and user sign-on.

2.3.9.4.3 The Contractor shall design and implement hardware abstraction layer for workstations running under the single terminal approach. The hardware abstraction layer shall allow applications, including the application of the Core System, the application to be provided by the Contractor of Category D and other ISS-3 applications, running on the workstation to manipulate and share the peripherals through a generic interface or application function.

2.3.9.4.4 The Contractor shall work with and provide technical support to the Other Contractors for implementation of SMARTICS-2 workstations, self-service general application kiosks, self-service collection kiosks, self-service registration kiosks and self-service tag issuing kiosks, including but not limited to, the system installation, system integration, problem diagnosis and solving.

2.3.10 Functional Requirements for System Management and Backup Infrastructure

2.3.10.1 Integration with ITI

2.3.10.1.1 ITI will have an ESM tool in MCN and AN for system management and monitoring purposes. The System shall be integrated with the ITI to make use of the tool for system management and monitoring. If necessary, the Contractor shall upgrade the system management tool to accommodate the workload of the Core System. Tenderers shall provide the sizing details for the requirement of the Core System in Schedule 21 – “Information Summary” of Part V.

2.3.10.1.2 The Contractor shall customise the ESM systems such that the centralised enterprise management console shall collect messages from any important source or component of SMARTICS-2, including the Simple Network Management Protocol (“SNMP”) alerts.

2.3.10.1.3 The Contractor shall customise the ESM systems such that administrators shall have a complete picture of the infrastructure environments of SMARTICS-2 and how the various components are behaving through the enterprise management console.

2.3.10.1.4 The Contractor shall customise the ESM systems such that it can effectively manage and control SMARTICS-2 in the following areas:

(a) system management;

(b) security management; and

(c) operations management.

2.3.10.1.5 If necessary, the Contractor shall upgrade the system management tools to accommodate the workload for SMARTCS-2.

2.3.10.1.6 The provided system management tools shall be shared with the Contractors of other Categories. The Contractor shall design the corresponding mechanism and provide the operation guidelines to Contractors of other Categories to follow, e.g., software distribution.

2.3.10.1.7 The Contractor shall provide any additional hardware and software required for the customisation and upgrade of the system management tools.

2.3.10.2 System Management

2.3.10.2.1 The System shall provide the overall management and monitoring for the systems and equipment across all layers of SMARTICS-2 (such as application systems, network, storage, servers, workstations, etc.).

2.3.10.2.2 The Contractor shall customise the system management tools to serve the following purposes for all critical components of SMARTICS-2:

(a) performance management;

(b) performance tuning and service level management;

(c) event and fault monitoring; and

(d) network management.

2.3.10.2.3 The Contractor shall customise the system management tools such that all the alerts shall be centrally managed by the enterprise system management console.

2.3.10.2.4 Performance management

2.3.10.2.4.1 The Contractor shall provide the performance management solution to perform real-time and proactive performance monitoring functions. The performance data shall be centrally analysed. The performance data will be collected from multiple data sources, including but not limited to server hardware, individual virtual machines, OS, application, database, storage, network, etc.

2.3.10.2.4.2 The solution shall be able to identify CPU, memory, disk I/O, processes and other key resources for performance monitoring. All identifiable performance metrics and faults shall be forwarded to a centralised management console.

2.3.10.2.4.3 The collected performance data shall be stored in a database or repository for performance tuning and capacity planning purposes.

2.3.10.2.4.4 The performance management solution shall be able to identify current and potential performance bottlenecks, inefficient or poorly performing components, likely failures of components, etc. and automatically trigger customised corrective and preventive actions upon detection of conditions that threaten applications availability or service levels.

2.3.10.2.5 Performance tuning and service level management

2.3.10.2.5.1 The solution shall be capable to analyse performance statistics and compare against the pre-defined threshold server level, warnings and alerts can be generated to the centralised management console.

2.3.10.2.6 Event and fault monitoring

2.3.10.2.6.1 The solution shall support the following features:

(a) able to pinpoint the cause of system or network problems by letting the administrator drill down to see all events that contributed to an alarm;

(b) all pre-definable events, alerts and warnings shall be directed and centralised to the enterprise management console;

(c) automated scripts can be created to address issues that require a specific defined solution or condition; and

(d) provide management reports and historical data analysis for proactive management of all system level exceptions or problems.

2.3.10.2.7 Network management

2.3.10.2.7.1 The Contractor shall perform problem and fault resolution, network change and upgrade, network management and network monitoring.

2.3.10.3 Hardware and software management

2.3.10.3.1 The Contractor shall be responsible to review the hardware and software continuously and advise ImmD if any hardware and software upgrade is required and if any hardware and software patches should be applied.

2.3.10.4 Security management

2.3.10.4.1 The Contractor shall customise the security management software to control access to computing and information resources of SMARTICS-2.

2.3.10.5 Operations management

2.3.10.5.1 The Contractor shall customise the operations management software to provide reliable availability of SMARTICS-2 service, including the tools for hardware and software management, software distribution, remote diagnosis, virus control, disk cloning and storage management.

2.3.10.6 Backup Infrastructure

2.3.10.6.1 General Requirements

2.3.10.6.1.1 The Contractor shall provide all necessary hardware, software and related services to implement the backup and recovery solution for the System. The Contractor shall also provide the disk-based backup system and necessary equipment at PDC(KC) and DDC(FL) to implement the backup infrastructure. The backup infrastructure shall support disk-to-disk, disk-to-disk-to-tape and disk-to-tape backup approach. The backup infrastructure shall support remote backup and transferring backup copy between PDC(KC) and DDC(FL).

2.3.10.6.1.2 The backup and recovery solution for the System shall cater all the system backup and data backup requirements at PDC(KC), DDC(FL), ROP branch offices and SIDCCs. The Contractor shall provide sufficient hardware and software including disk storage, tape storage and software licences of the backup and recovery solution for the System in ROP branch offices and SIDCCs.

2.3.10.6.1.3 A centralised backup infrastructure with global de-duplication among data centres shall be implemented to maximise backup resources utilisation and ease the overall backup management.

2.3.10.6.1.4 Data encryption shall be deployed in the backup solution and the tape backup device. Confidential and sensitive data shall be backed up in encrypted form. Data transferred between backup client and backup server shall be encrypted, when considered necessary, to assure confidentiality. Corresponding secured key store and key rollover infrastructure shall be in place.

2.3.10.6.1.5 The Contractor shall provide a backup server and a disk-based backup system in the Secured Zone in each data centre of PDC(KC) and DDC(FL). Backup agent shall be installed in each server of the System located in MCN and AN Trusted Zone to perform system and data backup. The backup server shall write backup archive to the disk-based backup system. The disk-based backup system located at PDC(KC) will replicate the archive to the disk-based backup system at DDC(FL) as an off-site backup.

2.3.10.6.1.6 A tape backup device shall be deployed at DDC(FL) to support storing long term data backup to tape media whenever necessary.

2.3.10.6.1.7 At each location of ROP branch offices and SIDCCs, a local backup solution with de-duplicated replication shall be implemented to integrate with the backup facilities at PDC(KC) and DDC(FL). A backup copy shall be stored in local and the backup shall be replicated to PDC(KC) and DDC(FL) for centralised backup. A backup server and a tape backup device shall be deployed in MCN of each location of ROP branch offices and SIDCCs. Backup agent shall be installed on each server located in MCN and AN to perform system and data backup. The backup server will write backup archive to the tape backup device.

2.3.10.6.2 System Backup and Recovery

2.3.10.6.2.1 The Contractor shall provide the functions and procedures for system backup and recovery for all servers and equipment of the System. System backup is required after any changes were applied to the system configuration. The Contractor shall perform drill on system recovery regularly at least once a year.

2.3.10.6.2.2 For PDC(KC) and DDC(FL), system backup of servers in both AN and MCN shall be performed using the backup infrastructure. One copy of the system backup shall be off-site, e.g., copy from PDC(KC) to DDC(FL) or vice versa, and one copy of the system backup shall be retained at local. The backup copy shall be transferred offsite without any manual logistics arrangement.

2.3.10.6.2.3 For ROP branch offices and SIDCCs, system backup of servers can be performed using local tape backup device (e.g. Linear Tape-Open ("LTO") tape) and / or archived to the SAN storage (with separate storage partition assigned in SAN). One copy of the system backup shall be off-site and one copy of the system backup shall be retained at local. The offsite backup copy shall be transferred offsite without any manual logistics arrangement.

2.3.10.6.2.4 The Contractor shall provide the functions and procedures for the backup and recovery of all front-end service layer equipment. Backup of the front-end service layer equipment is required after any change was applied to the front-end service layer equipment.

2.3.10.6.3 Data Backup and Recovery

2.3.10.6.3.1 The Contractor shall provide the functions and procedures for data backup and recovery for all servers and equipment of SMARTICS-2, including the System provided under Category D in ROP branch offices and SIDCCs. The backup infrastructure in ROP branch offices and SIDCCs shall at least support storage and generation of daily backup to support recovery of data in the last 10 days and at least support storage and generation of weekly backup to support recovery of data in the last 10 weeks.

2.3.10.6.3.2 As SMARTICS-2 contains confidential data, the data backup, including the database and file system backup, shall be encrypted.

2.3.10.6.3.3 For database servers, the agents of backup software shall work with the database’s native backup utilities for backup of databases and archive logs. Backup software shall be in place to support online database backup and backup of archive logs.

2.3.10.6.3.4 For the Central Service Layer of SMARTICS-2, data backup shall be performed using the backup infrastructure. One copy of the data backup shall be offsite from PDC(KC) to DDC(FL) (or vice versa) and one copy of the data backup shall be retained at local. The backup copy shall be transferred offsite without any manual logistics arrangement.

2.3.10.6.3.5 For the Central Service Layer, a regular regime of daily and weekly backup is required and the backup cycles shall be maintained. The backup infrastructure in PDC(KC) and DDC(FL) shall at least support storage and generation of daily backup to support recovery of data in the last 20 days and at least support storage and generation of weekly backup to support recovery of data in the last 20 weeks.

2.3.10.6.3.6 The System shall perform an automatic database backup nightly for each database of Local Service Layer after the office hour of ROP branch offices and SIDCCs. Sufficient disk space shall be available for a full nightly backup.

2.3.10.6.3.7 For the data in file system of Local Service Layer, backup shall be done by a disk-to-disk-to-tape copy solution. Dedicated disks shall be assigned for the backup of separate backup cycles.

2.3.10.6.3.8 The Contractor shall also be responsible for the data backup and recovery of local UPMS and local CDR at each of the ROP branch offices and SIDCCs, PDC(KC) and DDC(FL).

2.3.11 Functional Requirements for Cryptography and Security Infrastructure

2.3.11.1 Tenderers shall explain precisely in the Schedule 4 – "Technical Proposal and System Configuration" of Part V how the system security design will be protected and the details of relevant hardware features, system software features and application-level features.

2.3.11.2 Details of security requirements are described in Section 12 – "Security Requirements" of Part VII. The Contractor shall conduct security planning and implement the appropriate security measures and controls for the System according to the security requirements set out in the Contract. Formal testing and review on the security controls shall be performed prior to implementation of these security controls.

2.3.11.3 User Authentication

2.3.11.3.1 The Contractor shall provide all necessary hardware, software and related services to implement the user authentication solution for the System in ROP branch offices and SIDCCs.

2.3.11.3.2 UPMS of ITI is a centralised user identity management for ImmD applications and it provides common user authentication services to ISS-3 applications. SMARTICS-2 shall make use of UPMS to perform user authentication against the centralised repository of user profiles.

2.3.11.3.3 UPMS manages user, post and role relationship. SMARTICS-2 shall define roles and functions permitted to roles.

2.3.11.3.4 User and terminal profiles are centrally managed by UPMS. The user credentials and terminal profile on the centralised UPMS at PDC(KC) and DDC(FL) will be synchronised to the local UPMS at ROP branch offices and SIDCCs.

2.3.11.3.5 The Contractor shall implement SMARTICS-2 user authentication process which checks the user's credentials against the local UPMS services for the ROP branch offices and SIDCCs, the centralised UPMS services for the users in HQ, control points and other immigration offices. Once the user credentials are authenticated successfully, the SMARTICS-2 application server shall proceed to the role-based authorisation checking.

2.3.11.3.6 The local UPMS will maintain the user sign-on status and synchronised to the centralised UPMS at PDC(KC) and DDC(FL) to facilitate central management and tracking. When SMARTICS-2 users sign-off the application, the user sign-on status shall be reset at local UPMS and synchronised to the centralised UPMS.

2.3.11.3.7 The local UPMS shall be shared among ISS-3 systems in the ROP branch offices / SIDCCs (i.e. sharing of local UPMS server in ROP branch office with e-Passport-2 users and / or other ISS-3 systems).

2.3.11.3.8 Details of UPMS are set out in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII.

2.3.11.4 Role-based Authorisation Access Control

2.3.11.4.1 The Contractor shall design and develop the role-based access control on user authorisation and corresponding maintenance functions. Transaction ID will be assigned to every online transaction, together with relationship defined among other attributes such as Business Role and Location Code according to the business roles in SMARTICS-2. Users assigned with the predefined business role(s) will then inherit the access rights of associated functions.

2.3.11.5 Transaction Logging

2.3.11.5.1 All user activities shall be logged in the application transaction log centrally in a single relational database. With all these logs, powerful reporting tools can be used to generate detail reports on various events. Users can define their own filter for locating exactly the events they are interested in. When a transaction is terminated improperly, user actions related to the incomplete transaction shall also be logged as far as possible. When a transaction is completed successfully, the completed transaction should log the action details for audit purpose.

2.3.11.6 Data Encryption

2.3.11.6.1 According to the current IT Security Guidelines, all stored information classified as CONFIDENTIAL or above shall be encrypted. RESTRICTED information is recommended to be encrypted before storing and shall be encrypted when stored in mobile devices or removable media assigned to individuals. CONFIDENTIAL / RESTRICTED information shall be encrypted when transmitted over an un-trusted communication network. The Contractor shall observe and comply with these guidelines as published on the website of OGCIO from time to time, unless and to the extent any provisions therein are inconsistent with any express requirements of the Contract unless otherwise agreed by the Government on a case by case basis.

2.3.11.6.2 The Contractor shall provide the necessary equipment to support encryption of sensitive information, such as user password and system account password stored in local repository or system files. User password shall be encrypted during transmission and stored in encrypted format in any media, including backup media.

2.3.11.6.3 The Contractor shall provide the necessary equipment to support the encryption of sensitive data on workstations, standalone mode workstations, kiosks, servers and storages.

2.3.11.6.4 Asymmetric encryption shall be at least 2048-bit key length for Ron Rivest, Adi Shamir and Len Adleman (“RSA”) or equivalent. Symmetric encryption shall be at least 256-bit key length for the Advanced Encryption Standard (“AES”) or equivalent. Hashing shall be at least SHA-256 or equivalent.

2.3.11.6.5 The encryption, decryption and key protection standard shall be fully complied with the security policies, standards and guidelines of ImmD. According to the Security Regulations of the Government, for keys that are used for decrypting information classified as CONFIDENTIAL or above, they must be stored separately from the corresponding encrypted information.

2.3.11.6.6 There shall be a key manager for key management and key storage.

2.3.11.6.7 The data key shall be protected by the asymmetric RSA algorithm or other algorithm with equivalent or higher security level. The key shall not be delivered between the storage device and the key manager in plain text format.

2.3.11.6.8 The Contractor shall provide and deploy encryption appliances for SAN storage for each per Local Service Layer at ROP branch offices and SIDCCs, Central Service Layer at PDC(KC) and DDC(FL).

2.3.11.6.9 The Contractor shall provide and deploy encryption appliances for the external application and staging servers at PDC(KC) and DDC(FL).

2.3.11.6.10 The Contractor shall implement HSMs for each Local Service Layer at ROP branch offices and SIDCCs, Central Service Layer at PDC(KC) and DDC(FL).

2.3.11.6.11 The HSM shall be set up with high availability and ensure the integrity and security of cryptographic operations in a robust way. It shall be complied with the industry regulatory standards.

2.3.11.6.12 The HSM shall at least support Public-Key Cryptography Standards (“PKCS”) #11, Java Cryptography Architecture (“JCA”), Microsoft Cryptographic Application Programming Interface (“CAPI”) and OpenSSL.

2.3.11.6.13 The HSM shall be able to fully integrate with SMARTICS-2 application and provide the required cryptographic functions:

(a) true hardware accelerated random number generation;

(b) symmetric key and asymmetric key pair generation;

(c) encryption and decryption;

(d) RSA; and

(e) digital signing.

2.3.11.6.14 The Contractor shall design and develop the access control to allow only authorised access to use the HSM.

2.3.11.6.15 The Contractor shall ensure the secure deletion of information before the faulty parts can be returned to the vendor.

2.3.11.7 Key and Certificate Management System

2.3.11.7.1 A Key and Certificate Management System (“KCMS”) solution will be provided under Category B for the CPMS to manage the life cycle of the card management keys / certificates and card application keys / certificates so that smart cards and card applications can be securely protected.

2.3.11.7.2 The Contractor of Category A shall perform key / certificate distribution and key / certificate update of HSMs for the System in data centres, ROP branch offices and SIDCCs during Contract Period. The keys for HSMs will be generated by KCMS.

2.3.11.7.3 The Contractor shall implement another Key Management Sub-system solution to centrally manage the life cycle of the data encryption keys / certificates and communication keys / certificates so that they can be securely protected. The Key Management Sub-system solution shall meet requirement of network and communication security specified in Section 12.4 of Part VII and requirement of data security specified in Section 12.5 of Part VII.

2.3.11.7.4 The Key Management Sub-system shall facilitate the management of encryption key life cycle by simplifying, automating and strengthening key management process.

2.3.11.7.5 The Key Management Sub-system shall be provided at least one resilient pair in PDC(KC), DDC(FL), all ROP branch offices and SIDCCs due to its highly critical nature.

2.3.11.7.6 The Key Management Sub-system shall be able to communicate with the HSM for storing keys and maintains the life cycles of the keys and certificates, such as :

(a) communication keys for edge routers;

(b) communication certificates for secure connection, such as SSL certificates;

(c) communication keys / certificates for external interface parties;

(d) encryption keys stored in HSM;

(e) data encryption keys for external interfaces, such as requests stored in the staging server at ITI AN; and

(f) encryption keys for SAN storage and local storage of handheld smart card readers.

2.3.11.7.7 The Key Management Sub-system shall be responsible for key generation, including renewal of keys and certificates, and secure the key distribution process.

2.3.11.8 Mutual Authentication

2.3.11.8.1 The mutual authentication scheme provided under Category B which will be used for reading chip information in the smart identity card by using card admin key residing in the programmable HSM or SAM cards. The Contractor of Category A shall be responsible to deploy MA scheme to ROP application including but not limited to workstations, self-service kiosks, mobile devices and handheld smart card readers.

2.3.11.8.2 The Contractor shall make use of the MA scheme to integrate and communicate with ROP application to complete the new smart identity card chip and card face data access.

2.3.11.8.3 The existing smart identity card adopts SAM as the MA protocol. The new smart identity card, which is provided under Category B, may adopt other MA scheme, the Contractor shall provide MA services to cater the co-existence of both existing and new smart identity card during transition and it shall be transparent to the System.

2.3.11.8.4 The new MA scheme shall support asymmetric authentication protocol which offers additional features that are not easily obtainable with symmetric authentication protocol, including non-repudiation and true data origin authentication.

2.3.11.8.5 The Contractor shall coordinate with the Contractor of Category B and provide the new MA scheme for the access to on-card application from authorised workstations / peripherals.

2.3.11.9 External Interface

2.3.11.9.1 External Department users will submit requests to ImmD through the external web servers at DM Zone of ITI AN.

2.3.11.9.2 The Contractor shall design and implement the External Interface solution for the external department users to access the external web servers at DM Zone of ITI AN in PDC(KC) (and DDC(FL) for site resilience) to perform submission and enquiry functions via GNET.

2.3.11.9.3 The Contractor shall work out with the ITI Contractor to integrate the System with CDR and CDS.

2.3.11.9.4 All temporary files created during processing on the External Web Servers shall be removed upon completion of the process or periodically such as by means of secure deletion so that recovery of which by others will not be possible.

2.3.11.9.5 Host-based IDS software shall be installed to protect the External Web servers.

2.3.11.9.6 All data transmitted from external parties shall be encrypted using data encryption technology.

2.3.11.9.7 All server keys shall not be stored on the hard disks. Tenderers shall propose and the Contractor shall implement a tamper resistance solution to secure key storage, key access and key update to prevent unauthorised access, duplication and tampering of keys in Schedule 4 – "Technical Proposal and System Configuration" of Part V.

2.3.11.10 Encryption and Decryption of e-EEP

2.3.11.10.1 The Contractor shall implement a solution to capture chip information stored in e-EEP which will be used for ROP application processing. Since the data stored in the chip is encrypted, the reading of e-EEP chip data shall involved proprietary encryptors / decryptors provided by e-EEP related party.

2.3.11.10.2 The Contractor shall also implement a solution to capture card face data in e-EEP with proposed OCR and RFID readers.

2.3.11.10.3 The Contractor shall design and implement the System which integrate and communicate with ROP application to complete the e-EEP chip and card face data access.

2.3.12 Development, Testing and Training Environments

2.3.12.1 The Contractor shall implement the Systems in non-production environments as specified in Section 17.7.1 of Part VII. The System in non-production environments shall be connected to the development network, where appropriate. The development network shall be extended from DDC(FL) to HQ so that testers and developers at HQ can perform testing and development at HQ.

2.3.12.2 Development Network

2.3.12.2.1 The development network shall have identical functions and features with that existing in corresponding production network equipment. The Contractor shall provide all network equipment and servers to the development network.

2.3.12.2.2 The development network including the WAN link for the development, testing and training environments shall be separated from the network for the production environment. Unless otherwise specified, the WAN link will be provided by the Government. The Contractor shall provide all other necessary hardware (including but not limited to the router), software and implementation services for setting the development network.

2.3.12.2.3 The Contractor shall provide sufficient equipment to support the development LANs which will locate in at least four (4) floors at HQ.

2.3.12.2.4 The location of user floors, number of user floors and number of network ports required are subject to change. The Contractor shall cater for any change of these as required by the Government.

2.3.12.2.5 The Contractor shall base on information provided in Sections 3.3.2 and 3.3.3 of Appendix C – "Description of IT Infrastructure of ImmD" to Part VII to design and implement the development network of the System.

2.3.12.3 Environment Setting

2.3.12.3.1 The Contractor shall set up the System for different environments as specified in Section 17.7 of Part VII.

2.3.12.3.2 The Contractor shall provide all necessary hardware, software and custom programs for the setting up of all these environments. The System in each of the environments as mentioned in Section 17.7 of Part VII shall be able to perform all functions of the System as required in the Project Specifications and this Annex. The user acceptance tests for future enhancement will share the servers of the environment for User Acceptance Tests. The development environment during the Implementation Period will become the maintenance environment in the Maintenance Period after the System rolls out.

2.3.12.3.3 The Contractor shall provide dedicated servers and equipment in DDC(FL) for the non-production environments. The Contractor shall make use of the virtualisation technology for sharing of the hardware and software to set up the requirement environments. Different network zones can be formed by using VLAN separated by firewall appliance.

2.3.12.3.4 The System for Overall SMARTICS-2 System Integration Tests environment and Overall SMARTICS-2 User Acceptance Tests environment shall also be used for carrying the Resilience Test and Load Test. For Load Test, the Contractor shall adjust the resources allocation of different testing environments so that a testing environment can be created to support Load Test in a production-like manner.

2.3.12.3.5 The Contractor shall put in place local area networks to support environments as mentioned in this Section 2.3.12.

2.3.12.3.6 The Contractor shall extend the ITI development network from DDC(FL) to HQ to facilitate the development and testing at HQ.

2.3.12.3.7 The Contractor shall provide the hardware and software as deployed for the System in production environment for the testing environments. The hardware and software for the testing environments shall be identical to those for the production environment except that the hardware for the testing environments may have reduced storage capacity. The hardware, software and configuration for the testing environments shall be able to simulate the production environment.

2.3.12.3.8 The training environment will be hosted at DDC(FL) for users to carry out training. The training data will be restored periodically in the training environment. The Contractor shall implement a mechanism to restore the backup image periodically for the training environment.

2.3.12.3.9 Virtual machines for training servers shall be hosted on the production physical machines to fully utilise the standby resources in DDC(FL).

2.3.12.3.10 For the training and testing environments, the hardware and software shall meet the workload requirements specified in Section 5 – “Workload Requirements” of Part VII.

2.3.12.3.11 For development and testing environments, the Contractor shall provide hardware and software with sufficient capacity to support the daily workload from ImmD users, Contractor’s teams as well as in-house project teams of ImmD.

2.3.12.3.12 The Contractor shall provide version control software for all these environments. The software shall be used by all the Contractors of SMARTICS-2 (regardless of the Category) and the in-house project teams of ImmD, i.e., the Contractor of this Category shall provide sufficient software licence for use by its project team. A separate version control repository for sole use by ImmD in-house project teams shall be provided. The Contractor shall provide assistance to all the Contractors of SMARTICS-2 and the in-house project teams of ImmD on the use of version control software.

2.3.12.3.13 The Contractor shall provide testing automation tools for all these environments. The software shall be used by the Contractor of this Category and in-house project teams of ImmD. The Contractor shall provide assistance to the in-house project teams of ImmD on the use of testing automation tools.

2.3.12.3.14 The Contractor shall provide separate server equipment for the following non-production environments:

(a) development;

(b) testing (SIT, Integrated System Integration Tests (“iSIT”), UAT, Integrated User Acceptance Tests (“iUAT”) and fire-fighting); and

(c) training.

2.3.12.3.15 The same version of software shall be used in production and all these environments unless during testing period for software upgrade.

2.3.12.3.16 All these environments, including the testing environments of SIT, iSIT, UAT, iUAT, shall be totally independent, having independent copies of programs, database sub-system and data. Each environment, including the testing environments of SIT, iSIT, UAT, iUAT, shall have separate databases filled with non-production data for testing or training. The testing environment for fire-fighting can make use of the iSIT or iUAT environment during Maintenance Period to simulate production problems and perform urgent technical support.

2.3.12.3.17 During normal situations, computing resources of some non-production environments can be shared with other environments.

2.3.12.3.18 The training environment shall be segregated from the production environment. Any access to production data shall be prohibited.

2.3.12.3.19 Appendix B – “Extract of the Feasibility Study Report on the Implementation of SMARTICS-2” to Part VII sets out the recommended development, testing and training facilities for SMARTICS-2.

2.3.12.4 Off-site Development Location

2.3.12.4.1 The Contractor shall set up a dedicated and enclosed area at a location within HKSAR for the sole purpose of carrying out the Implementation Services for the System to be stationed by those members of the Implementation Team which are not required to be stationed within the ImmD premises (“Off-site Development Location”). These members of the Implementation Team may not be located in any overseas jurisdiction including the Mainland China unless the Government approves on a case by case basis.

2.3.12.4.2 The Contractor shall implement effective physical security measures to prevent unauthorised access to the Off-site Development Location. The measures shall include:

(a) use of dedicated access control system as stipulated in Section 2.3.12.4.3 of this Annex to control physical access to the Off-site Development Location; and

(b) use of surveillance monitoring system as stipulated in Section 2.3.12.4.4 of this Annex with round-the-clock recording at the Off-site Development Location.

2.3.12.4.3 The dedicated access control system shall log information on every entry and exit, including date, time and identity of the Contractor Personnel, at the Off-site Development Location. The records shall be kept for at least three (3) months. Upon request by ImmD, the Contractor shall provide the records to ImmD for inspection.

2.3.12.4.4 The surveillance monitoring system shall include sufficient number of CCTV cameras and shall be installed to provide round-the-clock monitoring of the Off-site Development Location and all entrance / exit area. The records of CCTV shall be kept for at least three (3) months. Upon request by ImmD, the Contractor shall provide the video records to ImmD for inspection.

2.3.12.4.5 The selection of the Off-site Development Location and the physical security measures to be implemented at the Off-site Development Location by the Contractor of Category A shall be agreed by the Government.

2.3.12.5 Off-site Development Infrastructure

2.3.12.5.1 The Contractor shall bear all the costs, including hardware, software and related services, to set up an off-site development infrastructure (“Off-site Development Infrastructure”) at DDC(FL) or any other premises provided by the Government for the Contractor Personnel to carry out the Implementation Services.

2.3.12.5.2 The Off-site Development Infrastructure shall be able to access the development resources of the System, including but not limited to Source Codes and Project

Documentation. The Off-site Development Infrastructure shall include facilities for security and access control of the development resources, including authentication, authorisation and activity logging.

2.3.12.5.3 The Contractor shall set up workstations at its own cost at the Off-site Development Location to access the Off-site Development Infrastructure for carrying out the Implementation Services. The Contractor shall be responsible to provide a secure and dedicated network connection between the Off-site Development Location and the Off-site Development Infrastructure for the purpose. The Contractor shall bear all the costs for such secure network connection, including but not limited to the necessary network equipment, security devices and WAN line services.

2.3.12.5.4 The Off-site Development Infrastructure shall provide security features such that the workstations and all other equipment at the Off-site Development Location shall not be able to keep or enabled to keep local copy and perform printing of the development resources in any manner. The control of the aforementioned security features for the workstations at the Off-site Development Location shall be centrally managed under the Off-site Development Infrastructure and shall not be over-written at the Off-site Development Location.

2.3.12.5.5 The design, setup and management of the Off-site Development Infrastructure shall be subject to prior and on-going security vetting and inspection by the Government and shall comply fully with the security regulation and guidelines of the Government. The Off-site Development Infrastructure shall be subject to the IT security risk assessment after the SA&D stage for the System as stipulated in Section 12.3 of Part VII.

2.3.12.5.6 Tenderers shall state, in Schedule 4 – “Technical Proposal and System Configuration” of Part V, the design of the Off-site Development Infrastructure for the implementation of the System.

2.3.13 Development and Testing Tools

2.3.13.1 The Contractor shall develop the application of the System with its own development and testing tools. The same version of application development tools shall be provided to ImmD for code review and software packaging for different testing environment as well as for production deployment.

2.3.13.2 Simulation software shall be provided by the Contractor at its cost to facilitate the simulation of workload during Load Test and for routine testing.

2.3.14 Requirements for Future Expansion

2.3.14.1 The architecture, hardware, software and implementation design shall be flexible for future expansion to cater for additional workload at existing ROP branch offices and also the setup of new ROP branch offices and new SIDCCs.

2.3.14.2 The Contractor shall deliver a software package to enable setting up the System at a new ROP branch office or new SIDCC by execution of the software package.

In addition, the Contractor shall provide Project Documentation containing detailed and step-by-step procedures, instructions and technical advice for the installation and running of such software package and extension of the System to the new ROP branch offices or new SIDCCs so that each new office will enjoy the same services provided by the System as available to the other existing ROP branch offices or SIDCCs. As part of the System acceptance process, the software package and the Project Documentation containing instructions on the relevant procedures shall be subject to acceptance by the ImmD. The Contractor shall provide necessary assistance to facilitate the acceptance process.

2.3.15 Storage Format of Fingerprint Images and Templates

2.3.15.1 Tenderers shall propose the solution for the storage of fingerprints in the System in Schedule 4 – "Technical Proposal and System Configuration" of Part V. The proposed solution shall not be locked onto a particular vendor and can change to other fingerprint matching system without having to recall applicants to replace their HKIC or to conduct another conversion exercise. The System shall support the storage of fingerprint image in WSQ[2] format, which is currently stored in SMARTICS.

2.3.15.2 The proposed format for storing the fingerprints shall be non-proprietary so that the Government may select other biometrics technology in the future when necessary.

2.3.15.3 The Contractor shall provide encryption solution to store the fingerprint images and fingerprint templates in the System, including the fingerprint templates to be stored in the chip of new smart identity card.

2.3.15.4 The Contractor shall provide any necessary hardware, software, services and Custom Programs to support the encryption solution and provide the extraction, decryption and matching of fingerprint templates solution for the System, including but not limited to HKIC registration and issuance process, self-service registration kiosks, self-service collection kiosks and self-service general application kiosks.

2.3.15.5 The Contractor shall provide necessary services and Custom Programs to support the extraction, decryption and matching of fingerprint templates solution for the ImmD business operations, including but not limited to automated clearance at control points, self-service kiosks for passport application submission and Macao automated passenger clearance enrolment.

2.3.16 Storage Format of Facial Image

2.3.16.1 The Contractor shall provide all necessary solution to ensure that the facial images to be stored in the disk-based WORM device of IMS will conform to the latest specifications of ICAO 9303.

[2] The Wavelet Scalar Quantization algorithm (WSQ) is a compression algorithm for gray-scale fingerprint images and it has become a standard for the exchange and storage of fingerprint images.

2.3.16.2 The storage of facial image shall be mandatory and be optimally compressed as per the standard specified in report issued by National Institute of Standards and Technology (“NIST”).

2.3.16.3 The facial image shall be interoperable and have sufficient resolution by allowing different face recognition algorithms to undertake matching on the supplied electronic facial data.

2.3.16.4 The facial image stored shall have sufficient resolution to show small features such as moles and scars to facilitate identity verification.

2.3.16.5 Tenderers shall propose the format of digital facial image in conformance with ICAO latest recommendations and other ImmD’s requirements and state in Schedule 4 – “Technical Proposal and System Configuration” of Part V.

3 WORKLOAD REQUIREMENTS

3.1 Tenderer's Responsibility

3.1.1 The System, when integrated with the Systems of other Categories, ITI and other Integral Systems, shall fulfil the workload requirements specified in Section 5 of Part VII and this Section. In order to maintain the high serviceability of the System, the hardware and software for this Category shall be able to sustain the required availability and reliability.

3.2 Contractor's Obligations concerning the Workload Requirements

3.2.1 Capacity Requirements for System Environments

3.2.1.1 The Contractor shall provide sufficient computer resources required for the System to be set up in various system environments to support the purposes of production, development, testing, training and disaster recovery as specified in Part VII and this Annex.

3.2.1.2 The Contractor shall provide sufficient computer resources in terms of disk storage, database instances required for the System.

3.2.1.3 In addition to meeting the workload requirements, the Contractor shall provide additional spare server capacity of at least 50% for all servers in the production environment so as to cater for vertical transaction growth as well as workload surge.

3.2.1.4 For each environment in the non-production environments, the Contractor shall provide required storage capacity of at least 10% of the total storage capacity of the production environment.

3.2.2 Transaction Volumes

3.2.2.1 The hourly peak transaction volumes in year 2018 are projected in Appendix E – "Sizing and Transaction Volume" to Part VII. The System based on the configuration proposed by the Tenderer must be capable to handle transaction volumes as projected in the aforesaid Appendix for at least ten (10) years from the Completion Date, tentatively up to 2028 (on the assumption that the System will first be rolled out in the year of 2018). Information regarding the growth of ROP business is covered in Section 5.2.3 of Part VII and Appendix E – "Sizing and Transaction Volume" to Part VII for Tenderer's reference when calculating projections for subsequent years.

3.2.3 Data Volumes

3.2.3.1 The projected raw data volumes for SMARTICS-2 for the year 2018 and the estimated annual growth rate are listed in Appendix E – "Sizing and Transaction Volume" to Part VII. The System based on the configuration proposed by the Tenderer must be able to handle data volumes as projected in the aforesaid

Appendix for at least ten (10) years after the Completion Date, tentatively up to 2028 (on the assumption that the System will first be rolled out in the year of 2018).

3.2.4 Data Storage

3.2.4.1 The projected transaction volumes and data volumes are described in Appendix E – "Sizing and Transaction Volume" to Part VII. Tenderers shall propose in Table 5-4.1(A) of Schedule 4 – "Technical Proposal and System Configuration" of Part V for the configuration for the IMS to support the existing massive storage of digital images including the documents, photos, fingerprints captured, as well as new digital images to be captured during the territory-wide HKIC replacement exercise for 8.8 million people and the normal daily ROP operation until 2028.

3.2.4.2 For SMARTICS, the assumed number of document pages for each application for normal ROP business is five (5), and one (1) photo and two (2) fingerprints will be captured for each application. The following is the minimum quality metrics of the images in SMARTICS.

Type of Image	**Quality metrics**	**Dimensions**
Document Page	A4, 200 dpi, bi-tonal	11.69 inch x 8.27 inch
Digital Photo	Facial portrait, 1068 x 828 pixels, true colour, support at least 600 dpi output of 1.38 inch x 1.78 inch	1.38 inch x 1.78 inch
Digital Fingerprints	Two thumbprints, 500 dpi, 256 grayscale	1 inch x 1 inch

3.2.4.3 For SMARTICS-2, the assumed number of document pages for each application for normal ROP business is five (5) and that for the replacement exercise is three (3), as derived from past statistics. One (1) photo and two (2) fingerprints will be captured for each application. The following is the minimum quality metrics of the images for SMARTICS-2.

Type of Image	**Quality metrics**	**Dimensions**
Document Page	A4, 300 dpi, 256 grayscale	11.69 inch x 8.27 inch
Digital Photo	Facial portrait, 1200 x 1600 pixels, true colour, support at least 600 dpi output of 1.58 inch x 1.97 inch	1.58 inch x 1.97 inch
Digital Fingerprints	Two thumbprints, 500 dpi, 256 grayscale	1 inch x 1 inch

3.2.4.4 The Contractor shall provide the imaging servers for storing the indices of all digital images and solutions to meet the performance requirements for the System.

3.2.4.5 The Contractor shall provide one more set of similar disk-based WORM storage device and servers in the disaster recovery site for long term off-line archiving.

4 SYSTEM PERFORMANCE REQUIREMENTS

4.1 Tenderer's Responsibility

4.1.1 The System, when integrated with the Systems of other Categories, ITI and other Integral Systems, shall meet the Performance Criteria as specified in Schedule 12 – "Performance Criteria" of Part V for the workload specified in Section 3 of this Annex.

4.1.2 To the extent the Tenderer propose a better system response time than those as specified in Section 4.2.6 or 4.2.7 of this Annex, it shall state, in Schedule 12 – "Performance Criteria" of Part V, the committed system response time for the System. To the extent the Tenderer commits a better system response time (in terms of seconds), that commitment shall be binding and forms part of the Contract (if the Contract is awarded to it) and supersedes the system response time specified below. The Tenderer is not invited to make any change to the definition and calculation of the system response time for each activity as specified below. Any proposed change will be ignored and will not form part of the Contract.

4.2 Contractor's Obligations concerning the System Performance Requirements

4.2.1 References to "System" in this Section mean the System when integrated with the Systems of other Categories, ITI and other Integral Systems. All measurement of the system performance of the relevant activities as specified in this Section shall relate to the System as integrated with the Systems of other Categories, ITI and other Integral Systems. Unless otherwise specified, the system response time set out in this Section for each relevant activity shall apply even if the conduct of the activity requires the operation of the System of other Categories or any part thereof. During the System Acceptance Tests of the System, the system performance of the relevant activities as specified in this Section will be measured when the Load Test, Reliability Test and Overall SMARTICS-2 User Acceptance Tests are conducted.

4.2.2 The elapsed time, defined in this Section shall include the processing time for all the required functions and the delay of all round-trip data transmission on the network.

4.2.3 The System shall not exceed the system response time requirements as documented in the tables below for the peak transaction volume as stated in Appendix E – "Sizing and Transaction Volume" to Part VII as one of the criteria for passing the System Acceptance Tests and also throughout the Transition Period, system nursing period, SIDCC Maintenance Period and Maintenance Period.

4.2.4 Without prejudice to the generality of the above, at least 95% of the system activities of each of the type as mentioned in Sections 4.2.6 and 4.2.7 of this Annex must not exceed the system response time in respect of each Given Period and during the System Acceptance Tests and also throughout the Transition

Period, system nursing period, SIDCC Maintenance Period and Maintenance Period.

4.2.5 The required computer system response time includes the processing time for all the required functions and the delay of all round-trip data transmission on the network. It is assumed that all round-trip data transmission to be one (1) second for transaction without images and three (3) seconds for transaction with images through WAN line.

4.2.6 Online Processing

4.2.6.1 Activities in the System applications in ROP offices and SIDCCs

System Activity	**System Response Time (Seconds)**	**Definition of System Response Time** (Note)
(a) Online update and enquiry function without image retrieval / update	2	The elapsed time between (i) pressing of the "Enter" key (or clicking of the button that is equivalent to submitting a request) and (ii) the appearance of the LAST character of the screen in the next display.
(b) Online update and enquiry function with image retrieval / update	5	The elapsed time between (i) pressing of the "Enter" key (or clicking of the button that is equivalent to submitting a request) and (ii) the appearance of the entire replied image on the screen in the next display.
(c) Enquiry of photo or fingerprint image from disk-based WORM storage device	5	The elapsed time between (i) pressing of the "Enter" key (or clicking of the button that is equivalent to submitting a request) and (ii) the appearance of the entire replied image on the screen in the next display.
(d) Enquiry of document image from disk-based WORM storage device (i) First image of an application	5	The elapsed time between (i) pressing of the "Enter" key (or clicking of the button that is equivalent to submitting a request) and (ii) the appearance of the entire replied image on the screen in the next display.
(ii) Subsequent image of the same application	2	The elapsed time between (i) pressing of the "Enter" key (or clicking of the button that is equivalent to submitting a request)

System Activity	System Response Time (Seconds)	Definition of System Response Time (Note)
		and (ii) the appearance of the entire replied image on the screen in the next display.
(e) Fingerprint capturing	3	The elapsed time between placing the live fingerprint onto fingerprint scanner (enrolment) and the display of enrolment result on screen after the generation of digitised fingerprint image.
(f) Fingerprint verification with database or chip of the smart identity card	4	The elapsed time between placing the live fingerprint onto fingerprint scanner (verification) and the display of verification result on screen.
(g) Fingerprint matching (at Verification Office) against previous record	4	The elapsed time between the issue of command to start fingerprint matching and the display of matching result on screen.
(h) Facial recognition	4	The elapse time between (i) the applicant steps on a designated area in front of the proposed camera and (ii) the return facial recognition result. It includes: ● capture of face image; ● detect liveliness; ● match captured face image with photo stored in chip of new smart identity card; and ● return with facial recognition result.
(i) Face verification with database	2	The elapse time between receiving the face image and returning the 1:1 face matching result.
(j) Photo image capturing by portrait camera	3	The elapsed time between the issue of command to start photo capturing and the completion of the operation.
(k) Scanning of an A4 size paper in 300 dpi 256 grayscale using document scanner	2	The elapsed time between the issue of command to start document scanning and the completion of the operation (excluding warm up time).
(l) Shroff printing	2	The elapsed time between the issue of command to start shroff printing and the actual printing of the first character by document printer.

System Activity	**System Response Time (Seconds)**	**Definition of System Response Time** (Note)
(m) Extra allowance for transaction without image through WAN line	+1	-
(n) Extra allowance for transaction with image through WAN line	+3	-

Note: The system response time is the performance requirement of an end-to-end system activity from user point of view. The Contractor may arrange to run different system processes concurrently in order to achieve a better performance.

4.2.7 Background Processing

4.2.7.1 Activities in the System applications in ROP offices and SIDCCs

	System Activity	**System Response Time (seconds)**	**Definition of System Response Time**
a.	Updating of ROP transactions created in ROP branch offices / SIDCCs to the database server residing in the PDC(KC)	30	The elapsed time between (i) the creation or updating of source information and (ii) the completion of updating of the information at the destination platform.
b.	Synchronisation of user profile in UPMS to ROP branch offices / SIDCCs	300	
c.	Synchronisation of records maintained in CDR to the database residing on the Central Service Layer and Local Service Layer for local mode support	1200	

4.2.7.2 Records such as transaction logs and record created locally shall be uploaded from local repository to central repository for the batch processing so that the batch cycle could be started every night.

5 DATA CONVERSION AND MIGRATION REQUIREMENTS

5.1 Tenderer's Responsibility

5.1.1 The design of the System proposed by Tenderers shall comply with the data conversion and migration requirements set out in this Section 5.

5.2 Contractor's Obligation concerning the Data Conversion and Migration

5.2.1 The Contractor shall be responsible for overall planning, study, design, coordination and provision of data conversion services for converting all data indices, transaction logs, textual data and images of SMARTICS (excluding only those data generated by the CPMS of the Existing Systems which is to be replaced by new CPMS of Category B) and then to migrate such converted data into the System (including the new IMS) including but not limited to, the following:

(a) SMARTICS ROP database in HQ;
(b) SMARTICS ROP database in ROP branch offices;
(c) indices, data and image files, including fingerprints, application forms and photos in IMS and optical libraries of SMARTICS;
(d) SMARTICS ROP database in DSOP;
(e) LDAP database for SMARTICS users;
(f) appointment booking records for SMARTICS in e-Services database; and
(g) identity card records related to applications made prior to the issuance of computerised identity card.

5.2.2 The Contractor shall provide suitable hardware, software, tools, functions and services needed to perform the data conversion and migration. It should be noted that hardware and software items which are provided by the Contractor for the data conversion and migration exercise only, are not to be procured by the Government and shall not be quoted in Schedules 1 and 2 of Part V.

5.2.3 The Contractor shall develop or supply programs with corresponding validation and integrity check to perform the data conversion and migration.

5.2.4 The Contractor shall be responsible to design, develop and implement functions to perform consistency checking at different stages, platforms and environments, as required by the Government, during the data conversion and migration.

5.2.5 The Contractor shall provide hardware, software, tools, develop or supply programs to facilitate users for conducting full data verification.

5.2.6 The Contractor shall work with and directly liaise with the contractors of the Existing Systems to ensure a smooth rollover from the SMARTICS to SMARTICS-2.

5.2.7 The Contractor shall observe the following during the data conversion and migration:

(a) no interruption to existing production services and computer systems;

(b) procedures to reconcile data before and after conversion and migration;

(c) proof of data integrity; and

(d) logs and deliverables for audit trail.

5.2.8 In conjunction with the data conversion and migration plan and switchover plan, the Contractor shall provide the corresponding fallback and recovery procedures and a contingency plan if the exercise cannot be completed within the schedule or completed successfully. The Contractor shall provide fallback services for the execution of the fallback plan to ensure a smooth and quick changeover from the SMARTICS-2 to SMARTICS. The following points shall be addressed in the fallback plan:

(a) identify types of problem (with severity level graded) which may lead to partial fallback or total fallback;

(b) devise decision tables to help classifying each type of problem;

(c) identify functions for supporting the fallback situation and estimate the effort required; and

(d) identify all tasks, personnel, hardware and software required in different fallback situations and activities.

5.2.9 The Contractor shall cater for the data conversion and migration of digitalised images related to identity card records in connection with applications made prior to the issuance of computerised identity card. In carrying out the conversion and migration service, microfiche record containing details of the records in electronic format will be provided to the Contractor and the Contractor shall create indices to link the records to the digital images in the database in order to facilitate speeding retrieval of these identity card image records in connection with applications made prior to the issuance of computerised identity card using same types of retrieval keys as other records enquiry.

5.2.10 The Contractor shall convert and migrate the Chinese characters in SMARTICS ROP databases with reference to the mapping tables defined and provided by the Government.

6 HARDWARE REQUIREMENTS

6.1 Tenderer's Responsibility

6.1.1 Tenderers shall propose in Schedule 1 of Part V all hardware specified in this Section 6 (apart from those excluded in Sections 6.2.2.5.7 and 6.2.2.5.13 of this Annex) and other hardware elsewhere specified in this Annex that it shall be supplied by the Contractor to the Government. All such hardware and their quantity shall comply with all the requirements set out in this Annex including this Section 6.

6.1.2 Whenever it is so specified, the quantities of hardware components as specified in Section 6.2 of this Annex are the minimum quantities required and are subject to review after the Contract award. They are essential requirements which Tenderers shall adhere to when making proposals in the Schedules of Part V and in other parts of their tenders. Tenderers shall exercise their own judgment to determine if higher specifications and / or higher quantities are necessary to ensure that the System will comply with all of the essential requirements notwithstanding the specified minimum quantities. If so, Tenderers shall propose higher quantities of these hardware components according to their expertise and the detailed sizing calculations based on their proposed solution.

6.1.3 Unless and to the extent specified in this Section, any hardware necessary for performing the Implementation Services shall be supplied by the Contractor at its own cost, and shall not be purchased by the Government. The Tenderer may not propose such hardware in Schedule 1 - "Hardware" of Part V including all hardware and facilities required for the Off-site Development Location and Infrastructure specified in Sections 2.3.12.4.1 and 2.3.12.5.1 of this Annex.

6.1.4 Tenderers shall adhere to the requirements set out in Section 17.7 of Part VII and Section 2.3.12.3 of this Annex concerning the environments in which the System shall be implemented.

6.1.5 The whole of Appendix B – "Extract of the Feasibility Study Report on the Implementation of SMARTICS-2" to Part VII forms part of the Contract requirements including the selected technical system options specified in Section 5 of Appendix B.

6.2 Contractor's Obligations concerning the Hardware Component Requirements

6.2.1 General Requirement

6.2.1.1 When implementing the System, the Contractor shall adhere to its proposal in the Schedules of Part V including Schedule 1 – "Hardware" of Part V, and all supplied hardware components and their quantity shall be compliant with all essential requirements set out in this Annex, subject to any modifications as approved or stipulated by the Government in the SA&D stage.

6.2.1.2 If any hardware or quantity thereof is subsequently found to be necessary to ensure that the System complies with the Overall Specifications, Reliability Levels and Performance Criteria, but has not been proposed by the Contractor during the tendering stage, the Contractor shall supply such hardware at its own cost.

6.2.1.3 Section 6.3 of this Annex contains all the specifications for each type of Hardware. Each type of Hardware as proposed by the Tenderer shall comply with these specifications as applicable to that type.

6.2.1.4 The System shall comprise at least the hardware components listed in Section 6.2 of this Annex (apart from those specified in Sections 6.2.2.5.7 and 6.2.2.5.13 of this Annex). The requirements for each individual component are set out in Section 6.3 of this Annex. The distribution and deployments given in Section 6.2 of this Annex are subject to change at the sole discretion of the Government.

6.2.1.5 For the avoidance of doubt, this is not the only Section which contains the requirements applicable to the hardware to be supplied by the Contractor. All provisions in the Contract shall be applicable in accordance with the terms thereof. Without prejudice to the generality of the foregoing, the Sections relevant to the hardware as specified in the last column of each of the tables contained in this Section are not the only Sections which may be relevant. They are only provided for reference purposes. The specific mention of such Sections only shall be without prejudice to the applicability of all other provisions set out in the Tender Documents / Contract which are applicable or otherwise relevant.

6.2.2 Hardware Quantity and Allocation Requirements

6.2.2.1 Network Equipment

6.2.2.1.1 Requirement on the minimum quantities of major network equipment of the System for the ITI MCN, ITI AN, Extended MCN and Local Kiosk Network at individual locations for the production environment:

For Normal ROP Business

Network Equipment	**Minimum Quantity at Location**								**Section no. of related Hardware Specifications**
	HQ	**ROP Branch Office**					**DDC(FL)**	**PDC(KC)**	
		ROP -HK	**ROP -K**	**ROP -KT**	**FTO**	**YLO**			
Edge Router (Large)	-	-	2	2	2	2	-	-	6.3.1.1.2
Distribution Switch (Large)	-	-	-	-	-	-	2	4	6.3.2.1.2
Distribution Switch (Medium)	2	2	2	2	2	2	-	-	6.3.2.1.3
Access Switch (Large)	-	-	-	-	-	-	1	2	6.3.2.2.2
Access Switch (Medium)	32	10	6	6	6	6	5	10	6.3.2.2.3

Network Equipment	Minimum Quantity at Location								Section no. of related Hardware Specifications
	HQ	ROP Branch Office					DDC(FL)	PDC(KC)	
		ROP -HK	ROP -K	ROP -KT	FTO	YLO			
Access Switch (Small)	*	4	4	4	4	4	-	-	6.3.2.2.4
Firewall	*	8	8	8	8	8	*	*	6.3.3.1
Network Module Device	2	-	-	-	-	-	-	-	6.3.4
Load Balancer	*	2	2	2	2	2	*	2	6.3.8

For Territory-wide HKIC Replacement Exercise

Network Equipment	Minimum Quantity at Location									Section no. of related Hardware Specifications
	SIDCC (tentative locations)									
	HKI	KW	KE	TW	TM	YL	SS	ST	TKO	
Edge Router (Large)	2	2	2	2	2	2	2	2	2	6.3.1.1.2
Distribution Switch (Medium)	2	2	2	2	2	2	2	2	2	6.3.2.1.3
Access Switch (Medium)	6	6	6	6	6	6	6	6	6	6.3.2.2.3
Access Switch (Small)	4	4	4	4	4	4	4	4	4	6.3.2.2.4
Firewall	8	8	8	8	8	8	8	8	8	6.3.3.1
Load Balancer	2	2	2	2	2	2	2	2	2	6.3.8

Note: The quantity of network equipment marked as an asterisk (*) shall be proposed by the Tenderer.

Table 7A-6.2.2.1.1 Minimum Quantity of the Major Network Equipment for ITI MCN, ITI AN, Extended MCN and Local Kiosk Network for the Production Environment

6.2.2.1.2 Requirement on the minimum quantities of major network equipment of the System for the ITI AN and General Kiosk Network to support MSK_GEN at individual locations for the production environment:

For Normal ROP Business

Network Equipment	Minimum Quantity at Location						Section no. of related Hardware Specifications
	HQ	ROP Branch Office					
		ROP-HK	ROP-K	ROP-KT	FTO	YLO	
Edge Router (Small)	1	-	1	1	1	1	6.3.1.1.3
Access Switch (MSK_GEN)	1	1	1	1	1	1	6.3.2.2.5

Network Equipment	Minimum Quantity at Location (cont’d)		Section no. of related Hardware Specifications
	DDC(FL)	PDC(KC)	
Edge Router (Large)	1	1	6.3.1.1.2
Access Switch (MSK_GEN)	*	*	6.3.2.2.5

Network Equipment	Minimum Quantity at Location (cont'd)								Section no. of related Hardware Specifications
	Control Point								
	APS	AKA	LWS	HHS	LMC	LSC	MKT	STK	
Edge Router (Small)	1	1	2	1	1	1	1	1	6.3.1.1.3
Access Switch (MSK_GEN)	1	1	2	1	1	1	1	1	6.3.2.2.5

Network Equipment	Minimum Quantity at Location (cont'd)						Section no. of related Hardware Specifications
	Control Point (cont'd)						
	CFT	MFT	SBC	TFT	KCT	HZMB HKBCF	
Edge Router (Small)	1	1	1	1	1	1	6.3.1.1.3
Access Switch (MSK_GEN)	1	1	1	1	1	1	6.3.2.2.5

Network Equipment	Minimum Quantity at Location (cont'd)				Section no. of related Hardware Specifications
	Immigration Office outside HQ				
	HKO	EKO	WKO	STO	
Edge Router (Small)	1	1	1	1	6.3.1.1.3
Access Switch (MSK_GEN)	1	1	1	1	6.3.2.2.5

For Territory-wide HKIC Replacement Exercise

Network Equipment	Minimum Quantity at Location									Section no. of related Hardware Specifications
	SIDCC (tentative location)									
	HKI	KW	KE	TW	TM	YL	SS	ST	TKO	
Edge Router (Small)	1	1	1	1	1	1	1	1	1	6.3.1.1.3
Access Switch (MSK_GEN)	1	1	1	1	1	1	1	1	1	6.3.2.2.5

Note: The quantity marked as an asterisk (*) shall be proposed by the Tenderer.

Table 7A-6.2.2.1.2 Minimum Quantity of the Major Network Equipment for ITI AN and General Kiosk Network for the Production Environment

6.2.2.1.3 Requirement on the minimum quantities of necessary network equipment for the connection of development, testing and training environments:

Network Equipment	Minimum Quantity at Location		Section no. of related Hardware Specifications
	DDC(FL)	HQ	
Distribution Switch (Large)	*	-	6.3.2.1.2
Distribution Switch (Medium)	2	-	6.3.2.1.3
Access Switch (Large)	*	*	6.3.2.2.2

Network Equipment	Minimum Quantity at Location		Section no. of related Hardware Specifications
	DDC(FL)	HQ	
Access Switch (Medium)	2	1	6.3.2.2.3
Access Switch (Small)	2	*	6.3.2.2.4
Access Switch (MSK_GEN)	*	*	6.3.2.2.5
Firewall	2	*	6.3.3.1
Load Balancer	2	-	6.3.8

Note: The quantity marked as an asterisk (*) shall be proposed by the Tenderer.

Table 7A-6.2.2.1.3 Minimum Quantity of the Network Equipment for the Development, Testing and Training Environments

6.2.2.1.4 The training sites will be located in HQ or locations to be designated by the Government and they are attached to development or production network in DDC(FL) such that workstations at the designated location can access the training environment, details will be confirmed by the Government during SA&D stage. To fully utilise the standby resource in DDC(FL), virtual machines for training servers will be hosted on the production physical machines. The Contractor shall provide necessary network equipment for the connection of training environment to MCN at DDC(FL). Access control shall be in place to separate production and training environment.

6.2.2.2 Servers and Storages

6.2.2.2.1 Requirements on the minimum quantities of servers and storages of the System at ROP branch offices and SIDCCs of the Local Service Layer for the production environment:

For Normal ROP Business

Location	Security Zone	Environment	Server Name	Type	Virtualisation	Minimum Quantity per ROP Branch Office	Minimum Quantity for 5 ROP Branch Offices	Section number of related Hardware Specifications
ROP Branch Offices (ROP-HK, ROP-K, ROP-KT, FTO and YLO)	MCN Secured Zone	PROD	Web and Application Server	PC Server	*	**2**	**10**	6.3.7
	MCN Secured Zone	PROD	Workflow Server	PC Server	*	**2**	**10**	6.3.7
	MCN Secured Zone	PROD	Database Server	PC Server	*	**2**	**10**	6.3.7
	MCN Secured Zone	PROD	Report Server	PC Server	*	**2**	**10**	6.3.7
	MCN Secured Zone	PROD	MCN Backup Server	PC Server	*	**1**	**5**	6.3.7
	MCN Restricted Zone	PROD	UPMS Server	PC Server	*	**2**	**10**	6.3.7
	MCN Restricted Zone	PROD	MCN Infrastructure Server	PC Server	*	**2**	**10**	6.3.7
	AN Kiosk DMZ	PROD	Kiosk Web/App/Staging Server	PC Server	*	**2**	**10**	6.3.7
	AN Kiosk DMZ	PROD	AN Infrastructure Server	PC Server	*	**2**	**10**	6.3.7
	MCN Secured Zone	PROD	SAN Switch	Device	**-**	**2**	**10**	6.3.11.2
	MCN Secured Zone	PROD	SAN Storage	Storage	-	**1**	**5**	6.3.11.3.4
	MCN Secured Zone	PROD	Encryption Appliance for SAN	Storage	-	*	*	6.3.11.4
	MCN Secured Zone	PROD	HSM	Storage	-	**2**	**10**	6.3.9
	MCN Secured Zone	PROD	Tape Backup Device	Device	-	**1**	**5**	6.3.11.5.2

For Territory-wide HKIC Replacement Exercise

Location	Security Zone	Environment	Server Name	Type	Virtualisation	Minimum Quantity per SIDCC	Minimum Quantity for 9 SIDCCs	Section number of related Hardware Specifications
SIDCCs (HKI, KW, KE, TW, TM, YL, SS, ST and TKO)	MCN Secured Zone	PROD	Web and Application Server	PC Server	*	**2**	**18**	6.3.7
	MCN Secured Zone	PROD	Workflow Server	PC Server	*	**2**	**18**	6.3.7
	MCN Secured Zone	PROD	Database Server	PC Server	*	**2**	**18**	6.3.7
	MCN Secured Zone	PROD	Report Server	PC Server	*	**2**	**18**	6.3.7
	MCN Secured Zone	PROD	MCN Backup Server	PC Server	*	**1**	**9**	6.3.7
	MCN Restricted Zone	PROD	UPMS Server	PC Server	*	**2**	**18**	6.3.7
	MCN Restricted Zone	PROD	MCN Infrastructure Server	PC Server	*	**2**	**18**	6.3.7
	AN Kiosk DMZ	PROD	Kiosk Web/App/Staging Server	PC Server	*	**2**	**18**	6.3.7
	AN Kiosk DMZ	PROD	AN Infrastructure Server	PC Server	*	**2**	**18**	6.3.7
	MCN Secured Zone	PROD	SAN Switch	Device	-	**2**	**18**	6.3.11.2
	MCN Secured Zone	PROD	SAN Storage	Storage	-	**1**	**9**	6.3.11.3.4
	MCN Secured Zone	PROD	Encryption Appliance for SAN	Storage	-	*****	*****	6.3.11.4
	MCN Secured Zone	PROD	HSM	Storage	-	**2**	**18**	6.3.9
	MCN Secured Zone	PROD	Tape Backup Device	Device	-	**1**	**9**	6.3.11.5.2

Note: Virtualisation and quantity of servers and storages marked as an asterisk (*) shall be proposed by the Tenderer.

Table 7A-6.2.2.2.1 Minimum Quantity of the Major Servers and Storages of the System at ROP Branch Offices and SIDCCs for the Production Environment of the Local Service Layer

6.2.2.2.2 Tenderers may consider integrating backup servers with tape backup device in ROP branch office and SIDCC to save equipment rack space and equipment cost.

6.2.2.2.3 Requirement on the minimum quantities of servers and storages of the System at HQ, PDC(KC) and DDC(FL) of the Central Service Layer for the production environment:

For Normal ROP Business

Security Zone	Environment	Server Name	Type	Virtualisation	Minimum Quantity at Location			Section number of related Hardware specifications
					HQ	PDC(KC)	DDC(FL)	
AN DMZ	PROD	AN Web and Interface Server	PC Server	*	-	**2**	**1**	6.3.7
AN TZ	PROD	AN Infrastructure Server	PC Server	*	-	**2**	**1**	6.3.7
AN TZ	PROD	AN Application and Staging Server	PC Server	*	-	**2**	**1**	6.3.7
AN TZ	PROD	AN Backup Sever	PC Server	*	-	**2**	**1**	6.3.7
MCN Restricted Zone	PROD	IMS Fax Servers	PC Server	*	-	**2**	**1**	6.3.7
MCN Restricted Zone	PROD	Infrastructure Server	PC Server	*	**2**	**2**	**1**	6.3.7
MCN Restricted Zone	PROD	UPMS Server	PC Server	*	**2**	**2**	**1**	6.3.7
MCN Secured Zone	PROD	Infrastructure Server	PC Server	*	-	**2**	**1**	6.3.7
MCN Secured Zone	PROD	Web and Application Server	Midrange	*	-	**2**	**1**	6.3.6
MCN Secured Zone	PROD	Workflow Server	Midrange	*	-	**2**	**1**	6.3.6
MCN Secured Zone	PROD	Report Server	Midrange	*	-	**2**	**1**	6.3.6
MCN Secured Zone	PROD	Batch Processing Server	Midrange	*	-	**2**	**1**	6.3.6
MCN Secured Zone	PROD	Database Server	Midrange	*	-	**2**	**1**	6.3.6
MCN Secured Zone	PROD	IMS Server	Midrange	*	-	**2**	**1**	6.3.6
MCN Secured Zone	PROD	Backup Server	Midrange	*	-	**2**	**1**	6.3.6
MCN Secured Zone	PROD	SAN Router	Device	-	-	**2**	**1**	6.3.11.1
MCN Secured Zone	PROD	SAN Switch	Device	-	-	**2**	**1**	6.3.11.2
MCN Secured Zone	PROD	SAN Storage at PDC(KC)	Storage	-	-	**1**	-	6.3.11.3.2

MCN Secured Zone	PROD	SAN Storage at DDC(FL)	Storage	-	-	-	**1**	6.3.11.3.3
MCN Secured Zone	PROD	Encryption Appliance for SAN	Storage	-	-	*****	*****	6.3.11.4
MCN Secured Zone	PROD	HSM	Storage	-	-	**2**	**2**	6.3.9
MCN Secured Zone	PROD	Disk-based WORM Device	Storage	-	-	**1**	**1**	6.3.10
MCN Secured Zone	PROD	Disk-based Backup System	Storage	-	-	**2**	**1**	6.3.11.6
MCN Secured Zone	PROD	Tape Backup Device	Device	-	-	**1**	**1**	6.3.11.5.1

Note: The virtualisation / quantity marked as an asterisk (*) shall be proposed by the Tenderer.

Table 7A-6.2.2.2.3 Minimum Quantity of the Major Servers and Storages of the System at HQ, PDC(KC) and DDC(FL) for the Production Environment of the Central Service Layer

6.2.2.2.4 Tenderers may consider integrating the features of encryption appliance for SAN into the SAN switch and SAN storage to save the equipment cost and equipment rack space.

6.2.2.2.5 Requirement on the minimum quantities of servers and storages of the System for the non-production environments:

For Normal ROP Business

Location / Security Zone	**Environment**	**Server Name**	**Type**	**Virtualisation**	**Minimum Quantity**			**Section number of related Hardware Specifications**
					Development	**Testing**	**Training**	
DDC(FL) MCN Secured Zone	Development, Testing and Training	Web and Application Server	Midrange	*	**1**	**4**	**1**	6.3.6
DDC(FL) MCN Secured Zone	Development, Testing and Training	Workflow Server	Midrange	*	**1**	**4**	**1**	6.3.6
DDC(FL) MCN Secured Zone	Development, Testing and Training	Report Server	Midrange	*	**1**	**4**	**1**	6.3.6
DDC(FL) MCN Secured Zone	Development, Testing and Training	Batch Processing Server	Midrange	*	**1**	**4**	**1**	6.3.6
DDC(FL) MCN Secured Zone	Development, Testing and Training	Database Server	Midrange	*	**1**	**4**	**1**	6.3.6
DDC(FL) MCN Secured Zone	Development, Testing and Training	IMS Server	Midrange	*	**1**	**4**	**1**	6.3.6
DDC(FL) Secured Zone	Development, Testing and Training	Backup Server	Midrange	*	**1**	**4**	**1**	6.3.6
DDC(FL) AN DMZ	Development, Testing and Training	AN Web and Interface Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL)	Development, Testing	AN Infrastructure	PC Server	*	**1**	**4**	**1**	6.3.7

Location / Security Zone	Environment	Server Name	Type	Virtualisation	Minimum Quantity			Section number of related Hardware Specifications
					Development	Testing	Training	
AN TZ	and Training	Server						
DDC(FL) AN TZ	Development, Testing and Training	AN Application and Staging Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) AN TZ	Development, Testing and Training	AN Backup Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) MCN Restricted Zone	Development, Testing and Training	IMS Fax Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) MCN Restricted Zone	Development, Testing and Training	Infrastructure Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) MCN Restricted Zone	Development, Testing and Training	UPMS Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) MCN Secured Zone	Development, Testing and Training	Infrastructure Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) MCN Secured Zone	Development, Testing and Training	Branch Web and Application Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) MCN Secured Zone	Development, Testing and Training	Branch Workflow Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) MCN Secured Zone	Development, Testing and Training	Branch Database Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) MCN Secured Zone	Development, Testing and Training	Branch Report Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) MCN Secured Zone	Development, Testing and Training	Branch Backup Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) MCN Secured Zone	Development, Testing and Training	Branch UPMS Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) MCN Restricted Zone	Development, Testing and Training	Branch MCN Infrastructure Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) AN Kiosk DMZ	Development, Testing and Training	Branch Kiosk Web / App / Staging Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) AN Kiosk DMZ	Development, Testing and Training	Branch AN Infrastructure Server	PC Server	*	**1**	**4**	**1**	6.3.7
DDC(FL) MCN Secured Zone	Development, Testing and Training	SAN Switch	Device	-	**2**			6.3.11.2
DDC(FL) MCN Secured Zone	Development, Testing and Training	SAN Storage	Storage	-	**1**			6.3.11.3.4
DDC(FL) MCN Secured	Development, Testing and Training	Encryption Appliance for SAN	Storage	-	*****			6.3.11.4

Location / Security Zone	Environment	Server Name	Type	Virtualisation	Minimum Quantity			Section number of related Hardware Specifications
					Development	Testing	Training	
Zone								
DDC(FL) MCN Secured Zone	Development, Testing and Training	HSM	Storage	-	**2**			6.3.9
DDC(FL) MCN Secured Zone	Development, Testing and Training	Disk-based WORM Device	Storage	-	**1**			6.3.10
DDC(FL) MCN Secured Zone	Development, Testing and Training	Disk-based Backup System	Storage	-	**1**			6.3.11.6
DDC(FL) MCN Secured Zone	Development, Testing and Training	Tape Backup Device	Device	-	**1**			6.3.11.5.2

Note: The virtualisation / quantity marked as an asterisk (*) shall be proposed by the Tenderer

Table 7A-6.2.2.2.5 Minimum Quantity of the Major Servers and Storages of the System for the Non-production Environments

6.2.2.2.6 Without prejudice to the generality of the foregoing, Tenderers may consider sharing the usage of SAN storage and SAN related equipment for the non-production and production environments at DDC(FL) to save the equipment cost and equipment rack space, with proper access control to the production and non-production environments to be in place.

6.2.2.3 Equipment Racks and Keyboard-Video-Mouse Switch

6.2.2.3.1 Requirement on the equipment racks:

The floor space to be provided in computer room to accommodate the equipment racks of the System at data centres, HQ, ROP branch offices and SIDCCs is stipulated in Table 7A-6.2.2.3.1. The Contractor shall provide sufficient equipment racks of 42 rack-unit (“RU”) each and make use of the provided floor space to house the proposed equipment. The Contractor shall provide equipment rack space of 21 RU in each computer rooms at ROP branch offices, SIDCCs, PDC(KC) and DDC(FL) to house the hardware equipment provided by the Contractor of Category D.

For Normal ROP Business

Locations	Equipment Rack Space Provided (Qty.)	Section no. of Related Hardware Specifications
ROP Branch Office		6.3.20
ROP-HK	3	
ROP-K	3	
ROP-KT	3	
FTO	3	
YLO	3	
Data Centres and Headquarters		
PDC(KC)	6	

Locations	**Equipment Rack Space Provided (Qty.)**	**Section no. of Related Hardware Specifications**
DDC(FL)	6	
HQ	2	

For Territory-wide HKIC Replacement Exercise

Locations	**Equipment Rack Space Provided (Qty.)**	**Section no. of Related Hardware Specifications**
SIDCC (tentative locations)		6.3.20
HKI	3	
KW	3	
KE	3	
TW	3	
TM	3	
YL	3	
SS	3	
ST	3	
TKO	3	

Note: Available space for equipment rack at PDC(KC) and DDC(FL) maybe updated during SA&D stage.

Table 7A-6.2.2.3.1 Equipment Rack Space Provided in the Computer Rooms at data centres, HQ, ROP Branch Offices and SIDCCs.

6.2.2.3.2 The Contractor shall provide sufficient KVM switch for the proposed equipment in each computer rooms at ROP branch offices, SIDCCs, HQ and PDC(KC) and DDC(FL). The hardware specifications of KVM switch is given in Section 6.3.21 of this Annex.

6.2.2.4 Uninterruptible Power Supply ("UPS")

6.2.2.4.1 Requirement on the UPS equipment:

6.2.2.4.1.1 The Contractor shall provide sufficient UPS equipment in computer rooms at all ROP branch offices and SIDCCs for the equipment to be installed in the computer rooms, including the network components, servers and storage devices and any other major equipment provided by the Contractor to support the production operation of the System. The hardware specifications of UPS is given in Section 6.3.5 of this Annex.

6.2.2.4.1.2 The UPS equipment provided by the Contractor shall have network management module for remote management and support SNMP.

6.2.2.5 Number of Functional Desks, Kiosks and Related Equipment

6.2.2.5.1 The following table sets out the required number of functional desks and kiosks to be set up in each of the ROP branch offices performing the respective business functions for these desks and kiosks as specified in Section 2.3.3 of this Annex:

For Normal ROP Business

Location	Functional Desks and Kiosks													
	Supervisor Desk	Reception Desk	Registration Desk	Assessment Desk	Verification Desk	Shroff Desk	Collection Desk	Mobile Registration / Card Collection Device	Self-service Registration Kiosk (to be provided under Category C)	Self-service Collection Kiosk (to be provided under Category C)	Self-service General Application Kiosk (to be provided under Category C)	Electronic Cabinet for Cards (to be provided under Category C)	Handheld Smart Card Reader	Total
ROP-HK	13	7	43	18	-	3	7	-	-	2	2	1	-	96
ROP-K	19	5	33	15	-	4	6	-	-	2	2	1	-	87
ROP-KT	9	4	17	8	-	2	4	-	-	1	2	1	-	48
FTO	5	3	12	5	-	2	3	-	-	1	2	1	-	34
YLO	5	3	12	5	-	2	3	-	-	1	1	1	-	33
Total	51	22	117	51	-	13	23	-	-	7	9	5	-	298

Table 7A-6.2.2.5.1 Number of the Functional Desks and Kiosks of the System in ROP Branch Offices

6.2.2.5.2 The following table sets out the required number of functional desks and kiosks to be set up in each of the SIDCCs:

For Territory-wide HKIC Replacement Exercise

Location	Functional Desks and Kiosks													
	Supervisor Desk	Reception Desk	Registration Desk	Assessment Desk	Verification Desk	Shroff Desk	Collection Desk	Mobile Registration / Card Collection Device	Self-service Registration Kiosk (to be provided under Category C)	Self-service Collection Kiosk (to be provided under Category C)	Self-service General Application Kiosk (to be provided under Category C)	Electronic Cabinet for Cards (to be provided under Category C)	Handheld Smart Card Reader	Total
SIDCC (tentative location)														
HKI	7	4	25	13	-	-	6	-	19	3	1	1	-	79
KW	7	4	24	12	-	-	5	-	17	3	1	1	-	74
KE	7	4	23	11	-	-	5	-	16	2	1	1	-	70
TW	7	4	21	11	-	-	5	-	15	2	1	1	-	67

Location	Functional Desks and Kiosks													
	Supervisor Desk	Reception Desk	Registration Desk	Assessment Desk	Verification Desk	Shroff Desk	Collection Desk	Mobile Registration / Card Collection Device	Self-service Registration Kiosk (to be provided under Category C)	Self-service Collection Kiosk (to be provided under Category C)	Self-service General Application Kiosk (to be provided under Category C)	Electronic Cabinet for Cards (to be provided under Category C)	Handheld Smart Card Reader	Total
TM	6	3	12	6	-	-	4	-	8	1	1	1	-	42
YL	6	3	14	7	-	-	4	-	10	2	1	1	-	48
SS	6	3	14	7	-	-	4	-	10	2	1	1	-	48
ST	6	4	16	9	-	-	4	-	12	2	1	1	-	55
TKO	6	3	11	5	-	-	4	-	6	1	1	1	-	38
Total	58	32	160	81	-	-	41	-	113	18	9	9	-	521

Table 7A-6.2.2.5.2 Number of the Functional Desks and Kiosks of the System in SIDCCs

6.2.2.5.3 The following table sets out the required number of functional desks and kiosks to be set up in other ImmD offices:

<u>For Normal ROP Business</u>

Location	Functional Desks and Kiosks													
	Supervisor Desk	Reception Desk	Registration Desk	Assessment Desk	Verification Desk	Shroff Desk	Collection Desk	Mobile Registration / Card Collection Device	Self-service Registration Kiosk (to be provided under Category C)	Self-service Collection Kiosk (to be provided under Category C)	Self-service General Application Kiosk (to be provided under Category C)	Electronic Cabinet for Cards (to be provided under Category C)	Handheld Smart Card Reader	Total
ImmD offices at HQ														
Card Personalisation office	9	-	-	-	-	-	-	-	-	-	-	-	-	9

Location	Functional Desks and Kiosks													
	Supervisor Desk	Reception Desk	Registration Desk	Assessment Desk	Verification Desk	Shroff Desk	Collection Desk	Mobile Registration / Card Collection Device	Self-service Registration Kiosk (to be provided under Category C)	Self-service Collection Kiosk (to be provided under Category C)	Self-service General Application Kiosk (to be provided under Category C)	Electronic Cabinet for Cards (to be provided under Category C)	Handheld Smart Card Reader	Total
Verification Office	-	-	-	-	26	-	-	-	-	-	-	-	-	26
System Controller (SS(IT))	9	-	-	-	-	-	-	-	-	-	-	-	-	9
Training Site	2	-	4	-	-	-	-	-	-	-	-	-	-	6
UAT Site	6	2	2	2	2	2	2	2	1	1	1	1	1	25
Offices under ROP Sub-division	77	-	-	-	-	-	-	2	-	-	-	-	-	79
Travel Documents (Issue) Section	3	-	-	-	-	-	-	-	-	-	-	1	-	4
Travel Documents and Nationality (Application) Section	1	-	-	-	-	-	-	-	-	-	-	-	-	1
Control Support Section	2	-	-	-	-	-	-	-	-	-	-	-	-	2
Foreign Domestic Helpers Section	1	-	-	-	-	-	-	-	-	-	1	-	-	2
Extension Section	2	-	-	-	-	-	-	-	-	-	2	-	-	4
Quality Migrants and Mainland Residents Section	1	-	-	-	-	-	-	-	-	-	1	-	-	2
Other Visas and Permits Section	-	-	-	-	-	-	-	-	-	-	1	-	-	1
Employment and Visit Visas Section	1	-	-	-	-	-	-	-	-	-	1	-	-	2
ImmD offices outside HQ														
Investigation Offices in Skyline Tower	9	-	-	-	-	-	-	-	-	-	-	-	25	34
Investigation Offices in Airport	2	-	-	-	-	-	-	-	-	-	-	-	-	2
Immigration – Hong Kong Island Travel Documents Issuing Office	2	-	-	-	-	-	-	-	-	-	1	-	-	3

Location	Functional Desks and Kiosks													
	Supervisor Desk	Reception Desk	Registration Desk	Assessment Desk	Verification Desk	Shroff Desk	Collection Desk	Mobile Registration / Card Collection Device	Self-service Registration Kiosk (to be provided under Category C)	Self-service Collection Kiosk (to be provided under Category C)	Self-service General Application Kiosk (to be provided under Category C)	Electronic Cabinet for Cards (to be provided under Category C)	Handheld Smart Card Reader	Total
Immigration – East Kowloon Office	2	-	-	-	-	-	-	-	-	-	1	-	-	3
Immigration – West Kowloon Office	1	-	-	-	-	-	-	-	-	-	1	-	-	2
Immigration – Sha Tin Office	2	-	-	-	-	-	-	-	-	-	1	-	-	3
Immigration Section of Beijing Office	2	-	-	-	-	-	-	-	-	-	-	-	-	2
Office of the Government of the HKSAR in Guangzhou	2	-	-	-	-	-	-	-	-	-	-	-	-	2
Office of the Government of the HKSAR in Chengdu	2	-	-	-	-	-	-	-	-	-	-	-	-	2
Office of the Government of the HKSAR in Shanghai	2	-	-	-	-	-	-	-	-	-	-	-	-	2
Total	140	2	6	2	28	2	2	4	1	1	11	2	26	227

Table 7A-6.2.2.5.3 Number of the Functional Desks and Kiosks of the System in other ImmD Offices

6.2.2.5.4 The following table sets out the required number of functional desks and kiosks to be set up in control points:

For Normal ROP Business

Location		**Supervisor Desk**	**Self-service General Application Kiosk (to be provided under Category C)**
Control Point	Hong Kong International Airport (Terminal 1) (“APS”)	8	4
	Hong Kong International Airport (Terminal 2) (“AKA”)	2	1

Location		Supervisor Desk	Self-service General Application Kiosk (to be provided under Category C)
	Lo Wu (“LWS”)	7	5
	Hung Hom (“HHS”)	2	2
	Lok Ma Chau (“LMC”)	1	1
	Lok Ma Chau Spur Line (“LSC”)	3	2
	Man Kam To (“MKT”)	2	1
	Sha Tau Kok (“STK”)	2	1
	China Ferry Terminal (“CFT”)	2	2
	Macau Ferry Terminal (“MFT”)	2	2
	Shenzhen Bay (“SBC”)	3	4
	Tuen Mun Ferry Terminal (“TFT”)	3	2
	Kai Tak Cruise Terminal (“KCT”)	2	2
	Hong Kong-Zhuhai-Macao Bridge Hong Kong Boundary Crossing Facilities (“HZMB HKBCF”)	6	6
Total		45	35

Table 7A-6.2.2.5.4 Number of the Functional Desks and Kiosks of the System at Control Points

6.2.2.5.5 The following table sets out the minimum quantities of equipment and peripherals to be installed at each functional desk and each kiosk:

Functional Desk and Kiosk	Major Functions to be Supported		Equipment and peripherals to be installed																	
			Workstation and Monitor (with keyboard)	Additional Monitor (with keyboard)	Additional Monitor	Computer and Touch Screen Monitor	Mobile Device	Chinese Input Device	Slip Printer	OCR Reader	OCR and RFID Reader	Barcode Reader	Smart Card Reader for existing smart identity card	Smart Card Reader for new smart identity card	Document Scanner	Document Printer	Fingerprint Scanner (Enrolment)	Fingerprint Scanner (Verification)	Portrait Camera	ROP140 / ROP140A Automatic Collecting Device
Supervisor Desk	Supervisor Desk functions, Record Maintenance functions, Jury Unit functions,	ROP branch offices, SIDCCs and control points	1	-	-	-	-	1	-	-	-	-	1	1	1	1	-	-	-	-

Functional Desk and Kiosk	Major Functions to be Supported		Equipment and peripherals to be installed																	
			Workstation and Monitor (with keyboard)	Additional Monitor (with keyboard)	Additional Monitor	Computer and Touch Screen Monitor	Mobile Device	Chinese Input Device	Slip Printer	OCR Reader	OCR and RFID Reader	Barcode Reader	Smart Card Reader for existing smart identity card	Smart Card Reader for new smart identity card	Document Scanner	Document Printer	Fingerprint Scanner (Enrolment)	Fingerprint Scanner (Verification)	Portrait Camera	ROP140 / ROP140A Automatic Collecting Device
	ROP Certificate Unit functions, CRU and ITEU functions, MPIC/OPIC functions	Other ImmD offices	1	-	-	-	-	1	-	-	-		-	-	1	1	-	-	-	-
Reception Desk	Reception Desk functions.		1	-	-	-	-	1	-	-	1	1	-	-	-	-	-	-	-	-
Registration Desk	Registration Desk functions	ROP branch offices	1	1	-	-	-	2	-	-	-	1	-	-	1	1	1*	-	1^	-
		SIDCCs	1	1	-	-	-	2	-	-	-	1	-	-	1	1	1*	-	1^	-
Assessment Desk	Assessment Desk functions	ROP branch offices	1	-	-	-	-	1	-	-	-	1	-	-	1	1	-	1	-	-
		SIDCCs	1	-	-	-	-	1	-	-	-	1	-	-	1	1	-	1	-	-
Verification Desk	Verification Desk functions		1	-	-	-	-	1	-	-	-		-	-	1	1	-	-	-	-
Shroff Desk	Shroff Desk functions		1	-	-	-	-	1	-	-	-		-	-	-	1	-	-	-	-
Collection Desk	Collection Desk functions	ROP branch offices	1	-	1	-	-	1	-		-	1	$1^{\#}$	1	-	-	-	1	1	-
		SIDCCs	1	-	1	-	-	1	-	1		1	-	1	-	-	-	1	1	-
Mobile Registration / Card Collection Device	Mobile Registration Unit functions		-	-	-	-	1*^	-	-	-	-	-	-	-	-	-	-	-	-	-
Self-service Registration Kiosk (to be provided under Category C)	Self-service Registration Kiosk functions in SIDCCs		-	-	-	1	-	1	-	1	-	-	1	-	-	1	1*	-	1^	-
Self-service Collection Kiosk (to be provided under Category C)	Self-service Collection Kiosk functions	ROP branch offices	-	-	-	1	-	-	-	-	-	-	-	-	-	-	-	1	1	$1^{\%}$
		SIDCCs	-	-	-	1	-	-	-	-	-	-	1	-	-	-	-	1	1	-
Self-service General Application Kiosk (to be provided under Category C)	Self-service General Application Kiosk functions		-	-	-	1	-	1	1	-	1	-	1	1	-	-	-	1	-	-

* Fingerprint scanner to be installed in registration desks, self-service registration kiosks and fingerprint scanning feature of mobile registration / card collection device shall be capable of the same fingerprint enrolment functions.

# Two workstations in each location of ROP branch offices will be required to be equipped with the facilities to read existing smart identity card at collection desk for supporting the issuance of existing smart identity cards.

^ Portrait camera to be installed in registration desks, self-service registration kiosks and portrait image capturing feature of mobile registration / card collection device shall be capable for the same portrait image capturing functions.

% ROP140 / ROP140A automatic collecting device to be installed in self-service collection kiosk shall be able to provide genuineness checking and automatic collection function of ROP140 / ROP140A as specified in Section 2.3.3.2.23.2 of this Annex.

▨ Cells shaded in grey presents equipment and peripherals that will be acquired by the Government separately.

Table 7A-6.2.2.5.5 Equipment to be Installed at each Functional Desk or each Kiosk

6.2.2.5.6 The following total minimum quantities of equipment and peripherals to be installed in all functional desks and kiosks at all ROP branch offices, SIDCCs and other ImmD offices, control points (as set out in Sections 6.2.2.5.1 to 6.2.2.5.5) shall be complied with and provided by the Contractor of this Category:

For Normal ROP Business

Functional Desk / Kiosk	Equipment and Peripherals to be provided by the Contractor							
	Mobile Device	Smart Card Reader for existing smart identity card	Smart Card Reader for new smart identity card	Fingerprint Scanner (Enrolment)	Fingerprint Scanner (Verification)	Portrait Camera	ROP140 / ROP140A Automatic Collecting Device	Handheld Smart Card Reader
Section no. of Related Hardware Specifications	6.3.22	6.3.14	6.3.13	6.3.15	6.3.16	6.3.18	6.3.27	6.3.19
Supervisor Desk (including Training Site)	-	98	98	-	-	-	-	-
Registration Desk	-	-	-	117*	-	117^	-	-
Registration Desk (Training Site)	-	-	-	4*	-	4^	-	-
Assessment Desk	-	-	-	-	51	-	-	-
Collection Desk	-	10[#]	23	-	23	23	-	-
Mobile Registration / Card Collection Device	2*^	-	-	-	-	-	-	-
Self-service Collection Kiosk	-	-	-	-	-	-	7[%]	-
Other	-	-	-	-	-	-	-	25
Total	2	108	121	121	74	144	7	25

For Territory-wide HKIC Replacement Exercise

Functional Desk / Kiosk	Equipment and Peripherals to be provided by the Contractor							
	Mobile Device	Smart Card Reader for existing smart identity card	Smart Card Reader for new smart identity card	Fingerprint Scanner (Enrolment)	Fingerprint Scanner (Verification)	Portrait Camera	ROP140 / ROP140A Automatic Collecting Device	Handheld Smart Card Reader
Section no. of Related Hardware Specifications	6.3.22	6.3.14	6.3.13	6.3.15	6.3.16	6.3.18	6.3.27	6.3.19
Supervisor Desk	-	58	58	-	-	-	-	-
Registration Desk	-	-	-	160*	-	160^	-	-
Assessment Desk	-	-	-	-	81	-	-	-
Collection Desk	-	-	41	-	41	41	-	-
Self-service Registration Kiosk	-		-	113*	-	113^	-	-
Total	-	58	99	273	122	314	-	-

Notes:

* Fingerprint scanner to be installed in registration desks, self-service registration kiosks and fingerprint scanning feature of mobile registration / card collection device shall be capable of the same fingerprint enrolment functions.

# Two workstations in each location of ROP branch offices will be required to be equipped with the facilities to read existing smart identity cards at collection desk for supporting the issuance of existing smart identity cards.

^ Portrait camera to be installed in registration desks, self-service registration kiosks and portrait image capturing feature of mobile registration / card collection device shall be capable for the same portrait image capturing functions.

% ROP140 / ROP140A automatic collecting device to be installed in self-service collection kiosk shall be able to provide genuineness checking and automatic collection function of ROP140 / ROP140A as specified in Section 2.3.3.2.23.2 of this Annex.

Table 7A-6.2.2.5.6 Equipment to be Provided by the Contractor for Functional Desks or Kiosks

6.2.2.5.7 Tenderers should note that the workstation, monitor, Chinese input device, OCR reader, barcode reader, OCR and RFID reader, document scanner, slip printer, and document printer in production environment for Supervisor Desk, Reception Desk, Registration Desk, Assessment Desk, Verification Desk, Shroff Desk and Collection Desk will be acquired by the Government separately.

6.2.2.5.8 The Contractor shall be responsible to review the equipment and peripherals and provide the specifications of the equipment and peripherals for all functional desks to the Government at SA&D Stage including those mentioned in Section 6.2.2.5.7 of this Annex.

6.2.2.5.9 The Contractor shall provide equipment and peripherals for all functional desks and peripherals for self-service registration kiosks and self-service collection kiosks in UAT site, as the tables below, to facilitate the user acceptance testing.

For Normal ROP Business

Functional Desk / Kiosk	Equipment and Peripherals to be provided by the Contractor in UAT site																		
	Workstation and Monitor (with keyboard)	Additional Monitor (with keyboard)	Additional Monitor	Computer and Touch Screen Monitor	Mobile Device	Chinese Input Device	Slip Printer	OCR Reader	OCR and RFID Reader	Barcode Reader	Smart Card Reader for existing smart identity card	Smart Card Reader for new smart identity card	Document Scanner	Document Printer	Fingerprint Scanner (Enrolment)	Fingerprint Scanner (Verification)	Portrait Camera	ROP140 / ROP140A Automatic Collecting Device	Handheld Smart Card Reader
Section no. of Related Hardware Specifications	6.3.23			-	6.3.22	-	-	6.3.24	6.3.26	6.3.25	6.3.14	6.3.13	6.3.12	6.3.17	6.3.15	6.3.16	6.3.18	6.3.27	6.3.19
Supervisor Desk	6	-	-	-	-	6	-	-	-	-	2	2	6	6	-	-	-	-	-
Reception Desk	2	-	-	-	-	2	-	-	2	2	-	-	-	-	-	-	-	-	-
Registration Desk	2	2	-	-	-	4	-	-	-	2	-	-	2	2	2*	-	2^	-	-
Assessment Desk	2	-	-	-	-	2	-	-	-	2	-	-	2	2	-	2	-	-	-
Verification Desk	2	-	-	-	-	2	-	-	-	-	-	-	2	2	-	-	-	-	-
Shroff Desk	2	-	-	-	-	2	-	-	-	-	-	-	-	2	-	-	-	-	-
Collection Desk	2	-	2	-	-	2	-	2	-	2	2	2	-	-	-	2	2	-	-
Mobile Registration / Card Collection Device	-	-	-	-	2*^	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Self-service Collection Kiosk (to be provided under Category C)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	$1^{\%}$	-
Other	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1
Total	18	2	2	0	2	20	0	2	2	8	4	4	12	14	2	4	4	1	1

For Territory-wide HKIC Replacement Exercise

Functional Desk / Kiosk	Equipment and Peripherals to be provided by the Contractor in UAT site																		
	Workstation and Monitor (with keyboard)	Additional Monitor (with keyboard)	Additional Monitor	Computer and Touch Screen Monitor	Mobile Device	Chinese Input Device	Slip Printer	OCR Reader	OCR and RFID Reader	Barcode Reader	Smart Card Reader for existing smart identity card	Smart Card Reader for new smart identity card	Document Scanner	Document Printer	Fingerprint Scanner (Enrolment)	Fingerprint Scanner (Verification)	Portrait Camera	ROP140 / ROP140A Automatic Collecting Device	Handheld Smart Card Reader
Section no. of Related Hardware Specifications	6.3.23			-	6.3.22	-	-	6.3.24	6.3.26	6.3.25	6.3.14	6.3.13	6.3.12	6.3.17	6.3.15	6.3.16	6.3.18	6.3.27	6.3.19
Self-service Registration Kiosk (to be provided under Category C)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1*	-	1^	-	-

* Fingerprint scanner to be installed in registration desks, self-service registration kiosks and fingerprint scanning feature of mobile registration / card collection device shall be capable of the same fingerprint enrolment functions.

^ Portrait camera to be installed in registration desks, self-service registration kiosks and portrait image capturing feature of mobile registration / card collection device shall be capable for the same portrait image capturing functions.

% ROP140 / ROP140A automatic collecting device to be installed in self-service collection kiosk shall be able to provide genuineness checking and automatic collection function of ROP140 / ROP140A as specified in Section 2.3.3.2.23.2 of this Annex.

Table 7A-6.2.2.5.9 Equipment to be Provided by the Contractor in UAT Site

6.2.2.5.10 Tenderers may consider combining two or more equipment and / or peripherals (as required in Section 6.2.2.5.6 of this Annex) into a single unit of hardware so as to save the equipment cost and space provided that the proposed hardware unit deliver all functions and features for those replaced equipment and / or peripherals, e.g. a smart carder reader that support existing smart identity card and new smart identity card with contactless interface for Supervisor Desk.

6.2.2.5.11 Section 6.2.2.5.10 of this Annex shall equally apply to the equipment and peripherals in UAT site (as required in Section 6.2.2.5.9 of this Annex).

6.2.2.5.12 The Contractor shall provide fingerprint scanner for enrolment purpose and portrait camera for installation in the self-service registration kiosk.

6.2.2.5.13 Tenderers should note that, apart from the equipment and the peripherals described in Section 6.2.2.5.7 of this Annex which will be provided the Government, all equipment and peripherals except fingerprint scanner and portrait camera for self-service registration kiosk, all equipment and peripherals except ROP140 / ROP140A automatic collecting devices for self-service collection kiosk and all equipment and peripherals for self-service general application kiosk and electronic cabinet for cards, including the main metal enclosure, will be provided by the Contractor of Category C.

6.2.2.5.14 The System shall support the number of functional desks and kiosks in ROP offices, SIDCCs, HQ, ImmD offices and control points as specified in this Section 6.2.2.5 to perform the respective business functions.

6.2.2.5.15 The Contractor shall provide a minimum quantity of fifteen (15) workstations for development and testing. The hardware specifications are given in Section 6.3.23 of this Annex.

6.3 **Hardware Specifications**

6.3.1 Network Routers

6.3.1.1 Edge Router

6.3.1.1.1 The equipment shall meet the general specifications set out in this Section.

a. Composition

(i) Shall include at least four (4) 100/1000 Mbps Ethernet ports;

(ii) Shall include at least one (1) USB port(s) for software and configuration file backup and distribution;

(iii) Shall be equipped with redundant power supplies; and

(iv) Shall include at least three (3) spare high-speed WAN interface card slots for future expansion.

b. Compatibility

(i) Shall align with the system configuration of existing network infrastructure specified in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII; and

(ii) Shall be compatible and interoperable with the existing network infrastructure and network equipment specified in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII.

c. Protocol Support

Shall support wide range of IPv4 and IPv6 services and routing protocols, including but not limited to:

(i) Border Gateway Protocol ("BGP");

(ii) Intermediate System-to-Intermediate System ("IS-IS");

(iii) Open Shortest Path First ("OSPF"); and

(iv) Policy-based Routing.

d. IP Multicast

(i) Shall support both IPv4 and IPv6 unicast, multicast and broadcast; and

(ii) Shall support IP Multicast by Protocol Independent Multicast ("PIM").

e. Quality of Service

(i) Shall support modular QoS policies on tunnels or VLANs; and

(ii) Shall support QoS classification based on differentiated services code point (“DSCP”) and application recognised.

f. Management

(i) Shall be manageable by ESM of ITI; and

(ii) Shall support, but not limited to, the following IPv4/v6 management protocols.

- SNMP; and
- Syslog

(iii) Shall support remote management such as Telnet and Secure Shell (“SSH”).

g. Performance

Shall support Internet Protocol Security (“IPSec”), Triple DES (“3DES”) and AES.

h. Availability and Redundancy

Support Virtual Router Redundancy Protocol (“VRRP”) or equivalent router redundant protocol.

i. Security

Shall support security features, including support comprehensive network security features, including but not limited to:

(i) asymmetric encryption with at least 2048-bit key length for RSA or equivalent, and symmetric encryption with at least 256-bit key length for the AES or equivalent;

(ii) hashing with SHA-256 or equivalent;

(iii) access control lists (“ACLs”);

(iv) routing authentication, authorisation, and accounting (“AAA”) / Terminal Access Controller Access-Control System Plus (“TACACS+”);

(v) IPSec;

(vi) SSH Protocol; and

(vii) SNMP.

j. Rack-mountable

(i) Shall be rack-mountable on Electronic Industries Alliance (“EIA”) 19” equipment rack with rack mount kits supplied; and

(ii) Shall be 3 RU or less.

k. Other common features

(i) Shall support IEEE 802.1q VLAN group;

(ii) Shall support User Datagram Protocol (“UDP”) relay service, and permit / deny the relay services by UDP port number;

(iii) Shall support forwarding of UDP broadcast including but not limited to BootP;

(iv) Shall support Dynamic Host Configuration Protocol (“DHCP”) relay that the router can forward DHCP frames;

(v) Shall support Generic Routing Encapsulation (“GRE”) tunnelling over IPSec, 3DES and QoS pre-classification before packets encrypted;

(vi) Shall support Network Time Protocol (“NTP”);

(vii) Shall support Network Address Translation (“NAT”);

(viii) Shall support remote reset of the routers; and

(ix) Shall allow all settings to be viewed and changed through the console port by character terminal or bundled configuration software running on a PC under Microsoft Windows platform.

6.3.1.1.2 Edge router (large) shall meet the specifications in Section 6.3.1.1.1 and this Section:

a. Performance

(i) Shall support at least 800 Mbps IPSec traffic throughput; and

(ii) Shall support maximum routing performance not less than 1500kpps.

6.3.1.1.3 Edge router (small) shall meet the specifications in Section 6.3.1.1.1 and this Section:

a. Performance

(i) Shall support at least 250 Mbps IPSec traffic throughput; and

(ii) Shall support maximum routing performance not less than 500 kpps.

6.3.2 **Network Switches**

6.3.2.1 Distribution Layer Switch

6.3.2.1.1 The equipment shall meet the general specifications set out in this Section.

.

a.	Composition	Shall be equipped with redundant power supply (“RPS”).
b.	Compatibility	(i) Shall align with the system configuration of existing network infrastructure specified in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII; and (ii) Shall be compatible and interoperable with the existing network infrastructure and network equipment of ITI described in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII.
c.	Protocol Support	Shall support wide range of services and routing protocols, including but not limited to OSPF, BGP and Routing Information Protocol (“RIP”).
d.	Quality of Service	Shall support QoS by assigning different priority to data flows and guarantee a certain level of performance for application.
e.	Management	(i) Shall be manageable by ESM of ITI; (ii) Shall support, but not limited to, the following IPv4/v6 management protocols: • SNMP; and • Syslog; (iii) Shall support remote management such as Telnet and SSH; and (iv) Shall support network traffic management, monitoring, and analysis.
f.	Availability and Redundancy	(i) Shall support failover and transparent to mission critical application; and (ii) Shall support load balancing and resilience capabilities.

g. Security

(i) Shall be capable to restrict network port access by static or dynamically learnt MAC address;

(ii) Shall support network security functions, including DHCP snooping, Address Resolution Protocol ("ARP") inspection and traffic storm control; and

(iii) Shall support the creation of access control list which can limit the network access based on layer 3 and 4 information.

h. Software Upgrade

Shall support online / in-service software upgrade without service interruption.

i. Rack-mountable

(i) Shall be rack-mountable on EIA 19" equipment rack with rack mount kits supplied; and

(ii) Shall be 2 RU or less.

j. Performance

(i) Shall support at least 800 Gbps switching capacity; and

(ii) Shall support at least 250 Mpps IPv4 and 125 Mpps IPv6 throughput.

6.3.2.1.2 Distribution switch (large) shall meet the specifications in Section 6.3.2.1.1 and this Section:

a. Composition

(i) Shall include sufficient quantity of SFP+ 10 GE ports with corresponding adapters (i.e. optical modules); and

(ii) Shall include at least two (2) spare SFP+ 10 GE ports with corresponding adapters (i.e. optical modules) for connecting additional switches in future.

6.3.2.1.3 Distribution switch (medium) shall meet the specifications in Section 6.3.2.1.1 and this Section:

a. Composition

(i) Shall include sufficient quantity of SFP+ 10 GE ports with corresponding adapters (i.e. optical modules);

(ii) Shall include at least two (2) spare SFP+ 10 GE ports with corresponding adapters (i.e. optical modules) for connecting additional switches in future;

(iii) Shall include sufficient quantity of SFP and SFP+ ports with corresponding adapters; and

(iv) Shall include at least two (2) spare SFP and SFP+ ports with corresponding adapters (i.e. optical modules) for connecting additional switches and firewalls in future.

6.3.2.2 Access Layer Switch

6.3.2.2.1 The equipment shall meet the general specifications set out in this Section.

a. Composition

Shall have built-in LEDs or other indicators to show the status of every network port and power supply.

b. Compatibility

(i) Shall align with the system configuration of existing network infrastructure specified in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII; and

(ii) Shall be compatible and interoperable with the existing network infrastructure and network equipment and network infrastructure of ITI described in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII.

c. Layer 2 Features Support

(i) Shall support IEEE 802.1s, IEEE 802.1w and IEEE 802.1q VLAN encapsulation;

(ii) Shall support link aggregation technology on uplinks;

(iii) Shall support Link Aggregation Control Protocol ("LACP") that allow the creation of Ethernet channeling with devices that conform to IEEE 802.3ad;

(iv) Shall support jumbo frames on all ports (up to 9216 bytes);

(v) Shall support pause frames (priority flow control (PFC) and IEEE 802.3x); and

(vi) Shall support per-port broadcast, unicast and multicast broadcast storm control for preventing faulty end node from degrading overall system performance broadcast storms.

d. Access Control List — Shall support at least 256 access control entries.

e. Quality of Service — Shall support QoS by assigning different priority to data flows and guarantee a certain level of performance for application.

f. Management

(i) Shall support port mirroring for traffic analysis so that frames being transmitted and received on one switch port can be copied to the other switch port;

(ii) Shall support the following management protocols but not limited to:

- SNMP; and
- Syslog; and

(iii) Shall support remote management such as Telnet and SSH.

g. Availability and Redundancy

(i) Shall be provided with hot-swappable and field-replaceable power supplies and fan modules;

(ii) Shall support power redundancy; and

(iii) Shall support in-service software upgrade.

h. Rack-mountable

(i) Shall be rack-mountable on EIA 19" equipment rack with rack mount kits supplied; and

(ii) Shall be in two (2) RU or less.

i. Other common features

(i) Shall support NTP; and

(ii) Shall support IP Multicast.

6.3.2.2.2 Access switch (large) shall meet the specifications in Section 6.3.2.2.1 and this Section:

a. Composition

(i) Shall include sufficient enhanced small form-factor pluggable (“SFP+”) 10 GE uplink ports with corresponding adapters for connecting to distribution switch; and

(ii) Shall include sufficient SFP+ 10 GE ports which support Fibre Channel over Ethernet ("FCOE") with appropriate transceivers.

b. Performance — Shall support hardware forwarding at least 500 Gbps or 590 million packets per second.

6.3.2.2.3 Access switch (medium) shall meet the specifications in Section 6.3.2.2.1 and this Section:

a. Composition

(i) Shall include sufficient 100/1000 Mbps Ethernet ports for workstation connections;

(ii) Shall include sufficient small form-factor pluggable ("SFP") ports for server connections; and

(iii) Shall include at least four (4) SFP+ 10 GE uplink ports with appropriate transceivers for connecting to the network backbone.

b. Performance — Shall support hardware forwarding at least 170Gbps or 130 million packets per second.

c. Stacking technology — Shall support stacking technology with sufficient units with the following functions:

(i) single management IP address;
(ii) master and slaves; and
(iii) automatic software upgrade through master switch.

6.3.2.2.4 Access switch (small) shall meet the specifications in Section 6.3.2.2.1 and this Section.

a. Composition

(i) Shall include sufficient 100/1000 Mbps Ethernet ports; and

(ii) Shall include sufficient 100/1000 Mbps Ethernet uplink ports.

b.	Performance	Shall support hardware forwarding at least 70 million packets per second.

6.3.2.2.5 Access switch (MSK_GEN) shall meet the specifications in Section 6.3.2.2.1 and this Section.

a.	Composition	(i) Shall include sufficient 100/1000 Mbps Ethernet ports; and (ii) Shall include sufficient 100/1000 Mbps Ethernet uplink ports.

6.3.3 **Firewall**

6.3.3.1 The equipment shall meet the specifications set out in this Section.

a.	Composition	(i) Shall include at least six (6) 10/100/1000 Mbps Ethernet ports; and (ii) Shall include dedicated 10/100/1000 Mbps management port;
b.	Availability and Redundancy	Shall support high availability with active / active and active / standby modes.
c.	Compatibility	(i) Shall support mechanism to assist the measurement of the IP service-level monitoring in the network; (ii) Shall be manageable by the proposed network management system; and (iii) Shall be compatible and interoperable with the network equipment of ITI described in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII.

d. Performance

(i) Shall support stateful inspection with throughput 600 Mbps or more (multi-protocol traffic);

(ii) Shall support 250,000 concurrent connections or more;

(iii) Shall support 15,000 firewall connections per second or more;

(iv) Shall support 250 Mbps AES VPN throughput or more;

(v) Shall support 250 IPsec VPN peers or more; and

(vi) Shall support 100 virtual interfaces (VLANs) or more.

e. Rack-mountable

(i) Shall be rack-mountable on EIA 19" equipment rack with rack mount kits supplied; and

(ii) Shall be in one (1) RU.

f. Management

Shall be manageable by ESM of ITI.

g. Other common features

(i) Shall support NTP; and

(ii) Shall conform to ICSA Firewall evaluation criteria, or Common Criteria Evaluation Assurance Level 4.

6.3.4 Network Module Device

6.3.4.1 The network module device to be installed into ITI distribution switch shall meet the specifications set out in this Section.

a. Composition

Shall include at least twelve (12) ports of 10 Gbps Ethernet ports.

b. Fibre transceivers

Shall include sufficient and appropriate transceivers with SFP+ interfaces for connecting to the proposed distribution switches to ITI.

c. Performance

Shall support at least 48 Gbps per slot capacity.

d. Compatibility

(i) Shall be able to be installed into the module card slot of the existing ITI MCN distribution switch in HQ with details described in Section 3.3.3.2.1.3(a) of Appendix C – "Description of IT Infrastructure of ImmD" to Part VII; and

(ii) Shall be compatible to the existing ITI MCN distribution switch in HQ with details described in Section 3.3.3.2.1.3(a) of Appendix C – "Description of IT Infrastructure of ImmD" to Part VII.

6.3.5 **UPS**

6.3.5.1 The Contractor shall provide sufficient UPS equipment and capacity for the System as stipulated in Section 6.2.2.4.1 of this Annex and meet the specifications set out in this Section.

a. Features / Performance

(i) Shall supply 220V sine wave AC power during normal operation for output voltage;

(ii) Output voltage distortion shall be less than 5% at full load;

(iii) Shall be able to regulate the output voltage against sags, spike;

(iv) Shall support each of the proposed hardware items to be installed for at least 30 minutes after a power supply interruption;

(v) Shall support generating SNMP traps via network; and

(vi) Shall support automatic and manual bypass feature.

b. Monitoring

(i) Shall support the monitoring of the UPS through the network connection;

(ii) Shall provide status display for the status of UPS; and

(iii) Shall provide audible alarm.

c. Others

Shall be rack-mountable on EIA 19" equipment rack with rack mount kits supplied.

6.3.6 Midrange Servers

6.3.6.1 The hardware for midrange servers shall meet the specifications set out in this Section.

a. Form Factor — Shall be rack-mountable on EIA 19" equipment rack with rack mount kits supplied.

b. Processor

(i) Shall support multiple processors (each processor being supported by multiple processor cores) of 64-bit CPU architecture;

(ii) Shall support clock speed at least 3.0 GHz or higher;

(iii) Shall have at least 8 MB shared L3 cache per processor card to deliver high performance;

(iv) Shall support de-allocating the failing processor core from the working system dynamically and have the workload reassigned to other working processors automatically; and

(v) Shall support virtualization technology.

c. Memory — Shall provide at least 64 GB DDR3 RAM.

d. Internal Storage — Shall be provided with at least two (2) dedicated hot swappable internal 10 K rpm or above SAS disks with individual capacity not less than 300 GB for each dedicated server partition, in RAID 1 configuration as internal storage for a single physical server.

e. LAN Interface

(i) Shall support virtualised network adapters for sharing sets of I/O interfaces among partitions with hardware acceleration;

(ii) Shall provide sufficient LAN interfaces containing 100/1000 Mbps Ethernet ports (with RJ45 connectors) and 10GE SFP+ ports supporting network interface hardware resilience;

(iii) Shall provide at least two dedicated 100/1000 Mbps ports and at least two 10GE SFP+ ports in different adapters

		for each of the dedicated server partitions requiring dedicated LAN interfaces; (iv) Shall support link aggregation and adaptive load balancing; (v) Shall support direct and dedicated cable connection between Ethernet ports on server and Ethernet ports on network switches; and (vi) Shall provide at least two (2) sufficient 10/100/1000 Mbps ports or 10 GE SFP+ ports.
f.	Host Bus Adapter (“HBA”) Interface	(i) Shall provide 2 x 8 Gbps or above FC adapters; and (ii) Shall support virtualized network adapters for sharing sets of I/O interfaces among partitions with hardware acceleration; (iii) Shall support cable connection between FC ports on servers and the FC ports on SAN switches.
g.	Virtualisation Technology Features	(i) Shall support server partition technology and provide flexibility to create necessary server partitions; and (ii) Shall be able to support at least two (2) dedicated server partitions with dedicated computing resources. .
h.	Power Supply	Shall include hot-swappable and redundant power supply and cooling fans.
i.	Peripherals	(i) Shall include DVD-ROM, DVD rewritable or DVD-RAM drive; and (ii) Shall include LTO Ultrium 6 or better tape drive for backup and/or restoration.
j.	Availability	Shall include clustering software and clustering feature in active-active or active-passive cluster.
k.	Operating System	Shall support UNIX based architecture.

l.	Expandability	CPU and memory shall support expansion of at least additional 100% memory size for vertical growth and future expansion.
m.	Others	(i) Shall be able to reboot and generate system dump automatically in case of system failure; (ii) Shall include hardware and software to monitor energy usage and to manage power saving dynamically according to the workload; (iii) Shall include clustering software for multiple physical servers and all server partitions for local resilience support; (iv) Shall be bundled with all necessary cables and installation media; (v) Shall include interface ports for KVM connection; and (vi) Shall include at least two (2) USB 3.0 ports or above.

6.3.7 **PC Servers**

6.3.7.1 The hardware for PC servers shall meet the specifications set out in this Section.

a.	Form Factor	Shall be rack-mountable on EIA 19” equipment rack with rack mount kits supplied.
b.	Chipset	Shall support x86 high-end processor or better performance chipset.
c.	Processor	(i) Shall be configured with at least two (2) 10-Core Intel Xeon E5 v3 family processor (or equivalent); (ii) Shall support clock speed at least 2.0 GHz; and (iii) Shall support at least 24 MB L3 cache per processor.
d.	Memory	Shall provide at least 32GB DDR3 RAM.
e.	Internal Storage	(i) Shall provide at least 2 TB of raw capacity; (ii) Shall support RAID 1 data protection; and (iii) Shall have at least two (2) internal SAS hot swap hard disks.

f.	Network Adapter	Shall provide at least four (4) Ethernet ports.
g.	Fibre Channel Host Bus Adapter	(i) Shall provide at least 2 x 8 Gbps or above FC adapters; and (ii) Shall support cable connection between FC ports on servers and the FC ports on SAN switches.
h.	Virtualisation Technology Features	Shall support server partition technology and provide flexibility to create necessary server partitions
i.	Power Supply	Shall include hot-swappable and redundant power supply and cooling fans.
j.	Peripherals	(i) Shall include built-in DVD-ROM, DVD rewritable or DVD-RAM drive; and (ii) Shall include tape drive for backup, restoration.
k.	Availability	Shall include clustering software and clustering feature in active-active or active-passive cluster.
l.	Expandability	CPU and memory shall support expansion of at least additional 100% memory size for vertical growth and future expansion.
m.	Operating System	Shall support various versions of Microsoft Windows on Standard and Datacenter Edition.
n.	Others	(i) Shall include clustering software for multiple physical servers; (ii) Shall be bundled with all necessary cables and installation media; (iii) Shall include interface ports for KVM connection; and (iv) Shall include at least two (2) USB 3.0 ports or above.

6.3.8 Load Balancers

6.3.8.1 The load balancers shall meet the specifications set out in this Section.

a.	Form Factor	Shall be rack-mountable on EIA 19" equipment rack with rack mount kits supplied.

b. Ports

Shall provide at least four (4) Gigabit Ethernet ports.

c. Compatibility

(i) Shall be monitored by ESM of ITI; and

(ii) Shall be compatible and interoperable with the network equipment of ITI described in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII.

d. Feature

(i) Shall perform load balancing based on IP-based protocols;

(ii) Shall support the formation of load balancer pair to allow automatic failover to a standby device;

(iii) Shall support static and dynamic load balancing methods, including round robin, least connection, response time, source & destination persistence hashing, algorithms related to observed or predicted loading and performance of destination servers; and

(iv) Shall provide dual power supply.

e. Performance

(i) Shall support traffic throughput of 5 Gbps;

(ii) Shall support Layer 4-7 traffic load balancing;

(iii) Shall support 100 K Layer-7 requests per second;

(iv) Shall support 60 K Layer-4 connections per second; and

(v) Shall support hardware SSL with 500 SSL TPS.

f. Others

Shall bundle with all necessary cables and accessories.

6.3.9 Hardware Security Module

6.3.9.1 The HSMs shall meet the specifications set out in this Section.

a. Form Factor

(i) Shall be rack-mountable on EIA 19” equipment rack with rack mount kits

			supplied; and
		(ii)	Shall be in 1 RU.
b.	Functions	(i)	Shall provide hardware key storage;
		(ii)	Shall support multiple partitions for independent key storage; and
		(iii)	Shall support cryptographic acceleration.
c.	Tamper resistant		Shall provide intrusion-resistant and tamper-evident features.
d.	Cryptographic algorithms	(i)	Shall support cryptographic APIs, such as PKCS#11, Java Cryptography Architecture / Extension (“JCA” / “JCE”); and
		(ii)	Shall support asymmetric encryption with at least 2048-bit key length for RSA or equivalent, and symmetric encryption with at least 256-bit key length for the AES or equivalent.
e.	Availability and Redundancy	(i)	Shall support high availability feature; and
		(ii)	Shall include at least two (2) network ports.
f.	Security certification		Shall be FIPS 140-2 level 3 or above.

6.3.10 Disk-based WORM device

6.3.10.1 The equipment shall meet the specifications set out in this Section

a.	Compatibility	Shall be monitored by ESM of ITI.
b.	Disk capacity	Shall support storage of data with usable size at least 25 TB in production environment of PDC(KC) and DDC(FL).
c.	File integrity	Shall provide data integrity check.
d.	Access control	Shall provide access control.
e.	Network interface	Shall provide SFP+ 10 GE ports and 10/100/1000 Mbps Ethernet connection.

f.	Data replication	Shall provide automatic data replication from PDC(KC) to DDC(FL).
g.	Disk hot-swapping	Shall support hot-swappable components of disk storage.
h.	Power Redundant Feature	Shall include redundant power supplies.

6.3.11 **Storage and Backup**

6.3.11.1 SAN Router

The equipment shall meet the specifications set out in this Section.

a.	Form Factor	Shall be rack-mountable on EIA 19” equipment rack with rack mount kits supplied.
b.	Fibre Channel ports and Gigabit Ethernet ports	(i) Shall support at least four (4) 8 Gbps FC ports; and (ii) Shall support at least two (2) Gigabit Ethernet ports.
c.	Build-in Feature	(i) Shall support advanced zoning; and (ii) Shall include Fibre Channel over IP (“FCIP”) activation software licences and full fabric activation.
d.	Fibre Channel over IP Tunneling Service	Shall support FCIP tunneling service to extend the SAN connection than the original support distance with the native fibre channel links.
e.	Fibre Channel Attachment	(i) Shall support 8 Gbps and 4 Gbps short wave, long wave and extended distance long wave SFP; (ii) Shall include 8 Gbps and 4 Gbps SFP transceiver for FC connection; (iii) Shall include copper transceiver of GE; (iv) Shall support E Port, EX Port, F Port, FL Port and M Port for fibre channel; and (v) Shall support VE Port (virtual E Port) for FCIP.
f.	Power Supply	(i) Shall include hot-swappable and redundant power supply; and (ii) Shall bundle with all necessary cables.
g.	Administration Interface	Shall include administrative tools for configuration.

h. Compatibility — Shall be compatible and interoperable with the SAN infrastructure of ITI described in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII.

6.3.11.2 SAN Switch

The equipment shall meet the specifications set out in this Section.

a. Form Factor — Shall be rack-mountable on EIA 19" equipment rack with rack mount kits supplied.

b. Compatibility

(i) Shall be monitored by ESM of ITI; and

(ii) Shall be compatible and interoperable with the SAN infrastructure of ITI described in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII.

c. Ports

(i) Shall provide at least 24 ports with activated ports;

(ii) Shall support universal ports self configure as E, F or FL Ports;

(iii) Shall provide fibre-optic cables and be available in various lengths in single-mode and multi-mode formats;

(iv) Shall support hot swappable small form- factor pluggables; and

(v) Shall provide at least four (4) spare activated ports with corresponding adapters for other systems and future expansion.

d. Virtualization — Shall support each host image behind the same physical HBA to connect to an F Port using a unique N Port ID to maximize port usage in a virtualised server environment.

e. Host Attachment

(i) Shall be attachable to and accessible by the proposed encryption appliance for SAN;

(ii) Shall support 8 Gb fibre channel attachment;

(iii) Shall support speed auto-sensing capabilities for providing backward compatibility with 4 Gbps, 2 Gbps and 1 Gbps fibre channel links; and

(iv) Shall support connection to other proposed SAN switches, SAN routers to form a multi-switch fabric for increased connectivity.

f. Maintenance

(i) Support hot-swappable components of SFP optical transceivers, power / fan modules; and

(ii) Support firmware upgrades are designed to be non-disruptive.

g. Redundant Feature

Shall include redundant power supplies.

6.3.11.3 SAN Storage

6.3.11.3.1 The equipment shall meet the specifications set out in this Section.

a. Storage Processor or Controller

Shall include redundant storage controller or processor.

b. Disk

(i) Shall provide hot-swappable FC or SAS disk drive in the capacity of not less than 300 GB with rotational speed 10,000 rpm or above; and

(ii) Shall support the following types of drives:

- solid-state drives or flash drives; and
- FC or SAS.

c. Protection

Shall support RAID 1, 5 and 6 data protection.

d. Compatibility

Shall support the proposed encryption appliance for SAN.

e. Operating System Support — Shall be attachable to and accessible by multiple platforms of the proposed midrange and PC server.

f. Power Supply — Shall support redundant power supply and power input.

g. Host Attachment — Shall include at least eight (8) FC 8 Gbps ports per controller.

h. Management Software and Monitoring — Shall include tools to perform storage management tasks.

i. Others
(i) Shall bundle with all necessary cables; and
(ii) Shall provide necessary rack mount kit.

6.3.11.3.2 SAN storage at PDC(KC) shall meet specifications in 6.3.11.3.1 and this Section.

a. Disk — Shall support storage of data with usable size at least 20 TB.

b. Memory — Shall include at least 16 GB cache, and expandable to at least 64 GB cache per storage controller.

6.3.11.3.3 SAN storage at DDC(FL) shall meet specifications in 6.3.11.3.1 and this Section.

a. Disk — Shall support storage of data with usable size at least 50 TB.

b. Memory — Shall include at least 32 GB cache, and expandable to at least 64 GB cache per storage controller.

6.3.11.3.4 SAN storage at ROP branch offices and SIDCCs shall meet specifications in 6.3.11.3.1 and this Section.

a. Disk — Shall support storage of data with usable size at least 8 TB.

b. Memory — Shall include at least 4 GB cache, and expandable to at least 8 GB cache per storage controller.

6.3.11.4 Encryption Appliance for SAN

6.3.11.4.1 The encryption appliance for SAN shall meet the specifications set out in this Section.

a.	Form Factor	Shall be rack-mountable on EIA 19" equipment rack proposed with rack mount kits supplied.
b.	Functions	Shall support encryption and decryption on the proposed SAN storage device.
c.	Compatibility	Shall be compatible and support the proposed SAN storage.
d.	Cryptographic algorithms	Shall support asymmetric encryption with at least 2048-bit key length for RSA or equivalent, and symmetric encryption with at least 256-bit key length for the AES or equivalent.
e.	Management and Monitoring	Shall provide management console.
f.	Others (desirable)	The encryption appliance for SAN can be proposed to be integrated with the proposed SAN switch or SAN storage, provided that all the security and data privacy requirements of the Government are met.

6.3.11.5 Tape Backup Device

6.3.11.5.1 The equipment shall meet the specifications set out in this Section.

a.	Tape Drive Support	Shall support tape drive of LTO Ultrium 6 or better.
b.	Tape Cartridges	Shall support tape cartridges of LTO Ultrium 6 media or better.
c.	Build-in Feature	(i) Shall include standard barcode reader for sequential or random access mode; (ii) Shall support tape encryption feature; and (iii) Shall include redundant power supply.
d.	Backup speed	Shall support sufficient data transfer rate.

e.	Administration Interface	Shall provide remote management console through a standard web interface.

6.3.11.5.2 Tape backup device in ROP branch offices and SIDCCs shall meet the specifications set out in Section 6.3.11.5.1 and this Section.

a.	Build-in Feature	Shall include at least 24 cartridge slots.

6.3.11.6 Disk-based Backup System

6.3.11.6.1 The equipment shall meet the specifications set out in this Section.

a.	Compatibility	Shall be compatible and interoperable with the proposed midrange and PC servers.
b.	Host Attachment	Shall include sufficient fibre channel ports.
c.	Disk Capacity	(i) Shall fulfil the minimum disk capacity requirement for storage and backup solution stipulated in Section 5.4 – "Data Volume Requirements" of Part VII; and (ii) Shall provide hot swappable disk drive in the capacity.
d.	Disk and data Protection	(i) Shall implement RAID 6 or other RAID level to provide fault tolerance of disk drives; and (ii) Shall support at least 256-bit AES encryption.
e.	Power Supply and connection cables	(i) Shall support redundant power supply and power input; and (ii) Shall bundle with all necessary cables.
f.	Data De-duplication	Shall support data de-duplication.
g.	Remote Replication	Shall support replication concurrently with backup and de-duplication.
h.	Access Control	Shall provide access control.
i.	Physical tape output	Support creation of physical tape from disk.
j.	Operating System and backup software Support	Shall be attachable to and accessible by multiple software platforms to the proposed operating systems.

6.3.12 **Document Scanner**

6.3.12.1 The equipment shall meet the specifications set out in this Section.

a.	Type	Flatbed colour document scanner with automatic duplex document feeder.
b.	Size	Shall support to scan A4 size document.
c.	Optical Scan Resolution	Shall support resolution at least 300 dpi x 300 dpi.
d.	Interface	Shall support USB interface 2.0 or above.
e.	Others	(i) WIA or TWAIN compliant; and (ii) Support standby or sleep mode when idle.

6.3.13 **Smart Card Reader for New Smart Identity Card**

6.3.13.1 The equipment shall meet the specifications set out in this Section.

a.	Contactless interface	(i) Shall provide contactless interface for reading new smart identity card; (ii) Shall support reading contactless cards including but not limited to ISO 14443 Type A and B; and (iii) The reading distance shall be within 10 cm.
b.	Contact interface	(i) Shall provide contact interface for reading new smart identity card; and (ii) Shall be ISO 7816 compliant.
c.	Card face information capturing capability	(i) Shall provide OCR function for reading card face of new smart identity card; and (ii) Shall be able to capture card face information that complied with ICAO specification 9303-Part 3 for authentication.
d.	SAM slot	Shall provide at least one (1) SAM slot.
e.	Indicator for operation status	Shall be able to indicate progress and result of card reading operation by audio or visual signal.
f.	Read / write speed	Shall support read / write speed up to 848 kbps for contactless interface or better.
g.	External I/O Interface	Shall include a USB 2.0 or above interface.

h. Other (desirable)	The smart card reader can be proposed to be integrated with the proposed smart card reader for existing smart identity card, provided that all requirements in both Sections 6.3.13 and 6.3.14 of this Annex (with at least two (2) SAM slots), the security and data privacy requirements of the Government are met.

6.3.14 Smart Card Reader for Existing Smart Identity Card

6.3.14.1 The equipment shall meet the specifications set out in this Section.

a.	Contact interface	(i) Shall provide contact interface for reading chip of existing smart identity card; and (ii) Shall be ISO 7816 compliant.
b.	SAM slot	Shall provide at least one (1) SAM slot.
c.	Indicator for operation status	Shall be able to indicate progress and result of card reading operation by audio or visual signal.
d.	External I/O Interface	Shall include a USB 2.0 or above interface.
e.	Other (desirable)	The smart card reader can be proposed to be integrated with the proposed smart card reader for new smart identity card, provided that all requirements in both Sections 6.3.13 and 6.3.14 of this Annex (with at least two (2) SAM slots), the security and data privacy requirements of the Government are met.

6.3.15 Fingerprint Scanner (Enrolment)

6.3.15.1 The equipment shall meet the specifications set out in this Section.

a. Image resolution	Shall have at least 500 dpi.
b. Image format	(i) Shall support output of fingerprint image in 256 grayscale; and (ii) Shall be able to produce fingerprint image in WSQ format.
c. Indication of operation status	Shall be able to indicate the operation status of the scanner, such as power on, image accepted and image rejected.

d.	Liveliness testing	Shall be able to detect liveliness of the fingerprint.
e.	Fingerprint scan	Shall support flat fingerprint scan.
f.	Anti-spoofing	Shall provide mechanism to detect and prevent spoofing.
g.	External I/O Interface	Shall include a USB 2.0 or above interface.
h.	Control by software	Shall be controllable by software in the workstation.
i.	Security	Shall provide security measures against unauthorised access or theft.

6.3.16 **Fingerprint Scanner (Verification)**

6.3.16.1 The equipment shall meet the specifications set out in this Section.

a.	Image resolution	Shall have at least 500 dpi.
b.	Image format	(i) Shall support output of fingerprint image in 256 grayscale; and (ii) Shall be able to produce fingerprint image in WSQ format.
c.	Indication of operation status	Shall be able to indicate the operation status of the scanner, such as power on, image accepted and image rejected.
d.	Liveliness testing	Shall be able to detect liveliness of the fingerprint.
e.	Fingerprint scan	Shall support flat fingerprint scan.
f.	Anti-spoofing	Shall provide mechanism to detect and prevent spoofing.
g.	External I/O Interface	Shall include a USB 2.0 interface or above.
h.	Control by software	Shall be controllable by software in the workstation.

i.	Security	Shall provide security measures against unauthorised access or theft.
j.	Fingerprint verification	Shall be compatible to software for fingerprint verification specified in Section 7.5.33 of this Annex.

6.3.17 **Document Printer**

6.3.17.1 The equipment shall meet the specifications set out in this Section

a.	Print Mechanism	(i) Laser; and (ii) Shall support automatic duplex printing.
b.	Print speed	Shall be able to print at least 30 ppm.
c.	Resolution	Shall support printing at least 600 dpi x 600 dpi.
d.	Interface	Shall support USB 2.0 interface or above.
e.	Drivers and cable	Shall be able to provide necessary cables, software and driver.

6.3.18 **Portrait Camera**

6.3.18.1 The equipment shall meet the specifications set out in this Section.

a.	Type	(i) Shall be digital camera to capture colour photo; and (ii) Shall be able to produce photo image that meet requirement in Section 3.2.4.3 of this Annex.
b.	File format	Shall be able to produce the photo image in JPEG and RAW formats.
c.	Auto focus	Shall support both auto focus and manual focus features.
d.	Resolution	Shall be two (2) megapixels or above.
e.	Adjustment controls	Shall provide automatic or manual settings to adjust shutter, exposure, aperture, light metering, brightness, contrast, focus and white balance.

f.	Zooming and eye / face detection	Shall provide optical zoom and eye / face detection feature to support sufficient quality photo capturing during ROP registration process.
g.	Indicator for operation status	Shall be able to indicate successful and unsuccessful operation by audio or visual signal.
h.	Flash light	Shall provide flash light.
i.	Mounting and Security	(i) Shall provide mounting to hold the camera; and (ii) Shall provide security measures against unauthorised access or theft.
j.	External I/O Interface	Shall include a USB 2.0 interface or above.

6.3.19 **Handheld Smart Card Reader**

6.3.19.1 The equipment shall meet the specifications set out in this Section.

a.	Processor	Shall provide at least 1 GHz processor.
b.	Internal Storage	Shall provide at least 1 GB flash memory.
c.	Power Supply	(i) Shall support at least eight (8) hours of mobile usage; and (ii) Shall include battery charger per device.
d.	External I/O Interface	Shall include at least one (1) USB port with USB 2.0 or above.
e.	Display	Shall have a display with touch screen function.
f.	Peripheral	(i) Shall bundle with cradle and / or USB cables for workstation connection for battery charging and data transfer; (ii) Shall include smart card reader for reading new smart identity card through contact interface; (iii) Shall include at least one (1) SAM slot; and (iv) Shall include fingerprint scanner for fingerprint scanning and verification specified in Section 6.3.16.
g.	Security	Shall provide data encryption.

6.3.20 Equipment Rack

6.3.20.1 The equipment shall meet the specifications set out in this Section.

a. Dimensions — Shall be with height at most 2130 mm (42 U), width not less than 600 mm, depth not less than 1200mm.

b. Standards — Shall conform to the EIA standard of 19" rack specification.

c. Weight capacity — Shall support at least 200 kg maximum allowable weight of internal components.

d. Grounding — Shall be earthed so that voltages that are induced into cabling (by lightning or other disturbances) are directed to earth.

e. Power strips — Shall come with four (4) sets of 6-way UK13A vertical power distribution units (“PDU”) and four (4) set of cables at least ten (10) meters long, compliant with BS1363 standard.

f. Rails — Shall come with two (2) front and two (2) rear vertical EIA rails, one in each corner of the cabinet, and have EIA universal square-hole pattern.

g. Markings — Shall mark with Unit Identification Markings in every 1 U & 5 U along the Vertical Mounting Angle.

h. Plates — Shall come with at least two (2) supporting plates.

i. Fans — Shall come with one vented top plate with at least three (3) roof mounted AC power cooling fans to meet with the environmental requirements of the equipment inside.

j. Side panels and doors — All side panels, front and rear doors shall come with key-lock. All side panels and doors shall be removable.

k. Front door — The front door shall be made of transparent glass for easy viewing of operation status of equipment inside and with perforate split on both left and right sides for air inflow.

l. Rear door — Shall come with perforated split steel rear door for access improvement and serviceability to rear of rack mounted equipment and better air flow.

m. Stabilisers — Shall come with one (1) heavy-duty and open integral plinth with cable routing and bolt down facility.

n. Cable management — Shall come with cable management brackets / tray to support and constraint data and power cords.

o. Casters — Shall come with caster wheels with locks for movement and fixing of location on the floor.

p. Levelling feet — Shall come with at least four (4) fully adjustable mounting angles for levelling.

q. Accessories

(i) Shall be bundled with sufficient number of accessories, e.g. panel fixings, mounting brackets, etc, to secure all parts of the rack in a proper way; and

(ii) Shall include enough screws, cup washer and cage nut.

r. Others — All the proposed hardware shall be mounted on this proposed rack with reasonable spare space at the back of each equipment for power cables, network cables and optical fibre connections.

6.3.21 **KVM**

6.3.21.1 The KVM shall meet the specifications set out in this Section.

a. General

(i) Shall be KVM switches with at least eight (8) channel ports;

(ii) Shall include built-in display;

(iii) Shall include built-in full-size US / Chinese layout keyboard; and

(iv) Shall include built-in touchpad with buttons control.

b. Compatibility

(i) Shall support to access the console display of all proposed servers; and

(ii) Shall be bundled with all necessary cables including but not limited to, the connection cables for the proposed servers.

c. Rack-mountable

(i) Shall be rack-mountable on EIA 19" equipment rack with rack mount kits supplied; and

(ii) Shall be in 1 RU.

d. Display channel switching

Shall be able to select monitoring channel using either push-button switch, hot keys, or via the on-screen display menu.

6.3.22 **Mobile Device**

6.3.22.1 The mobile device for mobile registration and collection shall meet the specifications set out in this Section.

a. Processor

Shall provide at least 1 GHz.

b. Memory

Shall provide at least 8 GB memory.

c. Display and video card

(i) Shall provide sufficient video display memory; and

(ii) Shall provide video display.

d. Smart Card reader for existing smart identity card

Shall provide smart card reader for reading of existing smart identity card and meet the requirement specified in Section 6.3.14.

e. Smart Card reader for new smart identity card

Shall provide smart card reader for reading of new smart identity card via contact interface and meet the requirement specified in Section 6.3.13b to g.

f. Fingerprint scanner (Enrolment)

Shall provide fingerprint scanner which support verification of fingerprint template for both existing smart identity card and new smart identity card and meet the requirement specified in Section 6.3.15.

g. Fingerprint scanner (Verification)

Shall provide fingerprint scanner which support verification of fingerprint template for both existing smart identity card and new smart identity card and meet the requirement specified in Section 6.3.16.

h. Portrait Camera

Shall provide a portrait camera and meet the requirement specified in Section 6.3.18.1.

i. Document Scanner — Shall provide a document scanner and meet the requirement specified in Section 6.3.12.1.

j. Document Printer — Shall provide a document printer and meet the requirement specified in Section 6.3.17.1.

k. Accessories
   (i) Shall include sufficient USB ports for connecting peripherals for items (d) to (j) and at least one (1) spare USB port;
   (ii) Shall provide keyboard with Chinese Support;
   (iii) Shall provide pointer device (i.e. Touch pad) or better; and
   (iv) Shall provide all necessary components including but not limited to adapters, power cords, cable and other accessories.

l. Others — Shall provide disk encryption feature on local disk.

6.3.23 Workstations for development and testing

6.3.23.1 The workstations for development and testing for ImmD in-house project team(s) shall meet the specifications set out in this Section.

a. Operating System
   (i) Shall include latest version of operating system that support both English and Traditional Chinese; and
   (ii) Shall equip with the latest version of operating system which can be downgradable to previous version.

b. Processor — Shall provide x86 CPU to support development and testing tasks.

c. Memory — Shall provide at least 4 GB memory.

d. Internal Storage — Shall provide at least 500 GB capacity.

e. Disk redundancy — Shall provide disk redundancy feature.

f. Display and video card
   (i) Shall include video adapter; and
   (ii) Shall provide one (1) LCD or LED display at least 21 inch.

g.	Network Adapter		Shall provide at least one (1) 10/100/1000 Base-T Ethernet adapter.
h.	Accessories	(i)	Shall include at least six (6) USB 3.0 ports or above;
		(ii)	Shall provide 104-Key keyboard with Chinese support;
		(iii)	Shall provide 3-button optical wheel mouse or better; and
		(iv)	Shall provide all necessary components including but not limited to adapters, power cords, cable and other accessories.
i.	Others	(i)	Shall support the proposed application development tools; and
		(ii)	Shall provide disk encryption feature on local disk.

6.3.24 **OCR Reader**

6.3.24.1 The equipment shall meet the specifications set out in this Section.

a.	ICAO standard support	Shall be able to capture card face information of existing smart identity card and complied with ICAO specification 9303-Part 1-4 for authentication.
b.	Barcode decode capability	Shall support well known format of symbology 1 dimensional (“1D”) and 2 dimensional (“2D”) barcodes including but not limited to UPC/EAN, PDF417, MicroPDF417 and QR Code.
c.	Indicator for operation status	Shall be able to indicate progress and result of card reading operation by audio or visual signal.
d.	External I/O Interface	Shall include a USB 2.0 interface or above.
e.	Illumination Source	Shall provide UV illumination source.

6.3.25 Barcode Reader

6.3.25.1 The equipment shall meet the specifications set out in this Section.

a.	Decode capability	Shall support well known format of symbology 1D and 2D barcodes including but not limited to UPC/EAN, PDF417, MicroPDF417 and QR Code.
b.	Motion tolerance	Shall provide motion tolerance feature to increase chance of successful scanning.
c.	Interface	Shall provide a USB interface.
d.	Indicator for operation status	Shall be able to indicate progress and result of card reading operation by audio or visual signal.
e.	Other (desirable)	The barcode scanner can be proposed to be integrated with the proposed OCR reader, provided that all the security and data privacy requirements of the Government are met.

6.3.26 OCR and RFID Reader

6.3.26.1 The equipment shall meet the specifications set out in this Section.

a.	RFID reading support	Shall be ISO 14443 A/B compliant.
b.	ICAO standard support	Shall be able to capture card face information that complied with ICAO specification 9303-Part 1-4 for authentication.
c.	Barcode decode capability	Shall support well known format of symbology 1D and 2D barcodes including but not limited to UPC/EAN, PDF417, MicroPDF417 and QR Code.
d.	Indicator for operation status	Shall be able to indicate progress and result of card reading operation by audio or visual signal.
e.	External I/O Interface	Shall include a USB 2.0 interface or above.

6.3.27 ROP140 / ROP140A Automatic Collecting Device (to be installed in self-service collection kiosk)

6.3.27.1 The equipment shall meet the specifications set out in this Section.

a.	Scanning Document	Shall possess the capability to scan the document and produce image(s) to perform genuineness checking on ROP140 / ROP140A mentioned in Section 2.3.3.2.23.2 of this Annex.
b.	Retrieve Information	Shall possess the capability to retrieve information from ROP140 / ROP140A mentioned in Section 2.3.3.2.23.2 of this Annex.
c.	Capturing and Storing Document	Shall be programmable to control the capturing of the paper document into the self-service collection kiosk or return the paper document to the applicants.
d.	Storage	Shall possess storage to store at least 300 paper documents.
e.	Error Detection	Shall be able to detect paper jam, storage full, etc.
f.	Indicator for Operation Status	Shall be able to indicate operation status.

7 SOFTWARE REQUIREMENTS

7.1 Tenderer's Responsibility

7.1.1 Tenderers shall propose in Schedule 2 – "Software" of Part V all necessary software components to be comprised in the System as well as programming tools or platforms for developing and maintaining all Custom Programs. All such software and quantity of software licences shall comply with all the requirements set out in this Annex including this Section 7.

7.1.2 Unless and to the extent specified in this Section, any software necessary for performing the Implementation Services shall be supplied by the Contractor at its own cost, and shall not be sold to the Government. The Tenderer may not propose such software in Schedule 2 – "Software" of Part V including any software required for the Off-site Development Location and Infrastructure specified in Sections 2.3.12.4.1 and 2.3.12.5.1 of this Annex.

7.1.3 Tenderers shall adhere to the requirements set out in Section 17.7 of Part VII concerning the environments in which the System shall be implemented when proposing the quantities of software in Schedule 2 – "Software" of Part V.

7.1.4 The proposed Contractor Supplied Software items shall meet the software requirements as specified in Sections 7.3 to 7.5 of this Annex.

7.1.5 The software items proposed by the Tenderer shall not have an expiry date (i.e. a perpetual licence shall be provided). If there is any licence control mechanism adopted in the Software, such mechanism shall not cause any interruption to the System under all circumstances. Regardless, the Contractor shall be responsible for removing any control which may be triggered under such control mechanism. The Government will not pay any licence fee for such removal unless such licence fee is already quoted and included in the one-time or annual licence fee for the relevant software in the Schedule 23 – "Price Schedule" of Part V.

7.2 Contractor's Obligations Concerning the Software Component Requirements

7.2.1 When implementing the System, the Contractor shall adhere to its proposal in the Schedules of Part V and other parts of its tender (including Schedule 2 – "Software" of Part V), and all supplied software components and quantity of such software must be compliant with all essential requirements set out in this Annex, subject to any modifications as approved or stipulated by the Government in the SA&D stage.

7.2.2 If any software or quantity of software licences is subsequently found to be necessary to ensure the System complies with the Overall Specifications, Reliability Levels and Performance Criteria, but has not been proposed by the Tenderers during the tendering stage, the Contractor shall supply such software and the appropriate quantity of software licences at its own cost.

7.3 General Software Requirements for equipment connected to PC

7.3.1 The Contractor shall provide the necessary software to control all Contractor Supplied Hardware specified in Sections 6.2.2.5.6 and 6.2.2.5.9 of this Annex that are installed on or connected to PC workstations of functional desks and kiosks. If these items of control software are to be called from user-written programs, they shall be in the form of Dynamic Link Libraries ("DLL") files or equivalent formats.

7.3.2 The control software must be able to be invoked from programs written in common language such as C, Visual Basic, .Net, Java, etc. in the Windows environment with latest ISO/IEC-10646 support.

7.3.3 The software specifications of such control software are given in Sections 7.5.21 to 7.5.24, 7.5.28 to 7.5.32 of this Annex. The control software shall be compatible with common software drivers used by these devices.

7.3.4 In addition to the control software, the Contractor shall provide software for fingerprint verification for new template, facial recognition and fingerprint minutiae extraction as required below.

For Normal ROP Business

Functional Desk / Kiosk	Major Functions to be Supported	Fingerprint verification[&] (New template)	Facial recognition	Fingerprint minutiae extraction program
Section no. of Related Software Specifications		7.5.33	7.5.25	-
Registration Desk	Registration Desk functions.	123	123	-
Assessment Desk	Assessment Desk functions.	53	-	-
Verification Desk	Verification Desk functions.	-	-	28
Collection Desk	Collection Desk functions.	25	25	-
Mobile Registration / Card Collection Device	Mobile Registration Unit functions.	4	4	-
Self-service Collection Kiosk	Self-service Collection Kiosk functions	8	8	-
Self-service General Application Kiosk	Self-service General Application Kiosk functions	55	-	-
Handheld Smart Card Reader		26	-	-
e-Channel, self-service kiosks for passport application submission and Macao automated passenger clearance enrolment		1600	-	-
Total		1894	160	28

Note:
& Software required for fingerprint verification of the existing template will be supplied by the Government.

For Territory-wide HKIC Replacement Exercise

Functional Desk / Kiosk	Major Functions to be Supported	Fingerprint verification& (New template)	Facial recognition verification	Fingerprint minutiae extraction program
Section no. of Related Software Specifications		7.5.33	7.5.25	-
Registration Desk	Registration Desk functions.	160	160	-
Assessment Desk	Assessment Desk functions.	81	-	-
Collection Desk	Collection Desk functions.	41	41	-
Self-service Registration Kiosk	Self-service Registration Kiosk functions	114	114	-
Self-service Collection Kiosk	Self-service Collection Kiosk functions	18	18	-
Self-service General Application Kiosk	Self-service General Application Kiosk functions	9	-	-
Total		423	333	-

Note:
& Software required for fingerprint verification of the existing template will be supplied by the Government.

Table 7A-7.3.4 Software and Quantity of Software Licences to be Provided by the Contractor for Functional Desks and Kiosks

7.4 Software Requirements of peripherals for self-service registration kiosks and self-service collection kiosks

7.4.1 The fingerprint enrolment scanner and portrait camera shall be supplied and installed in self-service registration kiosks by the Contractor of this Category whilst kiosks will be provided by the Contractor of Category C. The control software of the fingerprint enrolment scanner and portrait camera to be supplied by the Contractor of this Category shall be compatible and functional with self-service registration kiosks. The specifications of the self-service registration kiosks are given in Section 6.4.3 of Annex C to Part VII.

7.4.2 The ROP140 / ROP140A automatic collecting device shall be supplied and installed in self-service collection kiosks by the Contractor of this Category whilst kiosks will be provided by the Contractor of Category C. The control software to be supplied by the Contractor of this Category for the ROP140 / ROP140A automatic collecting device shall be compatible and functional with self-service collection kiosks. The specifications of the self-service collection kiosks are given in Section 6.4.4 of Annex C to Part VII.

7.5 Software Component Requirements

Section 7.5 contains all the specifications for each type of Software. Each type of Software as proposed by the Tenderer must comply with these specifications as applicable to that type.

7.5.1 Operating System

7.5.1.1 Operating System for Midrange Servers

7.5.1.1.1 The operating system for midrange servers shall meet the specifications set out in this Section.

a.	Compatibility across product line	Shall be 64-bit operating system and support the execution of all the software with application.
b.	System monitoring	Shall be able to monitor processes and perform system performance monitoring.
c.	Multiple session login support	Shall allow multiple sessions login concurrently.
d.	RDBMS support	Shall support the proposed RDBMS for the System.
e.	Remote printing support	Shall support printing by the printers connected to the internal network.
f.	Resilience feature	Shall support the switchover to a standby server.
g.	Disk mirroring software	Shall support disk mirroring function.
h.	LAN support	Shall support the proposed communication / network interface for connection to other UNIX hosts and PC LANs.
i.	NTP support	Shall support NTP.

7.5.1.2 Operating System running on PC Servers

7.5.1.2.1 The operating system running on PC servers shall meet the specifications set out in this Section.

a.	General requirement	Shall fulfil the specifications mentioned in Section 7.5.1.1.1 of this Annex.
b.	Architecture	Shall join the Windows domain of infrastructure server.

7.5.1.3 Operating System running on Infrastructure Servers

7.5.1.3.1 The operating system running on infrastructure servers shall meet the specifications set out in this Section.

a.	General requirement	Shall fulfil the specifications mentioned in Section 7.5.1.1.1 of this Annex.
b.	Architecture	Shall work as Windows domain controller and join the Windows domain of ITI.

7.5.1.4 Operating System running on UPMS Servers

7.5.1.4.1 The operating systems running on UPMS servers shall meet the specifications set out in this Section.

a.	General requirement	Shall fulfil the specifications mentioned in Section 7.5.1.1.1 of this Annex.
b.	Architecture	Shall be compatible and interoperable with the x86 platform of UPMS of ITI; and Shall support the proposed directory service software and user identity management software of UPMS of ITI.

7.5.2 Relational Database Management System (“RDBMS”)

7.5.2.1 The software for RDBMS shall meet the specifications set out in this Section.

a.	Platform Support	Shall be able to run on the proposed midrange and PC server platforms.

b. Features

(i) Shall be a Relational Database Management System;

(ii) Shall support ISO 10646;

(iii) Shall support unicode;

(iv) Shall support ODBC, JDBC, etc. database connectivity;

(v) Shall support Structured Query Language (“SQL”);

(vi) Shall include tools including graphical querying tool, report writer and form designer;

(vii) Shall support active-active or active-passive clustering;

(viii) Shall provide application development capability and built-in program debugger; and

(ix) Shall support exporting table data to an operating system file or tape and support importing the file or tape of table data to the database.

c. Database administration

Shall provide database administration, performance tuning and monitoring tools.

d. High availability

(i) Shall provide clustering functions and features; and

(ii) Shall provide active-active and active-passive cluster.

e. Replication

Shall support data replication.

7.5.3 Software for Web and Application Servers

7.5.3.1 The software for web and application servers shall meet the specifications set out in this Section.

a. Architecture

(i) Shall be able to run on the proposed midrange and PC server platforms; and

(ii) Shall support connection to the proposed software for RDBMS.

b. Standard

Shall support applications development based on open standards, such as XML, SOAP, WSDL and UDDI.

c. Client support

Shall support access from HTML browser via HTTP and TCP/IP.

d. Security standard

(i) Shall support Secure Sockets Layer ("SSL"); and

(ii) Support user and password based authentication.

e. Chinese language support

Shall support ISO 10646 and Unicode.

f. Error logging and diagnosis

(i) Shall capture and storage of error log for further analysis; and

(ii) Shall provide GUI for error logging diagnosis.

g. Administration

Shall provide administration console for status checking and function setting.

7.5.4 Software for Workflow Servers

7.5.4.1 The software for workflow servers shall meet the specifications set out in this Section.

a. Standard support

Shall support Business Process Model and Notation ("BPMN") 1.2 or above.

b. Functions for workflow definition

(i) Shall provide the definition of different processes to support workflow of ROP application mentioned in Section 2.3.3.2 of this Annex; and

(ii) Shall provide allocation of different job roles and user authority, i.e., mapping between users, workstations and steps of processes handled.

c. Workflow capability

(i) Shall provide automatic passing of case work data from one step to another step in a business flow so that no transfer of source documents is required in the office environment;

(ii) Shall provide function of duties segregation handled by different staff;

(iii) Shall provide internal control for enforcing the basic business rules based on certain status of each piece of case work; and

(iv) Shall support ad hoc actions, such as designated users can perform specified tasks and alter workflow.

d. Integration capability

(i) Shall be able to integrate with the application environment of the System; and

(ii) Shall support access to the proposed RDBMS.

e. Performance Monitoring

(i) Shall provide GUI to indicate the real-time status of workflow system; and

(ii) Shall provide reporting, tracking and deadline functionalities.

7.5.5 Software for AN Application and Staging Servers

7.5.5.1 Software for AN application and staging servers shall meet the specifications set out in this Section.

a. Requirements

(i) Shall support secure file transfer protocol for data exchange;

(ii) Shall support SSH protocol 2.0;

(iii) Shall support AES encryption algorithms with at least 256-bit key length;

(iv) Shall support Command-Line Interface (“CLI”);

(v) Shall support batch mode processing;

(vi) Shall support secure transfer with both client and server authentication; and

(vii) Shall support file transfer in encrypted form for processing sensitive data.

7.5.6 Virtualisation Software

7.5.6.1 Server Virtualisation Software (UNIX platform)

7.5.6.1.1 The server virtualisation software (UNIX Platform) shall meet the specifications set out in this Section.

a. General virtualisation

(i) Shall support multiple operating environments on the proposed servers;

feature

(ii) Shall support dynamic allocation of processor, memory and I/O resources among virtual machines (“VMs”);

(iii) Shall support dedicated and shared processor and I/O resources;

(iv) Shall support high availability feature; and

(v) Shall support dynamic allocation of storage capacity so that there is no need for dedicated storage capacity for each virtual machine.

b. Platform support — Shall support operating system on the proposed midrange platform.

c. Remote management — Shall provide remote management client for remote administration control.

7.5.6.2 Server Virtualisation Software (x86 platform)

7.5.6.2.1 The server virtualisation software (x86 Platform) shall meet the specifications set out in this Section.

a. General

(i) Shall support multiple operating environments on the proposed servers;

(ii) Shall support dynamic allocation of processor, memory and I/O resources among VMs;

(iii) Shall support dedicated and shared processor and I/O resources;

(iv) Shall support high availability feature; and

(v) Support dynamic allocation of storage capacity so that there is no need for dedicated storage capacity for each virtual machine.

b. Platform support — Shall support guest OS including but not limited to, the following:

(i) Windows for servers;

(ii) Windows for workstations;

(iii) Enterprise Linux; and

(iv) 32-bit and 64-bit operating systems.

c. Remote management — Shall provide remote management client for remote administration control.

7.5.6.3 Server Virtualisation Management Software (UNIX platform)

7.5.6.3.1 The server virtualisation management software (UNIX platform) shall meet the specifications set out in this Section.

a. General

(i) Shall provide an enterprise, scalable and centralised management hub for managing host and VMs;

(ii) Shall provide real-time monitoring of VM resources; and

(iii) Shall provide a single view pane for real-time performance, capacity and configuration management.

b. Platform support

Shall support the proposed midrange platform.

c. Security

(i) Shall provide customised roles and permissions to enhance security and flexibility with user-defined roles; and

(ii) Shall support audit trails to maintain record of significant configuration changes and the administrator who initiated them.

d. Notification

Shall provide automated notifications and alerts.

7.5.6.4 Server Virtualisation Management Software (x86 platform)

7.5.6.4.1 The server virtualisation management software (x86 platform) shall meet the specifications set out in this Section.

a. General

(i) Shall provide an enterprise, scalable and centralised management hub for managing host and VMs;

(ii) Shall provide real-time monitoring of VM resources; and

(iii) Shall provide a single view pane for real-time performance, capacity and configuration management.

b. Platform support

Shall support platforms for proposed PC servers.

c. Security

(i) Shall provide customised roles and

permissions to enhance security and flexibility with user-defined roles; and

(ii) Shall support audit trails to maintain record of significant configuration changes and the administrator who initiated them.

d. Notification Shall provide automated notifications and alerts.

7.5.7 Middleware

7.5.7.1 The middleware shall meet the specifications set out in this Section.

a. Compatibility Shall support the bi-directional message transfer across all proposed PC and midrange servers and their operating systems.

b. API Shall provide a standardised APIs for performing the basic operations on the message queues in various programming environments.

c. Distribution List Shall support sending a message to more than one destination queue using a dynamic distribution list.

d. Message / Correlation ID Shall support message identification which can be user defined or system generated.

e. Message Priority Shall support an application to assign a priority to a message.

f. Expiration Date Shall be able to specify message expiration date.

g. Clustering Support Shall be able to cluster multiple copies of middleware software.

h. CDS Support Shall support and enable message exchange with CDS provided by ITI.

7.5.8 Backup and Recovery Software

7.5.8.1 Backup and recovery software at ROP branch offices and SIDCCs

7.5.8.1.1 Backup and recovery software for backup servers at ROP branch offices and SIDCCs shall comply with the specifications set out in this Section.

a. Supporting environments to be backed up (i) Shall support hardware proposed for tape backup device specified in Section

6.3.11.5 of this Annex; and

(ii) Shall support the proposed PC server virtualisation software.

b. General

Shall provide the following features:

(i) Shall support backup and recovery for user data, system configuration and database in both dedicated and virtualised server environment;

(ii) Shall support incremental backup of files that have been modified;

(iii) Shall support selective files / folders data restore to another server; and

(iv) Shall support restore database to another server.

c. Fault tolerance

Shall support restart of failing backup and restore at the point of failure.

d. Security

Shall support assign different permission for different roles.

e. User Interface

Shall provide web-based for both administrative and client interfaces.

7.5.8.2 Backup and Recovery Software at PDC(KC) and DDC(FL)

7.5.8.2.1 The backup and recovery software for backup servers at PDC(KC) and DDC(FL) shall meet the specifications set out in this Section.

a. General

Shall provide the following features:

(i) Shall be compatible and support the proposed disk-based backup system specified in Section 6.3.11.6.1 of this Annex;

(ii) Shall support selective files / folders data restore to another server; and

(iii) Shall support restore database to another server.

b. Fault tolerance

Shall support restart of failing backup and restore at the point of failure.

c.	Security	Shall support assign different permission for different roles.
d.	User Interface	Shall provide web-based for both administrative and client interfaces.

7.5.9 **Software for IMS**

7.5.9.1 The software of image management software for handling image indexes and controlling permanent massive storage device shall meet the specifications set out in this Section.

a.	Administration	Shall provide administration console for status checking.
b.	Features	Shall provide functions specified in Section 2.3.3.2.31 of this Annex.
c.	User authentication	Shall support user authentication using username and password.

7.5.10 **Software for Disk-based WORM Storage Device**

7.5.10.1 The software for disk-based WORM storage device shall meet the specifications set out in this Section.

a.	Administration	Shall provide administration console for status checking and function setting on disk-based WORM device.
b.	Security control	Shall support access control and file integrity functions of disk-based WORM storage device stated in Section 6.3.10.1 of this Annex.
c.	User authentication	Shall support user authentication using username and password.

7.5.11 **Host-based IDS software(s)**

7.5.11.1 The host-based IDS software(s) shall meet the specifications set out in this Section.

a.	General	Shall provide the following functions to protect

computer systems against attacks:

(i) monitoring network or system activities for malicious activities or security policy violations;

(ii) identifying threats; and

(iii) generating alerts for administrative actions.

7.5.12 **Software for reporting server**

7.5.12.1 The software for reporting server shall meet the specifications set out in this Section.

a.	Report printing	Shall be able to generate page based report and support page size of A4 and letter.
b.	Data source and output format	(i) Shall be able to generate report to PDF; and (ii) Shall provide GUI for report format design.
c.	Administration	(i) Shall provide a web-based report management console for administration; and (ii) Shall be able to provide version control for report.
d.	Operating system support	Shall compatible with operating system specified for report server.

7.5.13 **Software for batch processing server**

7.5.13.1 The software for batch processing server shall meet the specifications set out in this Section.

a.	Request handling	Shall be able to monitor request from staging server, process the request and return result back to staging server.
b.	Operating system support	Shall be compatible with operating system specified for batch processing server.
c.	Job prioritisation	Shall be able to set job sequence and parallel job running.

7.5.14 Software for Directory Service

7.5.14.1 The software item(s) shall support the functionalities of UPMS of ITI including:

(a) directory service; and

(b) user identity management

7.5.14.2 The proposed directory service software shall be used to form the local profile repositories of UPMS with data structure that can facilitate the storage and manipulation of user and profile information for UPMS in immigration offices.

7.5.14.3 The software item(s) shall be compatible with the respective components of UPMS of ITI.

7.5.14.4 The software item(s) shall be compatible and interoperable with the UPMS of ITI described in Appendix C – "Description of IT Infrastructure of ImmD" to Part VII.

7.5.15 Software for Infrastructure Server

7.5.15.1 The software item(s) for infrastructure server shall provide the following functions:

(a) Domain Name System;

(b) Dynamic Host Configuration Protocol;

(c) Network Time Protocol; and

(d) Active directory / domain controller.

7.5.16 Software for ESM

7.5.16.1 The software of ESM shall provide the following functions:

(a) event management;

(b) system monitoring;

(c) software distribution;

(d) asset management;

(e) software for remote operation; and

(f) network management software.

7.5.16.2 The software shall support dedicated servers, virtualised servers, workstations for development and testing and network equipment.

7.5.16.3 The software item(s) shall be compatible with the respective components of ESM of ITI.

7.5.17 Application Development Tools (“ADT”)

7.5.17.1 The application development tools shall meet the specifications set out in this Section.

a. Application support — Shall support Java application development, such as Java Development Kit (“JDK”), JDBC, Java Servlet, Java Server Page (“JSP”), Enterprise Java Beans (“EJB”) and other application development languages.

b. Web services application development support — Shall support developing web services application.

c. Development support

(i) Shall support visual programming tools, screen editor and debugger; and

(ii) Shall include compiler to generate executable code.

7.5.18 Software for Workstations for Development and Testing

7.5.18.1 The software for workstations for development and testing shall meet the specifications set out in this Section.

a. General

(i) Shall include latest versions of operating systems that support English and Traditional Chinese language and support both 64-bit and 32-bit platforms;

(ii) Shall include word processing software licence;

(iii) Shall support hardware disk encryption feature mentioned in Section 6.3.23 of this Annex;

(iv) Shall include anti-virus software and ESM software licence; and

(v) Shall include Microsoft Windows Server Client Access Licenses (“CAL”) licence.

7.5.19 Testing Automation Tools

7.5.19.1 The testing automation tool shall meet the specifications set out in this Section.

a. Test case capturing — Shall be able to capture, store and replay user interactions of an application automatically.

b. Test case editing

Shall be able to edit and change the test case without recreating the whole testing scenario.

c. Workload simulation

Shall be able to generate huge workload to simulate peak load scenarios.

d. Check items highlighting

Shall be able to highlight check items with actual results different from expected results.

e. Test result analysis

Shall provide interactive reporting tools for presenting test results in different level of details to facilitate analysis.

f. Test case maintenance

Shall provide centralised repository for storing test cases and allow modification of the test cases to suit the modified application.

g. Data-driven test support

Shall support the input of multiple values for specified variables to simulate multiple test scenarios.

h. Clustering support

Shall be able to replay the test scenario in multiple machines concurrently.

i. Single point monitoring

Shall be able to control and monitor the testing running in multiple machines with one single control panel or workstation.

j. Check items definition

Shall be able to define and edit check items e.g. value of text to be displayed.

7.5.20 Software for Version Control

7.5.20.1 The software for version control shall meet the specifications set out in this Section.

a. Compatibility

Shall be compatible with the proposed software for application services and the application development tools.

b. Change log

Shall be able to keep track changes to files, e.g. user name and time stamp.

c. Storage and retrieval

(i) Shall be able to store / retrieve file revisions; and

(ii) Shall be able to restore a project to an earlier labelled release.

d.	File and version comparison	Shall be able to compare files to earlier version and compare versions to other versions.
e.	Merge	Shall be able to merge edits made to the same revision.
f.	Audit trail report	Shall provide audit trail for revision.

7.5.21 Control Software for Fingerprint Scanner (Enrolment)

7.5.21.1 The control software for fingerprint scanner (enrolment) shall meet the specifications set out in this Section.

a.	Functions to be provided	Shall support the proposed fingerprint scanner (enrolment) specified in Section 6.3.15.1 of this Annex.

7.5.22 Control Software for Fingerprint Scanner (Verification)

7.5.22.1 The control software for fingerprint scanner (verification) shall meet the specifications set out in this Section.

a.	Functions to be provided	Shall support the proposed fingerprint scanner (verification) specified in Section 6.3.16.1 of this Annex.

7.5.23 Control software for Document Scanner

7.5.23.1 The control software for document scanner shall meet the specifications set out in this Section.

a.	Functions to be provided	Shall support the proposed document scanner specified in Section 6.3.12.1 of this Annex.

7.5.24 Control software for Portrait Camera

7.5.24.1 The control software for portrait camera shall meet the specifications set out in this Section.

a.	Functions to be provided	Shall support the proposed portrait camera specified in Section 6.3.18 of this Annex.

7.5.25 **Software for Facial Recognition**

7.5.25.1 The software for facial recognition shall meet the specifications set out in this Section.

a.	Face detection	(i)	Shall support automatic face detection without user input; and
		(ii)	Shall support adjustable face parameters.
b.	Face image	(i)	Shall support functions of capturing human faces, into image;
		(ii)	Shall be able to verify captured image with the image from chip of new smart identity card; and
		(iii)	Shall support ISO 19794-5 format.
c.	Facial recognition	(i)	Shall support one-to-one facial verification; and
		(ii)	Shall support facial recognition from different sources including camera and live video.
d.	Development support		Shall include software development kit with API.
e.	Accuracy		FRR shall be 3% or less when FAR shall be at 0.1% or less.

7.5.26 **Software for Handheld Smart Card Reader**

7.5.26.1 The software for the handheld smart card reader shall meet the specifications set out in this Section.

a.	Requirements	(i)	Shall be built in with an operating system;
		(ii)	Shall contain an anti-virus function; and
		(iii)	Shall support the use of handheld smart card reader specified in Section 6.3.19.1 of this Annex.

7.5.27 **Anti-virus Software**

7.5.27.1 The software for anti-virus shall meet the specifications set out in this Section. Anti-virus solution of ITI is described in Appendix C – “Description of IT Infrastructure of ImmD” to Part VII.

a.	Requirements	(i)	Shall integrate with the anti-virus solution deployed by ITI;
		(ii)	Shall be compatible and support the proposed midrange, PC servers, workstations, mobile device and handheld smart card reader; and

(iii) Shall provide anti-virus management software that integrate with ITI.

7.5.28 Control Software for Mobile Device

7.5.28.1 The software for control software for mobile device shall meet the specifications set out in this Section.

a. Requirements	Shall support the use of mobile device specified in Section 6.3.22.1 of this Annex.

7.5.29 Control Software for OCR Reader

7.5.29.1 The software for control software for OCR reader shall meet the specifications set out in this Section.

a. Requirements	Shall support the use of OCR reader specified in Section 6.3.24.1 of this Annex.

7.5.30 Control Software for OCR and RFID Reader

7.5.30.1 The software for control software for OCR and RFID reader shall meet the specifications set out in this Section.

a. Requirements	Shall support the use of OCR and RFID specified in Section 6.3.26.1 of this Annex.

7.5.31 Control Software of Smart Card Reader for Existing Smart Identity Card

7.5.31.1 The software for control software of smart card reader for existing smart identity card shall meet the specifications set out in this Section.

a. Requirements	Shall support the use of smart card reader for existing smart identity card specified in Section 6.3.14.1 of this Annex.

7.5.32 Control Software of Smart Card Reader for New Smart Identity Card

7.5.32.1 The software for control software of smart card reader for new smart identity card shall meet the specifications set out in this Section.

a. Requirements	Shall support the use of smart card reader for new smart identity card specified in Section 6.3.13.1 of this Annex.

7.5.33 Software for Fingerprint Verification

7.5.33.1 The software for fingerprint verification shall meet the specifications set out in this Section.

a.	Requirements	(i)	Shall support the use of fingerprint verification services mentioned in Section 2.3.8.5 of this Annex;
		(ii)	Shall support the use of fingerprint scanner (verification) specified in Section 6.3.16.1; and
		(iii)	Shall be compatible and interoperable to current business services provided by the ImmD including but not limited to e-Channel, self-service kiosks for passport application submission and Macao automated passenger clearance enrolment.
b.	Fingerprint template format	(i)	Shall support to generate both new fingerprint template format provided by Contractor and ANSI-INCITS 378 format;
		(ii)	Shall support to store the live-captured fingerprint image into the workstation when the system runs in standalone workstation mode; and
		(iii)	Shall be able to extract fingerprint template minutiae.
c.	FAR		Shall be less than 0.1%.
d.	FRR		Shall be less than 0.01%.

7.5.34 Software for ROP140 / ROP140A Automatic Collecting Device

7.5.34.1 The software for ROP140 / ROP140A shall meet the specifications set out in this Section.

a.	Requirements	Shall support the use of ROP140 / ROP140A automatic collecting device mentioned in Section 6.3.27.1 of this Annex.

7.6 Requirements for the Custom Programs

7.6.1 The Contractor shall develop Custom Programs for the new automatic fingerprint extraction and verification functions in the System as stipulated in Section 2.3.8.5.9 of this Annex. All the source codes, including the fingerprint template minutiae extraction and fingerprint verification algorithms shall be delivered to the Government on the System Acceptance Date or upon the request of the Government. The Contractor shall provide to the Government for exclusive use of the proposed automatic fingerprint verification function for both historical fingerprint image in IMS and live captured fingerprint.

7.6.2 The Contractors shall design and implement Custom Programs to enable setting up the System to fulfil the Overall Specifications, Performance Criteria and Reliability Levels. The Contractor shall deliver to the Government the source, object and command codes of the Custom Programs in hardware-readable form, and the full documentation of the Custom Programs such as program specification(s) on the System Acceptance Date.

7.6.3 The Contractor shall be responsible for the design of the interfaces specifications between the System and the Systems of other Categories, and shall take on the role of Prime System Integrator for the proper integration of SMARTICS-2 comprising the systems of all Categories and other Integral Systems, as described in Section 2.3.2.12 of this Annex.

8 RESILIENCE AND DISASTER RECOVERY REQUIREMENTS

8.1 Tenderer's Responsibility

8.1.1 Tenderers shall propose all the hardware, software, custom programs, configuration of resilience equipment and systems to ensure compliance with the resilience and disaster recovery requirements as stated in the Contract including this Annex for the System.

8.1.2 Tenderers shall propose sufficient resilience provisions to ensure there is no single point of failure and to ensure the System to achieve the serviceability level as specified in Schedule 13 – "Reliability Specifications" of Part V.

8.1.3 Tenderers shall describe in Schedule 4 – "Technical Proposal and System Configuration" of Part V the design for switchover, local mode and standalone mode processing.

8.1.4 Tenderers shall describe in Schedule 4 – "Technical Proposal and System Configuration" of Part V the system backup and recovery approach and the estimated backup and recovery time for the System.

8.1.5 Tenderers shall describe in Schedule 4 – "Technical Proposal and System Configuration" of Part V the data backup and recovery approach and the committed backup and recovery time for the System.

8.1.6 Tenderers shall provide a description of methodology to carry out the disaster recovery plan in Schedule 14 – "Implementation Services" of Part V for recovering the System in the event of catastrophic system failure.

8.1.7 Tenderers may propose additional provisions without additional cost to improve resilience for Central Service Layer, Local Service Layer, WAN and remote access services in Schedule 4 – "Technical Proposal and System Configuration" of Part V.

8.1.8 Tenderers shall make use of the resilience and disaster recovery provisions provided by the Government as described in Section 8.2 of this Annex to propose the system configuration for resilience and recovery procedures.

8.2 Resilience and Disaster Recovery Provisions provided by the Government

8.2.1 Data Centre for System Production

8.2.1.1 The PDC(KC) will be used to accommodate the computing equipment and most of the backbone and wide area network equipment to support the production environment for the System. The resilience provision in the PDC(KC) includes UPS, Emergency Power Generator ("EPG") and air-conditioning system with backup cooling capacity.

8.2.2 Data Centre for System Development and Resilience

8.2.2.1 The DDC(FL) will be used to accommodate the network and computing equipment to support the resilience and DR environment which offers resilience and contingency services when the accessibility to the services in the PDC(KC) is lost or during disaster situation. The DDC(FL) will also serve as the non-production environment, including but not limited to, development and testing environments for the System. The resilience provision in the DDC(FL) includes UPS, EPG and air-conditioning system with backup cooling capacity.

8.3 Resilience and Disaster Recovery Requirements

8.3.1 The Contractor shall provide the System with resilience and disaster recovery facilities to safeguard service levels in case of a localised failure of system components and to ensure basic survival of vital business processes in a disaster situation.

8.3.2 The resilience level of the Central Service Layer and Local Service Layer and of the overall network for the System shall be better than or at least the same as the SMARTICS from all aspects. Details of these existing systems are described in Appendix A – "Description of Existing Systems" to Part VII.

8.3.3 Common Data Repository and Down-sized Open Platform

8.3.3.1 The resilience and disaster recovery design of the System shall make use of the resilience and disaster recovery facilities of the CDR and DSOP of the ITI Service Layer.

8.3.4 Central Service Layer

8.3.4.1 The Contractor shall ensure that there is no single point of failure for the Central Service Layer for the System.

8.3.4.2 To meet the high availability requirement of the Central Service Layer, a high availability system to be implemented at the ITI MCN and AN in PDC(KC). The HA configuration can be active-active and active-passive. In the event that a node is unavailable, another node shall be able to take over and continue to provide the services of the failed node. No matter which HA mode is implemented, the switchover time from primary to standby server shall be less than three (3) minutes.

8.3.4.3 In case the Central Service Layer at PDC(KC) is unavailable, the server(s) in the DDC(FL) shall be able to take up the production services **within one (1) hour or such shorter time** ("committed system switch over time") as committed by the Contractor in Schedule 12 – "Performance Criteria" of Part V. To the extent the Tenderer commits a shorter time, the Tenderer shall specify in Schedule 12 – "Performance Criteria" of Part V the committed shorter switch over time from Central Service Layer to the backup server(s) at the DDC(FL). In addition, subsequent production data replication from DDC(FL) to PDC(KC) shall be completed after service in PDC(KC) resume normal.

8.3.4.4 Data replication of the CDR between CDR distributor in data centres and local copy of CDR database in ROP branch offices and SIDCCs shall be completed every four (4) hours, subject to the confirmation by the Government during SA&D stage.

8.3.5 Local Service Layer

8.3.5.1 The Local Service Layer at ROP branch offices and SIDCCs for the System shall always be operative to perform SMARTICS-2 functionalities without performance degradation, without any single point of failure, in case of network failure or any server or equipment outage at the Central Service Layer and / or ITI Service Layer. The System shall be able to support the vital business operations at ROP branch offices and SIDCCs at the Local Service Layer.

8.3.5.2 The System shall meet the following requirements concerning the Local Service Layer at SIDCCs and ROP branch offices:

(a) There shall have no single point of failure; and

(b) High Availability clusters shall be implemented in ROP branch offices and SIDCCs. Each clustered database shall have at least two member servers. In the event that a member server is unavailable, the remaining nodes shall be able to pick up the workload to perform all the processes for the failed node. Each clustered application server shall have at least two member servers. In the event that a member server is unavailable, another node shall be able to take over the necessary resource group including the background processes of the failed node within three (3) minutes.

(c) Local mode and standalone mode switchover time
In case of outage of the WAN link or service provided in data centres, the servers in SIDCCs, ROP branch offices shall be able to operate in local mode within three (3) minutes. The local mode functions of the System shall be supported.

In case of outage of the Local Area Network in ROP branch office / SIDCCs, the selected ROP desks, self-service registration kiosk and self-service collection kiosk shall work in a standalone mode to handle the registration, preliminary assessment and HKIC issuance. The switching to standalone mode shall be completed within five (5) minutes.

8.3.6 Workstations

8.3.6.1 The SMARTICS-2 workstations shall have resilience hard disk installed to prevent data loss.

8.3.6.2 For the workstations that can be operated in standalone mode, data stored in the workstations shall be protected and facility shall be provided for subsequent data upload to servers upon service recovered. Proper status monitoring and audit trail shall also be in place.

8.3.7 Kiosks

8.3.7.1 The System shall allow for self-service registration kiosk and self-service collection kiosk to perform their functions under local mode and standalone mode. Tenderers shall specify in Schedule 4 – "Technical Proposal and System Configuration" of Part V for the design of kiosks running under local mode and standalone mode.

8.3.8 Wide Area Network

8.3.8.1 The resilience and disaster recovery requirements for wide area network are set out in Section 2.3.5.2 of this Annex.

8.3.9 Local Area Network

8.3.9.1 The resilience and disaster recovery requirements for local area network are set out in Section 2.3.5.3 of this Annex.

8.3.10 System backup and recovery

8.3.10.1 The Contractor shall implement the functions and procedures for system backup and recovery for all servers and equipment of the System in different network zones including MCN and AN at data centres, ROP branch offices and SIDCCs. System backup is required after any changes were applied to the system configuration.

8.3.11 Data backup and recovery

8.3.11.1 The Contractor shall implement the functions and procedures for data backup and recovery for all servers and equipment of the System.

8.3.11.2 The daily backup time for Local Service Layer and Central Service Layer shall not exceed three (3) hours.

8.3.11.3 The recovery time for the midrange servers and PC servers, including the reconfiguration and data recovery time, shall not exceed 24 hours.

8.3.11.4 For the Central Service Layer in MCN and AN, a regular daily and weekly backup regime is required. The off-site backup shall be made by tape backup device at DDC(FL) after data replication of backup data from PDC(KC) to DDC(FL). At data centres, adequate data restore facility shall be ready in case of restoration required.

8.3.11.5 For ROP branch offices and SIDCCs, on-site regular daily and weekly backup and off-site backup of servers are required by using tape backup device. The hardware and software requirements for the tape backup device are stipulated in Sections 6.3.11.5 and 7.5.8 of this Annex.

8.3.12 **Power supply**

8.3.12.1 The equipment at computer rooms and kiosks at ROP branch offices and SIDCCs shall be protected against power outage. The Contractor shall provide necessary UPS to meet this resilience requirement.

8.3.13 **Spare equipment**

8.3.13.1 Tenderers may propose any spare equipment in Schedule 1 – "Hardware" of Part V which is considered necessary.

8.4 Disaster Recovery Plan

8.4.1 The Contractor shall draw up disaster recovery plan in accordance with Section 14 – "Resilience and Disaster Recovery Requirements" of Part VII.

9 IMPLEMENTATION SERVICES

9.1 Supplement to the Scope of Implementation Services as specified in Section 17 of Part VII – "Project Specifications"

9.1.1 In addition to the Implementation Services as specified in Section 17 of Part VII – "Project Specifications", the Contractor shall also perform the Implementation Services as more particularly specified in this Section 9.

9.1.2 All activities shall be performed by the dates specified in the Implementation Plan. Where there are specific time requirements specified in this Section, the Implementation Plan shall comply with such specific time requirements. Where neither this Section nor Implementation Plan specifically mentions the completion date for an activity, that activity shall be completed in a timely manner to ensure activities which follow it will also be completed in a timely manner in accordance with the Implementation Plan.

9.2 Tenderer's Responsibility

9.2.1 In addition to the proposals required to be provided as specified in Section 17 of Part VII – "Project Specifications", the Tenderer of Category A shall submit the following proposals.

9.2.2 Tenderers shall provide the preliminary design of the interfaces between the System and other Systems of the SMARTICS-2 in Schedule 5 – "Preliminary Design for the Custom Programs" of Part V.

9.2.3 Tenderers shall provide the preliminary design of the application interface between the System and the CDS of the ITI, including the CDS for SMARTICS-2, in Schedule 5 – "Preliminary Design for the Custom Programs" of Part V.

9.3 Full System Integration Services

9.3.1 For SMARTICS-2, the Contractor shall act as the prime and overall system integrator and be responsible for the overall coordination with Contractors of other Categories, other project teams and Government contractors to ensure seamless system integration and production rollout of all the components of SMARTICS-2 as a whole including but not limited to, the Hardware, Software, Custom Programs to be supplied under other Categories, system interfaces among the Systems of other Categories, those programs developed by other project teams / contractors of the Government, the ITI, other Integral Systems, the respective interfaces with various systems and also those Government Supplied Hardware and Software, to ensure that SMARTICS-2 as a whole meets all the objectives and requirements stated in these Project Specifications (including all Annexes applying to different Categories).

9.3.2 The Contractor shall design and implement the CDS for SMARTICS-2 as more particularly described in Section 2.3.8.22 of this Annex and Appendix J – "List of Common Data Services for SMARTICS-2" to Part VII. The Contractor shall also make use of services of the ITI to ensure that the System will have access to the CDR. The Contractor shall work and cooperate with the ITI project team for the implementation of such services. In relation to local mode operation, the Contractor shall provide the CDR in local mode at each of the ROP branch offices and SIDCCs, the required data extraction from the CDR and the required services to be implemented in local mode operation.

9.3.3 Except to the extent expressly stated in the Annexes for the System of other Categor(ies), the Contractor shall be responsible for designing the interfaces between the System with each of the Systems of other Categories, each External System, the Government Supplied Hardware and Software and the ITI, and other Integral Systems as well as ensuring software coexistence, data consistency, data integrity, system recovery, data sharing and system security. The Contractor shall seek the input and agreement of each of the Other Contractors in relation to the design of the interface specifications between the System and the Integral System or component supplied by that Other Contractor during the SA&D stage. The mode of collaboration is more particularly described in Section 1.4 of Part VII.

9.3.4 The Contractor shall provide the configuration and specifications of all workstations of the System to be procured by the Government during SA&D stage.

9.3.5 The Contractor shall provide assistance to the Other Contractor who supplies the workstations of the System in relation to the setup of all such workstations and related server / network equipment of the SMARTICS-2.

9.3.6 As the Prime System Integrator, the Contractor shall monitor the overall progress of the implementation of the Systems of all Categories and work closely with Contractors of all Categories to ensure that the implementation of the respective components of SMARTICS-2 Project are within the specified schedule and according to this Contract. The Contractor shall take on the primary responsibility to carry out production rollout of SMARTICS-2. In doing so, it shall co-ordinate the other Contractors to ensure that they perform their respective duties under the Categories for which they are responsible in such production rollout and switchover. It shall also resolve all integration related issues arising from the integration of all Categories during such production rollout and switchover.

9.4 Application Integration Services

9.4.1 As the Prime System Integrator, the Contractor shall monitor the overall progress of the implementation of the Systems of all Categories and work closely with Contractors of all Categories to ensure that the implementation of SMARTICS-2 is within the specified schedule and according to this Contract.

9.4.2 The Contractor shall be responsible to coordinate the overall system analysis and design activities of SMARTICS-2 as a whole with Other Contractors.

9.4.3 The Contractor shall be responsible for the integration of all components, including CPMS, CabS, TAGS-2, CDS, existing smart identity card, new smart identity card, SMARTICS-2 applications running on MSK_GEN, MSK_REG, SCK, e-Services-2 platform with other components of SMARTICS-2 and coordinate with Other Contractors and the ITI team for the successful integration.

9.4.4 The Contractor shall make use of the CDS for the data access to the CDR and be responsible for the application integration.

9.4.5 The Contractor shall provide a standardised logging mechanism for the purpose of audit trail, system performance monitoring and problem diagnosis, which is to be followed by the System and the Systems of other Categories. The Contractor shall also be responsible for the log consolidation and reporting. The Contractor shall work with the Other Contractors for the implementation of the logging mechanism.

9.4.6 The Contractor shall where necessary seek the cooperation and input from Other Contractors to complete the application integration where necessary.

9.4.7 The Contractor shall conduct application integration test to ensure that all system components of the SMARTICS-2 as a whole are compatible, and all system interfaces of SMARTICS-2 as a whole are interoperable.

9.4.8 The Contractor shall perform problem diagnosis and repeated tests if incidents or problems occur while conducting application integration test.

9.4.9 The Contractor shall be responsible for rectifying any problems encountered in application integration test and where necessary seek the cooperation and input from Other Contractors to resolve the problems.

9.5 System Analysis and Design Services

9.5.1 The Contractor shall propose, during the SA&D stage, the specifications and quantities for the hardware and software items needed in light of configuration for the System. The Government will acquire separately the hardware and software of workstation, monitor, Chinese input device, barcode reader, document scanner, slip printer, and document printer for Supervisor Desk, Reception Desk, Registration Desk, Assessment Desk, Verification Desk, Shroff Desk and Collection Desk as described in Sections 6.2.2.5.1 to 6.2.2.5.5 of this Annex according to the proposed specifications. The Contractor shall ensure that notwithstanding the connection and integration of aforesaid hardware and software with the System, the System shall still comply with the Overall Specifications, Performance Criteria and Reliability Levels.

9.6 Custom Programs Development Services

9.6.1 All of the Custom Programs to be developed by the Contractor shall be designed and implemented as a software package with installation function to enable setting up the System at a new SIDCC or ROP office or setting up the new equipment at Front-end Service Layer including workstation, self-service registration kiosk, self-service collection kiosk, e-Cabinet, self-service general application kiosk and related peripherals at an existing ROP office by execution of the installation function in the software package. The Contractor shall provide Project Documentation containing detailed and step-by-step procedures, instructions and technical advice for the installation and running of such software package for extension of the System to the new SIDCC or ROP office or new equipment at Front-end Service Layer at an existing ROP office.

9.7 Environment Setup

9.7.1 The Contractor shall set up the development, testing and training environments as specified in Section 2.3.12 of this Annex.

9.8 Support to Government In-house Project Team

9.8.1 In addition to the User Acceptance Tests, Reliability Test, and Overall SMARTICS-2 UAT, the Contractor shall provide technical support and assistance to the Government for the conduct of tests for the application to be developed by the project teams of ImmD.

9.8.2 The Contractor shall assist the Government to acquire any additional hardware and software required for the System. The Contractor shall assist the Government in preparing the product specifications.

9.9 System Acceptance Tests, User Acceptance Tests, Overall SMARTICS-2 System Integration Tests and Overall SMARTICS-2 UAT

9.9.1 The Contractor shall perform its obligations in relation to the System Acceptance Tests, the User Acceptance Tests, Overall SMARTICS-2 System Integration Tests and Overall SMARTICS-2 UAT in accordance with Section 17.15 of Part VII.

9.9.2 The Contractor shall be in charge of and coordinate the Overall SMARTICS-2 System Integration Tests and Load Test. The Contractor shall be responsible to generate the test cases and data for the Overall SMARTICS-2 System Integration Tests and Load Test. The Contractor shall provide the necessary utilities to generate the data and to simulate the peak workload for conducting the Overall SMARTICS-2 System Integration Tests and Load Test.

9.9.3 The Contractor shall provide the testing automation tool to generate test cases and data in accordance with criteria provided by the users.

9.9.4 The Contractor shall participate and provide support to the Contractor of Category B in the Card Integration Test in Stage BS2.5 of the Implementation Plan of Category B including by providing the smart card readers together with the custom programmes for reading the smart cards using the module of mutual authentication of smart card provided by the Contractor of Category B.

9.10 Site Preparation

9.10.1 The Contractor shall provide the necessary cabling installation for connecting equipment (including but not limited to all Contractor Supplied Hardware, workstations, kiosks and e-Cabinets) of SMARTICS-2 to the Extended MCN, Local Kiosk Network, General Kiosk Network, MCN and AN of the ITI.

9.10.2 Upon site possession by the Contractor for cabling / equipment delivery and installation works, some locations may still be construction sites. In this connection, all appropriate laws, regulations and guidelines regarding aforesaid works and associated personnel working at the construction site shall be complied. Besides, the party overseeing the construction works and the site management of the concerned locations may issue any site instructions or guidelines from time to time, which should be followed by the Contractor. The Contractor shall be responsible for bearing any costs that may be incurred when complying with the aforesaid regulations and instructions.

9.11 Data Conversion and Migration

9.11.1 The Contractor shall perform the data conversion and migration services specified in Section 5 – “Data Conversion and Migration Requirements” of this Annex.

9.11.2 The Contractor shall be responsible to deliver contingency plan as specified in Section 5 – “Data Conversion and Migration Requirements” of this Annex.

9.12 System Rollout

9.12.1 As the Prime System Integrator, the Contractor shall take on the primary responsibility to carry out production rollout of SMARTICS-2 by phases. In doing so, it shall coordinate the other Contractors to ensure that they perform their respective duties under the Categories for which they are responsible in such production rollout. It shall also resolve all integration related activities and issues arising from the integration of all Categories during such production rollout, and seek the support and assistance from Other Contractors wherever necessary.

9.12.2 The Contractor shall ensure the smooth rollout of the System, coordinate with Other Contractors, including the contractors of Existing Systems, for providing plan, support and related services and activities during the switchover from SMARTICS to the System including but not limited to applications processing in the workflow, smart identity cards personalised in SMARTICS and to be collected in the System, etc.

9.13 Training

9.13.1 The Contractor shall provide the training specified in Section 20 – “Training Requirements” of Part VII.

9.14 Disaster Recovery Planning

9.14.1 The Contractor shall be responsible to deliver an overall disaster recovery plan for the System. In addition to the preparation of disaster recovery plan for the System, the Contractor shall consolidate the disaster recovery plan produced by the other Contractors for SMARTICS-2. The requirements are specified in Section 14 – “Resilience and Disaster Recovery Requirements” of Part VII.

9.15 System Nursing

9.15.1 The Contractor shall perform system nursing in accordance with Section 17.20 of Part VII.

9.16 Documentation

9.16.1 Project Documentation and deliverables provided by the Contractor shall include, but not limited to, the following:

Project Activities	**Project Documentation and Deliverables**
Project Initiation	1. Project Management Plan (“PMP”) • Master Project Management Plan • Project Organisation • Work Plan • Financial Management Plan • Communication Management Plan • Risk Management Plan • Quality Management Plan • Issue Management Plan • Change Request Management Plan 2. Overall Project Plan 3. Quality Plan
System Analysis & Design	4. System Analysis and Design Report • Management Summary • Business Activity Model • User Requirements • System Specifications • Data Specifications • Functional Specifications • Logical Processing Specifications

Project Activities	Project Documentation and Deliverables
	• Technical System Option • Implementation Plan 5. Detailed Project Plan 6. Development Standard 7. Discussion Notes 8. Outstanding Issues List
Application Development	9. Programming Standard 10. Database / File Specifications 11. Program Specifications 12. Detailed Project Plan 13. Disaster Recovery Plan 14. Fallback and Recovery Plan 15. Software Modules 16. Job Control Procedures 17. Unit Test Cases and Results
System Integration Test	18. SIT Plan and Specifications 19. SIT Results and Report 20. Overall SMARTICS-2 System Integration Test Plan and Specifications 21. Overall SMARTICS-2 System Integration Test Specifications and Results Report
User Acceptance Tests	22. UAT Plan, Specifications and Results Report 23. Overall SMARTICS-2 UAT Plan 24. Overall SMARTICS-2 UAT Results Report
Load Test	25. Load Test Plan, Specifications and Results Report
Resilience Test	26. Resilience Test Plan and Results Report
Site Preparation	27. Site Preparation Plan and Specifications 28. Accepted Site
User Training	29. Training Plan 30. Training Manual 31. Training Course Materials

Project Activities	Project Documentation and Deliverables
Data Conversion	32. Data Conversion and Migration Plan 33. Data Conversion and Migration Specifications 34. Database / file Specifications 35. Data Conversion and Migration Program Specifications 36. Data Conversion and Migration Software Modules 37. Data Conversion and Migration Test Cases and Results 38. Data Conversion and Migration Program Test Plan and Results 39. Verification Results Report 40. Computer Operations Procedures 41. Trial Conversion and Migration Plan 42. Fallback and Recovery Plan 43. Converted and Migrated Image 44. Converted and Migrated Data
Pre-production	45. Trial Run (Dress Rehearsal) Plan 46. System Recovery Test Plan and Results Report 47. Transaction / Response Test Plan and Results Report
System Installation and Production	48. System Installation Plan and Report 49. System Rollout plan 50. Fallback and Recovery Plan 51. Data Manual 52. Program Manual 53. System Manual 54. Application Operation Manual 55. Application User Manual 56. Computer Operations Procedures Manual 57. Database / System Administration Manual 58. Inventory List of Hardware and Software 59. System Installation and Migration Procedure Manual

Project Activities	Project Documentation and Deliverables
	60. Reliability Test Plan, Specifications and Results 61. System Maintenance Plan 62. Custom Programs 63. Installation Test Plan, Specifications and Results 64. Disaster Recovery Plan 65. Disaster Recovery Drill Report 66. Business Continuity Plan 67. System Administration Manual 68. Security Incident Handling Manual 69. Trade-in Plan
Post Implementation Review	70. Post Implementation Review ("PIR") Report, including: • System Functionality • System Performance • Project Achievement • Resource Utilisation • Productivity • Project Issue • Quality Review • Development • Project Management • Problems Encountered / experiences gained • Others 71. Project Evaluation Report ("PER") 72. Quality Record of Quality Assurance Review ("QAR") 73. Quality Review Results
All Stages	74. Project Progress Reports / Project Highlight Report

Table 7A-9.16.1 Project Documentation and Deliverables for Category A

9.16.2 An Application User Manual, with user interface diagrams, shall be provided to elaborate all the features and functions of the System.

9.17 System Changes

9.17.1 The Contractor shall provide at least an aggregate of 285 man-days of manpower resources, of which 25 man-days to be performed by project manager, 100 man-days to be performed by systems analyst and 160 man-days to be performed by analyst programmer for implementing System Changes from time to time or any time during the Implementation Period. Under no circumstances whatsoever may the Contractor deploy the man-power resources already allocated for other part of the Implementation Services to perform the System Changes. If there are any unused man-days or any part thereof at the end of the Implementation Period, they shall be carried forward to the Maintenance Period without any limit.

9.17.2 The Government may only consider paying additional charges at the charging rates as specified in Table 5-23.13(A) in Schedule 23 – "Price Schedule" of Part V for a proposed System Change if the man-days specified above have been used up or are not sufficient to implement the System Changes.

9.17.3 Upon a change agreement in relation to a System Change is constituted under the applicable provision of the Contract, all specifications of the System Change shall be treated as forming part of the Overall Specifications, and the System to be implemented by the Contractor shall comply with these specifications. All Deliverables including Documentation to be prepared and supplied shall relate to the System incorporating such System Change.

9.18 Other Services

9.18.1 The Contractor shall perform all work as the primary obligor to ensure that the System shall be Ready for Use by the Completion Date.

10 SYSTEM SUPPORT AND MAINTENANCE SERVICES

10.1 Supplement to the Scope of System Support Services as specified in Section 18 of Part VII – "Project Specifications"

10.1.1 In addition to the System Support and Maintenance Services as specified in Section 18 of Part VII – "Project Specifications", the Contractor shall also perform the System Support and Maintenance Services as more particularly specified in this Section 10.

10.2 Multi-contractor Cooperative Maintenance

10.2.1 The Contractor under this Category shall be acted as the Prime System Integrator for the System Support and Maintenance Services of the whole of SMARTICS-2. On this basis, the Contractor under this Category shall monitor the provision and progress of the System Support and Maintenance Services provided by the Contractor of other Categories.

10.3 Helpdesk Services

10.3.1 The Contractor shall operate the helpdesk to receive and log support calls relating to all kinds of reported problems relating to the System.

10.4 System Integration Services

10.4.1 The Contractor shall act as a Prime System Integrator in relation to the delivery of various services for the System Support Service of SMARTICS-2.

10.4.2 The Contractor shall be primarily responsible for fixing any issues arising from SMARTICS-2 during the Maintenance Period which are not the specific responsibilities of the Contractors of the other Categories. In this connection, it shall serve as a single point of contact (i.e. the Contractor of the whole of SMARTICS-2) to any third party.

10.5 Custom Program Bug Fixing

10.5.1 The Contractor shall perform bug fixing and provide on-site support, if necessary, to solve all problems related to the Custom Programs in the System (including the interfaces which connect the System to the Systems of other Categories or ITI or other Integral Systems or other existing or future systems).

10.5.2 Upon the request by the Government and without prejudice to the obligations of the Contractor specified in Section 10.5.1 of this Annex, the Contractor shall provide information, assistance and support to the Government and Other Contractors in relation to the Custom Programs of other Integral Systems.

10.5.3 The Contractor shall maintain and update the software packages as mentioned in Section 9.6.1 of this Annex by incorporating all applicable fixes from time to time implemented by the Contractor in the provision of custom program bug fixing services pursuant to Section 18.7.9 of Part VII – "Project Specifications" and this Section 10.5 and all applicable System Changes from time to time implemented.

10.6 System Administration

10.6.1 The Contractor shall perform system management and monitoring of the network equipment, servers and equipment connected to the System by making use of ESM.

10.6.2 The Contractor shall perform database management, database software maintenance, database reorganisation and database tuning.

10.6.3 The Contractor shall perform the database administration tasks for the System, including the local CDR.

10.7 System Changes

10.7.1 The Contractor shall provide at least an aggregate of 285 man-days of manpower resources per annum, including 25 man-days of project manager per annum, 100 man-days of systems analyst per annum, 160 man-days of analyst programmer per annum, throughout the Maintenance Period for implementing System Changes. If there are any unused man-days or any part thereof in a year, they shall be carried forward to the next year without any limit. Man-days originally allocated for a year may be used in a preceding year if the man-days allocated for that preceding year is not sufficient for a particular System Change, without any limit.

10.7.2 The Government may only consider paying additional charges at the charging rates as specified in Table 5-23.13(A) in Schedule 23 – "Price Schedule" of Part V for System Changes if the man-days for a year as specified in Section 10.7.1 of this Annex have been exceeded and that man-days for a future year will not be used for that System Change.

10.8 LAN, Workstations, Kiosks and Peripherals Support

10.8.1 The Contractor shall ensure the proper and continuing functional integration of all the end-user equipment with the System, including workstations, kiosks and their connected peripherals, network printers and horizontal network equipment.

10.8.2 The Contractor shall provide and maintain a backup image of each type of Hardware in the Front-end Service Layer to enable the re-installation of the Hardware for whatever reason.

10.9 Documentation

10.9.1 The Contractor shall maintain and update the following Documentation as part of the System Support and Services:

(a) Data Manual;

(b) Program Manual;

(c) System Manual;

(d) Application Operation Manual;

(e) Application User Manual;

(f) Computer Operations Procedures Manual;

(g) Database / System Administration Manual;

(h) Inventory List of Hardware, Software and Custom Programs;

(i) Fallback and Recovery Plan;

(j) Disaster Recovery Plan;

(k) Business Continuity Plan;

(l) Security Incident Handling Manual;

(m) System Maintenance Plan; and

(n) System Installation and Migration Procedure Manual.

10.9.2 The Contractor shall provide reports on the System Support Services from time to time performed by the Contractor including without limitation the following :

(a) Monthly Progress Reports;

(b) The System's compliance with the Reliability Levels in respect of each Given Period;

(c) The Contractor's compliance with the Service Levels in respect of each month of the Maintenance Period;

(d) Monthly Support Service Reports;

(e) Impact Analysis Report for System Change Requests as and when a System Change is requested;

(f) Annual Disaster Recovery ("DR") Drill Reports; and

(g) Annual Capacity Planning Study Reports.

10.10 Other Tasks and Duties

10.10.1 As part of the System Support Services, the Contractor shall from time to time upon the demand of the Government ensure that one or more member(s) of the Maintenance Team(s) (as requested by the Government) shall be physically on stand-by at a Location as stipulated by the Government and be prepared to provide emergency System Support and Maintenance Services on-site at that Location. The period of such stand-by may be any time outside the normal office hours of the

Maintenance Team stationed at the ImmD premises ("stand-by period"). The total hours of stand-by shall be at least 80 man-hours per annum of the Maintenance Period (regardless of the role performing such stand-by) to be provided free of any additional charge by the Contractor as part of the System Support Services ("Reserved Stand-by Hours"). In the event that the Reserved Stand-by Hours for a year have not been fully consumed by the Government during that year, the remaining man-hours shall be carried over to the year(s) after for use by the Government. For the avoidance of doubt, any time spent by member(s) of the Maintenance Team(s) (a) who is / are not required to be physically stationed at the Location(s) during a stand-by period; or (b) otherwise not at the request of the Government for emergency System Support and Maintenance Services, such time shall not be treated as consumption of the Reserved Stand-by Hours.

11 STAFF RESOURCES REQUIREMENTS

11.1 Staff Requirement for Implementation Team

11.1.1 Tenderer's Responsibility and Contractor's Obligations

11.1.1.1 Tenderers shall propose the Implementation Team to carry out the Implementation Services, in compliance with the requirements set out in this Section.

11.1.1.2 All nominees filling the Key Roles (i.e. key project staff) shall take up the lead roles and shall work on-site at the premises provided by the Government throughout the Implementation Period to provide the Implementation Services. At least the specified minimum number of nominee(s) for each Key Role shall be proposed by the Tenderer ("Minimum Number"), and each of which shall be a single individual who can himself / herself fulfil all of the requirements for that Key Role, including the experience and resource allocation requirements.

11.1.1.3 A person filling a Key Role in the Implementation Team shall not perform any other role whether it be a Key Role or non-Key Role in the same Implementation Team or other Implementation Team(s) of other Categor(ies) covered by the Contract (if any). For non-Key Roles, the provisions are more particularly set out in the applicable Section of Sections 17.2.3 to 17.2.4 of Part VII.

11.1.1.4 The Implementation Team shall include nominees to fill at least the following Key Roles with the minimum requirements of the numbers, IT experience and resource allocation as follows:

Key Roles	Minimum Number of Staff Required	Minimum Number of IT and Functional / Specialty Years of Experience (the number of the relevant system or infrastructure or network or application or database or equipment covered by the requisite number of years of experience may be one or more)	Minimum Staff Resources Required to be Allocated During the Implementation Period (excluding the quota of man-days reserved for System Changes as specified in Section 9.17 of this Annex)
Project Director	1	At least 15 years of post-qualification IT experience, which includes at least 11 years of functional / specialty experience in project management.	As when required for attending meetings and discussions for project-related matters.
Project	1	At least 11 years of	Full-time to perform

Key Roles	**Minimum Number of Staff Required**	**Minimum Number of IT and Functional / Specialty Years of Experience** **(the number of the relevant system or infrastructure or network or application or database or equipment covered by the requisite number of years of experience may be one or more)**	**Minimum Staff Resources Required to be Allocated During the Implementation Period (excluding the quota of man-days reserved for System Changes as specified in Section 9.17 of this Annex)**
Manager		post-qualification IT experience, which includes at least 6 years of project management experience, and at least 2 years of functional / specialty experience in the management of project(s) for the design and implementation of enterprise application system(s) with over 1000 users per enterprise application system.	the Implementation Services throughout the Implementation Period (including the whole of the Transition Period and the nursing period) and stationed at the premises of ImmD
Lead Systems Architect	1	At least 11 years of post-qualification IT experience, which includes at least 6 years of functional / specialty experience in technical system architecture design and / or implementation of enterprise application system(s) with over 1000 users per enterprise application system.	Full-time to perform the Implementation Services throughout the Implementation Period (including the whole of the Transition Period and the nursing period) and stationed at the premises of ImmD.
IT Specialist for network and system infrastructure	1	At least 9 years of post-qualification IT experience, which includes at least 5 years of functional / specialty experience in design and / or implementation of network and system infrastructure(s) with enterprise grade network equipment.	At least 9 man-months, in which at least 3 man-months must be allocated for SA&D and at least 6 man-months for system implementation (including development, System Acceptance Tests, UAT, and production rollout) and during

Key Roles	**Minimum Number of Staff Required**	**Minimum Number of IT and Functional / Specialty Years of Experience** **(the number of the relevant system or infrastructure or network or application or database or equipment covered by the requisite number of years of experience may be one or more)**	**Minimum Staff Resources Required to be Allocated During the Implementation Period (excluding the quota of man-days reserved for System Changes as specified in Section 9.17 of this Annex)**
			which periods shall be stationed at the premises of ImmD.
IT Specialist for virtualised server infrastructure	1	At least 9 years of post-qualification IT experience, which includes at least 5 years of functional / specialty experience in design and / or implementation of virtualised server infrastructure(s).	At least 9 man-months, in which at least 3 man-months must be allocated for SA&D and at least 6 man-months for system implementation (including development, System Acceptance Tests, UAT and production rollout) and during which periods shall be stationed at the premises of ImmD.
IT Specialist for storage and backup	1	At least 9 years of post-qualification IT experience, which includes at least 5 years of functional / specialty experience in the design and / or implementation of storage and backup infrastructure(s).	At least 9 man-months, in which at least 3 man-months must be allocated for SA&D and at least 6 man-months for system implementation (including development, System Acceptance Tests, UAT and production rollout) and during which periods shall be stationed at the premises of ImmD.

Key Roles	**Minimum Number of Staff Required**	**Minimum Number of IT and Functional / Specialty Years of Experience** **(the number of the relevant system or infrastructure or network or application or database or equipment covered by the requisite number of years of experience may be one or more)**	**Minimum Staff Resources Required to be Allocated During the Implementation Period (excluding the quota of man-days reserved for System Changes as specified in Section 9.17 of this Annex)**
IT Specialist for application architecture	1	At least 9 years of post-qualification IT experience, which includes at least 5 years of functional / specialty experience in the design and / or implementation of application architecture for web-based application system(s).	At least 12 man-months, in which at least 4 man-months must be allocated for SA&D and at least 8 man-months for the system implementation (including development, System Acceptance Tests, UAT and production rollout) and during which periods shall be stationed at the premises of ImmD.
IT Specialist for biometrics	1	At least 9 years of post-qualification IT experience, which includes at least 5 years of functional / specialty experience in the design and / or implementation of fingerprints identification related application(s).	At least 9 man-months, in which at least 3 man-months must be allocated for SA&D and at least 6 man-months for the system implementation (including development, System Acceptance Tests, UAT and production rollout) and during which periods shall be stationed at the premises of ImmD.
Lead Systems Analyst	3	At least 6 years of post-qualification IT experience, which includes at least 4 years of functional / specialty experience in the	Full-time to perform the Implementation Services throughout the Implementation Period (including the

Key Roles	Minimum Number of Staff Required	Minimum Number of IT and Functional / Specialty Years of Experience (the number of the relevant system or infrastructure or network or application or database or equipment covered by the requisite number of years of experience may be one or more)	Minimum Staff Resources Required to be Allocated During the Implementation Period (excluding the quota of man-days reserved for System Changes as specified in Section 9.17 of this Annex)
		design and / or implementation of web-based application system(s).	whole of the Transition Period and the nursing period) and stationed at the premises of ImmD.
Database administrator	1	At least 9 years of post-qualification IT experience, which includes at least 5 years of functional / specialty experience in the design and administration of database(s).	At least 12 man-months, in which at least 4 man-months must be allocated for SA&D and at least 8 man-months for the system implementation (including development, System Acceptance Tests, UAT and production rollout) and during which periods shall be stationed at the premises of ImmD.

Table 7A-11.1.1.4 Minimum Staff Requirements for Key Roles of the Implementation Team

11.1.1.5 The above are just minimum requirements but are not the recommended quantities of manpower resources required for the Implementation Services. In the event that additional individuals have to be hired to fill in the above-mentioned key roles or additional man-months have to be performed by the key roles to ensure that the System is Ready for Use by the Completion Date, the Contractor must do so at its own cost, and no additional payment will be made by the Government.

11.1.1.6 For the purposes of tender evaluation, the IT experience of a nominee fulfilling the Minimum Number for a Key Role will be calculated as at the Original Tender Closing Date (before any extension). After the Contract award, the experience of a new nominee to replace an out-going nominee for a Key Role or otherwise for a non-Key Role will be calculated as at the proposed date of joining the Implementation Team. Section 22.4 of Part VII sets out further requirements concerning the calculation of experience.

11.1.1.7 The Implementation Team shall also include other sufficient nominees of non-Key Roles (i.e. non-key project staff) working within Hong Kong to support the key project staff in providing the Implementation Services successfully. The duties of a non-Key Role can be shared by different individuals or the same individual can fill more than one role. At least the following non-Key Roles shall be included. The minimum requirements of the numbers and years of IT experience to be fulfilled by the person filling in each role are as follows:

Non-Key Roles	**Minimum Number of Staff Required**	**Minimum Number of Years of IT and Functional / Specialty Experience Required** **(the number of the relevant system or infrastructure or network or application or database or equipment covered by the requisite number of years of experience may be one (1) or more)**
Systems Analyst	3	At least 5 years of post-qualification IT experience, which includes at least 3 years of functional / specialty experience in the design and / or implementation of web-based application system(s).
Analyst Programmer	9	At least 3 years of post-qualification IT experience, which includes at least 2 years of functional / specialty experience in the implementation of web-based application system(s).
Systems Engineer for network infrastructure	2	At least 3 years of post-qualification IT experience, which includes at least 2 years of functional / specialty experience in installing, testing and system configuration of network equipment.
Systems Engineer for server, storage and backup	3	At least 3 years of post-qualification IT experience, which includes at least 2 years of functional / specialty experience in installing, testing and system configuration of server, storage and backup infrastructure(s).

Table 7A-11.1.1.7 Minimum Staff Requirements for the Non-Key Roles of the Implementation Team

11.1.1.8 Due to the high complexity of the System and implementation with tight schedule, Tenderers shall consider and propose sufficient and skilled manpower with well-organised and effective team structure to deliver efficient Implementation Services as detailed in the Project Specifications.

11.1.1.9 Upon commencement of the Implementation Period, the Contractor shall in accordance with its nominations as set out in Table 5-7.2(A) of Schedule 7 of Part V arrange the relevant nominees to fill in the Key Roles of the Implementation

Team to perform Implementation Services throughout the deployment periods as specified in Sections 11.1.1.4 and 11.1.1.7 of this Annex and subject thereto also in Table 5-7.3(A) of Schedule 7 of Part V. In the event of any inconsistency between the Schedules in Part V concerning the allocation of manpower resources to be performed by a role (Key Role or non-Key Role), the Schedule which stipulates the longer deployment period by that role shall prevail.

11.1.1.10 During the Transition Period and Nursing Period, the Contractor shall provide sufficient staff to provide the system nursing services. In addition to the key roles and non-key roles of the Implementation Team specified in Sections 11.1.1.4 and 11.1.1.7 of this Annex, the Contractor shall provide at least three (3) Systems Engineers for server, storage and backup, with same requirements as those stipulated in Section 11.1.1.7 of this Annex for the same non-Key Role of the Implementation Team, to provide the System Support Services during the Transition Period.

11.1.1.11 In performing the System Changes as part of the Implementation Services, separate additional man-power resources in the form of the quota to be provided over the Implementation Period (as stipulated in Section 9.17 of this Annex), which is not drawn from minimum staff resources of the Implementation Team as specified in Sections 11.1.1.4, 11.1.1.5 and 11.1.1.7 of this Annex shall be provided to perform System Changes. Roles in the Implementation Team who are required to be stationed in the ImmD premises shall not be deployed for performing the System Changes. The roles for performing System Changes shall be filled by individuals who comply with the same qualification and experience requirements specified in Sections 11.1.1.4 of this Annex for these roles to be determined from the date they are proposed to be deployed for performing the relevant System Changes.

11.1.2 Major Responsibilities of the Key Project Staff

11.1.2.1 The project director(s) shall be responsible to oversee the Implementation Services of the System. He / she / they shall work closely with the project directors or project managers in other Categories to ensure the successful implementation and system integration of the SMARTICS-2 as a whole. He / she / they shall articulate the project definition and scope statement, define and develop project plan, assign resources to the project, overall monitor and control the quality, progress and schedule of the project and liaise with different stakeholders regarding requirements definition, best practices in system development, performance measurement and management. He / she / they shall attend the Project Steering Committee ("PSC") and Project Assurance Team ("PAT") for the implementation of SMARTICS-2 for the interests of the Category. The project director(s) shall work closely with the project directors or project managers of other Categories to ensure the overall integration within the SMARTICS-2.

11.1.2.2 The project manager(s) shall report to the project director(s). He / she / they shall be responsible for the day-to-day project management in taking forward the implementation of the System, including project tracking and control, resolve project issues, apply quality control management, liaise with all relevant parties for the implementation, and ensure the project deliverables are provided on time and fulfilling user requirements. He / she / they shall attend PAT for the implementation of SMARTICS-2 for the interests of the Category. The project manager(s) shall work closely with the project managers of other Categories to ensure the overall integration within the SMARTICS-2.

11.1.2.3 The lead systems architect(s) shall report to the project manager(s). He / she / they shall be responsible for the overall design of the technical system architecture and orchestration for the implementation of the System, including the adoption, integration and transition of all related technologies and components as well as selecting technical options and performing system sizing. The lead systems architect(s) shall also work closely with the lead systems analysts, IT specialists and the Contractors of other Categories to ensure the overall integration within the SMARTICS-2.

11.1.2.4 The IT specialist(s) for network and system infrastructure shall report to the lead systems architect. He / she / they shall be responsible for providing expertise advice and technical support on network infrastructure, including structural cabling, to the lead systems architect(s) for the design and implementation of the project. The IT specialist(s) shall participate and take the lead in design workshops and discussions with the Government and Other Contractors, in particular, the Contractors of other Categories, contractors of the ITI project and the WAN service provider during the Implementation Period to explain the design, analyse, propose options, etc. to facilitate the overall integration of the SMARTICS-2 as a whole. He / she / they shall also lead the Implementation Team members to plan and carry out the system configuration, System Acceptance Tests, system rollout, etc., and provide support to ImmD during the User Acceptance Tests. The IT specialist shall possess hands-on experience for various components of the network infrastructure, including but not limited to, enterprise grade routers and switches.

11.1.2.5 The IT specialist(s) for virtualised server infrastructure shall report to the lead systems architect. He / she / they shall be responsible for providing expertise advice and technical support on virtualised server infrastructure to the lead systems architect(s) for the design and implementation of the project. The IT specialist(s) shall participate and take the lead in design workshops and discussions with the Government and Other Contractors, in particular, the Contractors of other Categories and the contractors of the ITI project during the Implementation Period to explain the design, analyse, propose options, etc. to facilitate the overall integration of the SMARTICS-2 as a whole. He / she / they shall also lead the Implementation Team members to plan and carry out the system configuration, System Acceptance Tests, system rollout, etc., and provide support to ImmD during the User Acceptance Tests. The IT specialist shall possess hands-on experience for various components of the virtualised server infrastructure for both UNIX and x 86 platforms.

11.1.2.6 The IT specialist(s) for storage and backup shall report to the lead systems architect. He / she / they shall be responsible for providing expertise advice and technical support on storage and backup to the lead systems architect(s) for the design and implementation of the project. The IT specialist(s) shall participate and take the lead in design workshops and discussions with the Government and Other Contractors, in particular, the Contractors of other Categories and the contractors of the ITI project during the Implementation Period to explain the design, analyse, propose options, etc. to facilitate the overall integration of the SMARTICS-2 as a whole. He / she / they shall also lead the Implementation Team members to plan and carry out the system configuration, System Acceptance Tests, system rollout, etc., and provide support to ImmD during the User Acceptance Tests. The IT specialist shall possess hands-on experience for various components of the centralised storage and backup infrastructure, including but not limited to, storage virtualisation equipment, enterprise grade storage, storage area network and backup solution.

11.1.2.7 The IT specialist(s) for application architecture shall report to the lead systems architect. He / she / they shall be responsible for the overall design and implementation of the application architecture for the System, including the design of relevant application framework, adoption, integration and transition of all related technologies and components, setup and configuration of application server software, application development and deployment tools. The IT specialist(s) shall participate and take the lead in design workshops and discussions with the Government and Other Contractors, in particular, the Contractors of other Categories and the contractors of the ITI project during the Implementation Period to explain the design, analyse, propose options, etc. to facilitate the overall integration of the SMARTICS-2 as a whole. He / she / they shall also lead the Implementation Team members to plan and carry out application design, system configuration, System Acceptance Tests, system rollout, etc., and provide support to ImmD during the User Acceptance Tests. The IT specialist shall possess hands-on experience for various components of enterprise grade application server software, application development and deployment tools.

11.1.2.8 The IT specialist(s) for biometrics shall report to the lead systems architect. He / she / they shall be responsible for the providing expertise advice and technical support on biometric identification related applications for the System. The IT specialist(s) shall participate and take the lead in design workshops and discussions with the Government and Other Contractors, in particular, the Contractors of other Categories and the contractors of the ITI project during the Implementation Period to explain the design, analyse, propose options, etc. to facilitate the overall integration of the SMARTICS-2 as a whole. He / she / they shall also lead the Implementation Team members to plan and design the biometric identification infrastructure, system configuration, System Acceptance Tests, system rollout, etc., and provide support to ImmD during the User Acceptance Tests. The IT specialist shall possess hands-on experience for design and / or implementation of fingerprints identification related applications.

11.1.2.9 The lead systems analyst(s) shall report to lead systems architect and lead other systems analyst(s) to work with other Implementation Team members to perform all aspects of SA&D tasks, including but not limited to, collecting user requirements, system analysis and design, documentation, conducting System Acceptance Tests and providing support to ImmD during the User Acceptance Tests and Overall SMARTICS-2 UAT, and performing production rollout for

SMARTICS-2. He / she / they shall possess hands-on experience for web-based application system implementation.

11.1.2.10 The <u>database administrator</u> shall report to the lead systems architect. He / she / they shall be responsible for the overall design and implementation of the database systems for the System, including technical database support on data analysis and modelling, database definitions and design, database performance tuning and monitoring and provision of advice to the development team. The database administrator shall participate and take the lead in design workshops and discussions with the Government and Other Contractors, in particular, the Contractors of other Categories and the contractors of the ITI project during the Implementation Period to explain the design, analyse, propose options, etc. to facilitate the overall integration of the SMARTICS-2 as a whole. He / she / they shall also support the Implementation Team members to plan and carry out the database design, system configuration, System Acceptance Tests, system rollout, etc., and provide support to ImmD in the User Acceptance Tests and Overall SMARTICS-2 UAT. The database administrator shall possess hands-on experience in the design and administration of database management.

11.1.2.11 The <u>systems analyst(s)</u> shall report to and assist the lead systems analyst(s) to perform all aspects of SA&D tasks, including but not limited to, collecting user requirements, system analysis, design, documentation, conducting System Acceptance Tests, giving support to ImmD in the User Acceptance Tests and Overall SMARTICS-2 UAT, and performing production rollout for SMARTICS-2.

11.1.2.12 The <u>analyst programmer(s)</u> shall report to systems analyst(s) to perform all aspects of software customisation, program development according to specifications, program testing, conducting System Acceptance Tests and giving support to ImmD in the User Acceptance Tests and Overall SMARTICS-2 UAT, and performing production rollout for SMARTICS-2.

11.1.2.13 The <u>systems engineer(s) for network infrastructure</u> shall report to the IT specialist(s) for network and system infrastructure and co-operate with other Implementation Team members for the installation, testing of network infrastructure, and so on.

11.1.2.14 The <u>systems engineer(s) for server, storage and backup</u> shall report to IT specialist(s) for virtualised server infrastructure or IT specialists for storage and backup and co-operate with other Implementation Team members for the installation, testing of server, storage and backup infrastructure, and so on.

11.2 Staff Requirement for the Maintenance Team(s)

11.2.1 Tenderer's Responsibility and Contractor's Obligations

11.2.1.1 Tenderers shall propose the Maintenance Team(s) to carry out the System Support and Maintenance Services for normal ROP business and dedicated to the territory-wide HKIC replacement exercise, in compliance with the requirements set out in this Section.

11.2.1.2 All nominees filling the Key Roles (i.e. key maintenance staff) shall take up the lead roles and shall work on-site at the premises provided by the Government throughout the Maintenance Period to provide the System Support Services. At least the specified minimum number of nominee(s) for each Key Role shall be proposed by the Tenderer ("Minimum Number") and each of which shall be a single individual who can himself / herself fulfil all of the requirements for that Key Role, including the experience and resource allocation requirements.

11.2.1.3 A person filling a Key Role in the Maintenance Team(s) shall not perform any other role whether it be a Key Role or non-Key Role in the same Maintenance Team for such System Support Services or the other Maintenance Team for the System Support Services dedicated to the territory-wide HKIC replacement exercise or the other Maintenance Team(s) of other Categor(ies) covered by the Contract (if any). For non-Key Roles, the provisions are more particularly set out in the applicable Section of Sections 18.1.2 to 18.1.4 of Part VII.

11.2.1.4 The Maintenance Team for normal ROP business shall include nominees to fill at least the following Key Roles, with the minimum requirements of the number, experience and resource allocation as follows:

Key Role	**Minimum Number of Staff Required**	**Minimum Number of Years of IT Experience and Functional / Specialty Experience Required** **(the number of the relevant system or infrastructure or network or application or database or equipment covered by the requisite number of years of experience may be one or more)**	**Minimum Staff Resources Required to be Allocated During the Maintenance Period (excluding the annual quota of man-days reserved for System Changes as specified in Section 10.7** of this Annex**)**
Project Manager	1	At least 11 years of post-qualification IT experience, which includes at least 6 years of functional / specialty experience in project management.	Full-time to perform System Support and Maintenance Services throughout the Maintenance Period and stationed

Key Role	**Minimum Number of Staff Required**	**Minimum Number of Years of IT Experience and Functional / Specialty Experience Required** **(the number of the relevant system or infrastructure or network or application or database or equipment covered by the requisite number of years of experience may be one or more)**	**Minimum Staff Resources Required to be Allocated During the Maintenance Period (excluding the annual quota of man-days reserved for System Changes as specified in Section 10.7** of this Annex**)**
			at the ImmD premises.
Systems Analyst for Application	1	At least 5 years of post-qualification IT experience, which includes at least 3 years of functional / specialty experience as systems analyst role in design and / or implementation of web-based application system(s).	Full-time to perform System Support and Maintenance Services throughout the Maintenance Period and stationed at the premises of ImmD.
Systems Analyst for Infrastructure	1	At least 5 years of post-qualification IT experience, which includes at least 3 years of functional / specialty experience as systems analyst role in design and / or implementation of IT infrastructure(s) involving server(s), virtualised server(s), storage and backup system(s).	Full-time to perform System Support and Maintenance Services throughout the Maintenance Period and stationed at the premises of ImmD.

Table 7A-11.2.1.4 Minimum Staff Requirements for Key Roles of the Maintenance Team for Normal ROP Business

11.2.1.5 The Contractor shall retain sufficient number of members from the Implementation Team in the Maintenance Team(s) to ensure the stability of the System.

11.2.1.6 The above are just minimum requirements but are not the recommended quantities of manpower resources required for the System Support Services. In the event that additional individuals have to be hired to fill in the above-mentioned key roles or additional man-months have to be performed by the key roles for the System Support Services, the Contractor must do so at its own cost, and no additional payment will be made by the Government.

11.2.1.7 For the purposes of tender evaluation, the experience of a nominee for a Key Role will be calculated as at the Original Tender Closing Date (before any extension). After the Contract award, the experience of a new nominee to replace an out-going nominee for a Key Role or otherwise for a non-Key Role will be calculated as at the proposed date of joining the Maintenance Team(s).

11.2.1.8 The Maintenance Team(s) shall also include other sufficient nominees of non-Key Roles (i.e. non-key maintenance project staff) working within the Hong Kong to support the key maintenance staff in providing the System Support Services successfully. The duties of a non-Key Role can be shared by different individuals or one individual can fill more than one role. At least the following non-Key Roles shall be included in the Maintenance Team for normal ROP business, with the minimum number and years of IT experience requirements specified as follows:

Non-Key Roles	**Minimum Number of Staff Required**	**Minimum Number of Years of IT and Functional / Specialty Experience Required** **(the number of the relevant system or infrastructure or network or application or database or equipment covered by the requisite number of years of experience may be one or more)**
Database Administrator	1	At least 5 years of post-qualification IT experience, which includes at least 3 years of functional / specialty experience in the design and administration of database(s).
Systems Analyst	1	At least 5 years of post-qualification IT experience, which includes at least 3 years of functional / specialty experience in system analysis and design.
Analyst Programmer	3	At least 3 years of post-qualification IT experience, which includes at least 2 years of functional / specialty experience in the implementation of web-based application system(s).
Systems Engineer for network infrastructure	1	At least 3 years of post-qualification IT experience, which includes at least 2 years of hands on functional / specialty experience in installing, testing and system configuration of network equipment.
Systems Engineer for server, storage and backup	1	At least 3 years of post-qualification IT experience, which includes at least 2 years of hands on functional / specialty experience in installing, testing and system configuration of server, storage and backup infrastructure(s).

Table 7A-11.2.1.8 Minimum Staff Requirements for the Non-Key Roles of the Maintenance Team for Normal ROP Business

11.2.1.9 At least the following non-Key Roles shall be included in the Maintenance Team for territory-wide HKIC replacement exercise and work on-site at the premises provided by the Government throughout the SIDCC Maintenance Period, with the minimum experience requirements and resource allocation as follows:

Non-Key Roles	**Minimum Number of Years of IT and Functional / Specialty Experience Required** **(the number of the relevant system or infrastructure or network or application or database or equipment covered by the requisite number of years of experience may be one or more)**	**Minimum Staff Resources Required to be Allocated During the SIDCC Maintenance Period** **(excluding the annual quota of man-days reserved for System Changes as specified in Section 10.7** of this Annex)
Project Manager	Same requirements as those stipulated in Section 11.2.1.4 of this Annex for the Key Roles of the Maintenance Team	6 man-months per annum
Systems Analyst for Infrastructure	Same requirements as those stipulated in Section 11.2.1.4 of this Annex for the Key Roles of the Maintenance Team	6 man-months per annum
Systems Engineer	At least 3 years of post-qualification IT experience, which includes at least 2 years of functional / specialty experience in installing, testing and system configuration of server, storage and backup infrastructure(s).	12 man-months per annum

Table 7A-11.2.1.9 Minimum Staff Requirements for the Non-Key Roles of the Maintenance Team for Territory-wide HKIC Replacement Exercise

11.2.1.10 In performing the System Changes as part of the System Support Services, separate additional man-power resources in the form of the annual quota (as stipulated in Section 10.7.1 of this Annex), which is not drawn from minimum staff resources of the Maintenance Team(s) as specified in Sections 11.2.1.4, 11.2.1.8 and 11.2.1.9 of this Annex, shall be provided to perform System Changes. Roles in the Maintenance Team(s) who are required to be stationed in the ImmD premises shall not be deployed for performing the System Changes unless otherwise approved by the Government on a case by case basis. These additional man-power resources shall include at least the roles fulfilling the experience requirements as specified below (whose compliance with the experience requirements shall be determined from the date they are proposed to be deployed for implementing the relevant System Changes).

Roles	**Minimum Number of Years of IT Experience and Functional / Specialty Required**
Project Manager	Same requirements as those stipulated in Section 11.2.1.4 of this Annex for the Key Roles of the Maintenance Team.
Systems Analyst	Same requirements as those stipulated in Section 11.2.1.8 of this Annex for the same non-Key Role of the Maintenance Team.
Analyst Programmer	Same requirements as those stipulated in Section 11.2.1.8 of this Annex for the same non-Key Role of the Maintenance Team.
IT Specialist	Same requirements as those stipulated in Section 11.1.1.4 of this Annex for the Key Roles of IT Specialists of the Implementation Team. Reference to IT Specialist may be an IT Specialist for network and system infrastructure, or IT Specialist for virtualised server infrastructure, or IT Specialist for storage and backup, or IT Specialist for application architecture, or IT Specialist for biometrics.
Database Administrator	Same requirements as those stipulated in Section 11.2.1.8 of this Annex for the same non-key Role of the Maintenance Team.
Systems Engineer	Same requirements as those stipulated in Section 11.2.1.8 of this Annex for the same non-Key Role of the Maintenance Team. Reference to Systems Engineer may be a Systems Engineer for network infrastructure, or Systems Engineer for server, storage and backup.

Table 7A-11.2.1.10 Minimum Experience Requirements for the Roles under the Annual Quota / System Changes

11.2.1.11 Upon commencement of the Maintenance Period, the Contractor shall in accordance with its nominations as set out in Table 5-7.5(A) of Schedule 7 of Part V arrange the relevant nominees to fill in the Key Roles of the Maintenance Team(s) to perform System Support and Maintenance Services throughout the Maintenance Period.

11.2.2 Major Responsibilities of the Roles of the Maintenance Team(s) and the Annual Quota

11.2.2.1 The project manager(s) shall perform overall on-going management of the project and ensure delivery of the project to time and quality. The project manager shall be the single contact point to conduct the project tracking and control for the System, resolve project issues, apply quality control management, liaise with Other Contractors to provide the System Support and Maintenance Services.

11.2.2.2 The systems analyst(s) shall report to the project manager(s) and perform all aspects of System Support and Maintenance Services, including production problem troubleshooting, system analysis and design, application development and implementation, and so on.

11.2.2.3 The analyst programmer(s) shall report to and assist the systems analyst(s) to perform all aspects of System Support and Maintenance Services, including production problem troubleshooting, technical support, system analysis and application programming, etc.

11.2.2.4 The IT specialist(s) shall report to the project manager(s), and be responsible for providing expertise advice on specialised technology areas related to the System and assist the Maintenance Team(s) in performing technical design and the System Changes.

11.2.2.5 The database administrator(s) shall report to the project manager(s), and be responsible for providing expertise advice on data analysis and modelling, database definitions and design, database performance tuning and monitoring related to the System and assist the Maintenance Team(s) in performing technical design and the System Changes.

11.2.2.6 The systems engineer(s) shall report to the project manager(s) and work with other Maintenance Team members in all aspects of System Support and Maintenance Services, including installation, modification of configuration, testing and troubleshooting for the network infrastructure, troubleshooting of server, storage and backup infrastructure and so on.