ALCATEL

NEWSLETTER

… For our customers
… reports on selected projects
… providing deep insight into telecommunication issues

Alcatel New Business

Issue October 2003

Editorial

Project News

Downloads and Links

Send comments or unsubscribe notification to:
Alcatel SEL AG
Zentrale Unternehmensentwicklung
Lorenzstr. 10
D-70435 Stuttgart
mailto: info.new-business@alcatel.de

Find more information on our web page:
http://www.alcatel.de/test_integration
Choose "Innovationsprojekte"

A Turning Point in Communications

When I look back at our newsletter from January this year, the title of the editorial was "2003 - a turning point in telecommunications?", which I can just repeat, but this time without the question mark. We had an extremely busy period, but also a successful one. Our major stories of the last newsletter have been restructuring the networks, security solutions, interconnection issues and mobile controlled media. All of those segments have been developing. In this issue we will show some of the progress.

Also, the web-site of our group has been face-lifted. Some of us have found some intellectual compensation from busy-ness by producing another book (one is on UMTS, the other on Java in telecommunications). We have been moving deeper into component based software based on J2EE, Web-Services and Storage Area Networks. In the development of new concepts, we had the support of many students from different universities in a truly international environment. We will continue those co-operations.

In fact, software will become the main driver in this business. Software is a natural follower of the microprocessor, which is moving into any kind of equipment. Increasingly, mobile networks will go beyond connecting people. Among the mobile equipment are machines, domestic appliances, consumer electronics, sensors and actuators. 2G and 3G networks get support from WLAN and Bluetooth to connect users and devices. All of this will need a communication infrastructure, that is, a concept for software and a service architecture. Many applications will need to communicate over longer distances. This will drive the concepts that we are developing for restructuring the networks.

There is one area of concern in this brave new world of total interconnection: Privacy and security. Solutions intended for protection against terrorism may go to far and lead to a climate of total supervision. The increasingly interconnected citizen is also a pretty transparent one. The same laws that apply to our daily live will apply to our digital life.

Technical solutions will need to be designed for protection of privacy. Also, the user will need some education when handling mobile equipment and living in an interconnected environment. In fact, security and privacy is one of our priorities in the design of solutions for lawful interception, service architectures and personal area networks. Our group has taken up those issues into the European community, where we contribute to new projects of the Framework Program 6 of the Information Society.

Dr. Stephan Rupp
Head of Services Dept.
Alcatel Stuttgart, Germany
Phone: +49 711 821 46448
Mail: s.rupp@alcatel.de

Restructuring of Telecommunication Networks –

Simplification of the Network Infrastructure by implementing Storage Networks and Web Services techniques

GPRS, Location Based Services (LBS), WLAN integration, Mobile Number Portability and UMTS are some of the new technologies that are responsible for the increasing complexity of today's networks. They require new network elements and applications to run and each of these applications need their own subscriber data (usually stored locally in the application's database), are managed from their own management systems and have their own interfaces to other systems. For Network Op-

erators, the effort to plan, to administrate and to introduce new services in those networks increases dramatically. Therefore, to simplify current and future telecommunication networks is an imperative for network operators and their suppliers. Alcatel has worked out some concepts on how this simplification could be achieved.

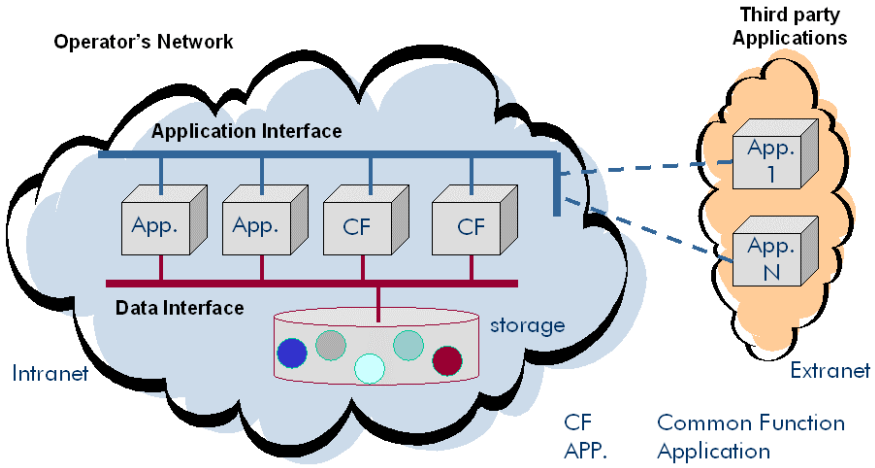


Fig. 2.1: Only Data Interface and Application Interface remain

Interface Consolidation

The variety of interfaces and protocols increases with rising functionality of a Telco- network. For new functions new network elements and new protocols are defined. Some simplification would be desirable where only two kinds of interfaces, a data interface and an application interface remain (Fig. 2.1).

An analogy of the IT industry will help readers to better understand this concept. Upgrading a PC is easy by plugging an additional board into the next free slot on the motherboard. The slot comprises access to the common processor busses. Taking this image for comparison, the upgrade of a network with a new function could mean to "plug" this new function onto the common data interface and the common application interface.

It is recommended to separate current network elements into common (elementary) functions and specific functions. Common Functions (CFs) are then at the disposal to all applications. Also third party applications could use them.

Web Services in Telecommunications

A very promising technology for the Application Interface and possibly also for the Data Interface are "Web Services". Web Services are already used in the business area, especially in Enterprise Application Interface (EAI) solutions. Server and client in a Web Services environment use the Extended Markup Language (XML) and the Simple Object Access Protocol (SOAP) for their communication. In order to make existing network elements and their incorporated functions look like a Web Service current communication protocols like MAP (Mobile Application Part) can be encapsulated in SOAP. All "encapsulated" network elements would have then a common application interface. New functions and applications can be designed as Web Service right from the beginning.

Web Service and their underlying principles have the potential to be a candidate for the application interface and perhaps also the data interface. It must be verified that the hard requirements in a Telco-network, like very short response times, can be fulfilled with this solution.

PoLoS, an example of Web Services implementation in telecommunications

We have tested some of those ideas in the PoLoS project (Platform for Location-Based Services), promoted by the

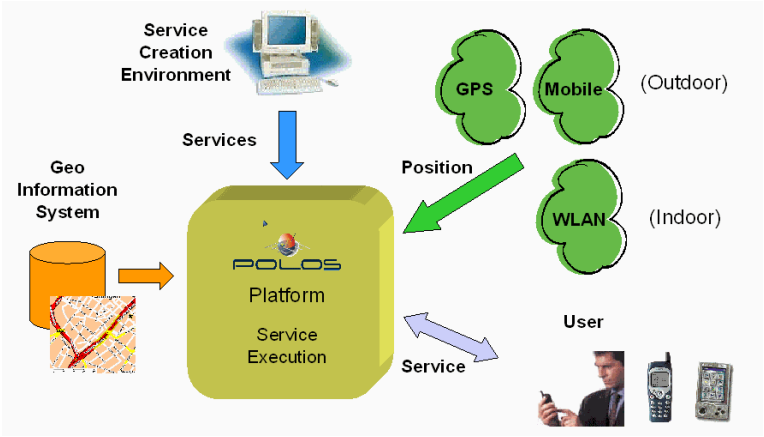


Fig. 2.2: General overview of the PoLoS project

European Union in the frame of the Information Society Technologies Program (IST).

The PoLoS project investigates existing and future services and latest technological achievements in the sector of Geographical Information Systems, positioning techniques and network interfaces in order to design and implement a platform capable of providing the full functionality needed to design, create and deploy Location-Based Services.

To achieve this functionality, the platform features a component-based architecture. The platform is independent of the underlying network infrastructure and the LBS creation is supported from a Service Creation Environment (SCE). The platform is applicable to several types of networks, including GSM/GPRS/UMTS networks as well as WLANs. It also supports GPS-enhanced devices that use the mobile networks only as transport medium (Fig. 2.2).

In order to quickly and effortlessly adapt the platform to different operator and provider environments Web Services techniques were used in the interfaces towards networks and service providers systems.

To show the advantages of using web services techniques in more detail, the interface between the PoLoS server and the networks providing the location information will be explained (Fig. 2.3).

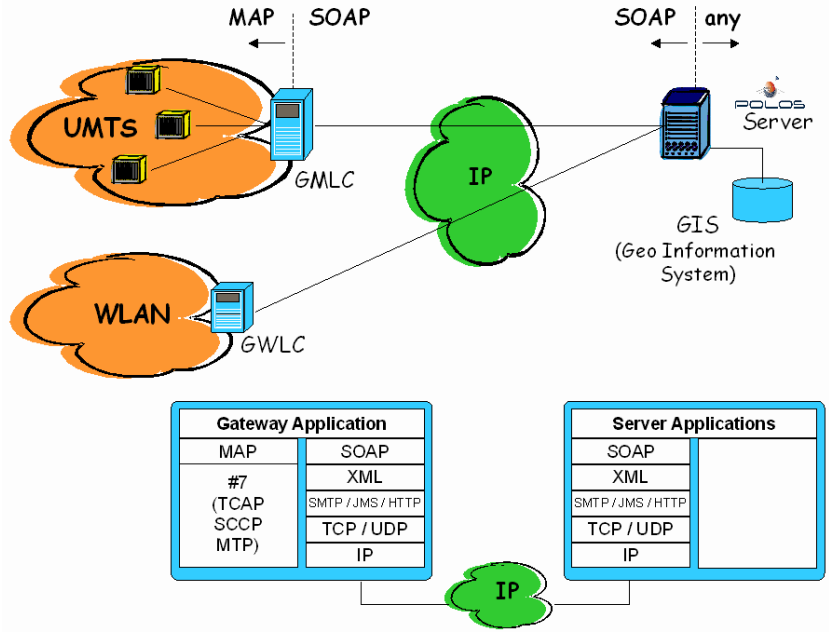


Fig 2.3: Web Services as Application Interface for LBS-Server in the EU-Project PoLoS

The PoLoS-Server provides the the Location Based Services and has therefore access to a Geographic Information System as well as to the positioning data of the users. The latter are provided by PoLoS-Gateways, which are attached to the various networks supported. (A Gateway Mobile Location Center, GMLC, in the GSM/UMTS network and a Gateway WLAN Location Center, GWLC, in the WLAN).

As can be seen in the protocol stacks the PoLoS- Gateway communicates with the mobile network using the MAP protocol, but a Web Services interface based on XML and SOAP connects the PoLoS-Gateway with the PoLoS-Server. As this is an open interface other LBS servers can be attached.

The functional interface offered by the PoLoS-Gateway is fully compliant with the Open Service Access (OSA) specification 3GPP TS 29.198-6 V5 (Parlay 4). By exposing its Web Services Description Language (WSDL) description file to LBS servers, those LBS servers (i.e. the PoLoS-Server) should be able to adapt, on-line, to this interface and use the parts of it they may need. In this way, integration issues like naming convention, parameters positioning, etc. are nicely avoided.

The whole system was set up in a week only and could be shown in a fully distributed environment between Athens, Stuttgart and Brussels.

Storage Area Networks in Telecommunications

Information is the most important asset an operator has. Information is about who the customers are, who the users are, what use they make of the services, when they used them and how long, the status of the network, etc. Obviously a company, which is unable to charge for the use of services (billing information), nor a company, which does not know its customers, can survive in today's environment.

In nowadays networks, data (information) are attached (or even belong) to a certain application and, therefore are spread across many comput-

ers, more or less isolated from other computers (applications). More, many databases keep a significant amount of identical data that have to be kept consistent across all applications. (Examples are Home Location Register, Authorization, Authentication and Accounting Server, Number Portability Database, etc.)

Data are stored on local disks. This kind of storage is called Direct Attached Storage (DAS). Such a configuration has two main problems.

The first one is operational cost. For security reasons backups must be prepared frequently up to several times a day, depending on how often data change. A heavy use of human effort is necessary, which is expensive. Current storage technologies like Storage Area Networks (SAN) provide a very optimized, highly available, highly automated and secure solution for data storage. In a storage network, data are physically consolidated in order to achieve economy of scale. The use of SAN in telecommunication would reduce Network Operators' OPEX significantly, increasing at the same time the recovery response following a catastrophe event.

The second problem nowadays concerning data is their unavailability to other applications. That will be illustrated with two examples.

Example 1. In order to offer mobile Pre-Paid services, the Service Control Point (SCP, a node of the Intelligent Networks) needs information, which is stored in the Home Location Register (HLR, a data base containing mobile user information). To reach this information, an interface called Customized Applications for Mobile network Enhanced Logic (CAMEL) has been defined. This interface has to be supported by both, the HLR and the SCP. Depending on the version of the CAMEL protocol, more or less HLR data is accessible to the SCP. Opening the HLR data to other applications would simplify the introduction of new applications and relieving the applications from caring on the right protocol in the right version.

Example 2. The Network Operation Center (NOC) of a certain operator detects some problems in the network. Usually each problem is given a certain priority that is assigned pending on the effect on the running business. If the problem affects some thousand users that have a best effort Quality of Service (QoS) in their contracts, the priority may be lower than if the problem affects to only one user who has a very demanding QoS agreement with the operator. The problem is that this type of weighting is only possible if the NOC applications have access to commercial data (customers, contracts, etc.), which is not the case today. In the same way, the Customer Care department would like to inform important customers about network problems before the customers realized by themselves that there is a problem. Again, network data and customer data have to be crosschecked to achieve that.

In Alcatel's new configuration proposal network elements are exempted from the storage of subscriber data. The data are hosted in dedicated servers especially optimized for data management (database servers) as shown in Fig. 2.4. The access to the data is realized via a common data interface. This architecture facilitates the integration of new application servers, speeds up the introduction of new services, facilitates the network management, simplifies network elements and uses standard state-of-the-art IT technologies (which is in most cases already established in the IT-environment of the network operator for e.g. applications running on the Business environment). So

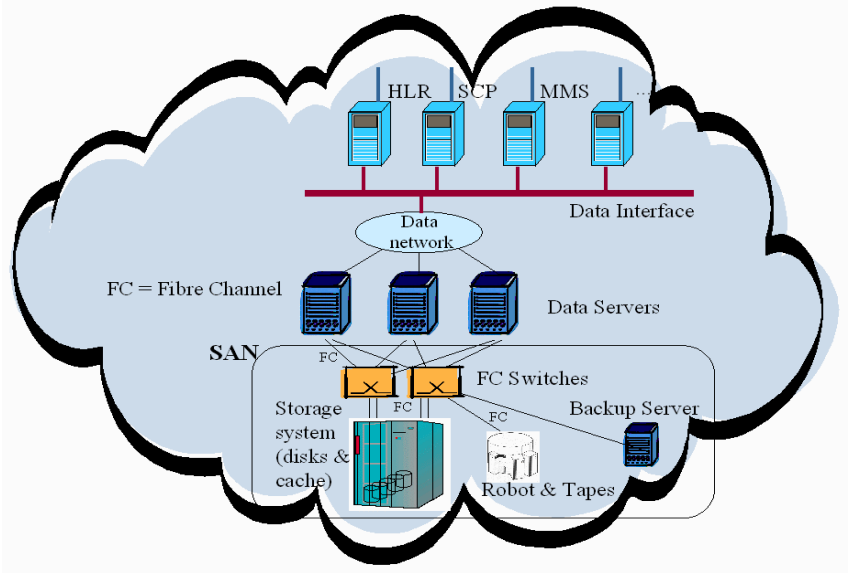


Fig. 2.4: Getting data out of network elements

technology, skills and know-how are already available inside the company. Management and provisioning systems have direct access to data and need not to involve other network elements. Finally, the functional range of the network elements will be downsized to their principal tasks - they don't need to care about storage, backup and recovery of subscriber data and can focus on their principal tasks in the network.

Rodolfo Lopez Aladros
Alcatel Stuttgart, Germany
Phone: +49 711 821 43284
Mail: R.Lopez-Aladros @alcatel.de

Franz-Josef Banet
Alcatel Stuttgart, Germany
Phone: +49 711 821 47890
Mail: FJ.Banet@alcatel.de

Lawful Interception (LI)

Legal Base

Each network operator which offers Telecommunication Services on a public base, has to install a functionality, which allows a Law Enforcement Agency (LEA) to keep the traffic data of selected customers under surveillance and record it. This obligation is according to prescriptions in German laws:

- **Article 10 Law (G 10)**, which rescinds the fundamental secrecy of information transfer stated in §10 of the German Constitutional Law in the course of prevention or prosecution of offences
- **Criminal Procedure** (Strafprozessordnung **StPO**) §§ 100a and 100b and **Law on Foreign Trade and Payment** (Außenwirtschaftsgesetz **AWG**) §§ 39 to 43, in which the offences are defined, which justify a rescind
- **Telecommunication Law** (Telekommunikationsgesetz **TKG**) §88 and the appendant **Telecommunication Surveillance Regulation** (Telekommunikations-Überwachungs-verordnung **TKÜV**), which details the obligations of operators.

The order about surveillance has to be signed by an independent judge and in severe cases even by the liable minister. To create further security against misuse, it is forbidden that an employee from the LEA works as an appointee of the operator for interception activation. In addition the interception activity shall be kept secret, control shall be possible by a restricted number of specifically authorised personnel only, even people carrying out normal network management tasks shall not have any visibility. It shall not be possible to detect the establishment of a surveillance, neither by subscribers using the connection nor a third party.

The LI-functionality of a network has to be certified by the regulator (RegTP).

German law also enact that the expenses for the LI-functionality are on the account of the operators and no reimbursement is possible and that personnel costs for operation are only refunded with the very low tariffs for witnesses.

Until 29. January 2002 only services of the Public Switched Telephone Network (PSTN) have been subject to surveillance. At this date the former version FÜV (Fernmelde-Überwachungsverordnung) was replaced by the TKÜV, which requests for surveillance of all public telecommunication services in all networks - including Internet and Cable Networks. The regulator has granted a transitional period, but the new interception functionalities shall be ready for operation latest at 1. January 2005. However, exception from the obligation are conceded for:

- all networks serving less than 1 000 subscribers
- transitional networks only interconnecting other networks
- public distribution services
- Internet access networks to which no subscribers are directly connected
- nodes providing interconnection to an Internet.

The last two exceptions mean, that the servers of an Internet provider do not need to provide for the interception functionality, but E-Mail servers have to. Networks having less than 10 000 subscribers can get some alleviation with respect to response times to an interception request.

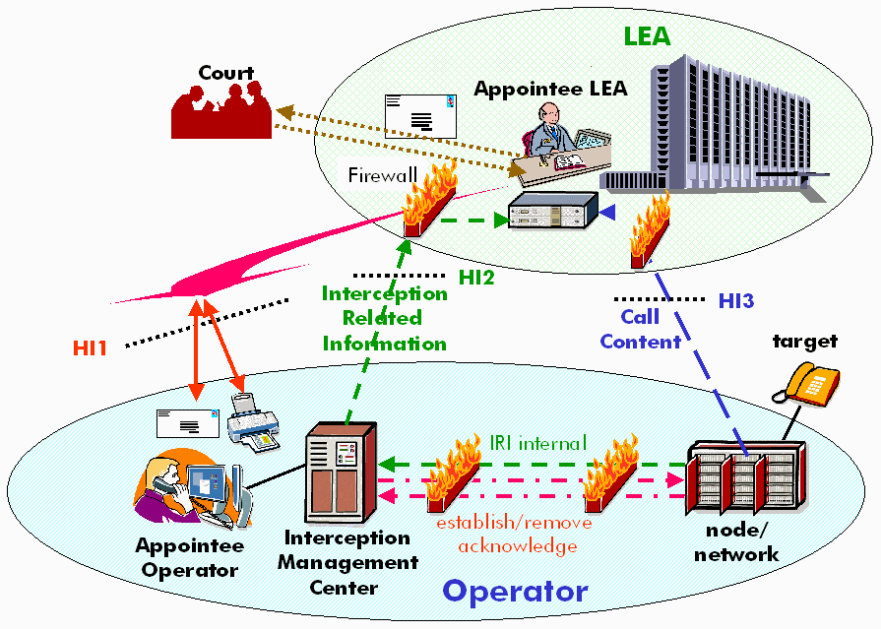


Fig. 3.1: Configuration for Lawful Interception

Technical Requirements

The principle configuration for Lawful Interception is shown in Fig. 3.1. At the border between the interception functionality and the LEA three so called "handover" interfaces HI1...3 are defined. Via HI1 the interception action is controlled by requests to establish and remove - including target identity, start- and maximum duration-time and LEA-address - in direction from the LEA and acknowledgements from the operator to the LEA. In most cases the HI1 is realised by facsimile and subsequent courier mail.

The traffic data that have to be delivered to the LEA is divided into two categories of information, which have to be transported via HI2 and HI 3. Via HI2 the Interception Related Information (IRI) has to be transported. It includes the signalling information dedicated to a call, time stamps and - if available - also information on supplementary services and the location of the target. At HI3 the Call Content (CC) - this is the information exchanged between the dialog partners - is available.

The HI2 and HI3 are normally connected via public dialled links to the LEA- favourably 64 kbit/s ISDN channels for CC. The IRI which have to use FTP as application protocol may also use ISDN-channels, but also packet links X21/X25 or secure Internet links are possible.

The operator has to protect the transmission. This means to ensure that:

- the only possible recipient is the LEA which ordered surveillance
- the links to the LEA can only be used for transmission of information gained by interception
- no third party can eavesdrop information, which means that - especially in case of transport in packet-switched networks - encryption may be necessary.
- The operator is not allowed to store information gained through an interception. Only in case that no link to the LEA is available, short time buffering of IRI with immediate deletion after effective transmission or time-out is permitted.

In order to be able to supervise the correct accomplishment of interception orders and prevent from misuse a log file of all interception actions has to be created by the operator. Latest every quarter of a year independent security personnel has to check the log file against the orders and inform the LEA when irregularities can be detected. If anything is correct the log file must be deleted immediately.

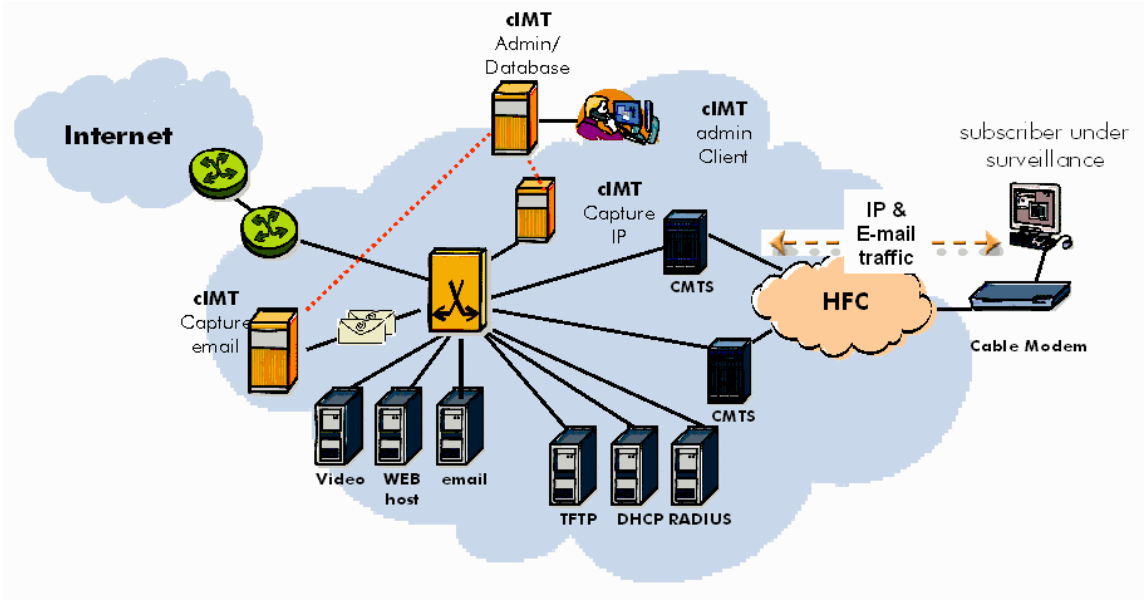


Fig. 3.2: Example Lawful Interception at Cable Operator

Solutions

As described before service providers offering E-mail have to support lawful interception for the E-mail traffic and operators, which provide direct internet service to end users, like Cable Operators or ADSL operators have to support interception of IP traffic. For this services Alcatel has introduced the central Internet Monitoring Tool cIMT A5451 which fulfils the requirements of the German RegTP and other regulatory authorities. The monitoring tool consists of the components:

- cIMT capture module to capture and record E-mail or IP traffic at a central point in the operators IP network. It is possible to have more than one capture module in a network.
- cIMT admin to control and administrate the cIMT capture modules.
- WEB based administration client to provision and configure the cIMT system

Fig. 3.2 shows one possible configuration with the cIMT system for a Cable Operator, who has to provide lawful interception for E-mail and IP traffic.

Besides the delivery of the necessary systems for lawful interception Alcatel can also provide the interception service itself. Alcatel Germany operates an own Network Operation Centre (NOC) which is equipped with the required staff and systems.

Uwe Stahl
Alcatel Stuttgart, Germany
Phone: +49 711 821 43159
Mail: U.Stahl@alcatel.de

Alcatel 8619 Voice Quality Analyser

Besides all the technical discussions concerning the realization of voice services on Next Generation Networks (NGN), the voice quality perception by a subscriber is crucial for him to accept, use and finally pay for that service. The **Alcatel 8619 Voice Quality Analyser (VQA)** (Fig. 4.1) accounts for that by supporting end to end measurements to determine the voice quality from the subscriber's point of view.

The most important criteria for voice quality are the so called listening quality and the mouth to ear delay of the voice signal. Listening quality considers - among others - the influences of speech processing functions, like voice compression, echo suppression, and error concealment for lost voice packets. Big delays disturb dialogues. Both parameters are calculated and output by the **Alcatel 8619 VQA** together with others, e.g. signal levels.

The **Alcatel 8619 VQA** builds on top of an integrated, high performing system platform. The whole **Alcatel 8619 product family** is based on a specific software shell, optimized for protocol processing, running on the Windows NT operating system. Together with the PCI interface cards designed for that platform a variety of applications are supported. By combining functional building blocks like protocol analysis, simulation, and emulation a big number of products has already been realized, among them are protocol testers (supporting more than 200 protocols), protocol gateways, conformance tester, etc.

The **Alcatel 8619 VQA** takes some of those available elements and adds the voice quality analysis. By emulating subscriber terminals a connection is automatically set up, a voice signal is played into one end, the voice signal at the other end is recorded and finally becomes analysed by processing the voice signals sent and received. Furthermore the system allows to trace the traffic at various points in the network in parallel to the measurement, to determine the influence of network elements to the voice quality.

Uwe Ackermann
Alcatel Stuttgart, Germany
Phone: +49 711 821 42104
Mail: uwe.ackermann@alcatel.de

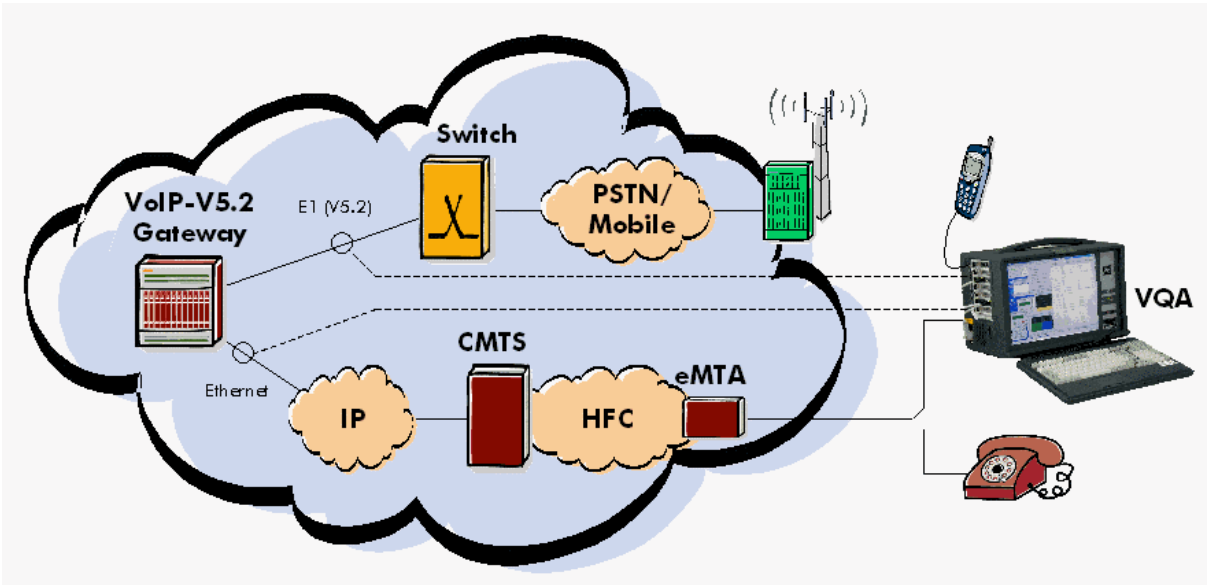


Fig. 4.1: Alcatel 8619 VQA in a Cable Environment

Emergency and Safety: The Project MESA

MESA is the abbreviation for "Mobile for Emergency and Safety Applications". It is a partnership project of the Telecommunication Standards Association (TIA) in the USA and the European Telecommunication Standards Institute (ETSI) under the patronage of the UNO and the EU and in co-operation with ITU for the specification of a digital broadband radio network for Public Protection and Disaster Relief (PPDS).

The partnership agreement was signed in January 2000 and agreed in January 2001, but it was triggered by the "Tampere Convention" agreed on in 1998 at the "International Conference on Emergency Telecommunication" (ICET-98), which identifies the necessity for worldwide identical and standardised telecommunication resources for rescue personnel and the unhindered and uninterrupted access to them. The project obtained a dramatic increase of its importance by the terrorist attacks, but also the numerous natural disasters happening in recent years.

What is the aim of the project MESA? It shall specify a digital broadband radio network with a bit rate of 2 Mbit/s or higher, allowing interconnection of different emergency services and bridging of long distances via satellite links. The following basic requirements have been defined:

- high bandwidth combined with rapid mobility – up to the speed of aeroplanes
- use of an unique frequency range being free of interference
- connectivity to global satellite and fibre links
- integration and enhancement of existing narrowband radio systems like TETRA, GSM, UMTS...
- worldwide deployment – also in developing countries – without national limitations and dependency on public infrastructures and power supply
- fast deployment and usability
- auto- and re-establishment and self-healing
- extra-ordinary security features and transparent encryption.

Fig 5.1 shows the relationship of MESA to existing radio systems with respect to bit rate, mobility and (possible) frequency range.

As main areas of interest for the application of MESA-conform systems have been identified:

- national and international support of police, law enforcement and juridical organisations
- advanced fire fighting, civil defence, anti-terrorism and disaster response

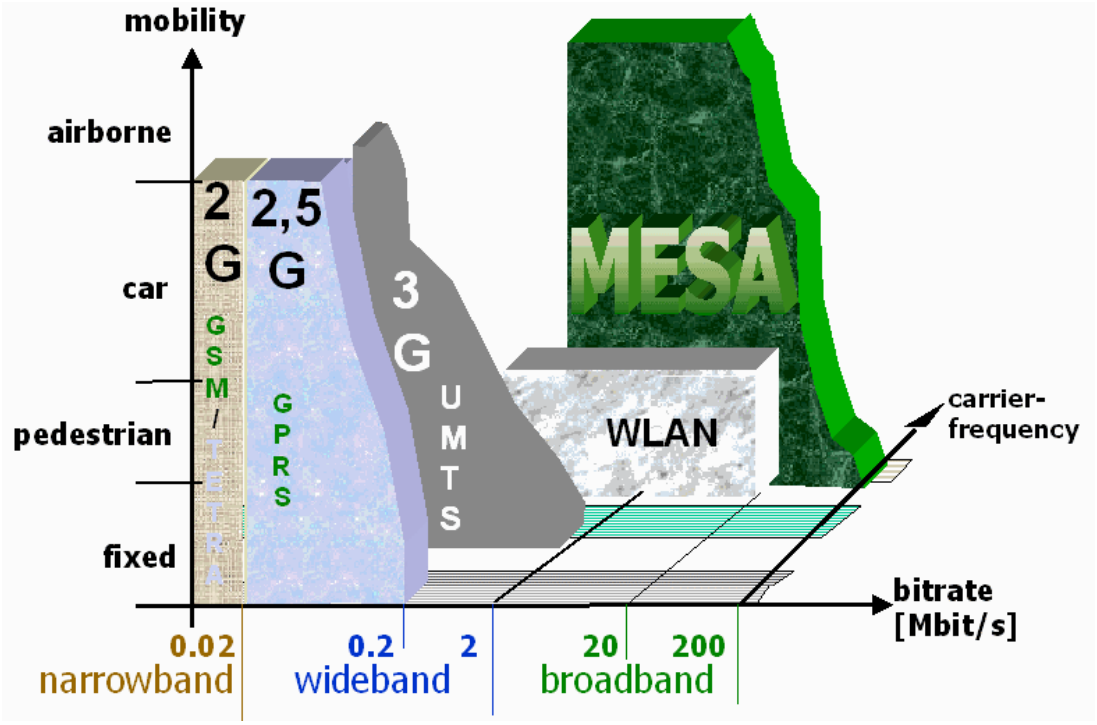


Fig. 5.1: Relationship of Technologies

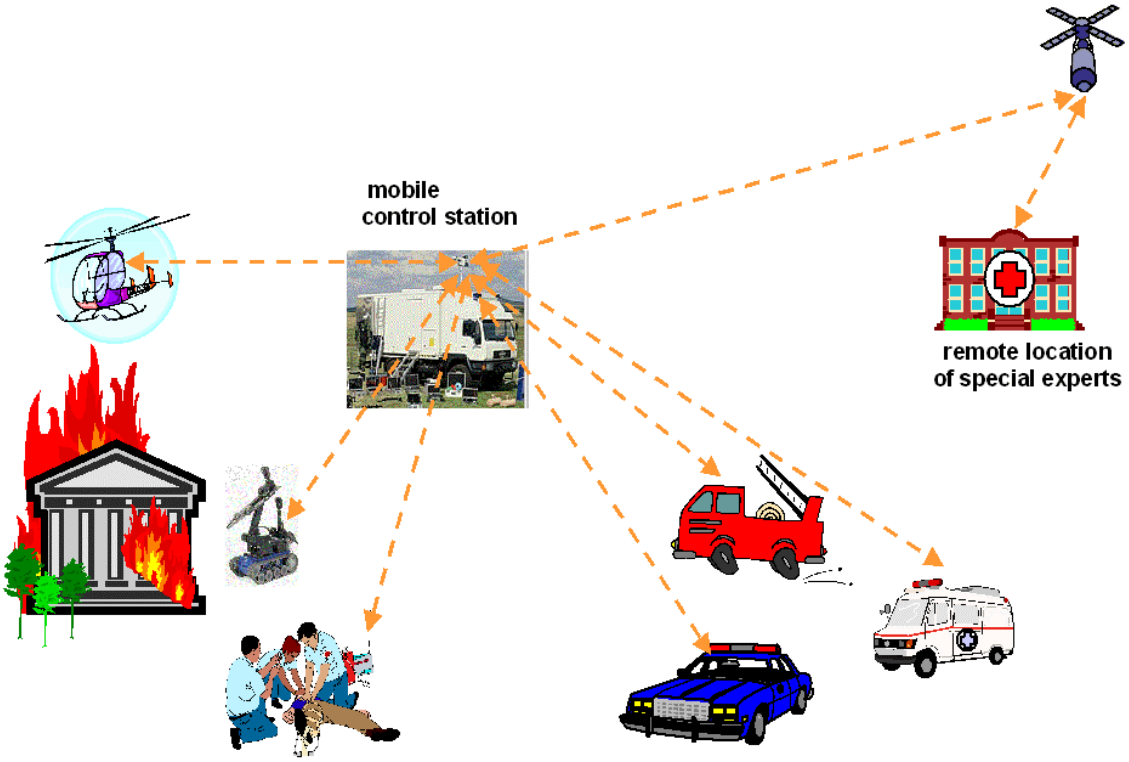


Fig. 5.2: Scenario for MESA

- peacekeeping operations
- emergency and tele-medicine
- control of mobile robotics
- advanced surveillance and security of critical and vulnerable locations like airports and nuclear power plants.

Fig. 5.2 gives a scenario for possible application of MESA in a disaster relief.

The Service Specification Sub-Group (SSG) of MESA has published in October 2002 three Statements of Requirements (SoR MESA TS 70.001 to 70.003) which are the base for the technical specifications to be created by the three Technical Specification Sub-Groups (TSG). The most urgent task of the TSG, however, is to get a frequency band allocated from the "World Radiocommunication Conference" (WRC).

This is a very difficult task which complicated in addition by the fact that European and American authorities - CEPT and CITEL - favour totally different ranges near 400 MHz or 5 000 MHz.

A first input was given to WRC 2003, but the next opportunity for an allocation will be not until WRC 2007.
Fortunately in parallel to the more basic and co-ordinating work in the MESA specification groups considerable work is done mainly in ETSI, but also in ITU working groups. Seven ETSI-TCs and three ITU-SGs have already created a number of detail specifications for MESA and have several additional in process.

Siegfried Schmoll
Alcatel Stuttgart, Germany
Phone: +49 711 821 43118
Mail: S.Schmoll@alcatel.de

From PAN to PN to satisfy the user's needs

GSM, UMTS and WLAN are just the beginning of an increasingly wireless infrastructure. Other technologies such as Bluetooth and Ultra Wide Band will in future supplement today's technologies. Indications are, that radio connections will go far beyond terminals for mobile people, but increasingly connect machines, appliances, consumer devices, sensors and actors. The majority of the applications will be data services. Among the applications are navigation services, remote diagnosis, information systems, teleservices including logistics and administration for remote equipment as well as personal area networks. Personal communication will gain a new dimension in this environment, where people communicate not only with other people but interact with various companions like computers, household equipment, control systems in the house or in the car and this not only in their close vicinity but potentially anywhere. If all these digital equipment can be controlled over several networks individually and support personal applications, we talk about Personal Networks (PNs). Fig. 6.1 gives an overview about Personal Networks.

Future technologies in such PNs will provide location- and context dependent services and can introduce new levels of personal comfort and safety. The heart of a PN is a core Personal Area Network (PAN), which is physically associated with the owner of the PN. Personal Area Networks (PAN) allow devices to work together and share information and services. Using technologies such as Bluetooth, Personal Area Networks can be created in the **home**, in the **office**, in a **car** or in **public places**. This network enables everyday devices to communicate wirelessly. For example, a PAN gives PDA users the ability to wirelessly synchronize with a desktop device, to access e-mail and the Internet, or to control/monitor household equipment like a washing machine (Fig. 6.2)

To interconnect these cluster of PANs, IP-based always on Networks like DSL, UMTS, WLAN are required.

Currently we are working on three activities in the area of Personal Networks:

1. Member of the MAGNET consortium (EU project IST FP6)
2. Developing a mobile controlled/monitored washing machine prototype together with one of the biggest household equipment supplier.
3. Developing a PAN based City Information System prototype.

The MAGNET project is characterized as follows: The MAGNET vision is that Personal Networks (PNs) will support users' professional and private activities, without being obtrusive and while safeguarding their privacy and security. The MAGNET

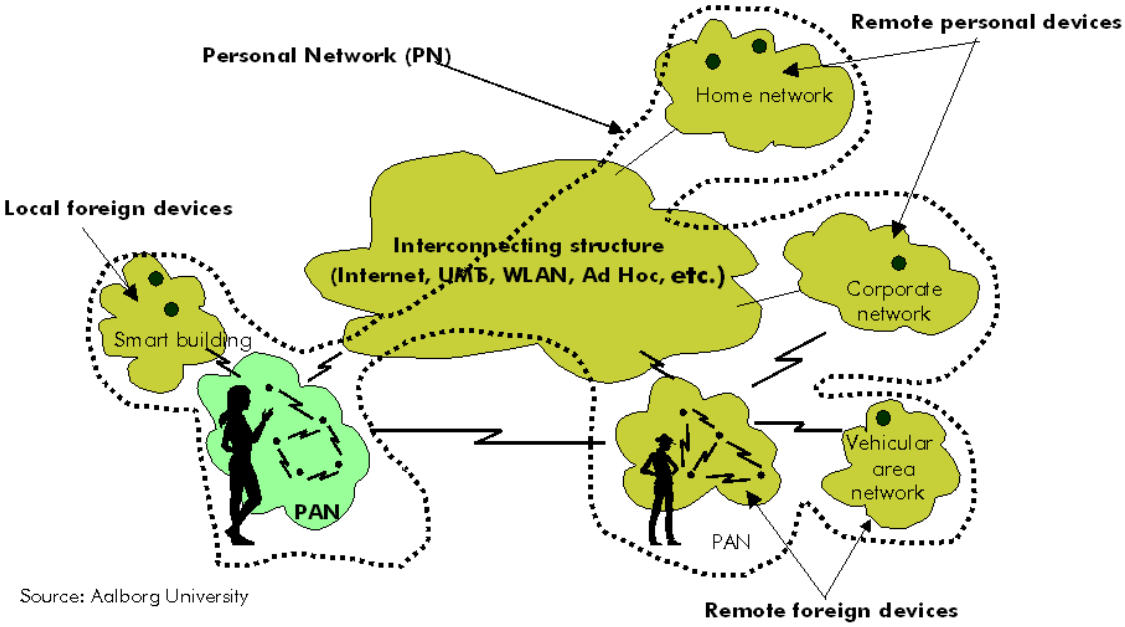


Fig. 6.1: Personal Network

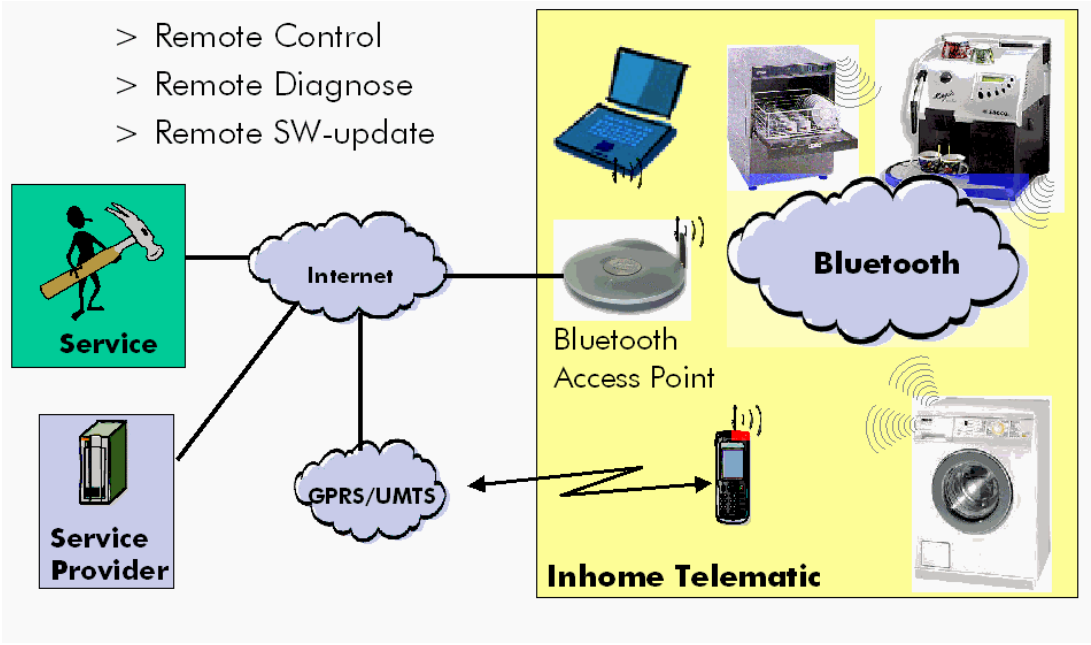


Fig. 6.2: Mobile controlled/monitored appliances

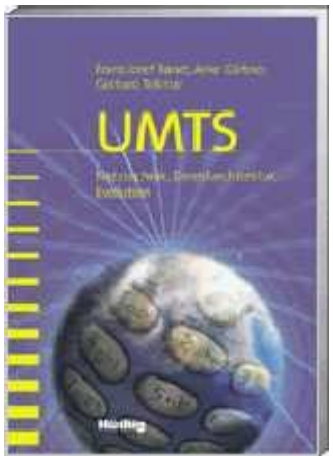
mission is to enable commercially viable PNs that are attractive, affordable and beneficial for end-users in their everyday life. The MAGNET overall objective is to design, develop, demonstrate and validate the concept of a flexible Personal Network (PN) that supports resource efficient, robust, ubiquitous service provisioning in a secure heterogeneous networking environment for nomadic users including user interfacing and socio-economic aspects. The MAGNET Consortium consists of 40 companies in 9 countries.

The target of the mobile controlled/monitored washing machine prototype is to demonstrate solutions, where all status information or malfunction can be displayed on a handheld or a mobile phone. If a mobile phone is used and a malfunction happens, additional a SMS can be sent automatically to the service hotline with a detailed error description. If the washing machine is integrated in a PAN, also fixed networks can be used for these additional services.

The target of the City Information System is to submit city information to e.g. tourists or their PDA or mobile Phone via Bluetooth.

Markus Jenisch
Alcatel Stuttgart, Germany
Phone: +49 711 821 40428
Mail: m.jenisch@alcatel.de

Recommended Readings



UMTS
Netzechnik, Dienstarchitektur, Evolution

Authors: Franz-Josef Banet, Anke Gärtner, Gerhard Teßmar

German Language

Published by: Huethig Fachverlag Heidelberg

http://www.huethig-telekommunikation.de/vmi/huethig/detail/pWert/5034

Java in der Telekommunikation
Grundlagen, Konzepte, Anwendungen

Authors: Stefan Rupp, Gerd Siegmund

German Language

Published by: dpunkt Verlag, Heidelberg

http://www.dpunkt.de/buch/3-89864-244-5.html