Intelligence Solutions
Lawful Interception and Monitoring

Nokia Siemens Networks

Using telecommunications to target terrorism and crime

State-of-the-art systems for communication monitoring

Contents

Never before has information been exchanged so rapidly and in so many ways. Needless to say, criminals and terrorist organizations have also been quick to realize the vast opportunities presented by modern telecommunications.

When it comes to fighting crime and thwarting terrorist attacks, law enforcement and government security agencies need the right communication tools to get results.

This is why state-of-the-art systems are an absolute 'must' in monitoring the communications of specific groups or individuals, for example in preventing criminal activities or collecting hard and fast evidence.

Network operators around the world are also increasingly involved in issues through the changes in legislation and standardization that require their equipment to be able to monitor or record all forms of telecommunications whenever necessary.

Based on ETSI compliant components, Nokia Siemens Networks Intelligence Solutions has the perfect and comprehensive solution for your needs, whether you are a network operator, a service provider, law enforcement or governmental agency. Our offer is scalable in size and capacity and with extendable interfaces, and even on a turnkey basis, if you like.

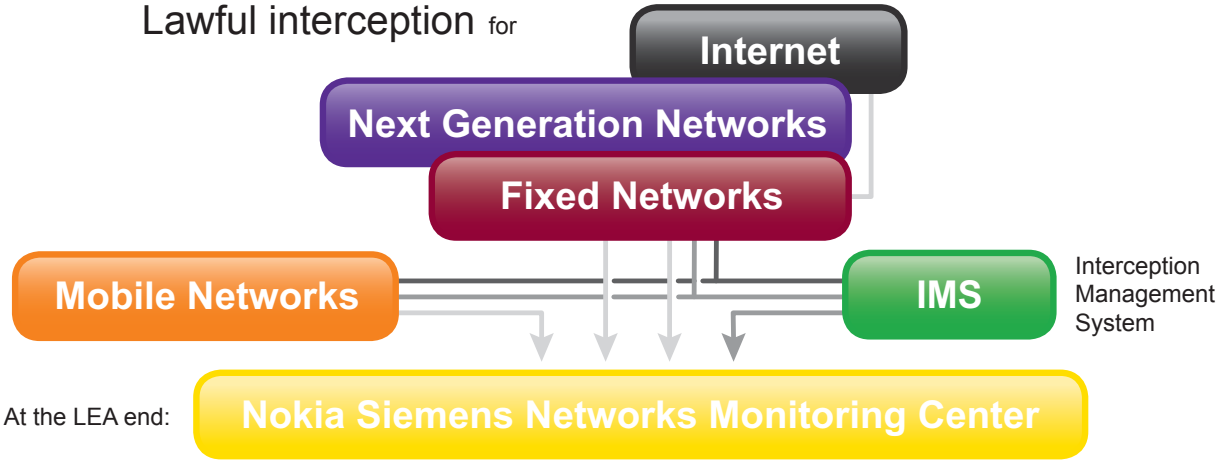
Nokia Siemens Networks Intelligence Solutions is worldwide the only vendor who can offer a complete end-to-end lawful interception solution.

We also offer you a wide range of services with worldwide support. Prior to and after project implementation – with 150 years of expertise in telecommunications and an internationally experienced team of security-cleared experts.

Our ‘Lawful Interception and Monitoring concept’ – the solution for the needs of all networks, LEAs, and government agencies.

At the network end:

Lawful interception for



Equipping network operators for all eventualities ...

Is it sufficient to install special equipment as the need arises?

There are many benefits with Nokia Siemens Networks LI solutions integrated in standard network equipment. The beauty of these is that they

- come from a single source
- do not require any additional space or camouflage
- are ready for operation at all times
- fulfill the most stringent of legal requirements
- do not interfere with regular network operations in any way
- function reliably, securely and discreetly on the basis of globally proven network technology
- permit centralized operation and system maintenance/ troubleshooting

Do you need high-security areas and specially trained staff for all switches?

This is no longer necessary if you use our efficient Interception Management System (IMS). With low space and cost requirements, IMS offers location as well as organization-independent and thus highly flexible administration of lawful interception. Even in its smallest configuration, it can handle

- central administration of more than 1,000 lawful interceptions at any one time in different networks
- integration of system users located far from the central IMS server or external users working with LI applications from other vendors

As a telecom carrier you probably already know that you are obliged to perform lawful interception in all your networks and for all the telecommunications services you offer. This means you need to have the equipment required by law and be prepared to act rapidly, if need be. After all, your operating license depends on it.

Understandably, however, you also want to minimize the resources deployed in lawful interception and prevent this from interfering with your core business. So, how can you make sure you are always prepared – in terms of both staff and technology – while remaining within your budget?

What about the need to invest in new solutions each time the requirements have changed?

Choose a system that can evolve over time and thus meet all your future needs. The network-end LI solutions from Nokia Siemens Networks can be

- scaled in size
- configured separately in terms of capacity
- adapted to comply with different legal requirements
- expanded if necessary to accommodate new standards and interfaces

Are there any additional precautions to protect the system and network from unauthorized access?

Security is already an integral component. LI solutions from Nokia Siemens Networks

- are based on standard network equipment, and thus not even detectable by experts
- function completely independently of regular network operations
- are operated centrally via a management system with a security-oriented user concept and sophisticated access protection
- additionally protect the network elements against unauthorized access through a special authentication process

Or perhaps would you rather avoid all the hassle?

Then let us do the work.

With a service mandate you can delegate the entire area of lawful interception to our security-cleared LI experts. These are well versed in all the relevant technical and legal issues on an international level.

Please have a look at page 23 for more on our comprehensive service offer.

Answering the transformation of the telecom landscape ...

Is a complete data inflow from all networks guaranteed?

You can be sure of this, if the network uses LI solutions by Nokia Siemens Networks. Collecting data from fixed and mobile public networks, Next Generation Networks and the internet provides you with

- Intercept Related Information (IRI), i.e. details on any successful or unsuccessful target activity
  - for example every telephone call that is diverted, any changes made on the subscriber line (such as feature activation and deactivation) or, in case of mobile networks, the subscriber's current location
- call content, i.e. the complete content of all voice, fax and data transmissions from or to the target
- notification of all LI-relevant incidents (e.g. setting up or activation/deactivation of lawful interception in the network)

* See page 12 for a list of targets that can be monitored using Nokia Siemens Network end-to-end solutions.

Can you decide which target-data needs to be intercepted?

You should only receive the data you really need. With this in mind the Nokia Siemens Networks LI solutions offer the following data delivery options

- separate delivery of call content and IRI
- joint delivery of call content and IRI (always the case for internet data transfers, otherwise optional)
- delivery of IRI only (converted on request into e.g. ETSI or text format)
- delivery to up to five LEAs (defining for each recipient either IRI only or both, IRI and call content)

Recent changes in legislation will place an even greater burden on you in the future. Meanwhile, new technologies and the ever-expanding range of network-independent services are transforming the telecommunications landscape into a virtual jungle, with a labyrinth of intertwining paths which makes it increasingly difficult for you to follow leads. Your job is getting more and more complex.

What you really need to do now – perhaps together with the responsible network operators – is to cast a critical eye over both the end-to-end systems used for collecting and transfering information and your own equipment which receives and analyzes the data.

Is it possible to monitor all types and sizes of data transfer?

Definitely, if you use the Nokia Siemens Networks Monitoring Center at your agency. This versatile system

- 'understands' all forms of voice, fax and data communication from all fixed and mobile networks based on components from leading vendors as well as Next Generation Networks (NGN) and the internet
- is designed as standard to process call content and IRI sent separately
- can also handle huge volumes of information (e.g. from the internet) – with no loss of quality or data – thanks to its highly efficient recording systems (e.g. with full duplex/high-speed mode, voice compression)

Is data interpretation sufficiently quick?

Our Monitoring Center helps to speed up your investigative work as it

- automatically saves the data received from the networks in case-specific folders, ruling out any confusion
- permits authorized individuals to quickly access the specific information needed
- facilitates and accelerates the monitoring/surveillance process and data analysis with a range of user-friendly, practical features
- offers new and efficient ways of pursuing leads (e.g. geographic information system)

Can the system easily be adapted?

No matter which new technical or organizational requirements come into effect, the modular Nokia Siemens Networks Monitoring Center keeps you flexible and up-to-date at all times, as it

- is continually enhanced, in parallel with the evolution of network technologies
- can be extended or modified at any time on the basis of existing hardware/software components
- grows in terms of size and capacity in accordance with your needs
- can be configured in line with current requirements and adapted to comply with different legislation

IMS – the secure manager for all networks

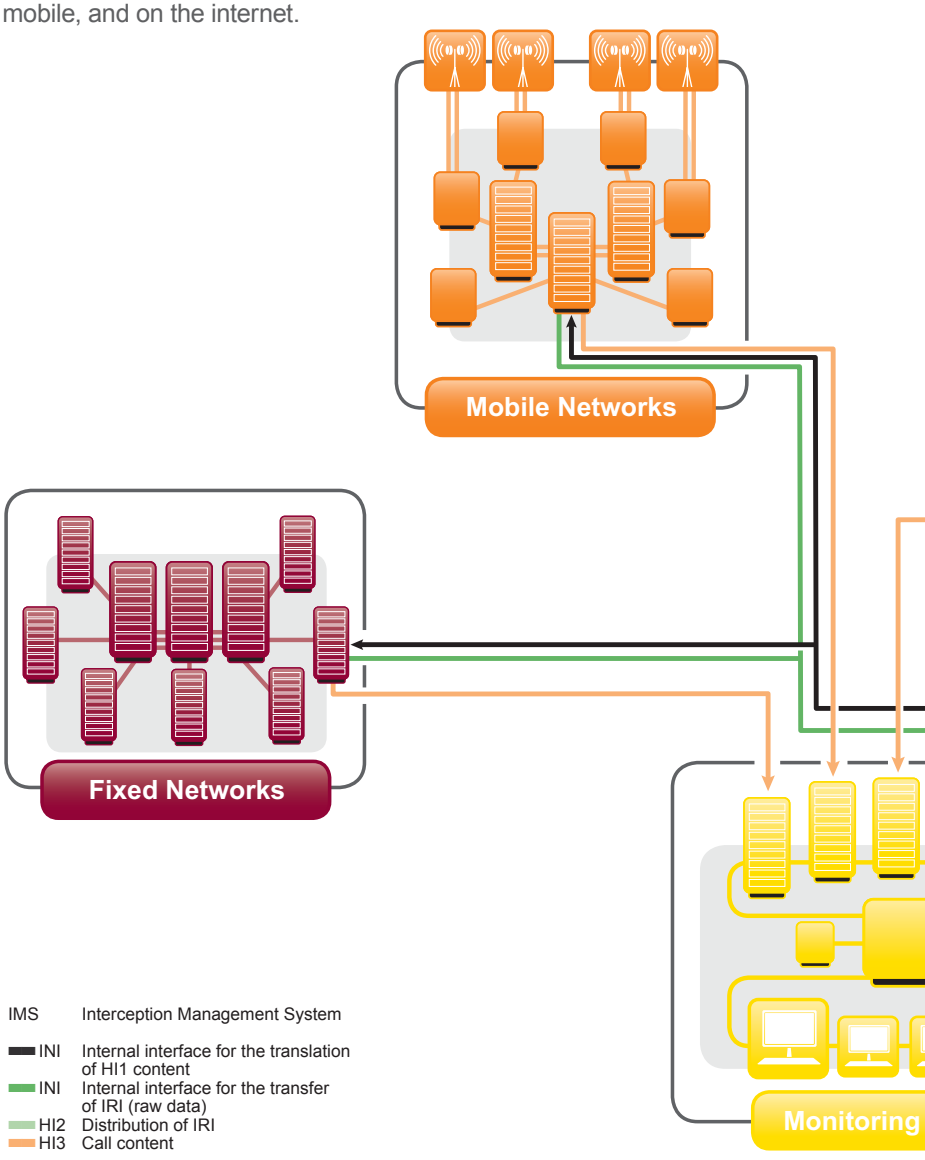
Universal

IMS is an interception management system for secure, reliable and verifiable central control of all LI-related tasks required at the network end: From setting up, starting, modifying and ending the LI instance in the network element to the administration of user-rights and auditing as well as alarm-handling and system maintenance/ troubleshooting. It is also used for mediation and distribution of IRI (Intercept Related Information, please see page 14) and for setting different filters in the data collectors used for internet surveillance.

As part of the Nokia Siemens Networks 'Lawful Interception and Monitoring concept', the IMS combined with the LI components and the Monitoring Center produces a comprehensive solution for all network and LEA requirements.

However, it can be used for vendor-independent central administration of lawful interception in all ETSI-compliant public networks: Fixed, mobile, and on the internet.

It can be used alone, in conjunction with other LI management systems, or even as an umbrella system.



An interception order has been issued. The instructions are clear. Now they need to be translated into machine language and communicated to the network.

How can this be done in a fast, economical and accurate manner? How to prevent any inadvertent or willful manipulation of the network element during the input procedure? Who checks that everything has been done properly? And what about discretion and data protection? – The answer is the Interception Management System (IMS).

Flexible

With IMS, tailor-made solutions can easily be created for a wide variety of circumstances

- with its client/server architecture, the system can be scaled to match any network size without compromising performance
- the range of offered functions also grows with the need and with special, optional feature-packages on the customer's request
- a special IMS function is available to assist in upgrading Nokia Siemens Networks network elements

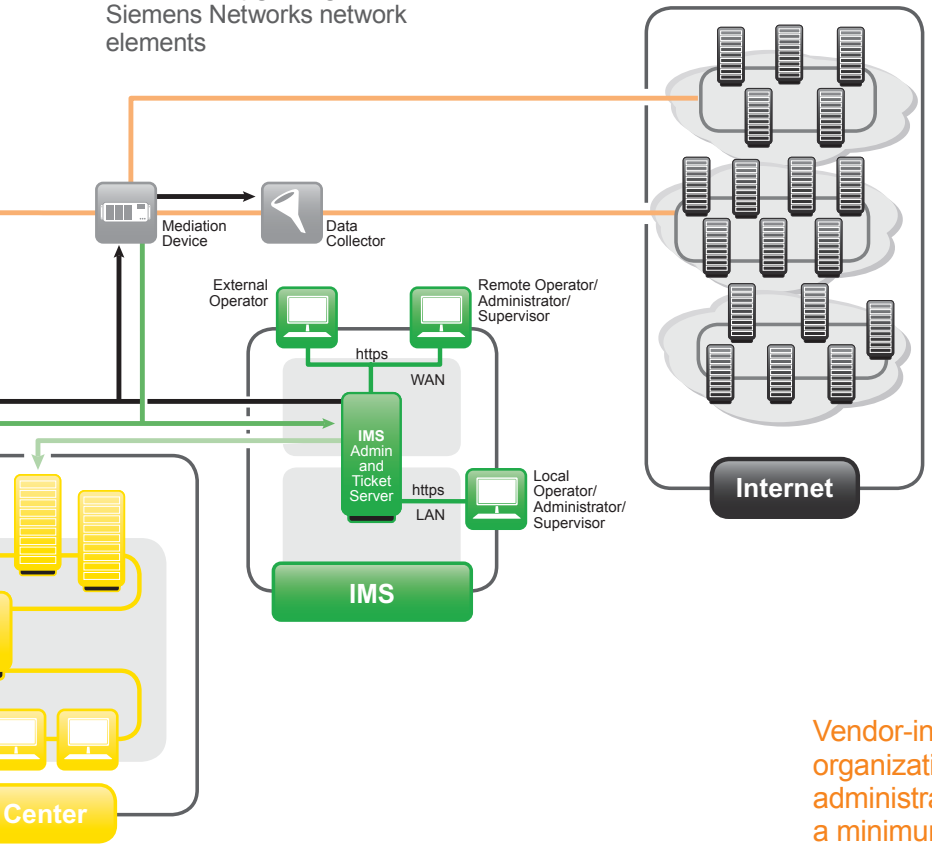
Depending on whether it is for stand-alone operation or in conjunction with other LI-operating systems, the individually configurable IMS can be used either for all LI tasks (full mode), for LI administration only (admin-mode) or for routing the IRI only (ticket-mode). This ensures a broad range of application variants for the system.

Region-independent

Now being operated in some 40 different countries around the world, IMS is globally deployed. Its security-oriented user-concept, which divides the tasks as standard into the functions of operator, administrator and supervisor, each of which with clearly defined rights, can easily be adapted to comply with different legislations.

IMS can be operated from user stations. These can be either centrally or remotely located. Remote access can be secured using VPNs. The IMS is further supported by the external operator interface. This also ensures IMS access to system-users operators, administrators, supervisors) working with an LI application by another vendor.

Other external interfaces, which may be extended as necessary, provide for the smooth integration of IMS into heterogeneous network infrastructures.



Vendor-independent. Regardless of the location and organization: IMS is all the network operator needs for administration of lawful interception in all networks with a minimum of financial and human resources.

IMS – the secure manager for all technologies and networks

Secure

Protected in a high-security area or by a firewall, IMS is operated completely separately from regular network management. The functions performed by IMS (e.g. setting up, modifying and ending lawful interception in the network or converting and distributing IRI) cannot be performed by a conventional network management system. Likewise, the IMS interception manager does not perform any standard network management functions.

IMS provides complete system and data protection by means of a hierarchically structured user concept. The GUI, strictly adapted to each specific task area, prevents users from exceeding their authority. No user of the system can access the content of the IRI transported via IMS to its authorized destination. An optional variety of system access blocks all unauthorized individuals (e.g. login with a chip card, sophisticated password system).

In addition, the LI-fixed network solutions include a special authentication procedure for additional security. This automatically comes into play in each dialog between IMS and the network element, optimally protecting the latter from sabotage.

Alert

As a LEA you can also protect yourself from sabotage or third-party monitoring by organizing yourself as a CUG (Closed User Group) in IMS. All activity in or via IMS, whether successful or not, to/from the network or to/from your Monitoring Center, is automatically logged and stored, allowing it to be checked at any time. Only the supervisor has access to this database.

Any attempt at external manipulation is immediately detected by a special IMS function. In all cases of unexpected or irregular incidents (such as network element or transmission failures), a sophisticated alarm system ensures that the relevant person is immediately notified (by a pop-up window, email, or SMS).

Our comprehensive security concept, which, as a rule, also incorporates https-based communication between IMS clients and the IMS server, redundant servers and interfaces as a rule, as well as an uninterruptible power supply, guarantees the best possible protection against unauthorized access and loss of data. This is also true when the system is operated from remote or external user stations.

High-performance browsers, for example, help the IMS Supervisor fulfill his control function. One of these is the log browser which makes it easier for him to keep an overview of the various procedures processed via IMS...

IMS prevents users from exceeding their authorization through user-specific menus, strictly tailored for the specific authorizations of operators, administrators and supervisors. A range of efficient and practical features simplify and speed up the execution of all the LI-related tasks to be performed on the network side.

Important for law enforcement agencies...

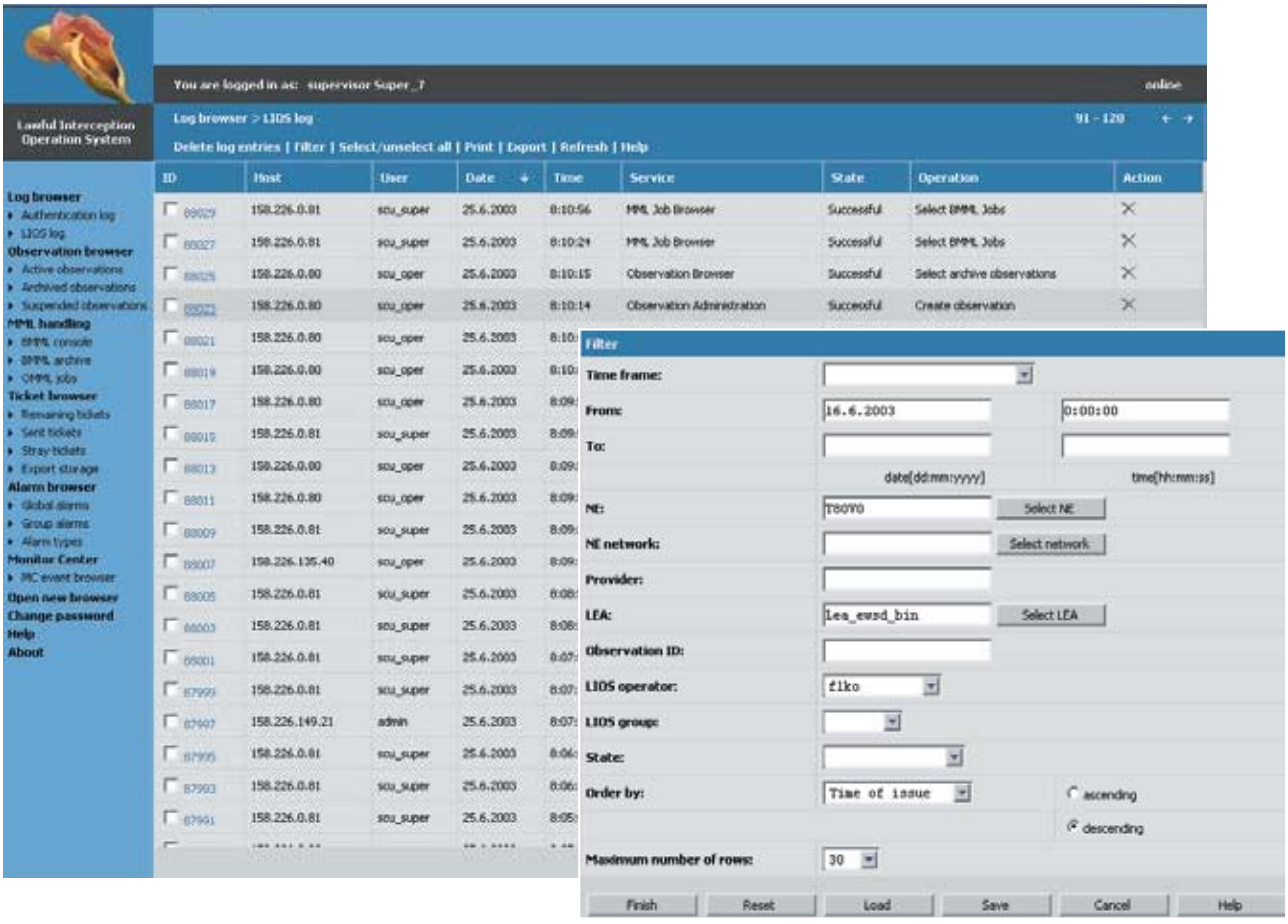
Intercept Related Information (IRI) which cannot be forwarded to you straight away is never lost. It can subsequently be retrieved via IMS only and, on your request, also be manually made available for you as a file on a removable storage medium.

Economical

The centralized interception provided by IMS, independent of both location and organization, results in substantial savings for you, the network operator, in terms of both space and staff.

A single IMS is enough to manage several thousand lawful interceptions running concurrently in various networks. Its Windows-based, user-friendly interface (see example below) and a maximum of automatic procedures minimize IMS input-errors, and simplify and speed up all steps involved.

... here the supervisor can define which processes he would like to see listed in the log browser



Lawful Interception and how it works ...

The Nokia Siemens Networks end-to-end LI solutions can be used to monitor the following targets

in fixed networks and Next Generation Networks

- all types of subscriber access
  - analog subscriber access
  - ISDN-BA and ISDN-PA
  - coin- or card-operated payphones
  - directory-number-based calls in IP networks
  - PBX directory numbers (if included in the signaling)
  - individual MSNs (multiple subscriber numbers) of an ISDN basic access
- switch-internal subscriber numbers
- FDNs (foreign directory numbers, i.e. switch-external directory numbers, such as in case of calls from or to extensions or directory numbers in transit traffic)
- nailed-up connections (dedicated lines)
- calls with call diversion
- conference calls (a special LI function combines the call content in this case)

in mobile networks

In addition to the targets of fixed networks and Next Generation Networks

- all types of mobile phones
- circuit-switched traffic in GPRS and 3G networks
- packet-switched traffic in GPRS and 3G networks

on the internet

- internet traffic at access points in the following areas
  - local loop / access provider
  - service provider
  - backbone

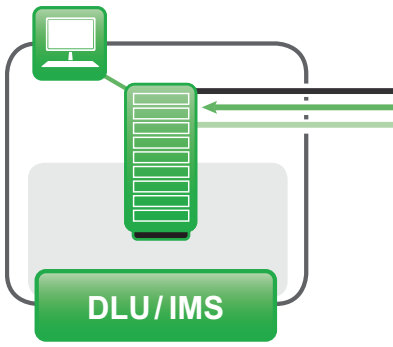
What are your main expectations of an end-to-end lawful interception solution?

As a network operator you want to be able to comply with the legal requirements at minimum cost and prevent any adverse effects on your core business.

As a law enforcement agency you want to be able to monitor a complete spectrum of targets, receiving only the relevant data from the network – as required by your organization.

The LI solutions as a part of our 'Lawful Interception and Monitoring concept', designed for deployment in various different networks, address the needs of both sides.

No need for camouflage. No extra space required. No interference with regular network operation: For the network operator, LI solutions integrated into standard network equipment are the most discreet, secure and cost-effective means of performing lawful interception in fixed and mobile networks from Nokia Siemens Networks. For you, the law enforcement agency, these solutions guarantee a complete, needs-oriented and confidential data inflow from all networks.



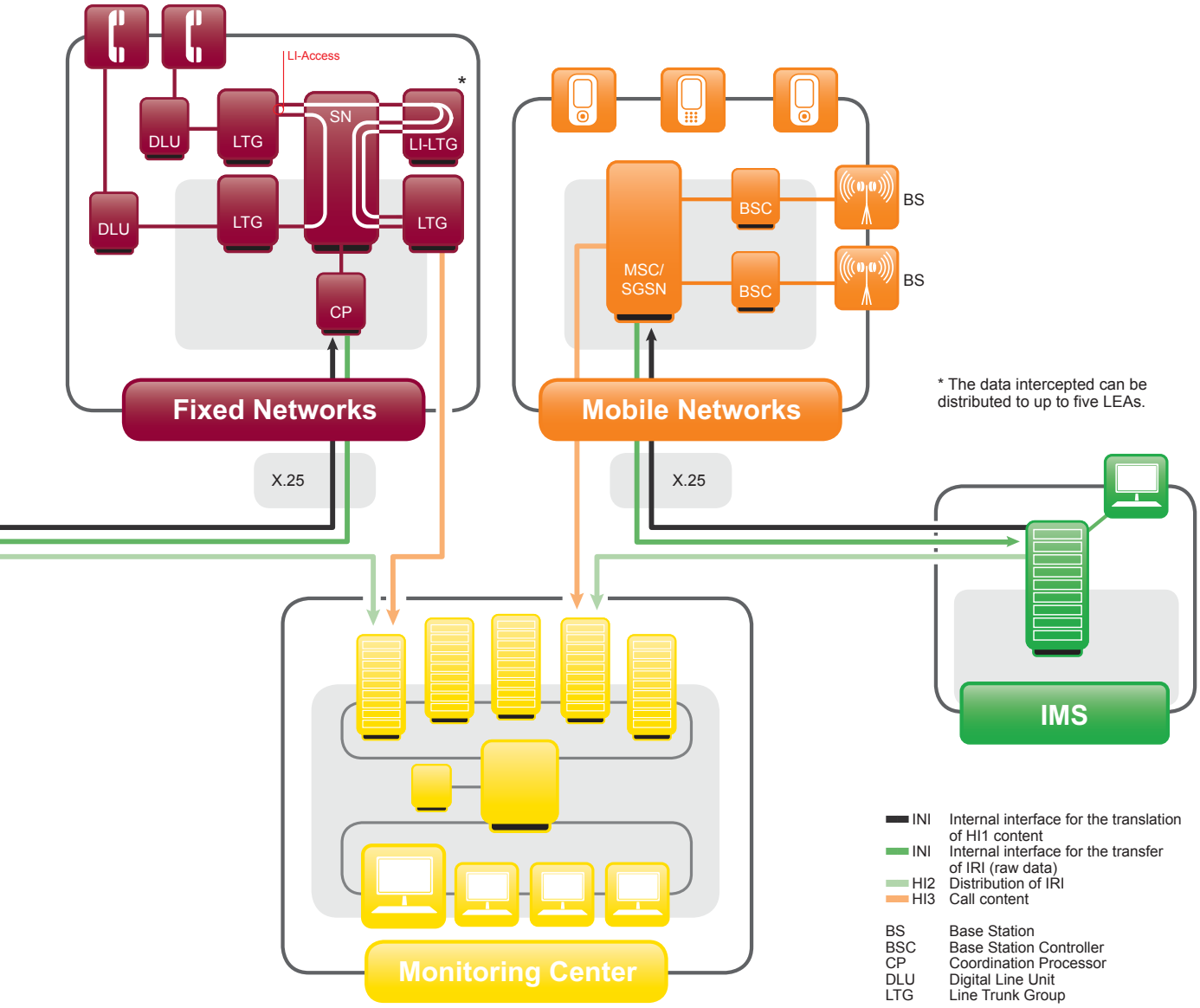
... in fixed and mobile networks ...

The lawful interception has been set up using IMS. Its starting and ending times have been defined. The subscriber line in question has already been marked for interception. At the defined time, IMS activates the interception in the network element. Once this has been done, LI begins to operate for the entire monitoring period.

Verifiable

Whenever a call becomes active on the line under surveillance, the call content (i.e. the entire content of incoming and outgoing phone calls, fax or data transmissions) is automatically intercepted and copied to a monitoring connection, which is established to the authorized LEA only for the duration of the current interception procedure.

Should any interruption or irregularity occur during this automatic procedure, the IMS operator in charge is immediately notified by email, SMS or a pop-up window. Using the messages on the IMS screen, the operator can check at any time whether data collection is running smoothly in the network.



... in fixed and mobile networks ...

Discreet

The establishment of a monitoring connection, the interception and recording of the data on the basis of standard network equipment is invisible to the target-subscriber. The process does not interfere with regular network operation in any way.

As the subscriber is not aware of the interception process, even if it starts after a call has become active, there is no risk that he may hear suspicious tapping noises and therefore perhaps cut short the call. Its recorded content is sent to the LEA's equipment directly from the switch. This is the reason why it cannot be intercepted or accessed at the IMS or manipulated in any way.

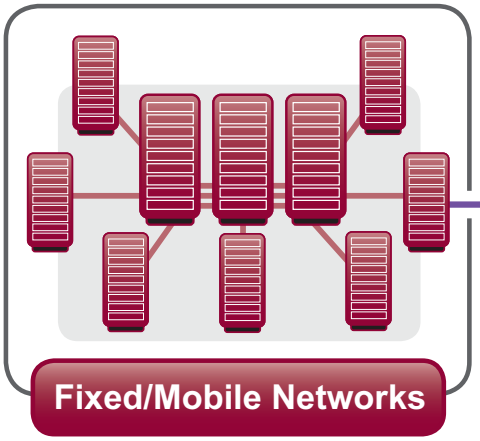
Comprehensive

Moreover, apart from the complete and discreet recording of call content, the Nokia Siemens Networks LI solutions also perform another important function: As soon as there is an activity (whether successful or not) on the monitored access, they also generate intercept related information (IRI). This may include information on the date and time of the call, the directory number of the other party, the call direction (incoming or outgoing), any call diversion procedures invoked, and (optional in mobile networks) the current location of the target subscriber. They also provide information on any technical or administrative changes made on the marked access (e.g. feature activation or deactivation).

Regardless of the call content, an IRI is first sent to IMS. From here it is forwarded via a data network (public X.25, ISDN or IP network) to the monitoring equipment of the LEA. Based on the unambiguously assigned ID criteria, the IRI is automatically correlated with the corresponding call content at the LEA. The transmission of this data on two completely separate paths is of benefit to the LEA for two reasons:

LEA-friendly

- you can decide in each case whether you need only the IRI (which often includes sufficient information in itself) or also the call content, thereby minimizing the data inflow, and thus also the time you need to evaluate it
- you can be assured that even if you do not receive any call content (for technical or other reasons), you will nevertheless have the IRI which – as already explained on page 11 – cannot get lost, even in the case of delivery problems



All the advantages of a tried-and-tested standard network solution have been incorporated into this network of the future. For you, the network operator, the LI solution for number-based traffic in Next Generation Networks is one more argument to move into the world of IP. For the LEA, this is an important addition to the range of targets it can monitor.

... in Next Generation Networks ...

Nokia Siemens Networks facilitates the migration process through a variety of solutions designed to incorporate existing TDM networks into an IP core network. Of course, this also includes an IP-based solution for LI, for secure and discreet interception of number-based traffic (i.e. voice and fax connection as well as ISDN data transmissions) in Next Generation Networks.

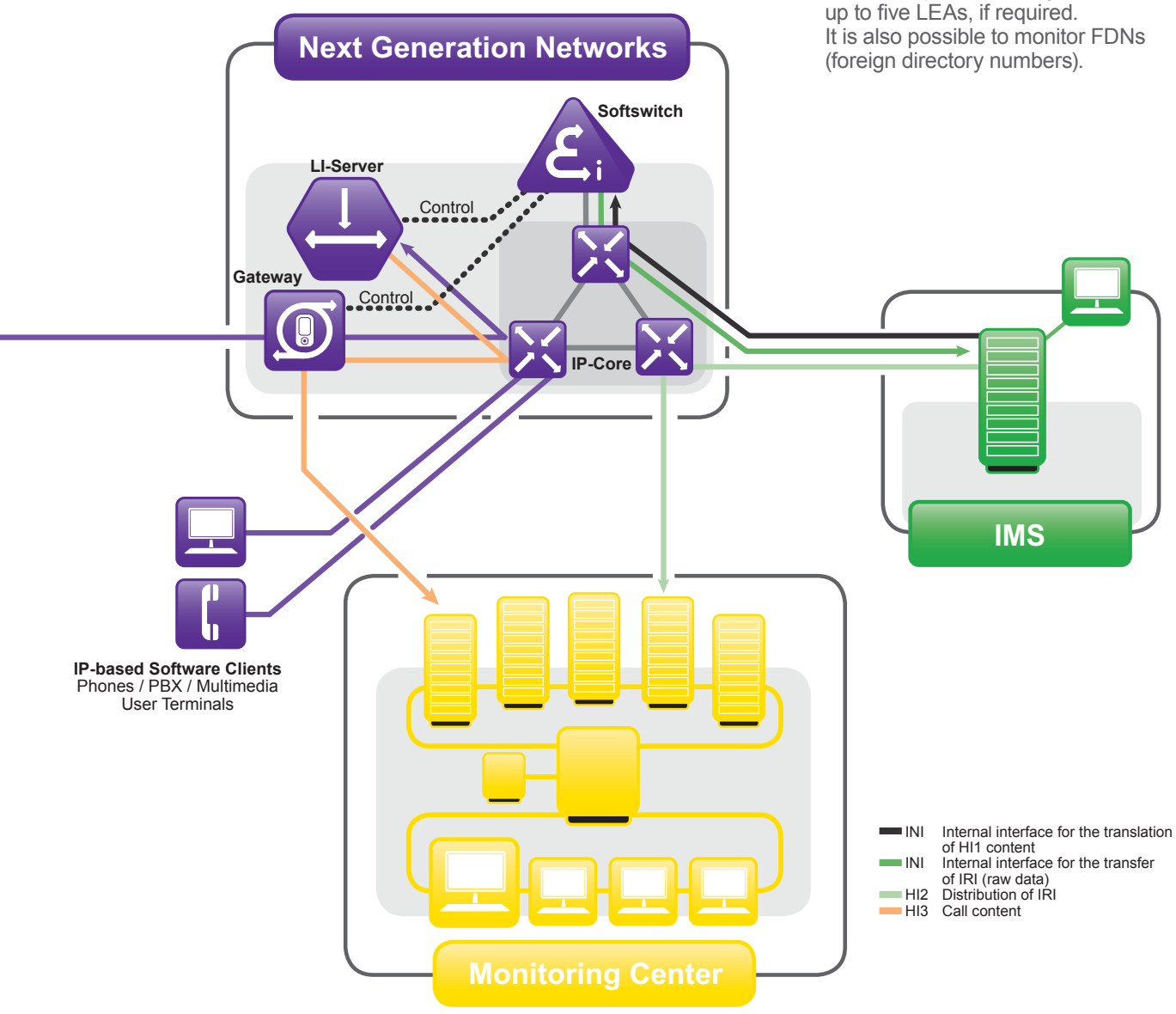
Future-oriented

As in TDM networks, the interception is set up, started and ended in a dialog between the IMS LI management system and the network element which controls the traffic to or from the monitored number. In this solution it is a standard softswitch.

Once the LI instance has been activated, this network element – in a dialog with various gateways – arranges for all the traffic concerning the target number to be routed via an LI server. Thanks to the appropriate precautions, the subscriber does not notice anything.

The packages duplicated in this server and readdressed in accordance with the instructions from the softswitch are then forwarded in the IP network to a gateway, from where they are sent to the LEA's monitoring equipment. The IRI generated in the softswitch reaches the LEA via IMS, independent of the call content.

Even in this purely IP-based solution, the intercepted data may be sent to up to five LEAs, if required. It is also possible to monitor FDNs (foreign directory numbers).



... and on the internet

The internet has become an increasingly complex formation of public and private computer networks that now also includes wireless transmission media. Every day masses of data pass through this global network used by more and more people who exchange information and keep in contact in many different ways.

The ETSI specifications on the monitoring of internet users are in place and are already met by the Monitoring Center. The Nokia Siemens Networks concept offers LEAs a comprehensive solution to help them fight crime on and via the internet. The end-to-end components of this solution are

Customized

By means of integrated LI functionality in the components of the IP network as well as by separate high-performance data collectors data can be intercepted and filtered based on predefined criteria.

According to the requirements, interception can be deployed at different access points: At the internet access provider, the internet service provider, or the internet backbone itself.

A mediation device used for adapting interfaces and also re-filtering, if necessary, distributes the required data to the LEAs.

Several types of data collectors with different interfaces and throughputs are available. Combined with individual mediation devices which also directly interface to LI-enabled IP network components, they produce perfectly tailored solutions.

As part of the Siemens 'Lawful Interception and Monitoring concept', these data collectors team up with the LI components and IMS or the Monitoring Center to produce a comprehensive solution that meets all the needs of both network operators and LEAs.

They can also be used on a vendor-independent basis for secure, reliable and verifiable collection of voice and data communication on the internet.

The integrated LI functionality and the data collectors outlined here record all types of IP-based telecommunication, including web sessions, email and chats, from

- internet service/acess providers
- internet backbone connections
- internet core computers and all other IP sources.

For the network operator the LI solution is a secure and yet flexible basis to easily record huge volumes of intercepted data in this telecommunications area. For the LEA it is an efficient means to pursue leads in the global network. And for the internet it is powerful, reliable and for lease, according to your preference.

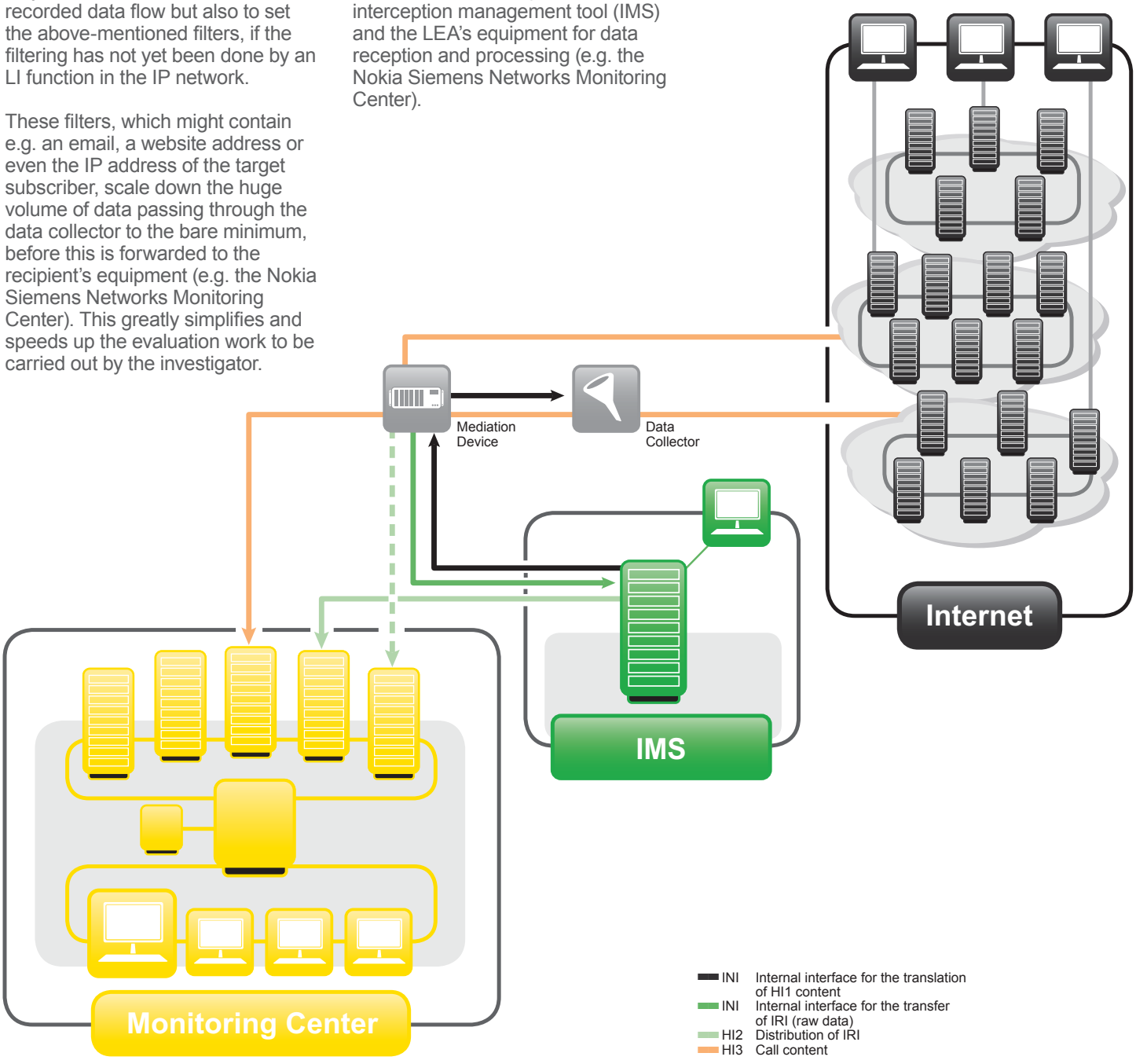
Efficient

Lawful interception is set up and managed in the data collectors by means of an appropriate and powerful interception management system such as IMS. This will be used by the the LI operator not only to define the destination of the recorded data flow but also to set the above-mentioned filters, if the filtering has not yet been done by an LI function in the IP network.

These filters, which might contain e.g. an email, a website address or even the IP address of the target subscriber, scale down the huge volume of data passing through the data collector to the bare minimum, before this is forwarded to the recipient's equipment (e.g. the Nokia Siemens Networks Monitoring Center). This greatly simplifies and speeds up the evaluation work to be carried out by the investigator.

Secure

Any system connected to the internet is at great risk of coming under attack. This risk has been minimized in the solution described. Virtual private networks, anti-virus and anti-hacker tools and special firewalls are used to protect both the interception management tool (IMS) and the LEA's equipment for data reception and processing (e.g. the Nokia Siemens Networks Monitoring Center).



Our Monitoring Center
a perfect match

The interception has been activated. The process is running. Information from various sources is flowing along different paths into your equipment.

What now?

The incoming data has to be decoded and allocated to its specific case. Any misunderstandings or confusion arising here could have serious consequences. During evaluation, even the tiniest of details may need to undergo more in-depth analysis.

How can you protect this valuable data from manipulation or theft? And what happens in the case of a power outage?

To meet this challenging task, law enforcement agencies in more than 60 countries around the world place their trust in the Nokia Siemens Networks Monitoring Center.

Versatile

Our Monitoring Center is an extremely versatile construction of software and hardware modules. Its various components work together in perfect harmony, enabling it to perform all the LI-related tasks of a law enforcement agency in a secure, reliable and verifiable manner; from decoding, converting, correlating and analyzing the information received, to its storage and interpretation, and even a wide range of administrative tasks. As part of the Nokia Siemens Networks 'Lawful Interception and Monitoring concept', the Monitoring Center teams up with the network components and the IMS to form a comprehensive solution that meets all the needs of both, network operators and LEAs.

By virtue of its ETSI compliance and modular architecture, it can also be incorporated into all monitoring solutions based on the telecom systems of other leading vendors.

The Nokia Siemens Monitoring Center monitors all types of voice, fax and data communication in fixed and mobile networks as well as in Next Generation Networks (NGN) and on the internet:

- telephone conversations
- fax and modem traffic
- SMS and MMS
- emails, web sessions, chats etc.

It also supports the reception, processing, correlation and evaluation of the IRI described on page 14. If preferred, it can be configured for countrywide monitoring of all fixed networks, mobile networks, NGN and the internet.

Flexible

Changes to requirements? Heterogeneous network infrastructures? New technologies to be addressed, higher data volumes to be handled, or more types of communication to be monitored?

This is all very easy with the Nokia Siemens Networks Monitoring Center. Its modular design, which comprises Front-End and Back-End components (see illustration), makes it extremely flexible. The individual Front-Ends which support the interfaces from the different telecommunications networks can be adapted to match a wide variety of communications systems and replaced or expanded as necessary.

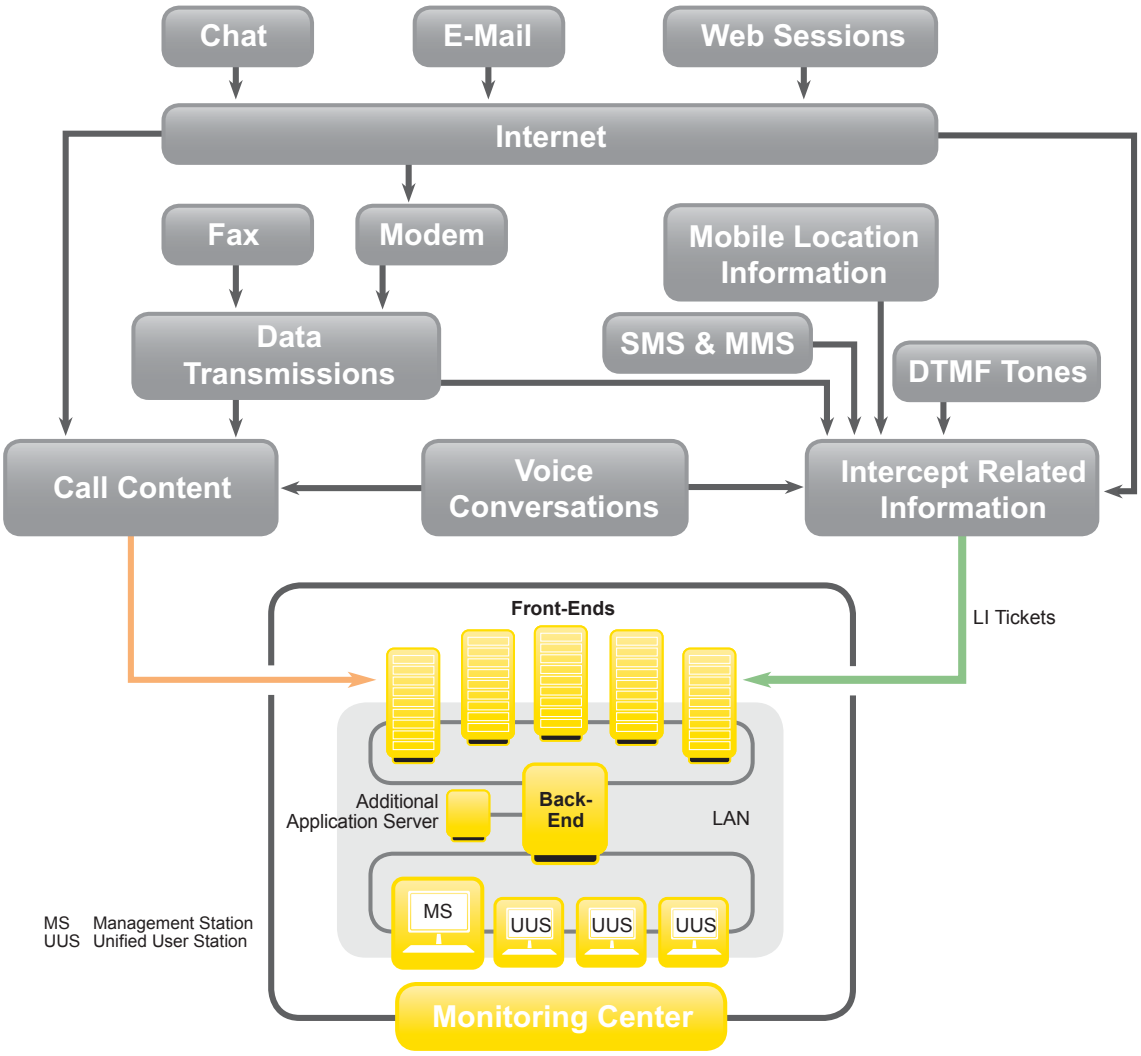
Thus, the system can be modified or expanded at all times on the basis of the existing hardware and/or software. For you, the LEA, this means you only need to invest in the elements you actually need, resulting in a customized solution that satisfies all your requirements at all times.

Deployed throughout the world, our Monitoring Center is everything a law enforcement agency needs for efficient monitoring and prompt evaluation of all types of telecommunication, today and tomorrow.

A perfect match, meeting all requirements.

The **Nokia Siemens Networks Monitoring Center** – assists LEAs in their investigative work by

- monitoring of all types of voice, fax and data communication in fixed and mobile public networks, the NGN and on the internet
- problem-free interaction with lawful interception solutions in heterogeneous network infrastructures
- extensive process automation (decoding, processing, assignment and storage of intercepted data)
- various recording modes (mono, stereo, full duplex, high speed) and voice compression
- automatic recognition of fax and modem data during call recording
- optimized on-screen presentation of data
- user-friendly features for timely data analysis
- add-ons (e.g. geographic information system, link analysis) for efficient ways to pursue leads



The Nokia Siemens Networks Monitoring Center

Process-optimized

As a primary function, the wide range of automated processes supports and facilitates the investigator's work. This begins with the incoming information. The various Front-Ends first decode the data received from the networks – widely varying in terms of both type and volume – and convert it into a uniform system-internal format. Subsequently, the processed data is forwarded to the Back-End.

The Back-End, where the incoming content and IRI are combined and automatically assigned to the corresponding interception case and stored in folders, offers a Windows-based user interface which is made up of two components.

The benefit is an immediate access to call content – even if IRIs are delayed. And this happens quite often.

The Management Station (MS) enables the system administrator to adapt the configuration of our Monitoring Center to the LEA's changing requirements at all times.

The Unified User Station (UUS) is a versatile part that assists the LEA in performing day-to-day monitoring tasks. It provides the LEAs with all recordings and other information from the network in an optimized form with the click of the mouse-button. The LEA can quickly and easily retrieve the LI information sent from the network from the folder in which it is stored. Thanks to system-internal fax and data demodulation/decoding, the recorded signals are displayed as readable documents on the screen (e.g. as a fax page or a web page).

User-friendly

Regardless of whether the LEA is monitoring phone calls, reading the content of a fax or SMS, or for instance evaluating an internet chat session, it always controls the individual processes on the user interface in the same intuitive manner, irrespectively of any system expansions.

Our Monitoring Center offers different operating modes for receiving and recording data intercepted in the network; some of these are automatically controlled, some manually configured, according to requirements.

This greatly simplifies the investigator's work and allows a more efficient deployment of system resources.

The system automatically detects if a fax or data transmission begins during the recording of a telephone conversation. It then accordingly switches to the 'high quality' or 'high speed' recording mode. This subsequently guarantees a successful demodulation of the digital signals during transmissions which use the entire bandwidth.

Various levels of compression available to economize on storage space when recording voice calls two modes available when setting up monitoring in IMS

- stereo (advantage: both conversation directions can subsequently be interpreted separately or together)
- mono (saves online capacity)

Bringing the LEA closer to its target…

The UUS (Unified User Station) of our Monitoring Center supports the LEA with a Windows-based user-friendly interface for data evaluation, for example in wiretapping.

Innovative

A significant number of add-ons are available to complete the scope of the Nokia Siemens Networks Monitoring Center.

Offering efficient means of pursuing leads, these are all most valuable to investigative work.

One example is location tracking by means of the Geographic Information System (GIS):

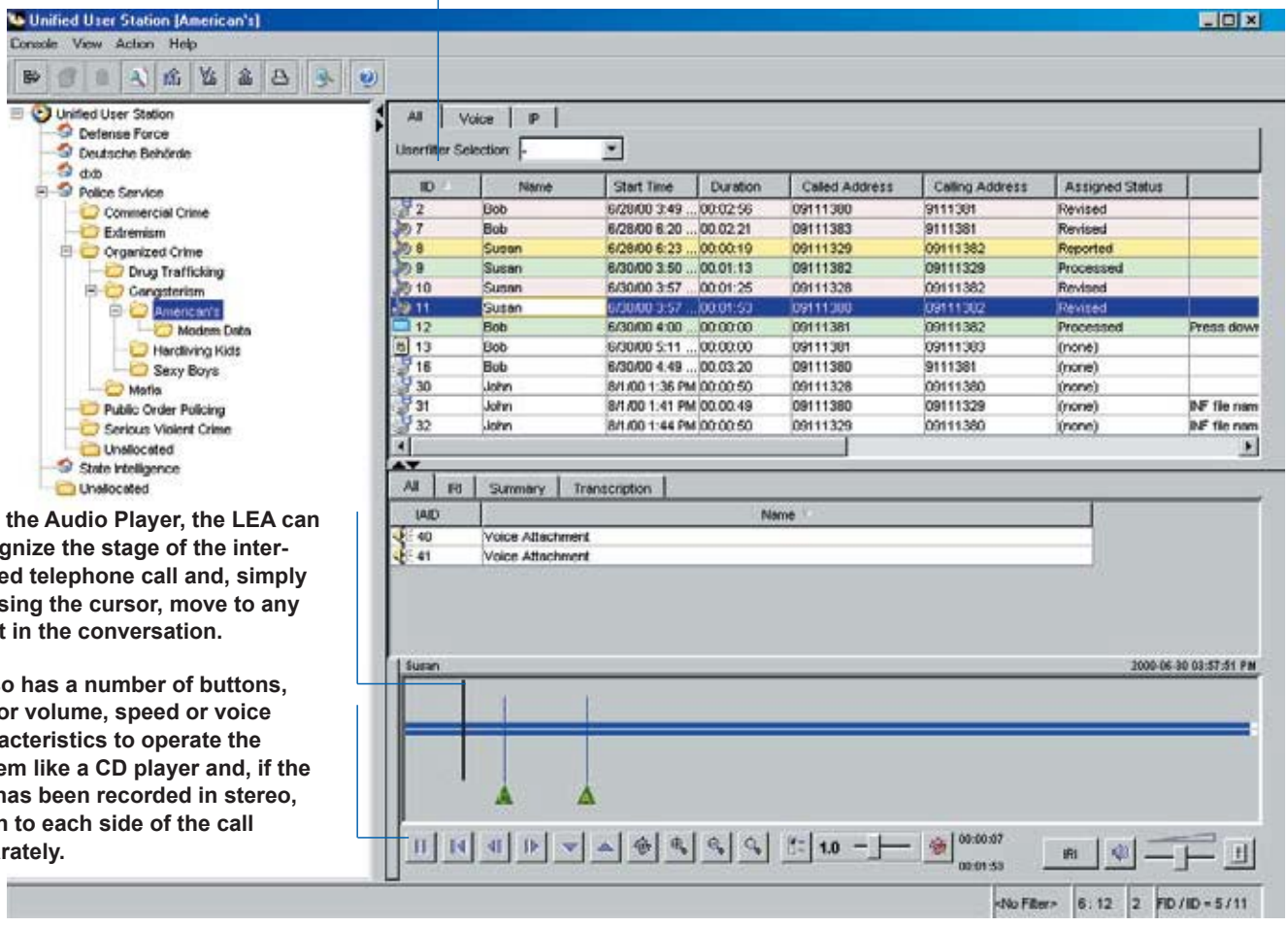
Within mobile telephone networks, this feature determines the current location of the marked mobile device (with variable accuracy within and between networks).

The obtained information is transmitted to the Nokia Siemens Networks Monitoring Center (in the form of IRI).

There it is visualized on a map on which the user's (or at least the phone's) current movements and route can be tracked live – as long as the corresponding data continues to flow.

System users have a number of different map views and layers to select from.

Powerful filters help the LEA to quickly identify the important conversation.



With the Audio Player, the LEA can recognize the stage of the intercepted telephone call and, simply by using the cursor, move to any point in the conversation.

It also has a number of buttons, e.g.for volume, speed or voice characteristics to operate the system like a CD player and, if the call has been recorded in stereo, listen to each side of the call separately.

Nokia Siemens Networks Monitoring Center

Reliable

When it comes to data and system protection, the Nokia Siemens Networks Monitoring Center is again an excellent choice, and one that also meets the customer's special needs.

Through its modular, multilevel security and control concept for authorities, administrators, groups of LEAs and individual LEAs, it can be adapted to meet the requirements of individual organizational structures and different legal requirements.

Unauthorized system access is prevented by means of a series of protective mechanisms involving individual passwords coupled with user-specific rights.

Special precautions have been taken to ensure that the case-specific folders, which store all the data intercepted in the course of monitoring, cannot be confused or mixed up under any circumstances.

An entire range of special system-internal measures protect the recorded data from manipulation, theft or destruction. If necessary, all of these mechanisms may be reinforced (e.g. against hacking or other internet threats) by firewalls, VPNs or virus/intrusion protection tools.

System components can also be duplicated to guarantee system availability and prevent the loss of any saved data. And in order to prevent data getting lost in the case of a power outage during monitoring, the Nokia Siemens Networks Monitoring Center can also be equipped with its own uninterruptible power supply system.

Our Services
rounding off the product

Worldwide

Service components prior to and during project implementation

- recommendations for optimizing system capacities
- project management
- system and network integration
- training for system users
- technical workshops
- tailored financing solutions and leasing arrangements

Service components after project implementation

- system support
- system maintenance
- hardware and software upgrades
- advice and system optimization

Individual

And then there are special services ...

... for the network operator

- comprehensive advice in meeting the legal requirements when planning LI solutions for new NGN and IP networks
- assumption of all the tasks involved in the case of judicially authorized interception (i.e. outsourcing the LI operator, administrator and supervisor functions to suitably qualified Nokia Siemens Networks experts)

... and for the law enforcement agency

- in-depth analysis of the monitoring possibilities (including traffic analyses)
- basic training in the field of lawful interception in IP networks

Nokia Siemens Networks offers a wide range of monitoring services for supporting both network operators and law enforcement agencies.

As part of the Nokia Siemens Networks 'Lawful Interception and Monitoring concept', these services team up with the LI-, IMS- or MC-features and produce a comprehensive solution that meets all needs of network operators and LEAs.

The components of LI and Monitoring at a glance

At the network end ...

IMS
An ETSI-compliant management system implemented in a client/server architecture as a vendor-independent solution, also used for the mediation and distribution of IRI. It provides centralized control and administration of lawful interception in public fixed and mobile networks, as well as in NGN and the internet

LI 1 – for monitoring all forms of telecommunication in public fixed networks
A solution based on standard network elements used to automatically duplicate/generate all data (call content and IRI) from any activity on a target and forward this to up to five LEAs.

LI 2 – for monitoring all forms of telecommunication in mobile networks
A solution based on standard network elements used to automatically duplicate/generate all data (call content and IRI) from any activity on a target and forward this to up to five LEAs.

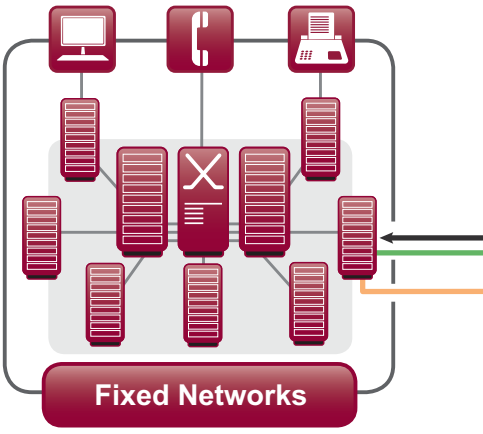
LI 3 – for monitoring number-based traffic in Next Generation Networks (NGN)
A solution based on standard network elements (softswitch and LI server), used in an NGN (IP core network with integrated TDM networks) to automatically duplicate/generate all data (call content and IRI) from any activity on a target and forward this to up to five LEAs.

LI 4 – for internet surveillance
A solution based on integrated LI functionality in IP components or on special equipment (powerful data collectors) used to duplicate and filter the flow of data to access points around the access provider, the service provider or the backbone. There are a number of different data collectors and, upon request, these are also available in combination with individually configured mediation devices (for interface adaptation and data distribution).

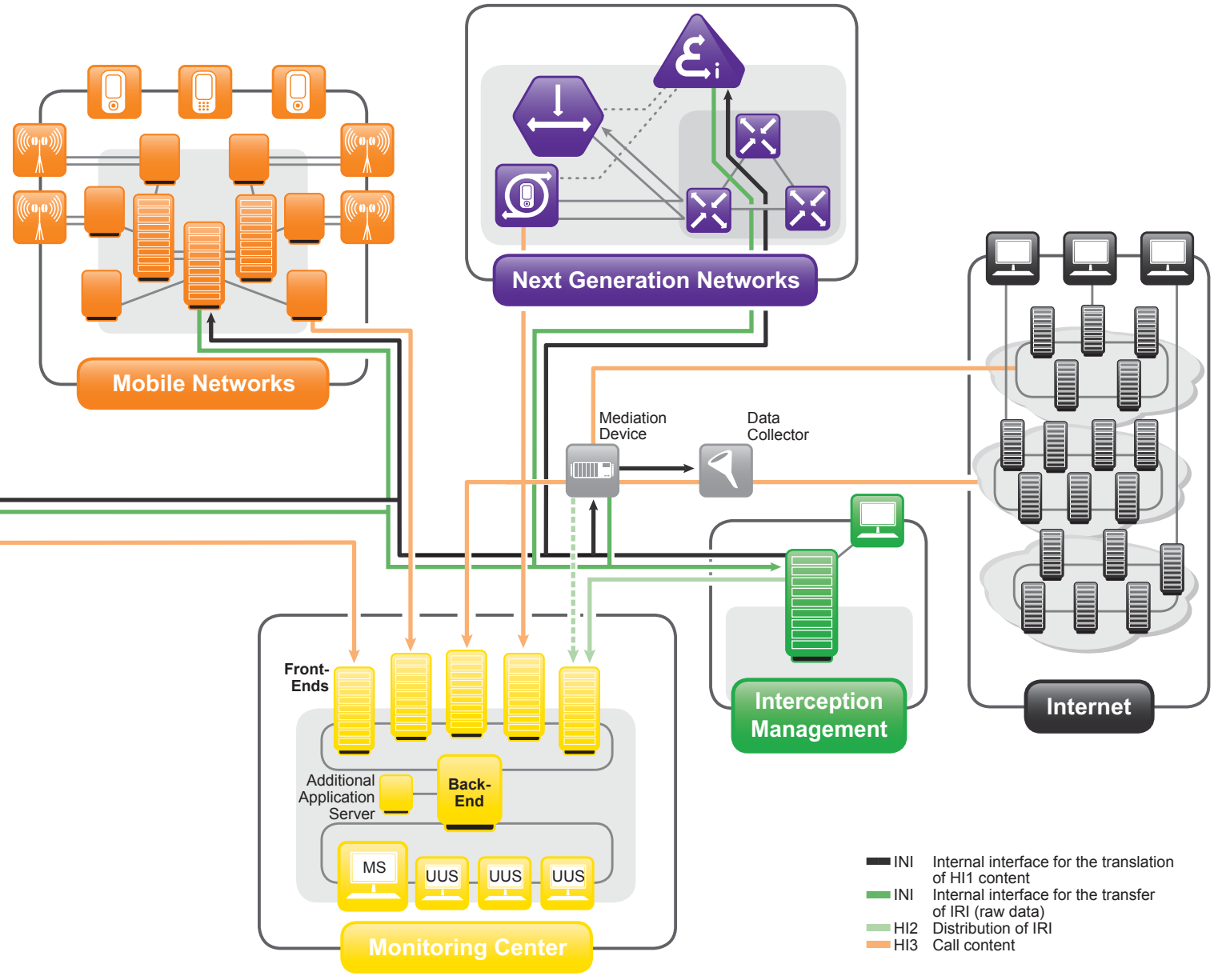
On the LEA side…

For receiving, processing and evaluating all types of voice, fax and data traffic from all fixed and mobile public networks, from Next Generation Networks and the internet.

Our Monitoring Center is a modular, vendor-independent and ETSI-compliant system, configured as standard to receive the call-content and intercept related information (IRI) separately.



The ‘Lawful Interception and Monitoring UUS concept’ offer solutions that meet the needs of both network operators and LEAs.



Our customers' benefits – at a glance

- individual, ETSI-compliant solutions, scalable in size and capacity for all network and LEA requirements
- secure, discreet, verifiable, cost- and space-saving performance of LI in all networks
- complete spectrum of possible targets
- immediate access to call content – even if IRIs are delayed
- nationwide monitoring
- fully automatic recording/generation and processing of all data from all activities of the target
- high level of system and data security
- great flexibility in the administration of LI instances (independent of location and organization)
- simple and fast data processing/evaluation through a maximum of process automation and user-friendly, practical functionality
- efficient ways to pursue leads

Our strengths – our customers' gain

Nokia Siemens Networks is a leading global enabler of communications services. The company provides a complete, well-balanced product portfolio of mobile and fixed network infrastructure solutions and addresses the growing demand for services. It is one of the world's largest telecommunications infrastructure companies and has operations in some 150 countries. Its headquarter is in Espoo, Finland. The merger has combined Nokia's former Networks Business Group and the former carrier related businesses of Siemens Communications.

The excellent quality of our end-to-end solutions is founded on our particular strengths:

IP convergence
Our convergence solutions open up an enitirely new world of IP services and solutions to our customers – with the same proven level of security and reliability as our voice communication. Futureproof migration strategies guarantee the best possible protection of your investments.

Broadband access
What is the use of the fastest network without high-speed access? Our broadband access products facilitate every kind of high-speed access to the widest range of services.

Optical networking
Offering almost unlimited bandwidth and continually breaking records in transmission speed, Nokia Siemens Networks optical networks lay the foundations for the data superhighways of the future.

Partners for profitable networks
Our customers' profitability is always our highest priority. Our products and services open up new business opportunities for them and help them optimize processes. We integrate their existing systems to protect their investments. Our solutions make communication more cost-effective and contribute to a faster return on investment.

Abbreviations

3G	3rd Generation Mobile Networks
CUG	Closed User Group
DTMF	Dual Tone Multi Frequency
ETSI	European Telecommunication Standards Institute
FDN	Foreign Directory Number
GSM	Global System for Mobile Communication
GPRS	General Packet Radio Service
GUI	Graphical User Interface
HI	Handover Interface according to ETSI
HI1	HI for manual or electronic transfer of lawful interception orders
HI2	HI Intercept Related Information (LI tickets)
HI3	HI Content of Communcation (Call content)
https	Hypertext Transfer Protocol, Secure
IMS	Interception Management System
INI	Internal Interface according to ETSI
IP	Internet Protocol
IPsec	Internet Protocol Security
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISDN-BA	ISDN Basic Access
ISDN-PA	ISDN Primary Rate Access
LAN	Local Area Network
LEA	Law Enforcement Agency
LI	Lawful Interception
LTG	Line Trunk Group
MMS	Multimedia Messaging Service
MS	Management Station
MSC	Mobile Switch Controller
MSN	Multiple Subscriber Number
NGN	Next Generation Networks
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
SMS	Short Message Service
TDM	Time Division Multiplex
UUS	Unified User Station
VPN	Virtual Private Network
WAN	Wide Area Network
WWW	World Wide Web
X.25	Data network protocol

Nokia Siemens Networks GmbH & Co. KG
Intelligence Solutions
DE-81359 Munich
Germany

Visiting address:
Hofmannstr. 51, Munich, Germany
Switchboard +49 89 722 00

Order No. C40100033B2007091EN

IS-sales.nsn@nsn.com
www.nokiasiemensnetworks.com

Intelligence Solutions
Monitoring Center

Nokia Siemens Networks

Keep your eyes open

Intelligence Solutions
Monitoring Center

The Third Millennium began with a world of open borders and easy trafficking, a global village where any major destination can be reached within 24 hours.

Never before could information be exchanged so rapidly and in so many ways.

Needless to say that criminal groups and terrorist organizations also have been quick to realize the vast opportunities presented by modern communications.

When it comes to fighting crime and thwarting terrorist attacks, law enforcement and government security agencies need the right tools to get results and fulfill their mandate. Therefore, state-of-the-art monitoring center solutions are an absolute 'must' for lawful interception (LI). By monitoring the communications of specific groups or individuals, law enforcement agencies (LEAs) can discover hidden patterns and criminal structures, anticipate and prevent crimes, and collect hard and fast evidence for prosecution.

The Nokia Siemens Networks Monitoring Center (MC) has been specifically developed to service the complex needs of law enforcement agencies worldwide. It is completely user-friendly in that it offers a unified view of all intercepted data, regardless of their source. No matter what kind of data or from whichever sort of network, the Monitoring Center presents them in a standardized way because its unique architecture can concurrently handle all technologies and vendors. It is both, flexible and scalable and performs the tasks of monitoring in an auditable, secure, reliable and verifiable manner, according to ETSI LI standards.

The Nokia Siemens Networks Monitoring Center is deployed all over the world. So far more than 90 Monitoring Center solutions have been installed in over 60 countries.

The Monitoring Center is the perfect match for LEAs' needs for efficient monitoring and prompt evaluation of all types of communication – today, tomorrow and after tomorrow.

Intelligence Solutions
Keep your eyes open

The Nokia Siemens Networks Monitoring Center can be used for intercepting communications in public fixed and mobile circuit-switched networks, Next Generation Networks (NGN) and the internet.

It has been designed for integration within every telecommunications network – with any type of modern standardized switch following the ETSI recommendation (e.g. Nokia Siemens Networks, Ericsson, Alcatel, Nortel, Lucent, Motorola, Huawei). Customers vastly benefit from this multi-vendor capability as it allows easy interaction with lawful interception solutions in heterogeneous network infrastructures.

The Monitoring Center monitors two general types of intercept: Voice and data.

However, within those two types it manages the following more specific types

- internet sessions (e.g. web sessions, e-mail, chat, VoIP)
- voice conversations
- fax transmissions
- location-based information for mobile networks (location-tracking, GIS)
- SMS and MMS messages
- modem transmissions including local loop internet
- call related information
- DTMF in-band transmissions

The Monitoring Center supports interceptions from the following sources

- fixed networks PSTN
- mobile networks GSM, CDMA, GPRS, UMTS
- Next Generation Networks (NGN)
- IP Networks: Local loop, ISP, and the internet
- trunk monitoring (passive interception)
- satellite monitoring (passive interception)
- surveillance equipment

The Monitoring Center is an extremely versatile construction of interoperating software and hardware modules. It performs all LI-related tasks on the intercepted information – storage and interpretation as well as a wide range of administrative tasks – in a secure, auditable, reliable and verifiable manner. Because of its LI-conceived modular architecture, it is flexible enough to be configured as an IP interception and delivery solution to other law enforcement monitoring facilities (LEMFs).

Intelligence Solutions
Lawful Interception

The Nokia Siemens Networks Monitoring Center offers different operating modes to receive and record the intercepted data, some of which are automatically controlled and some manually configured, according to the customer's requirements and operational needs.

The operating modes greatly simplify the investigative work of LEAs and allow them to deploy more efficiently Monitoring Center system resources

- to discover hidden patterns and unlawful activities
- to anticipate and prevent crimes
- to take action and provide evidence for prosecution – and –
- to secure peace and prosperity among law-abiding citizens

Service and target monitoring are two different types of lawful interception. They may differ in scale and intent, but they both use granular triggering and filtering to fulfill their ultimate purpose.

Service monitoring

- is pro-active, even in the worldwide web
- controls the entire communications spectrum of possible targets (e.g. suspected pedophile chat rooms and websites)
- checks either each single segment of intercept or those clearly defined
- trawls in both clear and dirty water, looks for potentially unlawful activities
- generates suspects who eventually become the object of target monitoring
- defines and refines new strategic or tactical approaches
- typically requires huge data storage but smaller archiving space
- is usually used by secret services

In contrast, target monitoring may be a result of service monitoring, but it is also an independent investigative method to be used by authorized groups.

Target monitoring

- is re-active
- checks on a particular person or defined groups
- collects specific data
- controls all activities of a defined target
- will possibly be used in a judicial process
- needs typically lesser data storage but larger archiving space
- is usually used by LEAs and police forces for collecting evidence on specific persons or groups

The Nokia Siemens Networks Monitoring Center has been designed to perform both service and target monitoring, according to the customer's needs and requirements with characteristic intercept features like

- detailed trigger mechanisms allowing the interception of the "needle in the haystack"
- fine filters permitting investigators to discern the important data
- hot monitoring warning investigators on the targets' activities, allowing near real-time listening, viewing and/or reading of the communication
- live monitoring for forwarding intercepted calls to agents in the field
- single unified view of all interception types presented to the user

The Monitoring Center's unified view for all intercepts greatly facilitates the tasks of LEAs. If need be, different national and international agencies may grant each other access rights and easily exchange crucial information. Consequently, the concept of agencies cooperating across institutional or national boundaries becomes reality.

The Monitoring Center – one solution for all networks, vendors and technologies meets the monitoring requirements of LEAs worldwide.

Highlights

- monitoring of all types of voice, fax and data communication in fixed as well as mobile public networks and the internet
- smooth interaction with lawful interception solutions in heterogeneous network infrastructures
- extensive process automation (decoding, processing, assignment and storage of intercepted data)
- various recording modes (mono, stereo, full duplex, high speed) and voice compression
- automatic recognition of fax and modem data during call recording
- optimized on-screen presentation of data
- user-friendly features for timely data analysis
- multi-language interfaces
- add-ons for completely new and efficient ways to pursue leads

Benefits

The Architecture
The Nokia Siemens Networks Monitoring Center architecture of Front-End and Back-End parts results from the necessity to interface with a wide range of networks and technologies. This design is the core essence of its success.

Front-Ends
The Front-End components are specific for the target network such as mobile networks or the internet. Multiple Front-Ends are used to connect to different switch manufacturers' interfaces and to appropriately scale to the size of the networks. The data vary widely in terms of type and volume and need to be converted into a uniform system-internal format. Consequently, all voice and other data received from networks are transformed into a single internal format and passed on to the Back-End.

Back-End
The Back-End receives the processed data from the Front-End components, correlates content and Intercept Related Information (IRI) and automatically assigns it to the corresponding folders as configured in the system. The Back-End offers a Windows-based user interface made up of two components:

The Management Station (MS)
The MS enables the system administrator to adapt the configuration of the Monitoring Center to the LEAs' changing requirements at anytime, and to perform routine administrative tasks such as adding new users or folders to the system.

The Unified User Station (UUS)
The UUS provides the LEA-user with all recordings and other information from the network in an optimized form. Thus, the user can easily and quickly retrieve the relevant LI information from the respective folders. System-internal fax and data demodulation and decoding allow the recorded signals to be displayed as readable documents on the screen (e.g. fax, SMS, web pages). Powerful filters help the LEA to quickly locate, listen to and replay relevant phone conversations.

The Nokia Siemens Networks Monitoring Center can never be outdated.

On-demand upgrades
The world of communications is ever-changing: New technologies and ways of communication are constantly invented, Next Generation Networks infrastructures established, higher data volumes need to be handled and multiple types of communications monitored.

Requirements may change – our Monitoring Center will remain the perfect match. Despite the complexity, its modular design of Front-End and Back-End components guarantee extreme flexibility. The individual Front-Ends, which supply the interfaces to the different networks, can easily be adapted to match new requirements. But either can be modified, expanded or replaced as necessary, at any time. Yet the management and presentation essentially remain the same. This has many benefits for the user: The system does not need to be expanded more than necessary. This means that there are no 'fork-lift' upgrades – no total software or hardware replacements. Customers only have to invest in those modules they actually need. The result is a tailored solution that satisfies their requirements at all times.

Scalable
Depending on the applications, the system installations can vary in size - from a few computers to an extensive system of many recorders, data collectors, system servers and clients. The complexity ranges from passive connection to a single trunk line that is responsible for monitoring an entire nation's fixed, mobile, NGN and internet networks.

Distributable
The Nokia Siemens Networks MC performs its monitoring and management tasks from a scalable, distributable and reliable platform (LAN, WAN, MAN) with facilities which ensure the safety of system and intercepted data.

Reliable
Intercepted data is valuable. Customers need to be able to rely on the Monitoring Center solution, which must protect the system sufficiently so that neither manipulation nor theft or even power outage can corrupt the data (e.g. server protection, UPS concepts, RAID strategy, etc.). In addition, the Monitoring Center offers mass storage and archiving solutions (e.g. NAS, SAN). Various levels of compression are available to economize on storage space, if needed.

The Nokia Siemens Networks Monitoring Center is extremely flexible

- it can be integrated into any existing infrastructure and is applicable to a vast range of monitoring tasks, whether fixed, mobile or internet
- it can be configured as an IP interception and delivery solution for other LEMFs
- it is – on-demand and without compromises – scalable and adaptable to the size of the organization

The Monitoring Center's secure environment comprises

- network security
- physical security
- logical security
- link security
- data and capability access security

The Monitoring Center has a modular, multilevel security and control-concept for authorities, administrators and LEAs. This can be adapted to meet the requirements of individual organizational structures and different legal requirements.

Special precautions have been taken to ensure that, under any circumstances, the intercepted data cannot be, confused or mixed up.

A range of special system internal and external measures (firewalls, VPNs, virus/intrusion protection tools, etc.) safeguard the recorded data against manipulation, theft or destruction. System components can also be duplicated to guarantee system availability and prevent the loss of stored data. Using an appropriately specified uninterruptible power supply (UPS) concept, the Monitoring Center has been designed to survive power outages.

The Nokia Siemens Monitoring Center is extremely secure and reliable because of its

- multiple, granular levels
- holistic security-concept
- flexible configuration
- sophisticated user-rights and access control mechanisms

Database
Its database allows for add-on applications. These can either be provided by Nokia Siemens Networks or the customer himself integrates the data in the infrastructure by means of defined interfaces.

Nokia Siemens Networks constantly seeks to augment the service-scope of the Monitoring Center, not only by addressing emerging communications trends but also by making further use of information which is already at hand and by providing additional intelligence. Hence a wide range of add-on applications is available, such as:

Mobile Location Tracking (MLT)
Based on a Geographical Information System (GIS), the MLT is an ideal solution to track, record, extrapolate, and anticipate the movements of mobile devices. Within mobile networks, the current location of marked mobile devices can be determined. The intercept related information (IRI) is transmitted to the Monitoring Center. There, the so-called footprints of the mobile device are visualized on a map on which the user's (or rather the device's) current movements and route can be tracked.

Link analysis
Link analysis may be used to find and graphically display correlating data of intercepted targets. This kind of information, which cannot be achieved manually, reveals previously unknown relationships between targets.

Plaese have a look at our application notes.

Ahead through innovation

The features of our Monitoring Center – at a glance

- universal monitoring center concept for all monitoring requirements within all telecommunication networks:
  - fixed networks PSTN (local and international exchanges)
  - mobile networks GSM, CDMA, GPRS, 3G (UMTS/W-CDMA)
  - Next Generation Networks (NGN)
  - IP Networks (local loop, access network, ISP and internet backbone)
- automatic correlation of communication content to IRI
- mono and stereo voice recording, optionally compressed
- full duplex/no compression recording for data demodulation (fax, internet, e-mails, etc.)
- customized add-on applications
- centralized or decentralized Monitoring Center
- transportable Monitoring Center (‘MC to go’)
- scalable and adaptable to customer requirements
- joint roadmap for upcoming telecommunications technology and Monitoring Center

By forming strategic alliances with other companies in highly specialized technological areas (e.g. data demodulation, speaker recognition, language identification, etc.), Nokia Siemens Networks follows a best-in-class principle and involves specialized partners to maintain its Monitoring Center solutions at the leading edge.

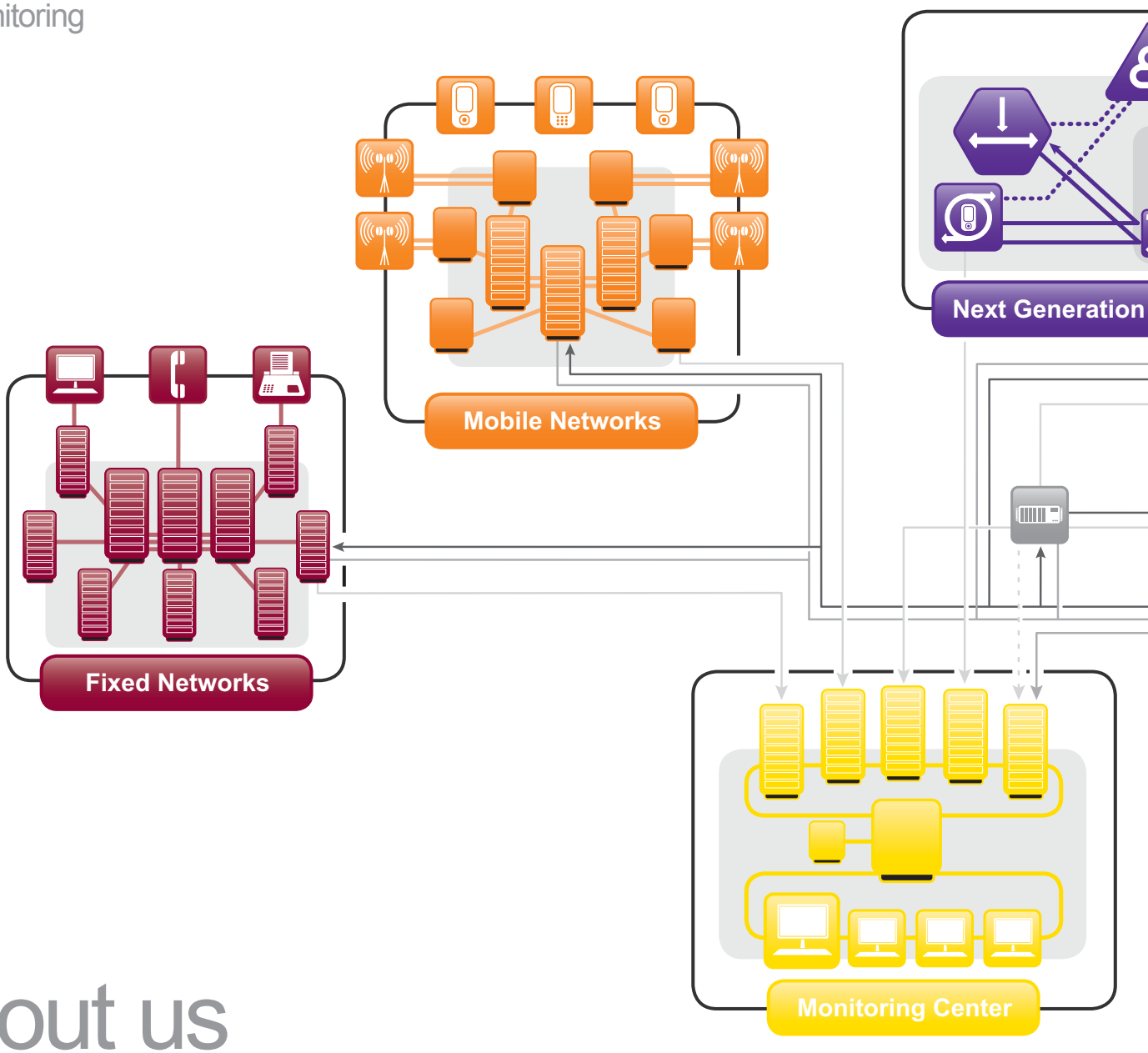
Nokia Siemens Networks has set standards around the world and across all technologies. In the context of this creative climate new ideas can grow, which allow us to remain at the forefront of developing innovative solutions like

- pre-ETSI LI IP
- country and vendor-specific ETSI standard adaptations
- IPIS (internet protocol interception system)
- LI-solutions for IP core routers
- generic systems designed for tailoring
- the transportable Monitoring Center – ‘MC to go’

Highlights

- tailored, ETSI compliant solutions, scalable in size and capacity, designed to address all network and LEA requirements
- optional configurable for other legal arrangements or country specific variations on ETSI
- secure, discreet, verifiable, cost- and space-saving performance of LI in all networks
- complete spectrum of interceptable network infrastructures
- nationwide monitoring possible
- fully automatic recording and processing of all data concerning all activities of the target
- high level of system and data security
- great flexibility: independent of location and organization
- simple, fast data processing and evaluation because of a maximum of process automation and user-friendly, practical functionality

Lawful Interception and Monitoring



About us

The Nokia Siemens Networks Monitoring Center is a well-founded choice and safe investment in a secure future. It represents the clear decision for a strong and stable company combining innovative power and strength to the advantage of all our customers. i.e. network operators, LEAs and government agencies.

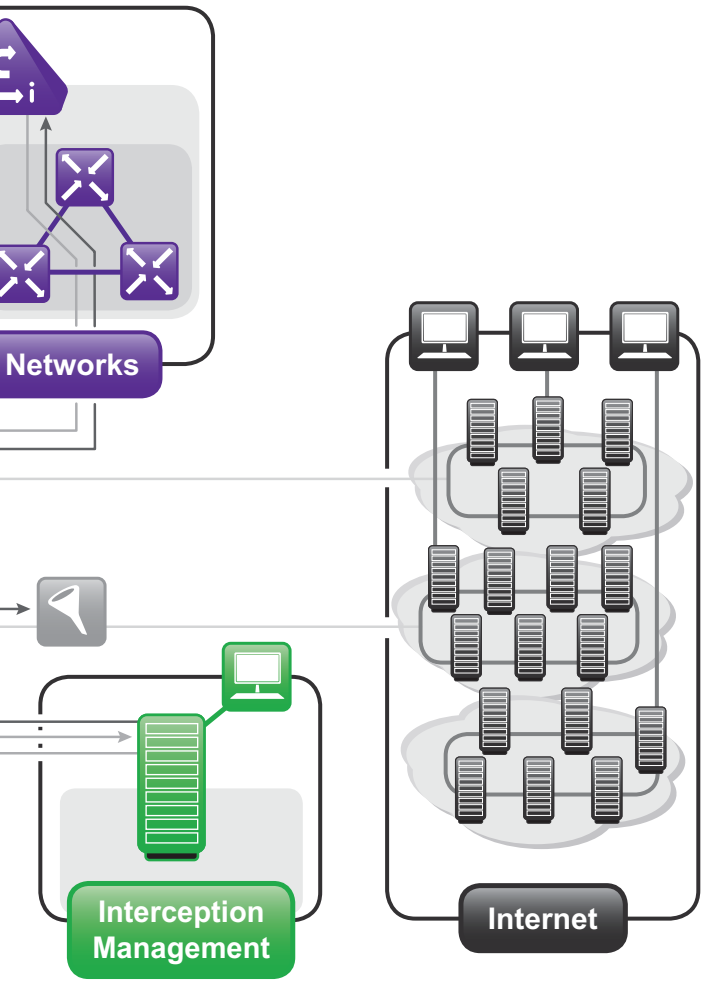
These benefit from a global service network and distribution system which include customized monitoring services and after-sales-support depending on their operational needs and demands.

Examples are

- consultation, network questionnaires and technical workshops
- all-round assistance in meeting legal requirements when planning LI solutions for new IP networks
- tailored financing solutions and leasing arrangements
- project management
- system and network integration
- training of system users
- system support
- system and capacity optimization
- system maintenance, hard- and software upgrades

The Nokia Siemens Networks business unit 'Intelligence Solutions' (IS) has a unique best-in-class experience with lawful interception and government agency requirements based on experience from numerous projects within its Monitoring Center product line. Deep understanding of security issues – inside military organizations, MOI, and other security services – as well as a broad security awareness contribute to IS' excellent relationships, which are based on trust, reliability and stability – result in long term, thoroughly satisfied customers.

Making the world safer with trend-setting intelligence solutions



Nokia Siemens Networks is one of the world's largest network communications companies – with 60,000 employees and a leading position in all key markets across the world. And, it is one of the three largest telecom suppliers in the world, with a growing customer base in over 160 countries across five continents. With 2006 pro forma revenues of €17 billion, the Nokia Siemens Networks business base is strong enough to lead the way successfully into the future.

List of Abbreviations

3G	3rd generation mobile networks
CDMA	Mobile network: Code Division Multiple Access
DTMF	Dual Tone Multi Frequency
ETSI	European Telecommunication Standards Institute
GIS	Geographical Information System
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
IP	Internet Protocol
IPIS	Internet Protocol Interception System
IRI	Intercept Related Information
IS	Business Unit Intelligence Solutions within Nokia Siemens Networks
ISP	Internet Service Provider
LAN	Local Area Network
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MAN	Metropolitan Area Network
MC	Monitoring Center
MLT	Mobile Location Tracking
MMS	Multimedia Messaging Service
MOI	Ministry of the Interior
MS	Management Station
NAS	Network Attached Storage
NGN	Next Generation Network
PSTN	Public Switched Telecommunications Network
RAID	Redundant Array of Inexpensive Disks
SAN	Storage Attached Network
SMS	Short Message Service
UMTS	Universal Mobile Telecommunications System
UPS	Uninterruptible Power Supply
UUS	Unified User Station
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
W-CDMA	Wideband CDMA

Nokia Siemens Networks GmbH & Co. KG
Intelligence Solutions
DE-81359 Munich
Germany

Visiting address:
Hofmannstr. 51, Munich, Germany
Switchboard +49 89 722 00

Order No. C40100031B2007091EN

IS-sales.nsn@nsn.com
www.nokiasiemensnetworks.com