Click here to view PowerPoint presentation; Press Esc to exit

# Information and Communication Infrastructure for National Security and Public Safety

**Magnus Wallmark**
Ericsson Microwave Systems AB
SE-431 84 Mölndal
SWEDEN

E-mail: magnus.wallmark@ericsson.com

## *SUMMARY*

*Creating an information and communication infrastructure for national security and public safety could be central for prevention of and defence against terrorism. The infrastructure should provide robust and secure access for any authorized user of voice and data services across various access technologies, both wireless and fixed. Virtually all types of existing, so called "legacy systems", and new information sources can be made as generally accessible services. The services can be accessed anywhere using existing communication infrastructure and any suitable type of terminal.*

*Which services to access in a certain situation is dynamically controlled so that all for the moment relevant information is made available and adequately presented. If the situation changes and the information need is altered, access to any other of the available services can be established immediately*

*The service network is based on open commercial network technology that is further developed to fulfil the security, robustness and flexibility requirements of interoperating public safety, national security and defence agencies.*

*Agencies, such as police, fire brigades and ambulance services have traditionally used dedicated systems to handle their communication needs. In many countries this has resulted in a number of incompatible systems meeting only the demands of each separate agency.*

*It is not necessary to have a separate transmission infrastructure; existing commercial and government networks can be reused. A combination of different wireless and fixed technologies such as GSM, CDMA, WCDMA/3G/UMTS/IMT2000, Tetra/Tetrapol, land radio, nationwide networks for Mobitex, wireline telephony, satellite links, radio or microwave links, Internet and WLAN can be used. The infrastructure supports heterogeneous access networks.*

## 1.0 INTRODUCTION

This paper describes a network concept for public safety, national security and defence applications that can be used for defence against terrorism.

The network provides robust and secure access for any authorized user of voice and data services across various access technologies, both wireless and fixed. Virtually all types of existing, so called "legacy systems", and new information sources can be made available as generally accessible services. The services can be accessed anywhere using existing communication infrastructure and any suitable type of terminal.

*Paper presented at the RTO SCI Symposium on "Systems, Concepts and Integration (SCI) Methods and Technologies for Defence Against Terrorism," held in London, United Kingdom, 25-27 October 2004, and published in RTO-MP-SCI-158.*

Which services to access in a certain situation is dynamically controlled so that all for the moment relevant information is made available and adequately presented. If the situation changes and the information need is altered, access to any other of the available services can be established immediately.

The service network is based on open commercial network technology that is further developed to fulfil the security, robustness and flexibility requirements of interoperating public safety, national security and defence agencies.

This symposium paper is intended for decision makers, responsible managers etc. within the area of public safety, national security and defence. It gives brief information about the possibilities created by currently available technologies.

## 2.0 INFRASTRUCTURE

Agencies, such as police, fire brigades and ambulance services have traditionally used dedicated systems to handle their communication needs. In many countries this has resulted in a number of incompatible systems meeting only the demands of each separate agency.

It is not necessary to have a separate transmission infrastructure; existing commercial and government networks can be reused. A combination of different wireless and fixed technologies such as GSM, CDMA, WCDMA/3G/UMTS/IMT2000, Tetra/Tetrapol, land radio, nationwide networks for Mobitex, wireline telephony, satellite links, radio or microwave links, Internet and WLAN can be used. The solution supports heterogeneous access networks.

The tremendous build-out of GSM public mobile networks around the world, with nationwide coverage, international roaming and complete functionality for voice, messaging, data and imaging, gives the public safety sector a new option when considering how to upgrade its communication and information systems. The public mobile networks will be further enhanced by adding 3G capabilities to existing networks. This will give much higher data speeds, allowing introduction of new services such as fast data transmission and video telephony.

One example illustrates the capabilities of existing GSM networks: the US government, as a result of the events of September 11, 2001, requested that priority functionality for public safety users be available in public mobile networks. Based on these requests, operators and vendors have together specified, demonstrated and implemented priority for public safety users in GSM networks in the US.

Most public mobile networks today have good coverage. However, if public safety authorities require better coverage in some areas than is provided by an existing public GSM network, the first alternative is to add new masts and antennas. This will also benefit public users in for example rural areas. Obviously, this is far less costly than a complete re-build, and the extra resources can directly improve the level of security.

To further enhance the coverage and availability for public safety users, national roaming can be used, as it is for the 112 service, the European equivalent of US 911 or 999 services today. This is not a technical issue but rather a legal and administrative issue for governments and operators.

It is also possible to communicate with users of satellite phones and other public telephone systems. Special communication systems can be connected via dispatch centres.

A number of mechanisms in GSM allow public safety users to have reserved capacity or priority in case of emergencies. One alternative is to dedicate certain radio channels for public safety users, the equivalent of building a separate radio network. Another method is the priority functions implemented in the US, where

in case of emergency, traffic channels can be handed over to high-priority users. These users get priority in queuing, while lower-priority users can be removed from a cell, for example by being handed over to another cell.

Security in GSM has many aspects. Besides built-in security functions such as authentication and encryption, additional security can be achieved by duplication of network components, national roaming to secure best possible coverage, redundancy and automatic switch-over in the network and base stations.

Group communication has an important role to play in the public safety sector. GSM Advanced Speech Call Item, ASCI, services provide group communication that can be configured in many flexible ways. These services use one radio traffic channel per cell for each group, avoiding unnecessary blocking of the radio network.

Push-to-talk is a function requested by end-users in public mobile networks today. This function allows pre-defined groups of users to communicate over a packet channel by pressing a special key. Push-to-talk is now being standardized for GSM and can be a useful service for public safety user groups.

Common terminals such as a standard cell phones, PC or PDA can be used as well as modified more robust terminals or specially designed terminals for public safety, national security and defence applications.

With about 400 million new GSM/3G terminals sold every year, there is a constant flow of new and sophisticated terminals entering the market. One example of a high-end phone for professional use is P900 from SonyEricsson.

## 3.0 DISPATCH AND COMMAND CENTER SOLUTIONS

Dispatch and command centres are important parts of wireless and fixed public safety, national security and defence networks.

Existing or new types of dispatch and control centres are connected to wireless networks via open, standardized network interfaces.

Ericsson's dispatch and command centre solution integrate system solutions for telephone and data communications for customers where 24-hour accessibility and reliability are absolutely essential. The solution handles national, regional and district levels and distributes traffic according to preconfigured patterns that can easily be reconfigured depending on national, regional or district requirements.

The current architecture is built on a distributed IP WAN infrastructure, which enables specialists all over the area covered by the system to co-operate and share all information, data and voice using VoIP. Alerts and actions can be directed to and shared by specialists in different locations. This includes any kind of land radio systems and telephony since they also are integrated at a server location.

Today, this concept is implemented in national systems, where operators in different regions can back up each other – all having access to all local data of the caller.

A wide range of features are available in the system such as: call-taking, dispatch, intelligent call queue, Geographic Information Systems, classification, logging, statistics, control of traffic signals and gates, object information presented as text and images, status and position of available resources, planned decision support based on simulated scenarios, time-controlled responses, integrated voice and data service networks, integrated wireless and fixed access networks, support for land radio systems, one system integrating all information, interworking with Wi-Fi (Wireless LAN or WLAN).

We have in applications supporting UN rescue operations, already seen how Wi-Fi (WLAN) can be used to establish communication quickly at disaster scenes. Ericsson also offers Wi-Fi integrated into GSM systems as an additional radio access for short-range coverage.

## 4.0 THE SERVICE NETWORK CONCEPT

The service network concept is based on an open architecture allowing information from compatible or encapsulated legacy systems as well as new distributed services. Which combination of information to be accessed by different users does not have to be predetermined but can be adapted according to the needs at each time.

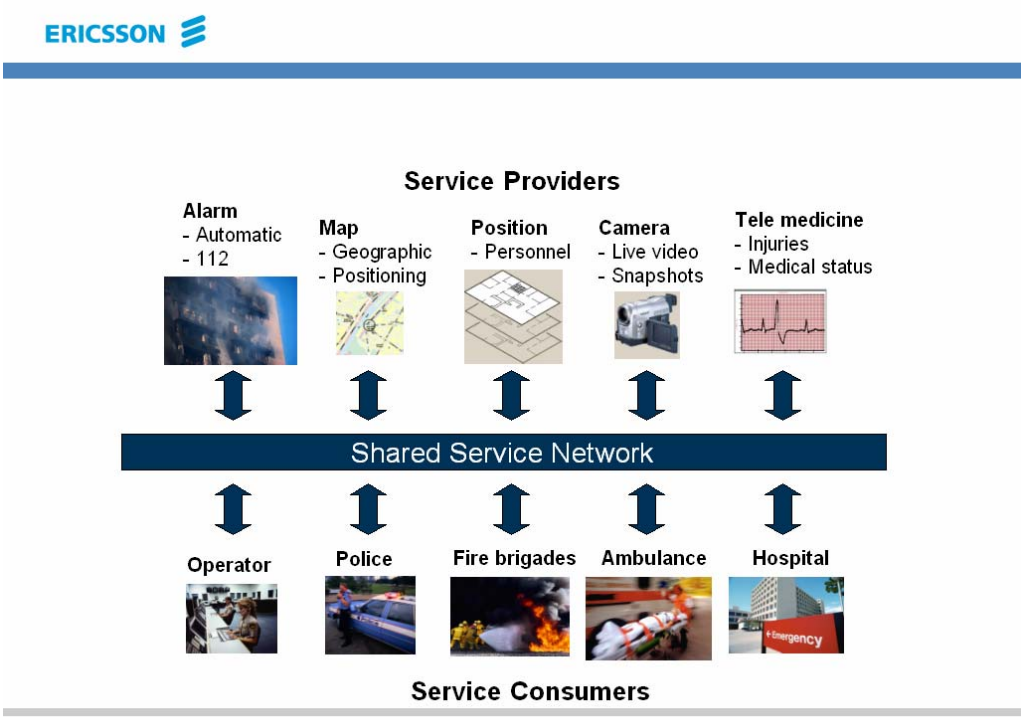


**Figure 1: Shared Service Network – access to services can be established dynamically when needed.**

The service network concept does not require new systems; its main function is to provide secure and flexible access to existing systems.

The service network is not to be regarded as a single system, but rather a system of systems infrastructure that is used together with independently developed and implemented services.

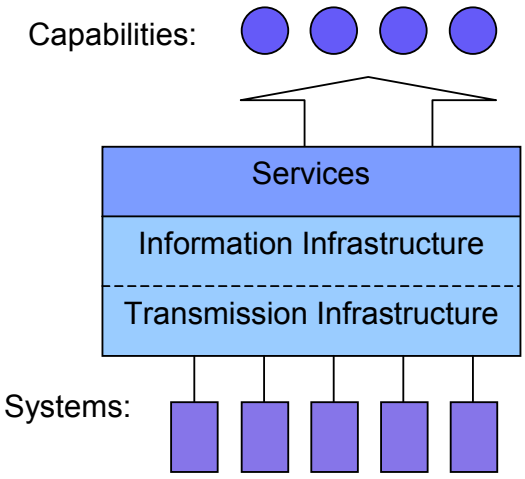


**Figure 2: The Service Network Architecture.**

Network security and robustness as well as the support for secure interoperability are inherent in the architectural solutions.

Services and service producing systems can be continuously added or removed, also in real time, without affecting the operation of the service network.

The service network is wholly scalable; services and capabilities can be developed and the range of services and systems can be extended over time in an evolutionary fashion.

The service network is based on open standards, allowing different system and service vendors to be engaged.

Next generation advanced dynamic services are:

- Situation adapted
- Dynamically created
- All over IP
- Distributed
- Easy to add new resources
- Easy to add new services
- Easy to add new terminal types
- Legacy systems can relatively easily be encapsulated
- Map services, combined IT and telecom services, database services, telematics, positioning, sensors (e.g. cameras, alarms, radars), weather services, command and control, live video.

## 5.0 SECURITY

Security is a core part of the network. Security mechanisms will allow mobile users to access voice and data services in a secure manner, according to defined secrecy, authorization and authentication schemes.

Some of the main security areas that should be addressed are:

- Security policy,
- Security infrastructure,
- Asset classification and control,
- Personnel security,
- Physical and environmental security,
- Communications and operations management,
- Access control,
- Non-repudiation,
- Encryption,
- Systems development and maintenance,
- Technical guidance,
- Network availability,
- Redundancy,
- Hot standby.

## 6.0 ARCHITECTURAL CONSIDERATIONS

The communications and information architecture should allow for rapid changes of the network, give seamless flow of information services, supply mobility, and provide multiple ways of interconnecting sub-networks.

From an IP point of view, the network should be non-hierarchical. The underlying bearer technology (SDH, Ethernet or other) can for practical and capacity reasons be formed in tiers. In the Internet world, backbone networks are often divided into core and edge networks, due to the traffic load and number of interfaces they are supposed to handle.

In five to ten years time, more and more networks will be ‘all IP’, i.e. they will carry also traditional circuit switched services like speech, video or sensor data.

For obvious reasons a military or national security networks needs to have transportable parts, either as an enhancement of capacity or coverage, or as a replacement for lost parts of a fixed infrastructure.

The strategic, fixed infrastructure, or the backbone network, is usually constituted of optical fibre and (D)WDM transmission technology. On top of that it is common to use technologies like Ethernet, ATM or SDH/Sonet. It is feasible to run IP over any of these technologies or protocols.

However, presence in new theatres of operations and connections to remote areas are more cost efficiently handled via satellite. Satellites bring great flexibility to the backbone, but at the cost of more signal delay.

The service of providing capacity over distance, which is what backbone networks are all about, could be either self-provided or sourced from one or several operators. In most cases redundancy is required to provide a high enough availability. Ericsson can advice on, provide, integrate and manage backbone networks.

A very important link in the communications chain is the access network. It controls the amount of bandwidth and the quality of service (QoS) parameters available to the terminal, the access point, or the user. The access networks can be either wired or wireless. In the latter case it is (generally) meaningful to talk about area or even volume coverage, as an important characteristic.

Often a high degree of mobility is required. Mobility comes in basically four shapes: the mobility of services (log in to a computer at another site or terminal and find your usual environment), the mobility of terminals (bring your laptop when you travel and access the intranet of your organization), the mobility of sessions (a data or speech call is handed over between base stations when a mobile phone is moving), and mobility of networks, where base stations or routers themselves are moving while in service.

Different technologies will produce complementary characteristics. It is therefore a necessity to have heterogeneity in the access networks. Select these with care, and thereby minimize life cycle cost for your combined access network. Certain adaptations may be required compared to off-the-shelf solutions, as introduction of mobile base stations for mobile systems (in the operator world, only the terminals and their sessions are mobile, not the network itself).

Good candidates as access networks are 3G mobile systems (high bandwidth, multi-service, medium range), satellite access (good coverage but high cost and often a wide area shares a limited capacity) and Ethernet (fixed connections). Other systems as HF radio (low capacity, but long range) or combat net radio (jamming resistant and extremely expensive) could be considered, for naval and army/tactical applications respectively, if bandwidth is not a primary concern. PMR systems, even digital, ISDN and analogue phone lines are not the selection of choice, primarily because of low level of added functionality and poor IP, and therefore multimedia, capabilities. They can however be included e.g. for backward compatibility reasons.

A special type of very useful access network is the point-to-point microwave radios that so successfully provides the radio access network connectivity in many operators' mobile networks, i.e. connect radio base stations to a core network.

Access networks can be self provided by the national agencies, but also be catered for by commercial operators. Mobile networks can be reinforced locally where an incident so requires or where ordinary coverage simply does not exist. Ericsson can advice on, provide (especially mobile networks, point-to-point and point-to-multipoint microwave radio links), integrate and manage access networks.