

# Intelligence Solutions Monitoring Center



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.

Please 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'



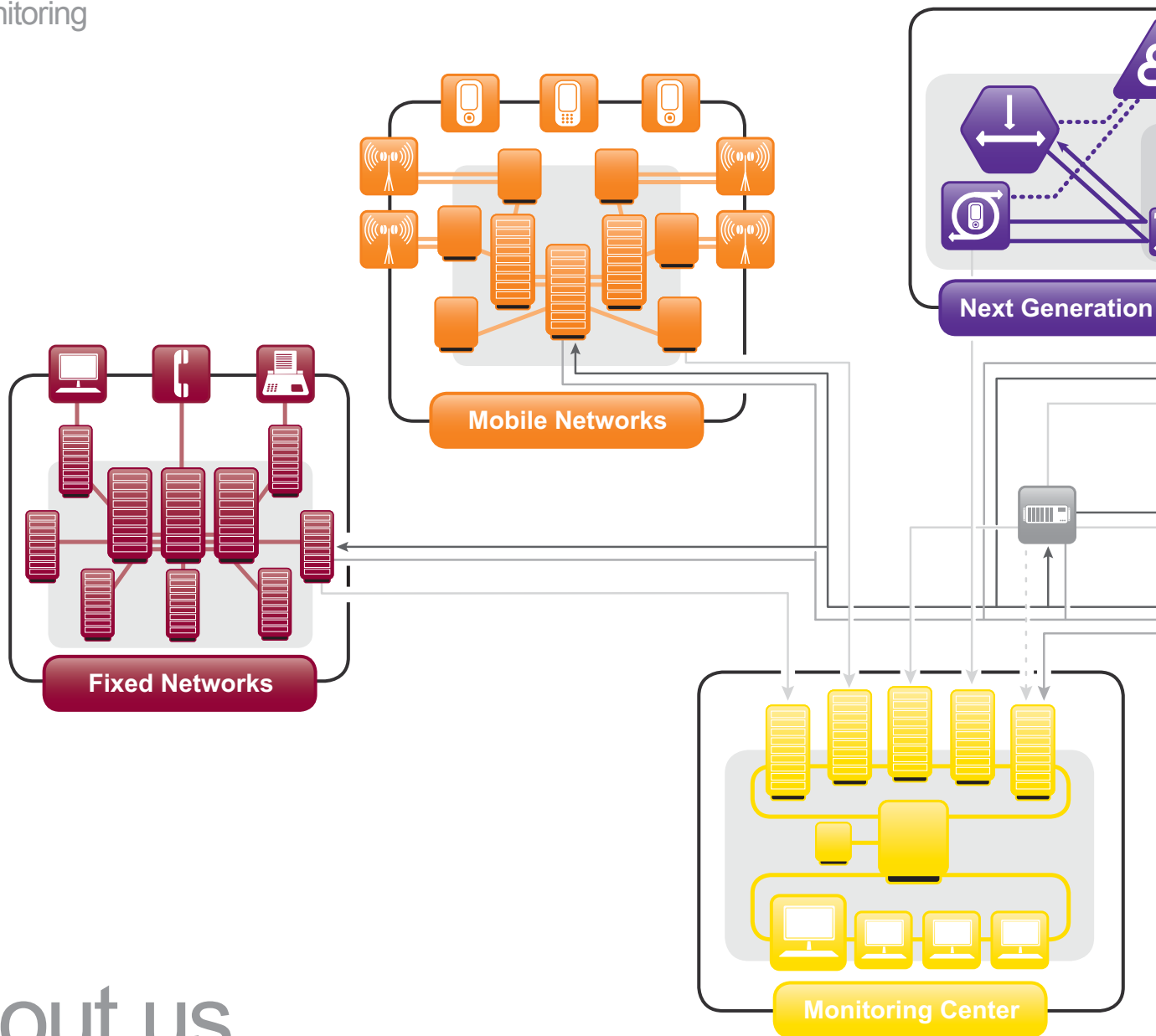


## Highlights

- 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.

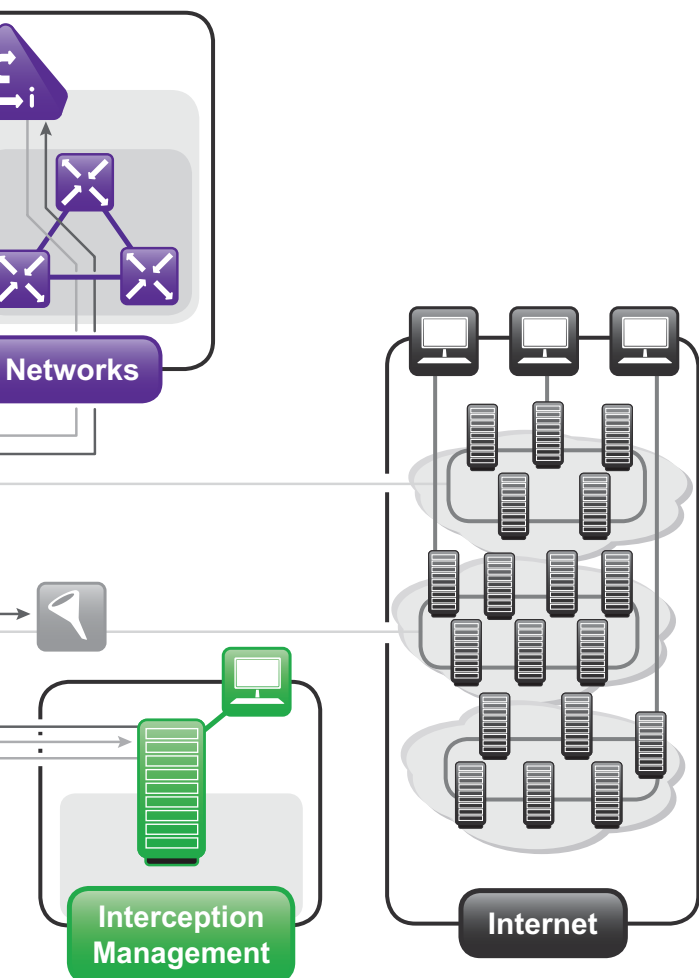
These benefit from a global service network and distribution system which include customized monitoring services and after-sales-support depending on their operational needs and demands.

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

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

Copyright © 2007 Nokia Siemens Networks. All rights reserved.  
Nokia Siemens Networks and the wave logo are registered trademarks of  
Nokia Siemens Networks.  
Other company and product names mentioned herein may be trademarks or  
trade names of their respective owners.  
Products and solutions herein are subject to change without notice.

Order No. C40100031B2007091EN

IS-sales.nsn@nsn.com  
[www.nokiasiemensnetworks.com](http://www.nokiasiemensnetworks.com)