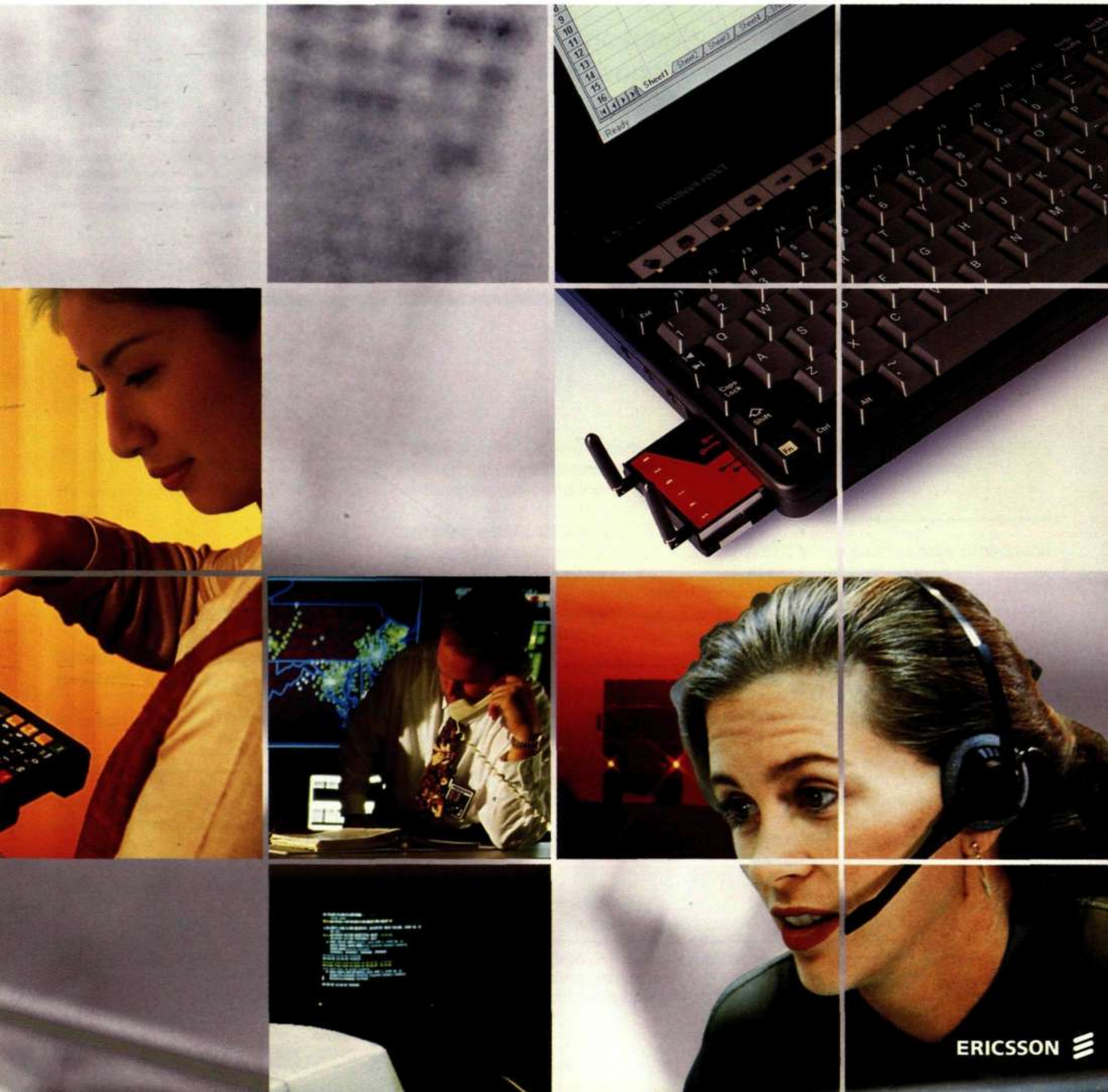
Ericsson REVIEW

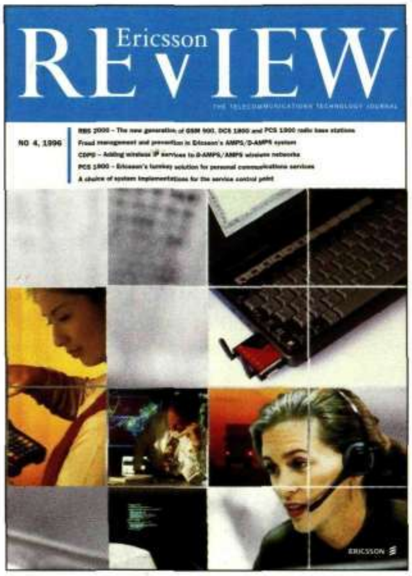
THE TELECOMMUNICATIONS TECHNOLOGY JOURNAL

NO 4, 1996



CONTENTS

No. 4 1996 • Vol.73



Cover:
The continuous evolution of hardware technologies and software applications is rapidly transforming the once-static telecommunications scene into an ever-changing mosaic of services and products.

CONTENTS
Previous issues

No. 4, 1995

The introduction of UniSwitch in AXE 10

Copper enhancement

MINI-LINK E – A new link for flexible transmission in cellular networks

Dynamic routing in circuit-switched networks

Ericsson Review – 70 years young

No. 1, 1996

Fixed cellular systems – an alternative way to provide basic telephony

New power distribution and earthing for AXE

Telecool Aero – A tailor-made cooling system for small telephone exchanges and containers

Ericsson echo cancellers – a key to improved speech quality

TEMS – A system for testing and monitoring air interfaces

No. 2, 1996

GSM 900/DCS 1800 – Ericsson's turnkey solutions for wireless communications services

Ericsson's new access network management system, E-ANMS

Remote upgrading and updating of AXE 10 software

The Ericsson DXX cross-connect system in mobile networks

No. 3, 1996

ARIDEM – a multi-service broadband access demonstrator

Polymeric microstructures technology for future low-cost, high-volume tele- and datacom components

The GSM 900, DCS 1800 and PCS 1900 systems in the wireless world of the future

Modular telecom power with internal optical communication

AIRLINE – the flexible radio access system

Ericsson Review © Telefonaktiebolaget L M Ericsson • Stockholm 1996. • Responsible publisher *Håkan Jansson* • Editor *Steve Banner* • Editorial staff *Eva Karlstein* • Layout *Paues Media* • Address Telefonaktiebolaget L M Ericsson S-126 25 Stockholm, Sweden • Fax +46 8 681 27 10 •Published in English and Spanish with four issues per year • Subscription one year USD 45

CONTRIBUTORS
in this issue

Björn Hesse, who joined Ericsson in 1995, is product manager working with market messages for GSM 900/DCS 1800/PCS 1900 base station products at Ericsson Radio Systems AB. He earned his MSc in Industrial and Management Engineering from the Linköping Institute of Technology in 1982.

Catharina Lundin is product manager in the strategic product management group at Cellular Systems, American Standards, Ericsson Radio Systems AB. She holds an MSc in Mechanical Engineering from the Royal Institute of Technology, Stockholm, and an MBA from George Mason University, Virginia.

Binh Nguyen is a systems engineer in the CSM 8800 Cellular Network Systems Design group of Ericsson Research, Canada. He is currently working with fraud features. He holds an MSc in Electrical Engineering, awarded by Concordia University, Canada.

Ben Ewart, senior product engineer, is responsible for analysis and documentation of AMPS/D-AMPS market requirements in the CMS 8800 Features and Services Applications group in Dallas. He holds a BSc in Electrical Engineering, awarded by Texas A&M University.

Lars Wetterborg, currently manager of the wireless data product management group in the American Standards business unit of Ericsson Radio Systems AB, has been working in the field of data communication since 1978. Previously he spent about ten years in different R&D organisations for software development. He earned his MSc in 1975.

Sven Hellsten is manager for base station product management in the CMS 40/PCS 1900 system, working at Market Operations for North and South America. He holds an MSc in Physics Engineering awarded by the Department of Technology at Uppsala University in 1990.

Robert E. Eubanks Jr. is currently project leader for the INX 2.2 Design project, developing the SCP-G. Previously, he worked on AXE design for the CCS (SS7) subsystem and on SMAS design. He joined Ericsson (US) in 1987. He has BSc and MSc degrees in Computer Science from University of Texas, Dallas.

Marko Hentilä is responsible for SCP-G product management in the Network Intelligence unit at Ericsson Telecom. After joining Ericsson in 1989, he was engaged in AXE software development, customer training, and local product management. He has an MSc in Electrical Engineering from Helsinki University of Technology.

Thomas Larsson, manager of the Ericsson Network Intelligence Platforms product management group, is responsible for product plans and strategies. He holds MSc degrees in Electrical Engineering from Northeastern University, Boston, and from the Royal Institute of Technology, Stockholm. He joined Ericsson in 1991.

Björn Hesse

Catharina Lundin

Binh Nguyen

Ben Ewart

Lars Wetterborg

Sven Hellsten

Robert E. Eubanks Jr.

Marko Hentilä

Thomas Larsson

FROM THE EDITOR

Steve Banner

"Can you guys come down and help us with this problem next time it happens ?" This was the gist of a particular call to Ericsson's Technical Assistance Centre in Montreal one day in the early 1990s from the engineering staff of a cellular network operator in a large American city. The problem they were referring to was unexpected and unexplained bursts of unusually high traffic over their network at seemingly random intervals, and at widely varying locations. After a few days of overloading the resources of the region in which it took place, and causing considerable annoyance to subscribers, the high traffic would suddenly disappear and the network would return to normal. It must be remembered that the cellular industry was still quite young at this time, and operators and manufacturers alike were on a steep learning curve. Therefore it was not surprising that no-one could put forward a theory to satisfactorily explain this previously unseen phenomenon. After weeks of checking and re-checking their forecasts and network planning calculations, the operator's engineers called on Ericsson for assistance with their investigations.

Several days later the unexplained peak reappeared in a new location and three radio network experts were quickly despatched southwards along with their test equipment. Upon their arrival in the city in question, they were driven to the base station that was at the heart of this latest mysterious disturbance to traffic. Before setting up their test equipment and preparing to work well into the night, the visiting experts decided to take the opportunity to walk to a nearby diner to have a quick meal. As they turned a particular corner, they noticed ahead of them a line of parked limousines. As they drew level with the first car, a man approached them with a line that must have felt like it came straight from the movies : "Psst ! Wanna make a phone call ? Anywhere in the world, as long as you like, twenty dollars !" It was thus, by pure fluke, that the team of visitors had discovered the source of the mysterious and mobile traffic overloads. Stolen mobile telephones had been used to establish a flourishing illegal business which moved to a new area every few days to avoid detection.

While the movie-like ending in this case is in some ways humorous, the above true example clearly illustrates the enormous potential cost of cellular fraud in terms of man-hours, lost revenue and customer dissatisfaction. While cellular systems have become much more complex and fraud-resistant since the early days of the industry, the methods used by fraudsters have also become more sophisticated. Ericsson's comprehensive portfolio of fraud-fighting features for its North American-standard cellular system (AMPS/D-AMPS), as described in this issue of Review, has therefore become a vital weapon in the battle against the many forms of cellular fraud.

The fruits of the continuous evolution of Ericsson's AMPS/D-AMPS system are also seen in the introduction of digital packet data into cellular networks. Ericsson's cellular digital packet data solution is designed to minimise cost to the operator by allowing the re-use of much of the existing cellular network equipment.

But the above developments are by no means the only changes to the wireless technology landscape. The GSM-based series of standards have spread throughout the world and established an enormous customer presence, with a correspondingly large series of radio networks. Advances in technology and design have allowed Ericsson to introduce a new and smaller generation of radio base stations – the RBS 2000 series. This family of base stations offers the operator a number of flexible alternatives in providing high-quality radio coverage.

The GSM-based PCS 1900 system also offers the operator a cost-effective and flexible means of providing service, with its well-proven architecture and wide range of subscriber services. Ericsson's system is described in this issue, along with a discussion on its future evolution.

However no description of telecommunication networks would be complete without considering the administration of services and the subscriber base – especially with the growing number of operators competing in the market. The increasing complexity and intelligence of networks calls for a corresponding evolution of service control points. The SCP-G system offers the operator an improved choice of systems to control and administer their customer base – without the need to use a row of black limousines as a business office!

Steve Banner
Editor

RBS 2000 – The new generation of GSM 900, DCS 1800 and PCS 1900 radio base stations

Björn Hesse

The dynamic growth of cellular networks is evident in many countries throughout the world. The penetration figures for mobile phones are even expected to rival those of the fixed phones in the near future.

GSM-based systems are leading the growth in radio network deployment, and Ericsson have been largely instrumental in making GSM a worldwide success. Starting in 1991 with the RBS 200 family of radio base stations, Ericsson have worked continuously to enhance and evolve the radio network technology.

The author describes Ericsson's approach to meeting the new requirements of the mass market, focusing on competitive cost, higher capacity, increased coverage, and improved voice quality.

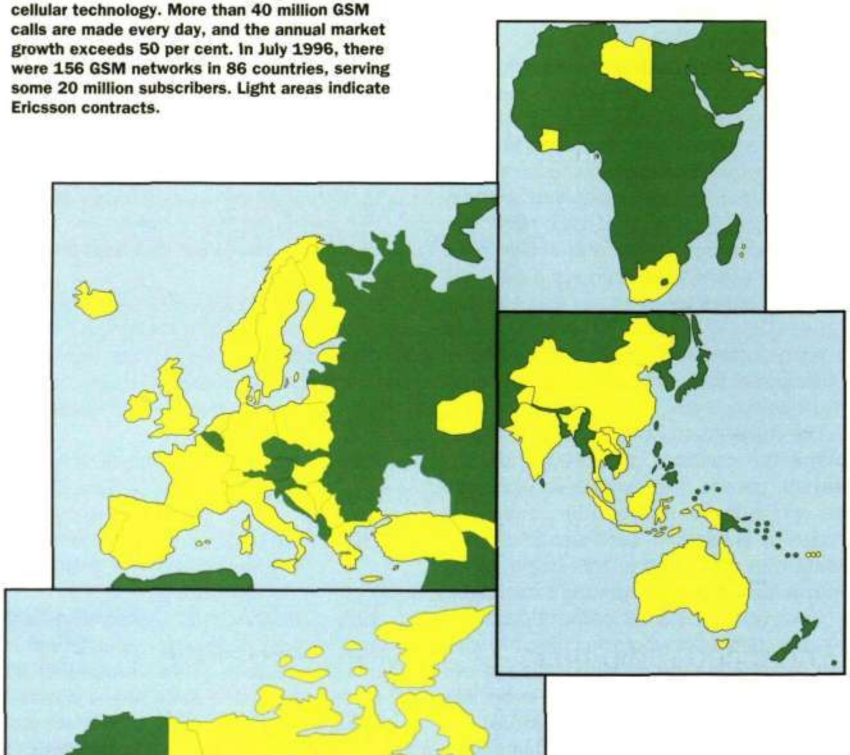


Fig. 1
GSM is the world's most widely deployed digital cellular technology. More than 40 million GSM calls are made every day, and the annual market growth exceeds 50 per cent. In July 1996, there were 156 GSM networks in 86 countries, serving some 20 million subscribers. Light areas indicate Ericsson contracts.

In only five years, GSM has captured the market as the world's most widely deployed digital cellular technology. Its worldwide success has been driven by three key factors:

- its evolutionary capabilities, from simply voice to a wide range of advanced data and personal services;
- its cost-effectiveness, from planning and implementation to operation;
- its fully open international standards, stimulating market growth and competition, and introducing a true multi-vendor environment.

The DCS 1800 and PCS 1900 systems are two adaptations of the GSM standard which respond to mass-market needs in a very cost-effective way. In Europe, GSM-based DCS 1800 offerings complement the established GSM 900 networks. In North America, PCS 1900 networks are now being introduced in Canada and the US.

RBS 2000 reduces operating and life-cycle costs

In the evolution from business applications to broader consumer usage, GSM operators must strengthen their networks and enhance their coverage and capacity offerings. Operators must also provide good indoor coverage in homes, offices and indoor public areas.

To satisfy the evolving requirements of the mass market, the stable and proven GSM network components – such as radio base stations – will be crucial. Radio base stations, RBS, represent the largest proportion of network infrastructure investments, as well as a significant part of operating costs. RBS-site rentals can be as high as 40 per cent of operating costs.

It is also becoming more difficult and expensive to find sites for suitable radio base stations, especially in high-capacity demand areas. Zoning regulations and special requirements from property owners often interfere with the operator's placement plans. Increasingly, operators must look for flexible and cost-effective solutions.

Complete turnkey concept

Ericsson have played a seminal role in the GSM story from the beginning. Starting in 1991 with the RBS 200 family of

Fig. 2
Ericsson's small, light-weight RBS offers flexible, and virtually "invisible" placement. The new micro-RBS offers increased channel capacity and coverage in limited areas and represents leading-edge radio technology.

radio base stations, Ericsson have worked continuously to enhance and evolve radio network technology. The new RBS 2000 family (Ericsson's implementation of base transceiver stations, BTS) makes the most of VLSI technology, miniaturisation and state-of-the-art ASIC design.

With the RBS 2000 family, site space is reduced and site ownership costs are cut. In addition, reliability and in-service performance are improved.

The low site acquisition and preparation costs, the rapid installation and commissioning – typically in just one hour – and minimised maintenance requirements result in reduced overall life-cycle costs. Together these make the RBS 2000 family an attractive choice for expanding cellular network operators.

RBS 2000 is a complete concept: a one-cabinet turnkey solution for both outdoor and indoor installations. It offers high capacity and stable radio network control functionality. Indoors, it minimises footprint, noise, and heat generation.

The transceiver architecture of RBS 2000 supports a wide choice of network topologies and configurations, offering flexible system roll-out options for the operator. RBS 2000 is completely pre-assembled, software-downloaded and fully tested at the factory before delivery.

Enhanced radio base station technology meets mass-market needs

In meeting the new requirements of the mass market, four key areas are especially important: competitive cost , higher capacity, increased and focused coverage, and improved voice quality.

Increased cost-effectiveness

In today's competitive environment, key business aims of every GSM operator include achieving the lowest cost per subscriber, and reducing operating costs in

Box A
Abbreviations

ALNA	Antenna-mounted low-noise amplifier
ASIC	Application-specific integrated circuit
BSC	Base station controller
BSS	Base station system
BTS	Base transceiver station
DCS	Digital cellular system
ETSI	European Telecommunications Standards Institute
GSM	Global system for mobile communications
ISDN	Integrated services digital network
MSC	Mobile switching centre
OSS	Operations support system
PCS	Personal communications system
PROM	Programmable read-only memory
PSTN	Public switched telephone network
RBS	Radio base station
TDMA	Time-division multiple access
VLSI	Very large scale integration

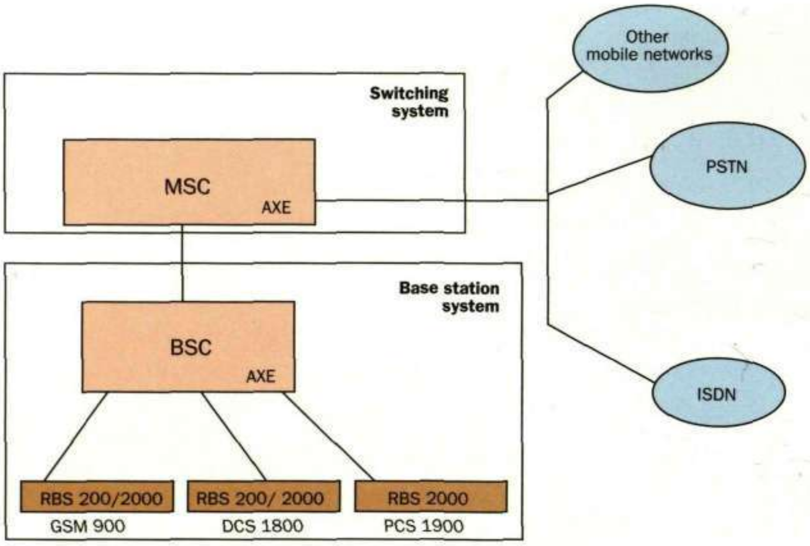


Fig. 3
GSM network infrastructure with switching system (SS) and base station system (BSS).

general. The RBS 2000 family of radio base stations (Box B) reduces maintenance costs, and minimises loss of revenue caused by base station downtime. This is accomplished through extensive supervision, in combination with fewer replaceable units in the base station.

Both indoor and outdoor models are based on the same modular units. This makes the base stations very cost-effective in terms of maintenance.

In addition, built-in unit redundancy supports reconfiguration in case of faults. The result is minimised fault impact and less downtime. Should a hardware failure make a visit to the site necessary, an indicator points out the faulty unit. The unit is then replaced on site in less than 15 minutes.

Furthermore, battery backup guarantees that the radio base station will operate without any loss of traffic in environments with unstable power supply.

The small size of Ericsson's RBS 2301 micro base station minimises the site cost. In addition, the micro-RBS has a number of antenna options which means that high antennas on the building can be avoided. This results in substantial savings in rental charges and cabling costs.

Box B
Model description

The RBS 2000 family comprises four radio base station models: RBS 2101, RBS 2102, RBS 2202, and RBS 2301.

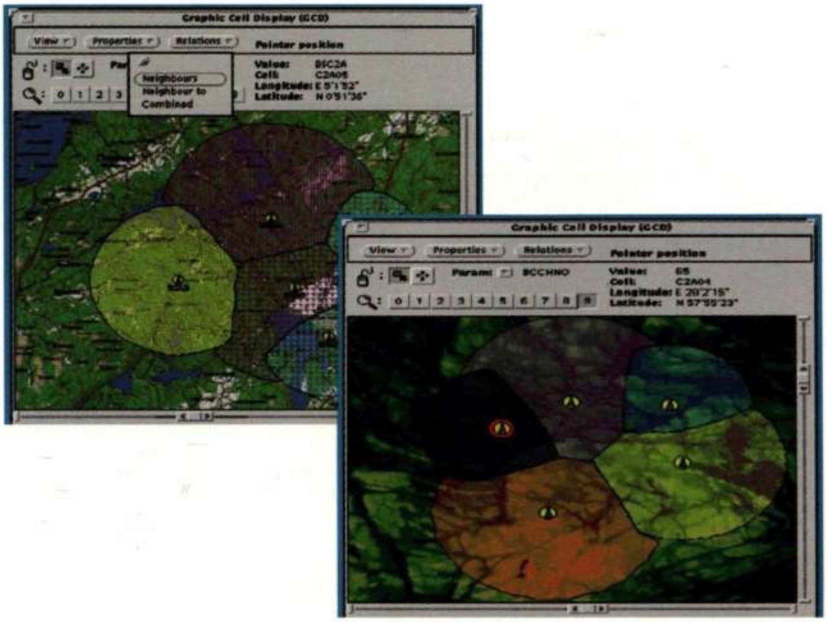
The RBS 2101 is an outdoor or indoor self-contained cabinet with up to two transceivers. It can be configured for omnidirectional cells, or up to three sectorised cells (with more than one cabinet). The flexible design offers the opportunity for a number of configurations and expansions as the network grows. There are different climate solutions for different environments. The RBS 2101 can be wall-mounted, installed at ground level or on a roof.

The RBS 2102 is an outdoor self-contained cabinet with up to six transceivers. It can be configured for omnidirectional cells, or up to three sectorised cells. The flexible design offers the opportunity for a number of configurations and expansions as the network grows. The RBS 2102 can be wall-mounted or installed at ground level or on a roof.

The RBS 2202 is an indoor cabinet with up to six transceivers. It can be configured for omnidirectional cells, or up to three sectorised cells. The flexible design offers the opportunity for a number of configurations and expansions as the network grows. The RBS 2202 can be installed in any indoor environment.

RBS 2301, the micro-RBS, is a cabinet for outdoor or indoor installation. It is used to increase capacity and for fill-in coverage for hot-spot areas, such as shopping malls. The RBS 2301 supports macrocells (when installed above roof-top level or on antenna masts), microcells (when installed on poles or walls), and indoor picocells. It offers a wide range of omnidirectional and directional antenna solutions. The micro-RBS can be configured in different colours for the best placement.

It takes one person a few minutes to install the RBS 2301. It can be mounted on an exterior or interior wall, or on a pole beyond the reach of vandals. In fault situations, the entire unit can be removed and replaced.



Value: BSC2A
Cell: C2A05
Longitude: E 5°1'32"
Latitude: N 0°51'36"

Param: BCCHNO
Value: 65
Cell: C2A04
Longitude: E 28°2'15"
Latitude: N 57°55'23"

Fig. 4
The highly graphic OSS user interface offers easy access to information on network performance – even to the level of individual radio base stations.

The operations support system, OSS, continuously monitors and controls all GSM system functions, resulting in smooth and disturbance-free operation. The OSS plays a key role in the maintaining and enhancement of network service quality. It provides dedicated applications, such as radio base station software, hardware and configuration management.

Remote operation and maintenance (from OSS and the base station controller, BSC), together with built-in intelligence, minimises on-site visits. The installation database of the radio base station stores all network hardware data, which is easily accessible in the BSC. During software function changes, new program revisions can be transferred to the radio base station without disturbance to its operation.

The installation database makes on-site fault localisation unnecessary. Hardware-related base station data that was previously accessible only on site is now obtainable in the BSC. Faulty units are detected and shown in the BSC alarm printout.

When faulty units are replaced, an automatic self-test function reduces repair time

Box C
Technical specification RBS 2101

Environment	Indoor/outdoor
Frequency band	GSM 900, DCS 1800 or PCS 1900
Number of transceivers	1-2
Number of sectors	1-3, with more than one cabinet
Transmission interface	1.5 Mbits/s (T1), 2 Mbit/s (E1)
Dimensions (HxWxD, in mm)	1167 x 705 x 450
Power into antenna feeder (typical value)	28 W / 44,5 dBm (GSM 900)) 22 W / 43,5 dBm (DCS 1800 / PCS 1900)
Receiver sensitivity (typical value)	≤ -107 dBm ≤ -109 dBm with ALNA (DCS 1800 / PCS 1900)
Power supply	188 - 275 VAC 45 - 65 Hz
Battery backup	Min. 3 minutes
Operating temperature	-33° - +55°C
Weather proofing	Min. level IP55 in IEC 529

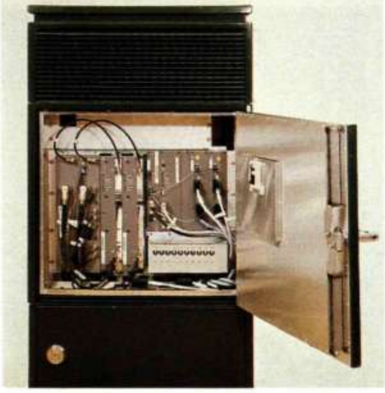


Fig C
The RBS 2101 is an outdoor or indoor self-contained cabinet with up to two transceivers.

Box D
Technical specification RBS 2102

Environment	Outdoor
Frequency band	GSM 900, DCS 1800 or PCS 1900
Number of transceivers	1-6
Number of sectors	1-3
Transmission interface	1.5 Mbits/s (T1), 2 Mbit/s (E1)
Dimensions (HxWxD, in mm)	1605 x 1300 x 710
Power into antenna feeder (typical value)	28 W / 44,5 dBm (GSM 900)) 22 W / 43,5 dBm (DCS 1800 / PCS 1900)
Receiver sensitivity (typical value)	≤ –107 dBm ≤ –109 dBm with ALNA (DCS 1800 / PCS 1900)
Power supply	188 - 275 VAC 45 - 65 Hz
Battery backup	1 hour
Operating temperature	-33° - +45°C
Weather proofing	Min. level IP55 in IEC 529

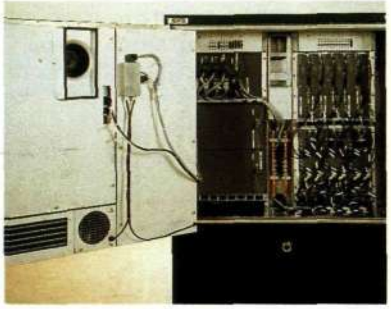


Fig. D
RBS 2102 is an outdoor self-contained cabinet with up to six transceivers.

Fig. 5
In addition to business usage, personal communications are now spreading rapidly among private users.

Box E
Technical specification RBS 2202

Environment	Indoor
Frequency band	GSM 900, DCS 1800 or PCS 1900
Number of transceivers	1-6
Number of sectors	1-3
Transmission interface	1.5 Mbits/s (T1), 2 Mbit/s (E1)
Dimensions (HxWxD, in mm)	1628 x 600 x 400
Power into antenna feeder (typical value)	28 W / 44,5 dBm (GSM 900)) 22 W / 43,5 dBm (DCS 1800 / PCS 1900)
Receiver sensitivity (typical value)	≤ –107 dBm ≤ –109 dBm with ALNA (DCS 1800 / PCS 1900)
Power supply	188 - 275 VAC 45 - 65 Hz
Battery backup	Optional
Operating temperature	+5° - +40°C

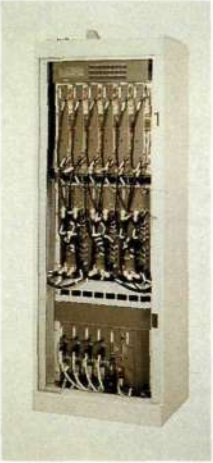


Fig. E
The RBS 2202 is an indoor cabinet with up to six transceivers. It has the smallest footprint on the market for six-tranceiver indoor BTS models.

further. All diagnostic information is stored in non-volatile memory in the replaced unit for later consultation in the repair shop.

The introduction of non-volatile memory and autonomous internal software distribution within RBS 2000 has also simplified program loading and function changes. Software downloading from the BSC is executed as a background process and results in no downtime.

Enhanced network capacity

The consumer market requires higher levels of service availability and quality –especially in dense user environments, such as shopping malls, airports, underground areas, parking garages, and leisure complexes.

One solution to increased capacity is based on tighter frequency reuse, in combination with hierarchical cell structures. Frequency hopping provides enhanced radio network capacity in small urban cells, where interference and fading are common.

The base station system, BSS, within the GSM systems ensures fast, accurate, and reliable handover of calls to the correct cell and channel. The BSS also manages the efficient distribution of traffic between cell layers.

Reusing frequencies by changing the cell structure into smaller cells is a standard feature of Ericsson's GSM systems. Three-level hierarchical cell structures offer high-quality service in environments with great variations in traffic density. Maximum capacity and quality are ensured at all times through efficient handovers between the different cell layers.

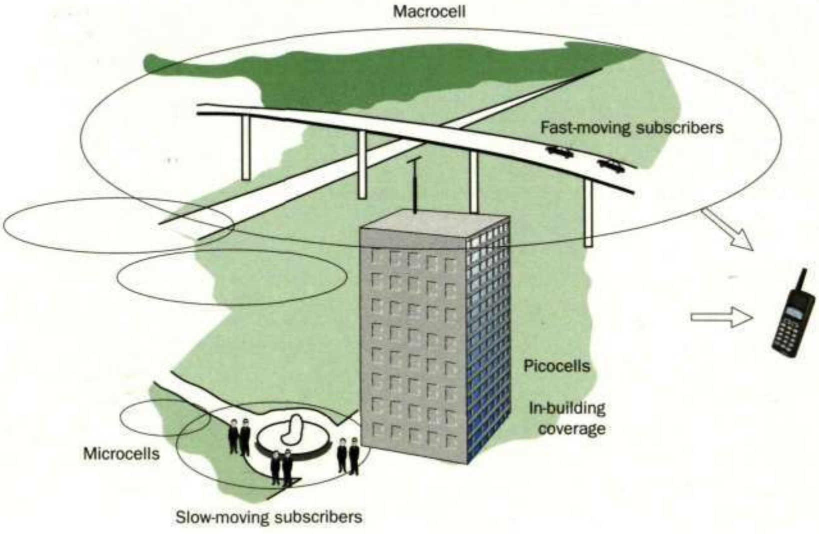


Fig. 6
The hierarchical cell structure concept allows differently sized cells – which are divided into layers – to co-exist in the same geographical area.

The hierarchical cell pattern handles fast moving vehicles (by means of macrocells), provides services to traffic hot spots as well as fill-in coverage (microcells), and offers dedicated indoor coverage (picocells).

In addition, half-rate speech-coding methods make it possible to use the equipment much more efficiently. Half-rate (HR) vocoders can double speech

Box F
Technical specification RBS 2301

Environment	Indoor/Outdoor
Frequency band	GSM 900 / DCS 1800 / PCS 1900
Number of transceivers	1-2
Number of sectors	1-3 with more than one cabinet
Transmission interface	1.5 Mbits/s (T1), 2 Mbit/s (E1)
Dimension (HxWxD, in mm)	535 x 408 x 160
Weight	< 28 kg
Volume	< 33 litres
Power into antenna feeder (typical value)	2.0 W/33 dBm
Receiver sensitivity (typical value)	≤ –107 dBm(GSM 900) ≤ –106 dBm (DCS 1800/PCS 1900)
Power supply	105 -275 VAC 45 - 65 Hz
Battery backup	min. 3 minutes
Operating temperature:	-33° - +45°C

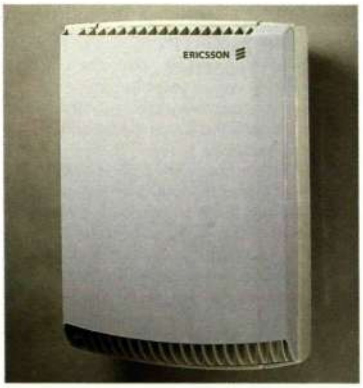
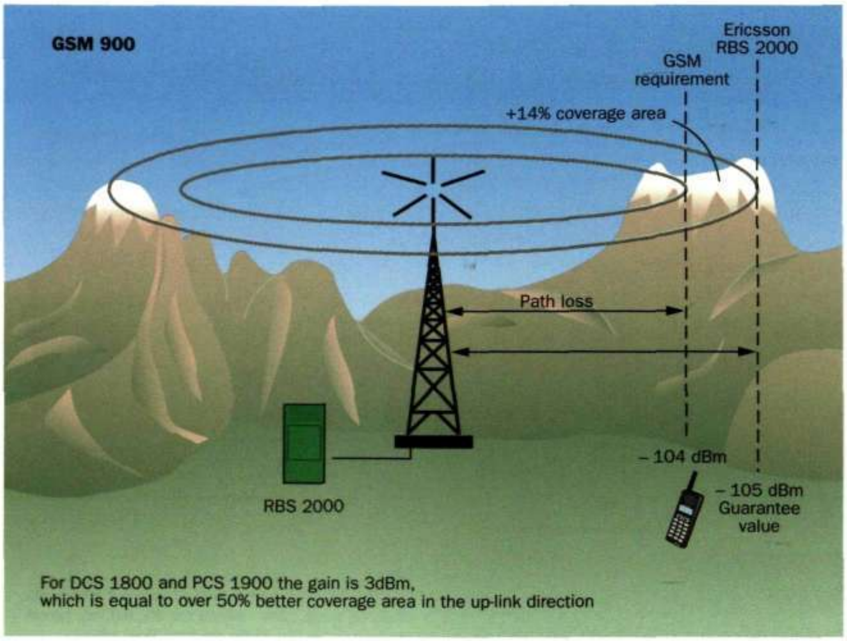


Fig. F
RBS 2301, the micro-RBS, is a two tranceiver cabinet for outdoor or indoor installation.



For DCS 1800 and PCS 1900 the gain is 3dBm, which is equal to over 50% better coverage area in the up-link direction

Fig. 7
Higher up-link sensitivity is provided through the antenna-mounted low-noise amplifier. At the same time, attenuation between the antenna and the radio base station is minimised.

capacity, due to the fact that two subscribers can share one time slot.

Improved coverage

To increase the number of subscribers, and thus competitiveness, GSM operators need virtually complete population coverage outdoors. But they also need new solutions for specific indoor coverage.

Ericsson solutions to better coverage include antenna-mounted low-noise amplifiers, ALNA, which extend cell ranges. They can also reduce the number of radio base station sites by as much as 30 per cent.

Ericsson indoor solutions cover both residential, business and public environments. GSM radio network technology paves the way for cost-effective implementation of indoor coverage.

The RBS 2000 family offers three main indoor solutions: multi-casting picocells, with distributed indoor antennas; single picocell and macrocell coverage from outdoor cells. This coverage, as well as the performance of the base stations, can be improved by means of ALNA technology.

Improved voice quality

Cellular users are now demanding PSTN-like levels of voice quality. The use of voice-controlled – or at least voice-based – value-added services, such as telephone banking and automated information services, also infers requirements for better intrinsic voice quality.

To meet these requirements, the GSM 13 kbit/s full-rate vocoder is now being enhanced. The new enhanced full-rate (EFR) coder comprises the latest advances in algorithm research and speech coding.

The new generation radio base stations

The RBS 2000 range of radio base stations includes both indoor and outdoor versions. All models are designed for capacity enhancements and extended coverage. They fulfil all relevant GSM specifications prepared by the ETSI standardisation forums.

Standard features

The RBS 2000 product family for GSM 900, DCS 1800 and PCS 1900 is specially designed to offer rapid and cost-effective roll-outs as well as low total life-cycle costs.

The outdoor models are vandal-proof, and the transmission equipment and battery backup are located inside the cabinet.

The six-transceiver indoor model has the smallest footprint on the market –

Box G
Base station system makes optimum use of frequency spectrum

The radio base station, RBS, is part of Ericsson's powerful base station system, BSS, which also comprises the base station controller, BSC. The BSS, together with the mobile switching centre, MSC, is crucial to cost-effective transmission and competitive network operation:

- The base station controller, BSC, is a high-capacity switch which provides total overview and control of radio functions, such as handover, management of radio network resources and handling of cell configuration data. It also controls radio frequency power levels in the RBSs, and in the mobile phones. BSCs also set transceiver configurations and frequencies for each cell.
- The radio base station, RBS, is the radio and transmission equipment required at a site. RBS functions include radio signal reception (from mobile phones) and quality measurements. Each transceiver in the RBS operates at a given pair of frequencies and can serve many cells.

The transmission interface between BSC and RBS is the A-bis interface. Link access protocol on D-channel (LAPD) multiplexing makes it possible to use "subrate" links – and to save transmission resources. In this way, four transceivers can share one time slot. The improvement in transmission efficiency over the A-bis interface can be as high as 20-30 per cent.

The MSC supervises one or more BSCs, which in turn can control a number of RBSs. Combining an MSC with a BSC will reduce both transmission, operation, and maintenance costs, making a combined MSC/BSC an economical solution when starting up a small cellular network.

Remote operation and maintenance

The RBS operation and maintenance is remote-controlled. The software stored in the flash PROM/RAMs of the RBS transceivers is controlled, loaded and upgraded from the BSC. Faults and disturbances are reported to the BSC, which automatically decides how to minimise the effect of faults on active call traffic.

In addition, faults are isolated per transceiver and do not affect adjacent transceivers in the same base station.

only 0.24 square metres – thus making it easy to place in any room.

Good coverage and high capacity result from the RBS 2000 family's superior radio performance with high output power and superior receiver sensitivity. High coverage levels imply fewer radio base stations in a given area, and thus lower costs.

The RBS 2000 base stations support macrocells, microcells and picocells and are equipped with frequency hopping, diversity and duplexing – features that enable the operator to provide cost-effective and high-quality radio performance.

GSM phase 2

The radio base stations support GSM phase 2+ mobile phones. Compared with GSM phase 1, the mobile phones have more end-user features. This means that the operator can increase competitiveness through new subscriber services. In addition, network resources are more efficiently used by phase 2 phones.

Conclusions

Radio base stations represent the largest proportion of network infrastructure investments, as well as a significant part of operating costs. Ericsson's new range of radio base stations – the RBS 2000 family – with its reduced overall life-cycle costs is thus an attractive choice for expanding cellular network operators.

The RBS 2000 family is the result of Ericsson's innovative technology development, making the most of VLSI technology, miniaturisation and state-of-the-art ASIC design.

The transceiver architecture of the RBS 2000 supports a wide choice of network topologies and configurations, offering flexible system roll-out options for the operator. The RBS 2000 base stations also fulfil all relevant GSM specifications prepared by the ETSI standardisation forums.

Fig. 8
Superior radio performance means high coverage but also better penetrations into buildings.

Box H
Efficient micro cellular technology

To cope with the increased number of mass-market subscribers, network capacity must be enhanced – especially in areas of high user density. However, the traditional wide-area macrocells do not solve the capacity problem in these special environments.

The most cost-efficient solution to achieve capacity enhancements is the introduction of a hierarchical cell structure, which implements microcellular technology; the smallest microcells covering a few hundreds of metres in radius.

The Ericsson range of radio base stations – the RBS 2000 – is ideal for building a cost-effective network, covering both macrocell, microcell, and picocell layers.

Microcellular networks can be used to provide capacity enhancements in two modes: targeted on traffic hot spots, or as a high-capacity network covering a central business district.

The necessity for smaller cell sizes to enhance capacity also implies increasing the number of RBSs, which means that they must be extremely cost-effective. Ericsson's new micro-RBS 2301 cuts site costs by up to 70 per cent and is very easy to install and maintain.

Compared with a base station with only one transceiver, the micro base station offers more than three times the traffic capacity.

The RBS 2000 family is the result of Ericsson's innovative technology development. Many technical functions have been reduced to application-specific integrated circuits (ASIC) which greatly reduces the heat generation inside the cabinets, and results in greater capacity in very small cabinets. The cooling system of the micro-RBS does not employ fans or moving parts. This makes the base station totally silent.

Micro-cellular networks also require high-capacity base station controllers, BSC, which can handle hundreds of cells and base stations in complex hierarchical layers. Larger BSCs also reduce the BSC site costs, as well as the signalling load on the cellular switch, the mobile switching centre, MSC.

Fraud management and prevention in Ericsson's AMPS/D-AMPS system

Catharina Lundin, Binh Nguyen and Ben Ewart

Ericsson, and all other wireless equipment providers, must be prepared, now and in the future, to deal with the threat of fraud. Losses of revenue to fraud are staggering – over USD 1 billion/year and, in some cases, as much as 40% of an operator's revenues. Moreover, fraud also undermines operators' credibility in the eyes of their subscribers, a further threat to revenues unless something can be done to turn the tables. Fortunately, something can be done – including Ericsson's direct attack on fraud by a variety of methods.

The authors describe Ericsson's fraud-fighting portfolio for AMPS/D-AMPS systems (CMS 8800), *and how operators of mobile telephone systems can* use its features to protect themselves and their subscribers from the most common types of fraud.

Fraud – one of the cellular industry's greatest problems

When operators first introduce cellular telephony into an area, their primary focus is on establishing capacity and coverage, and on signing up customers. However, as their networks mature and competition increases, financers expect a sound return on their investments. Irrecoverable losses as a result of fraud, for example, cannot be tolerated.

As it relates to lost revenue or to the loss of credibility as a service provider, fraud has been identified as one of the cellular industry's greatest problems. Because of fraud, one operator lost nearly 40% of revenues in 1993, and according to the Cellular Telecommunications Industry Association (CTIA), the annual global loss in revenue due to fraud now exceeds USD 1 billion. What is more, this figure does not account for the indirect costs of fraud, which include in-house teams of anti-fraud personnel, the cost of anti-fraud equipment, and the negative impact that fraud has on usage and subscriber growth through inconvenienced subscribers.

Fraud appears in many guises, and new forms are being contrived almost daily. Criminals who steal cellular phone service enjoy anonymity and other benefits, such as:

- personal use – ability to make an unlimited number of free calls;
- call-sell operations – portable operations that sell long-distance service at reduced rates;
- three-way calls – a three-way call can be set up to bypass regulations that prohibit communications between certain countries.

Cellular systems are vulnerable to fraud at several points in the network. To

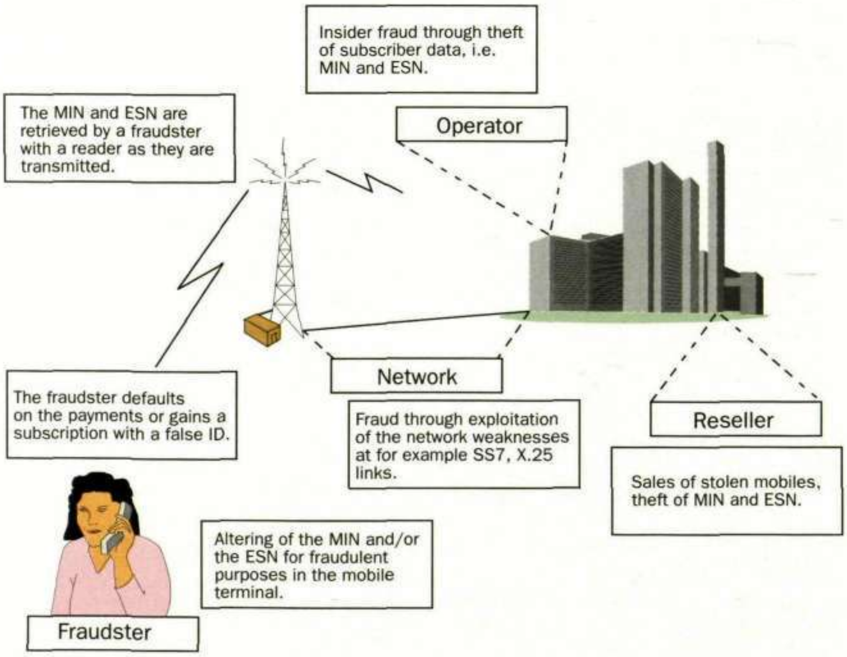

Insider fraud through theft of subscriber data, i.e. MIN and ESN.
The MIN and ESN are retrieved by a fraudster with a reader as they are transmitted.
Operator
The fraudster defaults on the payments or gains a subscription with a false ID.
Network
Fraud through exploitation of the network weaknesses at for example SS7, X.25 links.
Reseller
Sales of stolen mobiles, theft of MIN and ESN.
Altering of the MIN and/or the ESN for fraudulent purposes in the mobile terminal.
Fraudster

Fig. 1
Some vulnerable points in cellular systems.

date, the elements most frequently hit are the phone, the radio interface, and the signalling network. Internet is a popular forum for fraudsters who, in a matter of minutes, are able to post to a global audience detailed instructions on how telephone fraud is committed.

Because Ericsson were early to recognise the potential for fraud, they already offer many preventive features and tools in CMS 8800. Additionally, Ericsson recognise that the problem of fraud is growing in the world, and they continue to introduce new features that help to combat this problem.

Common types of fraud

Stolen handsets

Early cellular systems provided almost no protection against illegal access. To commit cellular fraud one needed only steal a cellular phone and then use it until the legitimate subscriber contacted his carrier — whose treatment for the problem generally consisted of turning the number off in the switch.

Subscription fraud

Another early form of fraud was perpetrated when a subscriber who, never intending to pay, signed up for service using false identification or fraudulently obtained customer information.

Cloning

Cloning, which is difficult to detect, can be described as the complete duplication of a legitimate mobile terminal, including the mobile identification number (MIN), the electronic serial number (ESN) and, in some cases, the subscriber's personal identification number (PIN). When cellular systems cannot distinguish between a clone and a legitimate subscriber, cloned telephones successfully pass pre-call validation checks, and thus may be used to make calls that are billed to legitimate subscribers.

There are three main reasons why perpetrators clone phones: to steal service, to maintain anonymity, and to create an "extension phone" service. The first two reasons are the main cause of lost revenue. Most cloners use the same MIN-ESN combination until they are denied service. However, sophisticated cloners alter the MIN and the ESN – creating "tumbling" phones – even before they are detected, in order to avoid raising suspicion or to avoid triggering any alarms.

The two most common ways of obtain-

Box A
Abbreviations

AC	Authentication centre
A-KEY	Authentication key
CAVE	Cellular authentication and voice encryption
CTIA	Cellular Telecommunications Industry Association
DCC	Digital colour code
ESN	Electronic serial number
FAD	Fraudulent activity detection
HLR	Home location register
I/O	Input/Output
MIN	Mobile identification number
MSC	Mobile switching centre
MSNB	Mobile station number
NPA	Area code/numbering plan area
PIN	Personal identification number
SME	Signalling message encryption
SSD	Shared secret data
TDMA	Time division multiple access
VP	Voice privacy

Box B
Summary of fraud types and CMS 8800 solutions

	Subscription fraud	Mobile terminal fraud	Insider fraud	Network fraud
Location of fraud	The user	The phone	The operator	The operator
Type of fraud	No payment False ID	Cloning Tumbling Hijacking	Theft of subscriber data	Exploitation of SS7 and X.25 links Attacks on nodes
Current solutions	Subscriber background and credit history check	Screening of ESN and MIN Validation Service and switch pulling PIN Authentication FAD Call barring	CTIA's recommendations for dealing with insider fraud	Terminal password Account password
Solutions being implemented		Analogue Authentication Call tear down A-Key management	PIN code masking	
Future features	Credit Limit Check Real time billing/ Bill monitoring		Restricted access	Secure network elements

Fig. 2
The fraudster is retrieving MIN/ESN combinations as they are transmitted over the air.

Special thanks to CTIA and the cellular carriers of California for contributing with the photographs in this article.

ing MIN and ESN combinations for use in cloning-related cellular fraud are theft of subscriber data from the operator, and interception – via a frequency scanner – of MIN-ESN combinations transmitted over the air interface. Since they are transmitted on the control channel each time a mobile terminal either registers with a mobile switching centre (MSC) or initiates or receives a call, the MIN and ESN are fairly easy to retrieve.

Mobile terminals present themselves to the network by providing the MIN and the ESN. The following paragraphs explain how the MIN and ESN are used, and why, in some circumstances, they cannot be used to determine whether or not a user is legitimate.

Each paired MIN and ESN represents a unique combination that may be used to validate a legitimate subscription. When a subscription is activated for the first time, the MIN and ESN are paired and stored in the operator's database, or home location register (HLR). From that point on, each time the mobile terminal requests access to the mobile switching centre, the MSC checks that the numbers transmitted to it by the mobile terminal match the numbers received from the HLR. If the numbers match, then the MSC processes the request.

Unfortunately, each time the system is accessed, both the MIN and the ESN are transmitted over the air interface without protection. Therefore, anyone with a special type of frequency scanner can intercept the MIN-ESN combinations and use them fraudulently. Many types of phone, for example, can easily be reprogrammed to use a new MIN and ESN.

Cloning/Tumbling

Perpetrators often have a reasonable knowledge of valid ranges for MINs and ESNs. Accordingly, they repeatedly attempt to gain access to the system by stepping the ESN, the MIN, or both until they succeed. In this way a perpetrator appears to be a different subscriber each time he makes a call.

Cloning/Roaming

Valid MIN-ESN combinations are stolen in one city and used in another.

Hijacking

The perpetrator "steals" an established voice channel as follows: First, he scans airborne signals waiting for a legitimate subscriber to initiate or to receive a call, and to pass any authorisation checks. Next, he overpowers the subscriber's phone, and usurps control of (or "hijacks") the voice channel. The hijacker then calls a third party, his desired destination, and drops the original call leg.

False base station

A perpetrator simulates the actual cellu-

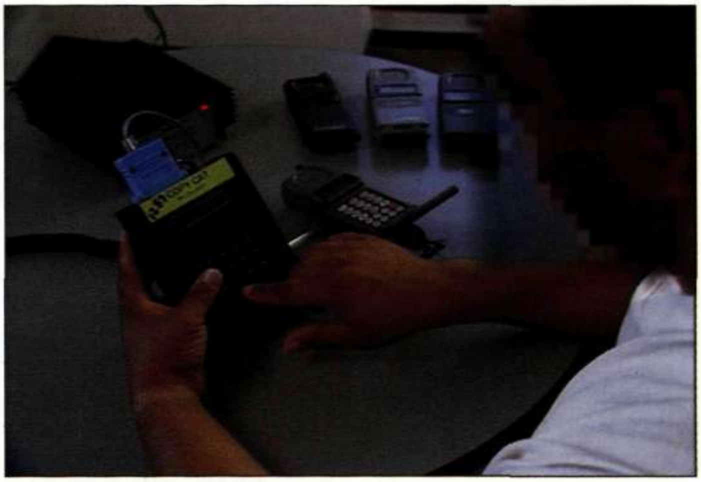


Fig. 3
The fraudster is altering the MIN and/or the ESN for fraudulent purposes in the mobile terminal.

lar system with a "base station" that actively forces nearby mobile terminals to transmit their MIN-ESN combinations along with other, perhaps secret, information.

Ericsson's fraud-fighting portfolio for CMS 8800

Recognising that fraud is a major threat to cellular operators, Ericsson have developed a portfolio of features that will help their customers to fight against fraudulent usage. The paragraphs that follow describe these features and explain how they can be used to detect or prevent fraud.

ESN screening

ESN screening prevents a system from serving visitors whose ESNs match the characteristics of a fraudulent serial number. If a match is detected, the caller is either disconnected or rerouted according to exchange data.

The screening process contains two steps: the ESN format check, and ESN verification.

ESN format check: When a visiting mobile subscriber (also known as a roamer) first accesses a system, the visited MSC validates the format of the mobile ESN before it requests serial number validation. The format check ensures that the ESN manufacturer code and the reserved area comply with standard formats.

ESN verification: When an automatic roaming mobile terminal registers with a visited MSC and accesses the system – that is, after a roaming mobile terminal's record has been retrieved from its home system and is stored in the visited MSC – the visited MSC compares the transmitted ESN with the stored ESN. When a manual roaming mobile terminal first accesses a visited MSC, the MSC checks the ESN against a barring list and then sends the ESN to a clearing house for validation. Different mobile switching centres handle invalid ESNs differently depending on the data in their exchanges; they might, for example, simply ignore the call, reroute it, or drop it.

MIN screening

When a mobile terminal attempts to access an MSC, the MSC compares the transmitted MIN to the national numbering format. If the formats do not match, then access is not granted.

Positive validation

The MIN-ESN combination of a roaming mobile terminal matches a valid record in the HLR.

Post-call validation

Call records are monitored, and invalid phones are taken out of service.

Pre-call validation

A query with the caller's MIN and ESN is

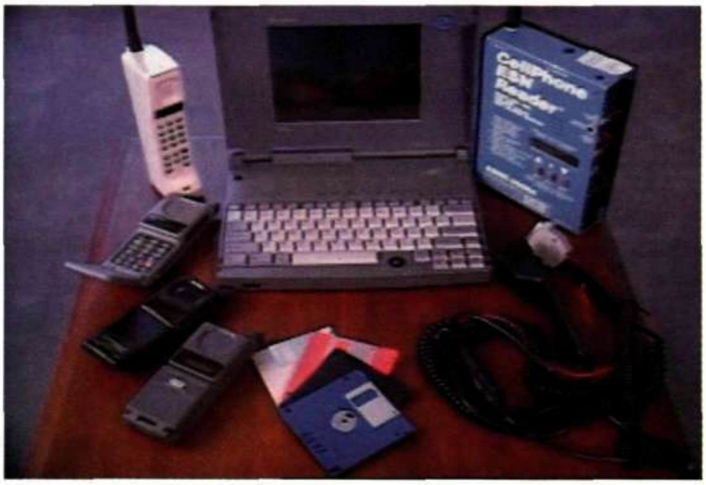


Fig. 4
Typical equipment used by fraudsters.

sent to the HLR during call set-up. This feature was made possible thanks to standardised network signalling protocols, such as IS-41.

Pulling a switch

Although pulling a switch is considered a last-ditch alternative when fighting fraud, occasionally this action must be taken to stem the tide of lost revenue. A pulled switch, which bars from access all mobile terminals whose MINs fall within a certain range, excludes both legitimate and cloned subscribers from service.

Pulling services

At times, the services that are most commonly abused – such as international calls or three-way calling – must be discontinued.

Personal identification numbers

As a short-term solution to fraud, some operators require their subscribers to use personal identification numbers (PINs) each time they make a call. Some subscribers, however, dislike having to remember, as well as enter, yet another series of digits each time they want to place a call. Nonetheless, by implementing PINs, one operator was able to decrease clone-related fraud by 70%.

Authentication

The roots of authentication can be traced back to the early 1990s, when IS-54 (the USA's TDMA air interface standard) was created. When authentication is used, the identity of a mobile terminal is not automatically accepted simply because its MIN, ESN or PIN are correct. Instead, the mobile terminal must be authenticated before its calls are processed. The authentication procedure, which allows the mobile terminal to be approved without transmitting any secret data, is accomplished through a numeric challenge from the authentication centre (AC) or from the MSC. To pass the challenge, the mobile terminal must perform advanced calculations, the results of which are accurate only if the mobile terminal has been programmed with the correct secret information.

Authentication utilises the cellular authentication and voice encryption (CAVE) algorithm, which is considered US military-grade technology. The algorithm is used together with a private key to generate authentication data. The primary private key, called the A-key, is solely stored in the AC and the mobile terminal. The A-key is used to generate a temporary private key, called shared secret data (SSD), that can be transmitted across the network. The authentication feature requires both the mobile terminal and the AC (or at times the MSC) to execute the CAVE algorithm with a common set of data. If the results match, the identity of the mobile terminal is authenticated and service is granted. Otherwise, the MSC rejects the mobile terminal's attempt to access the network. The AC can regenerate the mobile terminal's SSD automatically if the SSD is compromised. The

Box C
Numbers identifying a mobile terminal

Mobile identification number

Ordinarily, the mobile identification number (MIN), which is assigned to a subscriber's mobile terminal when it is activated, is identical with the dialled directory number.

Electronic serial number

The electronic serial number (ESN) is a 32-bit binary number that consists of three parts: the manufacturer code, a reserved area, and a manufacturer-assigned serial number. The ESN, which represents a terminal, is fixed and, supposedly, cannot be changed.

A-key can also be regenerated, but not automatically.

The authentication feature comprises several procedures, described below:

Global challenge
During the system access phase, the system challenges the mobile terminal, requiring it to execute the CAVE algorithm, using its A-key and information obtained from the system via the air interface. The result is returned to the system for validation.

Unique challenge
A unique challenge, which is initiated by the AC or the MSC, validates an individual mobile terminal using a set of data that is unique to the mobile terminal. The challenge is performed at call set-up or upon receipt of a flash request.

Base station challenge
A base station challenge allows the mobile terminal to validate a base station, thereby protecting the mobile terminal against attacks from false base stations.

Shared secret data update
A shared secret data (SSD) update can be performed as a matter of routine, or when there is reason to suspect that the SSD has been compromised.

Voice privacy
Voice privacy (VP) is a feature that supplements authentication procedures. It encrypts a subscriber's conversation as it travels through the air between a digital mobile terminal and a base station. Powerful and convenient voice privacy is possible through TDMA and the utilisation of CAVE.

Signalling message encryption
Signalling message encryption (SME), which is another supplement to the authentication procedures, protects subscriber information by encrypting a select subset of signalling messages between the base station and the mobile terminal.

Digital phones operating according to IS-54B and IS-136, as well as many new analogue phones, support authentication. As old phones are replaced with models that employ authentication, the base of clonable phones will shrink, making cloners much more visible to operators.

The deployment of authentication will limit fraud to two categories: subscription fraud and phone theft. These two types of fraud can probably never be eliminated, but they are more easily managed and prevented than cloning fraud.

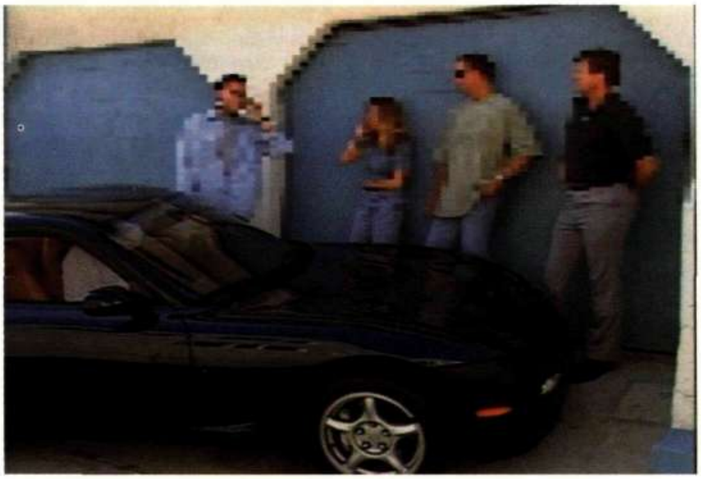


Fig. 5
In a call-sell operation cellular services are sold at discounted prices.

Fraudulent activity detection

The fraudulent activity detection (FAD) feature provides real-time surveillance of suspicious activities in the MSC and the HLR. In particular, this feature detects irregular events associated with a call, reports fraudulent events to an I/O device, and bars or disconnects calls when a fraudulent activity is detected. All subsequent attempts by a barred subscriber to access the system are routed to customer service or to an announcement.

The following events trigger an FAD printout:

- call attempts detected for a busy-marked subscriber;
- registration access for a busy-marked subscriber;
- location cancellation message received for a busy-marked subscriber
- unknown page response for a busy-marked subscriber;
- unknown multiple interexchange page response for a busy-marked subscriber;
- service call received for a busy-marked subscriber;

- premature registration;
- co-digital colour code (DCC)/co-channel violation detected for page response;
- control channel capability/mode mismatch detected for a system access;
- control channel capability/mode mismatch detected for registration access;
- control channel capability/mode mismatch detected for origination access;
- call from an old MSNB after NPA split.

Additional events may also be specified.

Call barring may be set at different levels:

- no outgoing calls barred;
- all outgoing calls barred;
- all outgoing international calls barred;
- all outgoing trunk and international calls barred;
- all calls except outgoing international calls barred;
- all calls except outgoing trunk and international calls barred.

Automatic call barring

The automatic call barring feature is invoked whenever a mobile terminal is inactive for a specific period of time. To then free the mobile terminal for use, the subscriber must enter his or her PIN code. Cellular users may think this feature a burden, but it is a very efficient tool for fighting fraud and for eliminating unbillable phone calls.

Call tear down

The call tear down feature is operated by command in real time, and disconnects fraudulent calls that are not connected to emergency or customer services. The command, which may be issued either automatically or manually, disconnects all call legs, including three-way and call-waiting calls. The means of identifying suspicious calls may reside in the MSC or in an external device.

A-key management

A-keys are issued and forwarded to the subscriber in a way that eliminates insider operator fraud. The A-key is used to authenticate the mobile terminal.

PIN code masking

PIN code masking conceals the issued PIN code from the subscriber data printout, thereby reducing the risk of insider operator fraud.

New features

New features are continuously being designed and introduced in CMS 8800. This article represents only a snapshot in time.

Other means

In order to win the war on fraud, complementary products from outside of Ericsson's fraud-fighting portfolio may also be used. In particular, because the Ericsson system is open, it can interface with other fraud-fighting systems.

Conclusion

Fraud is a serious concern for all members of the wireless industry. Subscribers feel abused when their phones stop working, or when they receive large bills for services that a fraudster used at their expense. Operators may offer to change a subscriber's MIN, but this is an inconvenient solution. Operator customer service departments must be well prepared to deal with unhappy customers who have been hit by fraud, since customers can easily change providers (resulting in increased "churn").

Carriers are likewise frustrated from having to absorb the costs of unauthorised calls. These losses, however, clearly signal that Ericsson have the opportunity, with its fraud-fighting portfolio, to make a direct, positive impact on the CMS 8800 operator's bottom line, by minimising or by altogether eliminating fraud.

CDPD – Adding wireless IP services to D-AMPS/AMPS wireless networks

Lars Wetterborg

Cellular digital packet data (CDPD) technology marks a new era of wireless data communication. Using existing cellular network infrastructure and frequency channels, this technology enables digital AMPS (D-AMPS) and AMPS wireless network operators to offer not only voice services but also packet data services for wireless Internet and corporate database access applications. This makes D-AMPS/AMPS the first global cellular system to support both voice and packet data services.

The author describes this new technology and its deployment in an D-AMPS-based network, its market applications, and Ericsson's solution for its implementation.

In 1992, a group of US-based operators with AMPS-standard wireless networks formed a consortium to steer the introduction of data services. The result was the cellular digital packet data (CDPD) system specification. CDPD technology enables D-AMPS/AMPS carriers to offer both voice and wireless Internet protocol (IP) services, using the same network infrastructure and channel frequencies.

From the outset, the design specification for CDPD is based on an open architecture, employing recognised standards and existing technology. In this way, the new wireless data system can be deployed quickly and competitively.

Now the consortium is responsible for the further evolution and maintenance of CDPD and has grown to encompass almost 100 network operators, system vendors and software application developers worldwide. In January 1995, it issued the latest release, version 1.1, of the CDPD system specification. Ericsson joined the group, now known as the CDPD Forum, Inc., in 1994.

Wireless IP

In their early specifications work, the CDPD consortium made some very important strategic decisions.

- CDPD should be compatible with the Internet and serve as a wireless extension to this network. As a consequence, each CDPD mobile is assigned an IP address. All user traffic in a CDPD backbone network consists of IP packets.
- IP is a packet switching type of protocol. Therefore, CDPD should be a packet switching network with a shared packet channel over the air interface. The principles underlying the air interface should be similar to those of Ethernet.
- IP is a connectionless protocol, which is why CDPD should only offer a connectionless service. CDPD, like all other IP networks, is based on the fact that most applications are using connection-oriented transport protocols, such as the transmission control protocol (TCP), between the end points to ensure data delivery and sequence.
- CDPD should enable infrastructure reuse. The same channel frequencies should be used for both voice and CDPD; thus it would be beneficial if the same base stations could handle both. It was realised that wireless packet data and circuit-switched services make widely differing demands on the network, in terms of switching and mobility management. It would be highly recommendable to allow CDPD to reuse existing routers and standard platforms from the computer industry. Products that support IP protocols and routing technologies have been available for many years. They could be leveraged when CDPD backbone products were to be developed.

Box A
Abbreviations

ARQ	Automatic retransmission request
CDPD	Cellular digital packet data
CSMA	Carrier sense multiple access
DSMA	Digital sense multiple access
GMSK	Gaussian minimum shift keying
IP	Internet protocol
MAC	Media access control
MDBS	Mobile data base station
MD-IS	Mobile data intermediate system
M-ES	Mobile end system
MSC	Mobile switching centre
PCMCIA	Personal computer memory card international association
RBS	Radio base station
RF	Radio frequency
TCP	Transmission control protocol

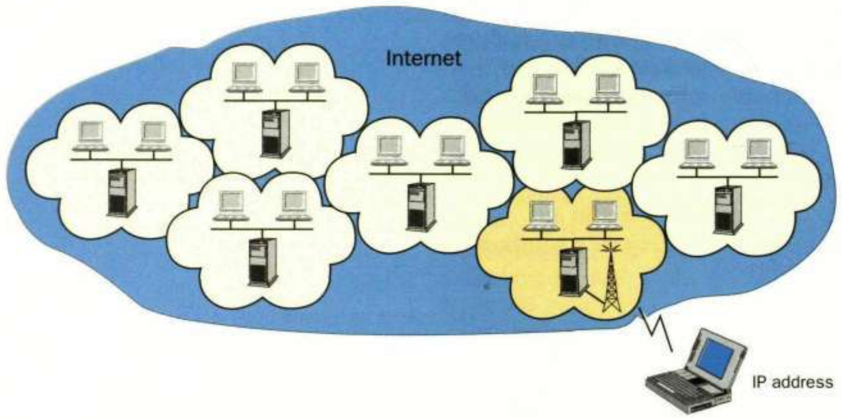


Fig. 1
A CDPD network has the same internal architecture as any other domain on the Internet. The only difference is that CDPD has mobile end-users. The architecture makes it natural for a CDPD operator to become a wireless Internet service provider.

- The backbone network should be open, and servers should be readily added to the backbone. This will make it easy for CDPD operators to differentiate by introducing value-added services; for example, wireless Internet access.

These strategic decisions imply that a CDPD network has the same structure as any other domain of the Internet – an Ethernet with a number of servers connected. In the case of CDPD the end-users just happen to be wirelessly connected, Fig. 1. Seamless Internet connectivity is provided without any address or protocol conversions. It is packet switched all the way.

CDPD technology deployment

D-AMPS/AMPS channels reside in the 800 MHz radio frequency range. GMSK (Gaussian minimum shift keying) modulation provides CDPD with a bit transmission rate of 19.2 kbit/s for the 30 kHz carrier spacing used in D-AMPS/AMPS.

CDPD is optimised for packet switching. In this transfer mode, data is split up into packets which are then routed individually through the network. Packet switching is best suited to "bursty" data transfer and makes optimum use of the frequency spectrum, since there is no call set-up or clear-down time, unlike with circuit-switched data. (Circuit switching is better suited to large data file transfer applications where a line is held open for the duration of the session.) Depending on the traffic profile and applications, many hundreds of users can share the same packet channel to send data.

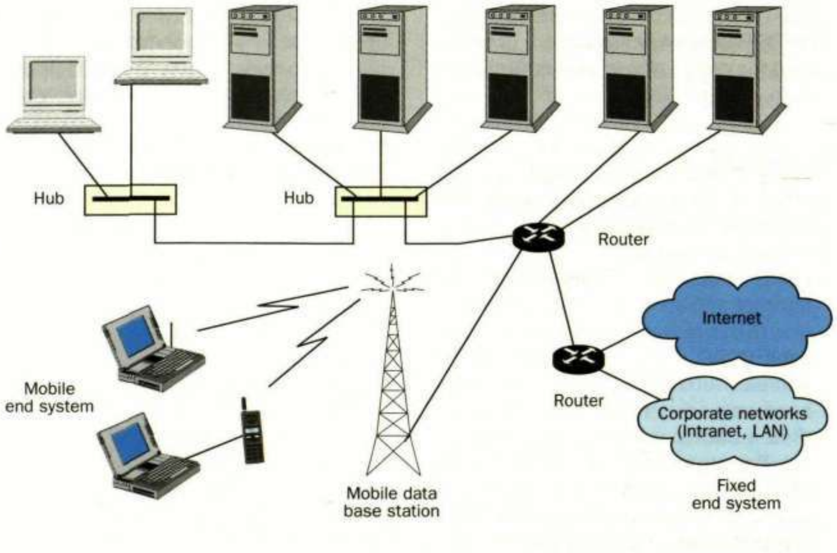


Fig. 2
The CDPD architecture is built around an open IP backbone network to which the network nodes are attached as servers. This architecture makes it easy to add new services as required by business conditions.

The CDPD technology allows for high-quality data transport. As the name implies, CDPD is digital and brings with it associated benefits on the air link: signal processing which can compensate for signal fading; media access control (MAC) layer reconstruction of corrupted data using error correction algorithms; and a link layer ARQ (automatic retransmission request) protocol to ensure correct reception of packets.

Security is guaranteed by automatic encryption of all data and authentication of all mobile users.

CDPD network elements

Data is sent over a CDPD network using the following key network elements, Fig. 2:

- The mobile end system (M-ES) enables the subscriber to send and receive data from the CDPD network. Several M-ESs implementations are available; for example: CDPD-enabled cellular phones, stand-alone modems and PC cards (PCMCIA) for integration with laptop computers.
- The mobile data base station (MDBS) provides CDPD radio coverage. The MDBS is responsible for the physical and MAC layers, while the link layer is relayed between the M-ES and the mobile data intermediate system (MD-IS). One MDBS should be able to handle several CDPD radio frequency (RF) channels distributed over the cells at the site. (A site is typically omni-directinal or three-sectored, thus having one or three cells.) Each CDPD RF channel is assigned to one CDPD channel stream.
- The MD-IS provides packet switching and mobility management. It keeps track of which channel stream a mobile end system is using and routes incoming packets accordingly.
- The accounting server collects raw account data from the MD-IS and presents it to a separate billing system. There is no billing system specified for CDPD. The idea is to use the same billing system for CDPD as for the voice service.
- The authentication server works with the MD-IS to verify the authenticity of the CDPD network user.
- The network management system handles the monitoring, administration and management of all CDPD network components.

In addition, a network also typically has a customer activation system for administrative control over customer and subscriber accounts.

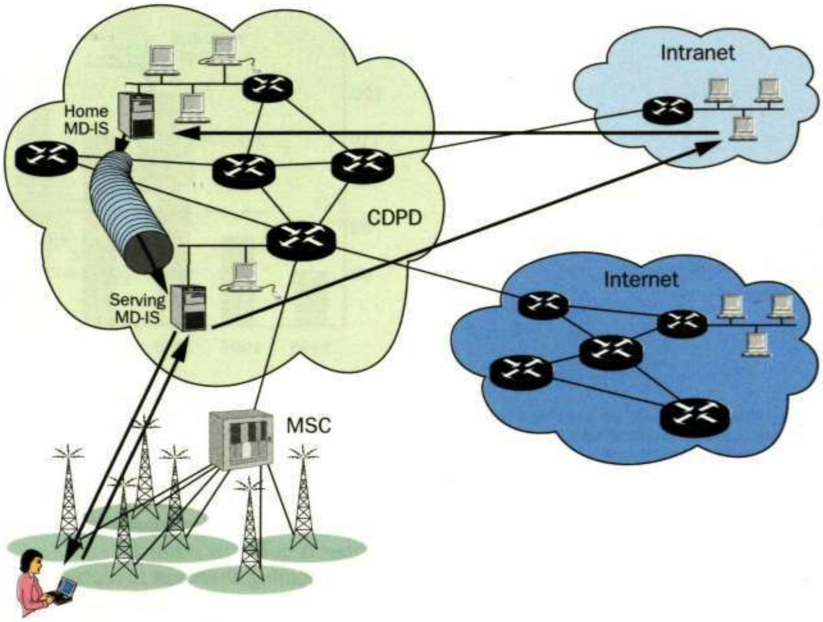


Fig.3
CDPD mobility management is based on the principles of mobile IP. IP packets are tunnelled to the serving area that the receiving end-user is visiting.

Mobility management

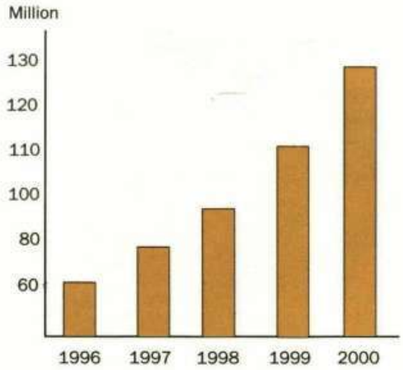
CDPD mobility management is based on mobile IP principles. The MD-IS is the central element in the process. An MD-IS is logically separated into a home MD-IS and a serving MD-IS. There are often several serving MD-ISs in a network, all connected to a home MD-IS.

A serving MD-IS manages one serving area. The mobile data base stations that provide coverage in this area are connected to the serving MD-IS, which has a database containing information about all subscribers currently visiting the area. The channel stream in which a subscriber is active is also indicated.

A home MD-IS contains a subscription database for its geographical area. Each subscriber is registered in the home MD-IS associated with his home area. The IP address of a subscriber points to his

Fig. 4
The estimated number of D-AMPS/AMPS subscribers world-wide.

🟫 Number of users



home MD-IS. The database keeps information on which serving area a subscriber is currently visiting.

An incoming IP packet is routed to the home MD-IS of the receiver, Fig. 3. After finding out in which serving area the subscriber is currently located, the IP packet is tunnelled to the corresponding serving MD-IS. This MD-IS checks in which channel stream the subscriber is active and forwards the packet to the mobile data base station responsible for that channel stream. The base station maps the channel stream to the CDPD RF channel in the appropriate cell.

CDPD has support for sleep mode. Packets are stored in the serving MD-IS in case a mobile end system is sleeping. Instead, notifications are sent on a regular basis in the CDPD channel. As the mobile wakes up – programmed to do so at predetermined intervals – it will initiate transmission of the stored packets.

If the system (except for sleep mode) is out of contact with mobile end systems, packets are only stored for the time it takes to perform the predetermined number of retransmissions. Then they are discarded. The principle applied is that of relying on the recovery procedures of the TCP or other higher-level protocols that the application uses on top of the IP. (This is also the general principle used by all other IP networks.)

In the other direction, the IP packets are assembled in the serving MD-IS using the link layer frames received from the MDBS. From the serving MD-IS the IP packets are routed to their destinations.

Needless to say, the mobile end system must be switched on before an end-user can send any data. The M-ES switch-on action sends a message to the serving MD-IS, identifying the user and his home MD-IS. User access rights and authentication processes are performed at the home MD-IS. A positive result grants the user access to the system.

A large number of M-ESs can share one single RF channel. Digital sense multiple access (DSMA) is the technique used to determine whether or not the RF channel is free so that the M-ES can make an access request and transfer data. DSMA is similar to the carrier sense multiple access (CSMA) protocol used in the Ethernet.

Market applications

AMPS and D-AMPS cellular networks presently span 82 countries and serve 63 million subscribers, providing a ready-made, broad market base for the roll-out of new services.

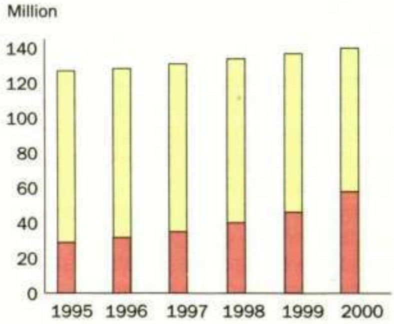
The popularity of wireless data is rising significantly. This is due to increasing use of portable PCs, cellular phones, Fig. 4, and the Internet in particular. The growth of the number of mobile workers is also dramatic (see Fig. 5); mobile workers being defined as those who work away from their office at least 20 per cent of the time.

From this it may be seen that the deployment of CDPD services provides D-AMPS/AMPS-based operators with a good opportunity to further leverage this market base. The estimate for the market share of CDPD by the year 2000 stands at 28 per cent of the total wireless data market.

CDPD can be deployed cost-effectively and rapidly through the reuse of existing

Fig. 5
The estimated number of mobile workers compared with the total number of employed workers in the US.

🟨 Employed workers
🟥 Mobile workers
Source: Probe Research



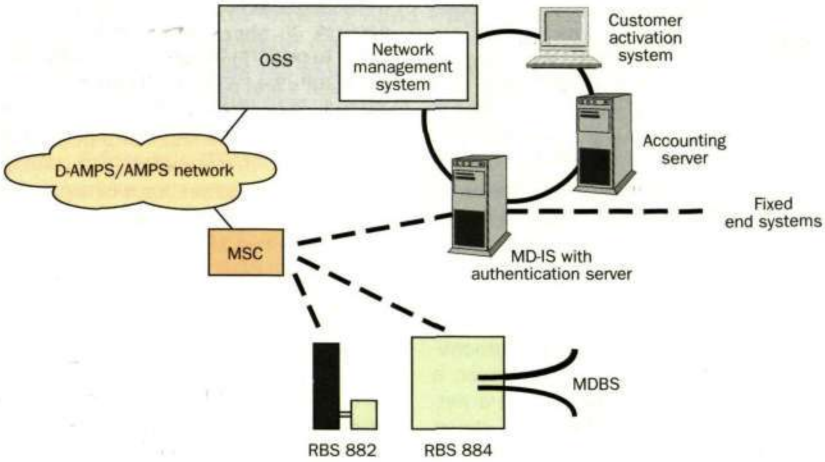

OSS
Network management system
Customer activation system
Accounting server
D-AMPS/AMPS network
Fixed end systems
MSC
MD-IS with authentication server
MDBS
RBS 882
RBS 884

Fig. 6
In Ericsson's solution, all the D-AMPS/AMPS base stations are reused for CDPD. In addition, the existing transmission links are utilised for CDPD traffic too.

D-AMPS/AMPS infrastructure and also the utilisation of D-AMPS/AMPS frequencies, which means that operators need not apply for new licences.

Subject to agreements, the large number of D-AMPS/AMPS networks worldwide allows for seamless roaming over a large part of the globe. This roaming capability also forms part of the CDPD system specification, which demands an open architecture for all manufacturers and software providers to ensure compatible systems and applications.

For subscribers, CDPD offers fast, secure and economical communications for a vast range of applications. All the technology used is already well proven, ensuring reliability.

The inherent support for the most widely used protocol – IP – combined with seamless roaming and virtual on-line speed, makes CDPD suitable for a large number of applications. Examples include: Internet and Intranet access, e-mail, database access, information services, telemetry applications, dispatch applications, vehicle location, credit-card transactions and alarm system applications.

The Ericsson solution

Ericsson is providing a complete CDPD system solution integrated with the CMS 8800 cellular network, Fig. 6. The CDPD solution is fully compliant with the latest version of the CDPD system specification, version 1.1.

The RBS 882 family of D-AMPS/AMPS base stations has been widely deployed in more than 30 countries. The RBS 884 is a new generation of D-AMPS/AMPS base stations serving both the 800 MHz and the 1900 MHz frequency bands.

Both the RBS 882 and the RBS 884 macro base stations are furnished with integrated CDPD-enabling technology. One processor board and a software package are sufficient to enhance the RBS 884 macro base station so as to be capable of supporting CDPD. All parts of the regular D-AMPS/AMPS base station are reused for CDPD, and the footprint remains unchanged.

The processor board and the software package are also required for the RBS 882. Since another type of transceiver is used in RBS 882, RBS 884 transceivers need to be added for the CDPD channels, together with an RBS 884 cabinet to accommodate the boards. Except for the RBS 882 transceivers, the entire regular D-AMPS/AMPS base station is reused for CDPD.

One design focus has been on the minimisation of cell site and life cycle costs by minimising spare part requirements and thereby field personnel and staff training needs. Another focus has been on providing a flexible software-based architecture. The MDBS is designed to be scaleable, matching different traffic levels at different cell sites. Channels are always dedicated to CDPD, ensuring constant availability of radio spectrum.

Since the MDBS solution is based on the RBS 884, it also brings with it support for future enhancements of the RBS 884 product line.

Other parts in the complete system solution includes mobile data intermediate systems with integrated authentication servers, an accounting server, a customer activation system and a network management system. All these products are UNIX applications running on standard computers. The total system capacity is mainly dependent on the processor power of the MD-IS. The fact that the products are based on standard UNIX computers means that more processors can easily be added as required.

Standard hubs and routers are used to connect the computers to one another and to the outside world. Existing transmission links are utilised to connect the serving MD-IS with the CDPD base stations. Dedicated time slots on the links from the base stations are multiplexed in the MSC into a separate link between the MSC and the MD-IS.

Ericsson officially announced its CDPD network solution at the CTIA show in Dallas, US, in March 1996. Regional and local market launches are continuing. Ericsson's first customer is Telecom New Zealand, for whom Ericsson has undertaken to supply the first CDPD network in the Southern hemisphere.

Installation and testing will begin this year and full commercial services will be available in mid 1997.

Ericsson's CDPD solution will be made generally available in December 1996.

Conclusions

An ever-increasing number of people are relying on mobile communications and are becoming dependent on information and communications tools. Already there is widespread use of laptop PCs and cellular phones. Combining these trends with the enormous success of the Internet makes cellular wireless IP access a natural evolution.

Ericsson's solution for CDPD thus represents a culmination of this evolution. Designed to reuse much of the original network equipment, this solution is a cost-effective and fast route to adding wireless IP data services to D-AMPS/AMPS networks. Its ability to work with an array of data networks and applications, including the Internet, makes it an exciting new business and communications opportunity.

PCS 1900 – Ericsson's turnkey solution for personal communications services

Sven Hellsten

The current trend of the wireless world – the evolution from mainly business user applications to broader consumer usage – is now becoming a reality in mature markets around the globe. Consumer demand and advancing technologies have led to the emergence of "personal communications services", or PCS systems as they are more often referred to. In North America in particular, Ericsson's GSM-based PCS 1900 and D-AMPS 1900 systems will be the keys to successful mass-market deployment of PCS, focusing on high subscriber penetration/high capacity, advanced services, and short time-to-market capabilities.

The author describes the GSM-based PCS 1900 system, its features and the advantages it offers the operator both now and in the future.

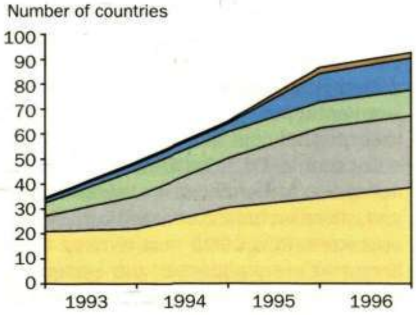


Fig. 1
Countries committed to GSM. GSM is the world's most widely deployed digital cellular technology. More than 40 million GSM calls are made every day, and the annual market growth exceeds 50 per cent.

Ericsson's PCS 1900 – a total turnkey system solution for personal communications services – is derived from the GSM standard which is the world's most widely-deployed digital cellular technology. There are more than 150 GSM-based networks in 86 countries around the world, serving over 30 million subscribers. Currently, more than 50,000 new GSM subscribers sign up every day.

Ericsson has played a seminal role in the GSM story from the beginning and has worked continuously to enhance and evolve the standard. A recent adaptation is the PCS 1900 system.

Evolution of a proven technology

The worldwide success of GSM has been driven by three key factors: its evolutionary capabilities (from voice only to a wide range of advanced data and personal services); its cost-effectiveness (from planning and implementation to operation); and its fully open international standards.

The open standards approach – leading to a true multi-vendor environment – has stimulated market growth and competition among system and handset suppliers, as well as amongst operators. The competition, and the broad deployment of GSM, have resulted in rapid time-to-market processes – for the benefit of both operators and end users.

First PCS networks in operation

PCS 1900 has been accepted by the American National Standards Institute (ANSI) as a standard for the 1900 MHz frequencies allocated in the US. To date, ten PCS 1900 operators have joined the North American PCS 1900 Interest Group (NAIG).

NAIG is a consortium of current and prospective PCS licensees, which jointly addresses issues that guarantee the positioning of PCS 1900 at the forefront of North American PCS technologies. At present, the licences held by Group members include 180 million potential subscribers.

In November 1995, the first commercial PCS 1900 network in the US was brought into operation by American Personal Communications (APC), serving the Washington/Baltimore area. By May 1996, APC had 100,000 customers in their network.

However, the use of PCS 1900 services is not limited to one operator's network. PCS 1900 offers seamless nationwide roaming between PCS 1900 systems in North America. In addition, both D-AMPS

Box A
PCS 1900 – part of the information age

The impact of wireless technologies on the fixed telecommunications market of the 21st century will be irrevocable, and cellular technologies will undoubtedly play a leading role.

PCS 1900 offers the framework of the future today. The level of specification and design implementation (based on GSM/PCS applications) is very high: sophisticated packet-switched data transmission; advanced "smart card" concepts; satellite services based on the GSM specification; and innovative dual-mode phone solutions.

In the future, the mobile terminal will become a multimedia communications device, capable of sending and receiving graphic images and video. PCS 1900 systems will connect to corporate LANs, enabling business people to share information through workgroup computing and videoconferencing applications.

In addition, satellite-based systems – covering the entire world – will be interconnected with PCS 1900 networks, thus also allowing increased mobility within areas with less developed infrastructures.

Through wireless local loop (WLL) applications, PCS 1900 systems can provide rapid implementation of communications services in the (traditionally wireline) local subscriber network. By means of home zone tariffs – geographically restricting the mobile usage – operators can attract new subscribers through competitive pricing schemes.

Fig. 2
The first network in the US using the 1900 MHz PCS frequencies is operated by American Personal Communications (APC). The PCS 1900 offering is marketed as Sprint Spectrum services.

1900 and international roaming are supported.

With PCS 1900, the North American vision of ubiquitous, all-in-one wireless communications is realised – triggering the profitable mass-market segment.

Total system solution improves operational economy

The move towards increased consumer usage, and the competitive situation of new PCS operators, are bringing on changes in the wireless market: wider differentiation in prices and tariffs; enhanced distribution channels for handsets and subscriptions; broader market segments; more advanced services; and lower overall cost structure.

Ericsson's PCS 1900 system allows operators to benefit from these trends and offers increased competitiveness to operators. PCS 1900 is a turnkey solution, and every aspect of the system is defined in the underlying standard. Everything needed for network operation is provided from one source.

PCS 1900 is part of GSM, one of the world's most powerful and evolutionary telecommunications platforms. GSM and PCS 1900 are based on the same modular and open-ended architecture, which makes the PCS 1900 system easy to expand and upgrade.

PCS 1900 solutions contribute to improved operational economy, allowing operators to be creative and diverse with their marketing strategies and service offerings. Since PCS 1900 is an extremely well-proven and secure system, the technology risk factor is eliminated.

Ericsson is the world's largest supplier of wireless systems, serving more than 40 per cent of the overall cellular market. This multinational company is active in more than 100 countries and has 40 technical development centres in 20 countries.

Increased competitiveness through service differentiation

The increased competition in the wireless market, combined with high subscriber penetration, forces operators to attempt to increase market share, air time and revenues. To succeed in these endeav-

Fig. 3
The development of Ericsson's handsets has resulted in spectacular weight reductions, and doubled talktime. The most recent model, CH 337, measures 130x49x24 mm (5.12x1.93x1.0 inch) and weighs only 193 grams (6.8 oz). The talktime is 4 hours, and the stand-by time 38 hours.

Box B
Abbreviations

ADPCM	Adaptive differential pulse code modulation
ANSI	American National Standards Institute
AUC	Authentication centre
BGW	Billing gateway
BSC	Base station controller
BSS	Base station system
BTS	Base transceiver station
EET	Ericsson engineering tool
EIR	Equipment identity register
GSM	Global system for mobile communications
GPRS	General packet radio services
HLR	Home location register
HSCSD	High-speed circuit-switched data
ILR	Interworking location register
IN	Intelligent network
ISDN	Integrated services digital network
LNA	Low-noise amplifier
MSC	Mobile switching centre
OSS	Operations support system
PCS	Personal communications services
PDA	Personal digital assistant
PIN	Personal identity number
PSTN	Public switched telephone network
SCP	Service control point
SIM	Subscriber identity module
SMAS	Service management system
SMS	Short message services
SOG	Service order gateway
SS	Switching system
SSP	Service switching point
VLR	Visitor location register

ours and to retain large subscriber bases, operators often seek to differentiate their service offerings.

Wireless data services

PCS 1900 is based on the ISDN call model, which means that a wide range of services can be provided from one single network. In addition, the wireless data services accessible through PCS 1900 make the concept of the "mobile office" a reality.

Data services include voice messaging, high-speed data communications, fax, short message services (SMS), and access to information services (such as e-mail, wire news, and credit card verification), as well as access to the Internet. Furthermore, the fax, phone and paging applications are all accessed through one number.

With SMS, messages (with up to 160 characters) can be received during an ongoing conversation. SMS makes it possible to introduce new competitive services, such as local weather forecasts, traffic reports and stock market indexes.

By bringing mobility to existing data applications, such as laptop and notebook PCs, total network utilisation will increase – thereby strengthening the competitiveness of operators.

Intelligent network services

PCS 1900 also offers advanced intelligent network (IN) services, enabling fast creation and deployment of value-added services, thus allowing operators to respond quickly and flexibly to market demands. Ericsson's mobile IN therefore represents a powerful service differentiation/personalisation tool.

The IN services can be divided into three groups: communications management services (such as call screening and call barring, which can be based on time and location criteria); personal numbering services (such as single personal number, based on the user's individual "time and location" profile); and location-based services (such as local traffic conditions and tourist information).

PCS 1900 has several inherent features which ensure the privacy, integrity and confidentiality of all voice and data calls. It also provides authentication and encryption to verify the identity of the user.

PCS 1900 handsets incorporate a SIM (subscriber identity module) "smart" card which contains the subscriber's personal identification and service profile information, such as billing, predefined speed-dial numbers and calling services. For added security, a personal identity number (PIN) can be attached to the SIM card.

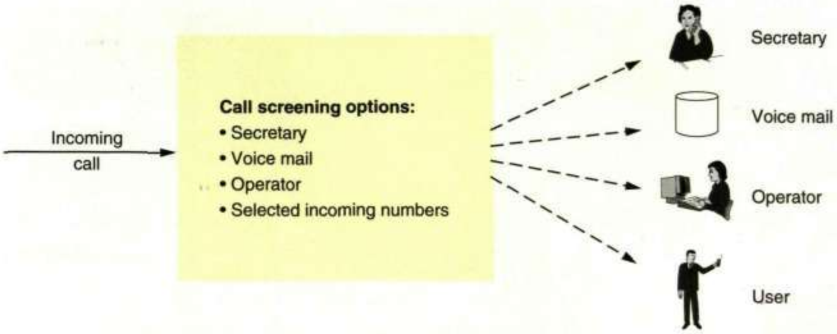


Fig. 4
By means of intelligent network (IN) services, such as call screening, users can choose among options according to real-time requirements.

Intelligent terminals and smart cards

Ericsson also supports the development of more intelligent terminals, such as personal digital assistants (PDA) with enhanced voice, data and information services. In the future, PDA users will be able to dial in, download e-mail, and access the World Wide Web – all through mobile communication connections.

An interface based on the GSM standard "Unstructured Supplementary Service Data" (USSD) technology can be used for rapid programming of personal assistants.

The SIM card is also evolving into a potent service differentiator thanks to the wide range of "over-the-air activation" (for example to register new subscriptions), and pre-paid SIM applications which it allows to be offered.

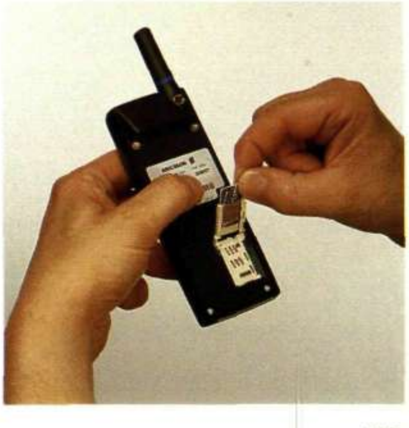
The principle of using the SIM card for payment is the same as that of buying a phone card for a payphone. The subscriber pays for a specified number of call units/minutes in advance, and the relevant amount of credit is loaded into the SIM card.

Furthermore, pre-paid SIM card applications decrease the fraudulent use of the cellular system, and minimise administrative overheads for operators.

Enhanced service to operators

The principle of service differentiation is also being applied by Ericsson in its role as a wireless system supplier. Through

Fig. 5
SIM "smart" cards contain the personal subscription information for each user. When renting a phone at home, or when going abroad, users can bring their personal SIM cards and insert them into the "new" phone. All subscriber information and personal features are then automatically programmed into the phone.



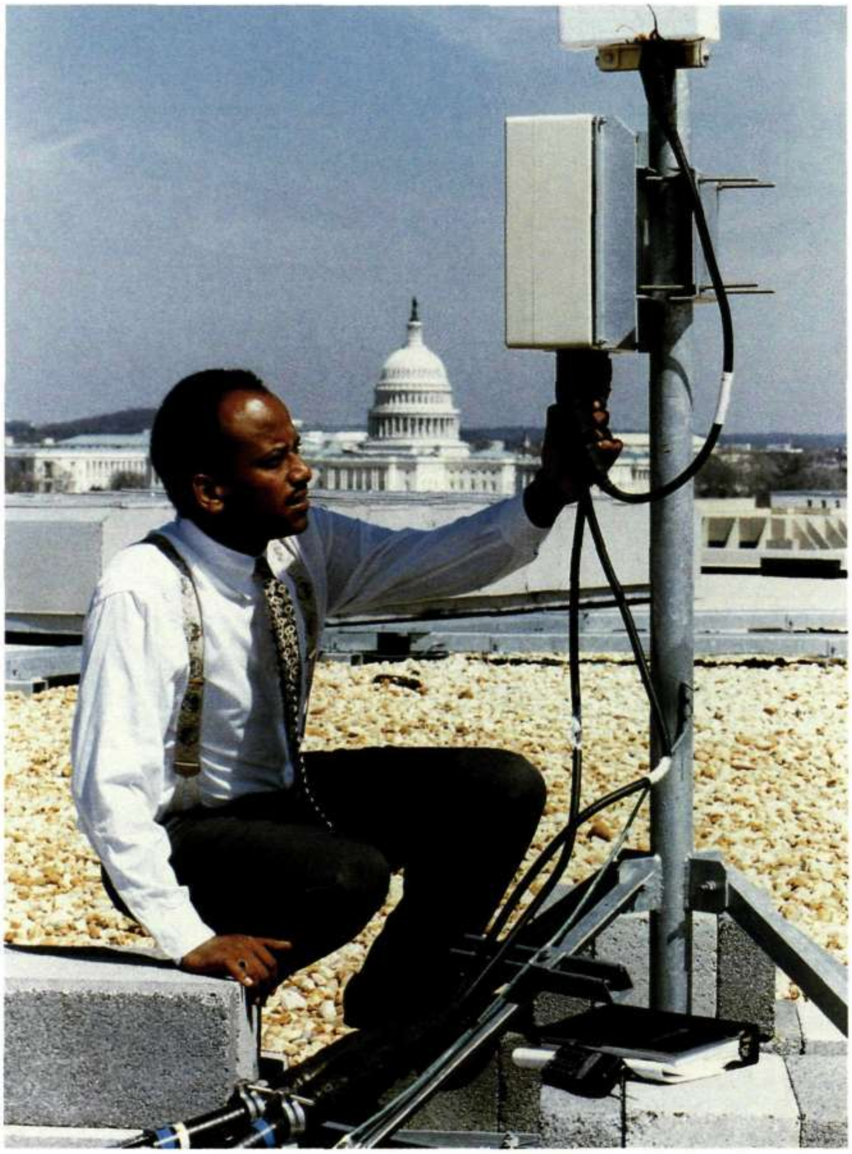


Fig. 6
In addition to hardware and software, Ericsson offers professional customer service and support. Together with operators, Ericsson analyses both business and system operations to reduce costs and improve system performance.

an enhanced customer service programme differing requirements amongst operators can be met and service offerings can be customised to the specific needs and capabilities of each operator.

The key to this programme is total flexibility – meeting the needs of new operators (with few telecom competencies), as well as those of long-established operators. The programme offers analysis and evaluation of operator activities, competencies and processes.

These latter three elements are defined as follows:

- *activities*: the definition of specific responsibility within the carrier organisation (for example regarding implementation, operation and maintenance, and system administration);
- *competencies*: the skills within the carrier organisation that can be deployed to carry out the activities;
- *processes*: the work flows (for example planning and engineering), comprising combinations of activities, which require a number of competencies.

Through the evaluation of the operator requirements, tailored Ericsson service packages can be offered. These packages cover four areas: professional services; implementation and integration; customer training and competence development; maintenance and support.

Together, these four areas cover every part of network operations – from advice on system performance, network planning and configuration of the network management system, to hands-on operation, maintenance and day-to-day support.

Well-proven architecture

PCS 1900 employs the same basic infrastructure and technology as the well-proven GSM system, and its 1800 MHz version – DCS 1800. In turn, several of the GSM/PCS network nodes are based on Ericsson's AXE switching system, at present in operation in more than 100 countries around the world.

The modular PCS architecture is divided into six main groups:

- The switching system (SS), where most call processing and subscriber-related functions are implemented.
- The base station system (BSS), where radio-related functions are concentrated.
- The service control point (SCP), which is the provider of mobile intelligent network services. The service management system (SMAS) provides service management functions.
- Network management products, such as the operations support system (OSS), which provides centralised network maintenance and operation, and the Ericsson engineering tool (EET) for network planning.
- Gateway products, such as service order gateway (SOG) and billing gateway (BGW), which provide centralised subscriber data handling.
- Adjuncts, which can be accessed and used by the PCS 1900 system.

Each of the six main groups are now described in further detail.

Switching system (SS)

Consists of:

- Authentication centre (AUC), which pro-

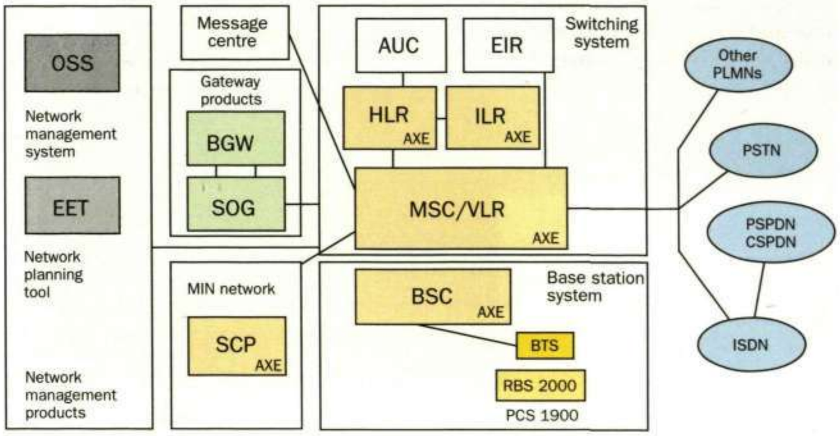


Fig. 7
PCS 1900 system components.

vides the authentication and encryption keys that confirm the identity of the user.
- Home location register (HLR), which stores and manages subscriptions and information about subscriber locations. The HLR database can be integrated with the MSC, or implemented as a separate node.
- Interworking location register (ILR), which offers roaming between cellular systems complying with different standards, such as PCS 1900 and AMPS.
- Equipment identity register (EIR), which prevents unauthorised use of handsets. The EIR database is often located together with the AUC, but can be implemented separately.
- Mobile switching centre (MSC), which performs the telephony switching functions.
- Visitor location register (VLR), which contains information about the handsets currently located in the MSC area. The VLR database is always integrated with the MSC.

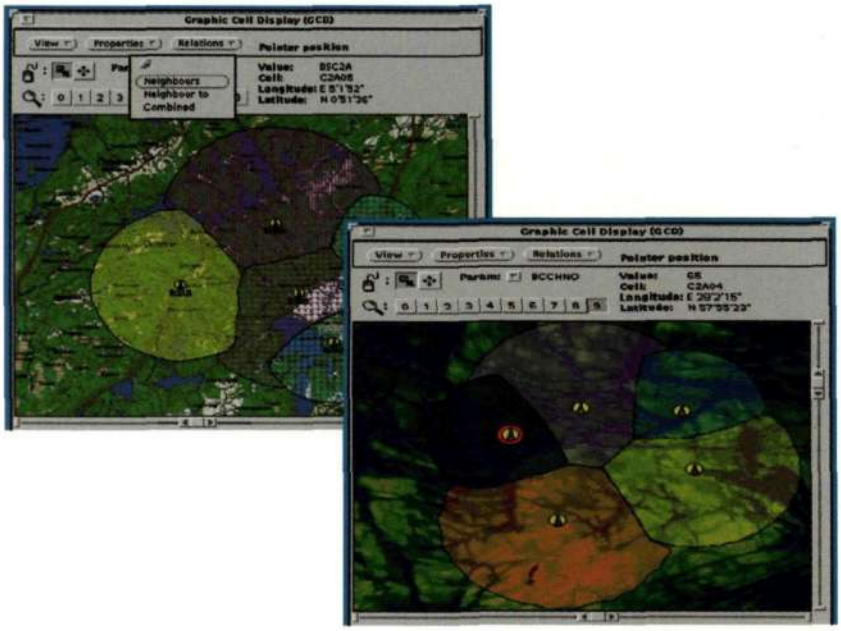
Base station system (BSS)
Consists of:
- Base station controller (BSC), a high-capacity switch, which provides total overview and control of radio functions, such as handover, management of radio network resources, and handling of cell configuration data. It also controls radio frequency power levels in the BTSs, and in the mobile phones. BSCs also set transceiver configurations and frequencies for each cell.
- Base transceiver station (BTS), which is the radio and transmission equipment required at a site. BTS functions include radio signal reception (from mobile phones) and quality measurements.

Service control point (SCP)
Consists of:
- The intelligent network (IN) node that executes service logic.
- The service management system (SMAS) that handles service design, deployment and management.

Network management
Available products include:
- Operations support system (OSS), which monitors and controls all system functions and nodes. The OSS also provides functions for radio network configuration management, network and radio traffic measurements, and report generation.
- Ericsson engineering tool (EET), which allows for planning and management of the radio network resources.

Gateways
Available products include:
- Service order gateway (SOG), which provides an interface to the network databases. The SOG is the single point of contact between the network infrastructure and the operator's customer care system (for subscription handling and administrative functions).
- Billing gateway (BGW), which provides an interface for the collection of subscriber call records. The BGW is the single point of connection between the network elements that produce billing information and the administrative billing system.

Adjuncts
Available products include:
- Message centre – using different messaging systems – which stores and forwards voice, fax and electronic mail, as well as short texts from paging networks.
- Digital cross-connect (DXX), which provides transport network solutions for both digital and analogue networks, as well as paging. DXX consists of modular hardware and software designed for rapid network deployment.
- MINI-LINK microwave products, which are integrated with existing wireline



Value: BSC2A
Cell: C2A06
Longitude: E 5°1'52"
Latitude: N 0°51'36"

Param: BCCHNO
Value: 65
Cell: C2A04
Longitude: E 29°2'15"
Latitude: N 57°55'23"

Fig. 8
The highly graphic operations support system (OSS) user interface offers easy access to information on network performance – even to the level of individual base stations.

networks, adding new levels of short-haul radio flexibility, as well as point-to-point transmission of both voice and data.

Continuous evolution meets mass-market needs

In addition to the service differentiation offerings – comprising wireless data services, IN value-added services, as well as PDA and SIM-card applications – Ericsson is focusing the PCS 1900 system development on five key areas: increased cost-effectiveness; enhanced network capacity; improved coverage; improved voice quality and advanced data services.

The following discussion covers each of these areas in turn, outlining Ericsson's efforts to satisfy the evolving service requirements of the mass market – thus bringing PCS 1900 into the wireless future of the 21st century.

Increased cost-effectiveness

It is not unfair to state that one of the major business aims of every GSM operator is to achieve the lowest cost per subscriber. Three key components of the Ericsson PCS 1900 architecture are crucial to achieving this goal: the operations support system (OSS), the switching system (SS) and the base station system (BSS).

The operations support system continuously monitors and controls all system functions, resulting in smooth and disturbance-free operation as well as providing low-cost operation and maintenance services.

The OSS plays a key role in maintaining and improving the service quality and capacity utilisation efficiency of the network. It provides applications for radio network planning, network configuration, network performance measurement, network supervision and mobile subscriptions administration.

The switching system, with the mobile switching centre (MSC), and the base station system (comprising base station controllers, BSC, and base transceiver stations, BTS), is crucial to efficient transmission and competitive network operation.

By pooling the transcoders of the network – and locating them in the MSC – subrate switching right through the network will be possible. Locating transcoders in the MSC also allows smaller BSCs.

In addition, Ericsson's range of BTSs, the RBS 2000 series, also contribute to cost-effective operation and maintenance. The BTS is remotely controlled and uses software directly loaded from the BSC. The Ericsson BTS can be commissioned on site in one hour.

Enhanced network capacity

To cope with the increased number of mass-market subscribers, network

Fig. 9
In addition to business usage, personal communications services are now spreading rapidly among private users.

capacity must be enhanced – especially in areas of high user density. The consumer market also requires high levels of service availability and quality – especially in dense user environments, such as shopping malls, underground areas, parking garages, sports grounds and leisure complexes. However, the traditional wide-area macrocells do not solve the capacity problem in these special environments.

The Ericsson solution to increased capacity is based on frequency hopping, used in combination with hierarchical cell structures. Frequency hopping provides enhanced radio network capacity in small urban cells, where interference and fading are common.

By means of wideband frequency hopping, the present 3/9 frequency reuse pattern will be improved to 1/3, which increases capacity up to three times.

Through further developments, 1/1 cell reuse will be possible. Frequency planning can then be simplified by combining wideband frequency hopping with fractional loading, thus reducing infrastructure and operating costs.

Reusing frequencies by changing the cell structure into smaller cells is a standard practice in Ericsson's PCS 1900 system.

The most cost-effective way of achieving capacity enhancements is to introduce a hierarchical cell structure, which implements microcellular technology; the smallest microcells covering a few tens or hundreds of metres in radius. Three-level hierarchical cell structures offer high-quality service in environments with great variations in traffic density. By adding a new layer, capacity is increased – without affecting the existing cell structure.

Microcellular networks can be used to provide capacity enhancements in four modes: fill-in coverage; customised coverage, supporting applications such as differentiated billing; hot-spot capacity; or as high-capacity networks, for example covering central business districts.

Through efficient handovers between the different cell layers, maximum capacity and quality are ensured at all times.

The hierarchical cell pattern not only handles fast-moving vehicles (by means of macrocells and umbrella cells), but also provides services to traffic hot spots as well as fill-in coverage (microcells), and

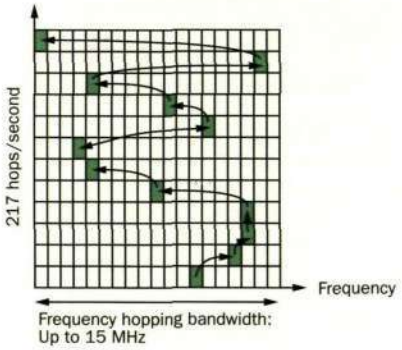


Fig. 10
Frequency hopping increases capacity by reducing interference. It balances the performance between stationary and fast-moving handsets. Even though there are 217 hops per second, hops never collide within a cell.

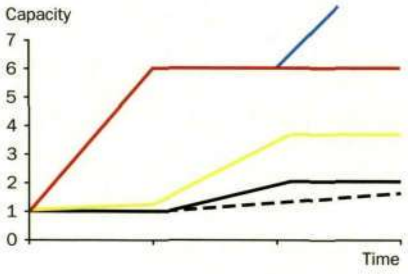
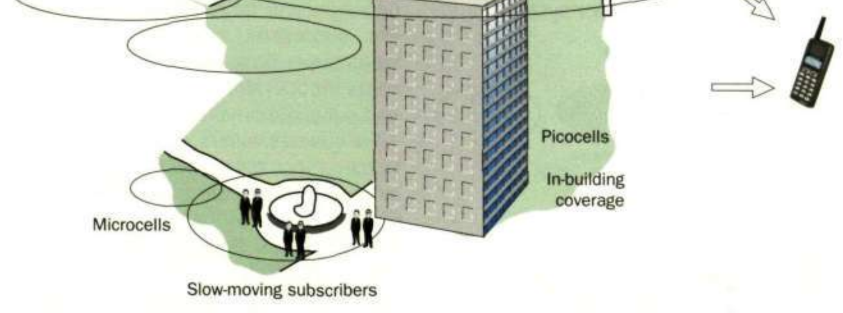


Fig. 11
Using a wide range of innovative solutions, the GSM network capacity can be increased 6-7 times over the next two to three years.

Fig. 12
The hierarchical cell-structure concept allows differently sized cells – which are divided in layers – to co-exist in the same geographical area. The layers do not interfere with one another because each of them uses different frequencies and time slots.



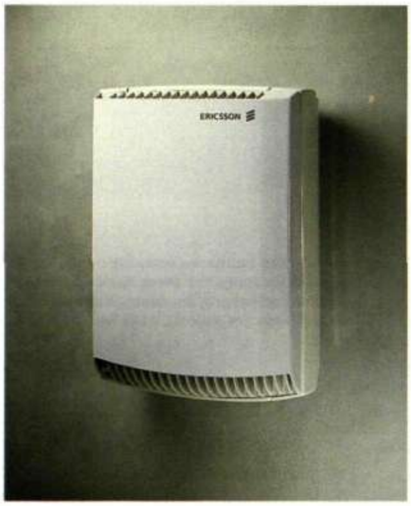
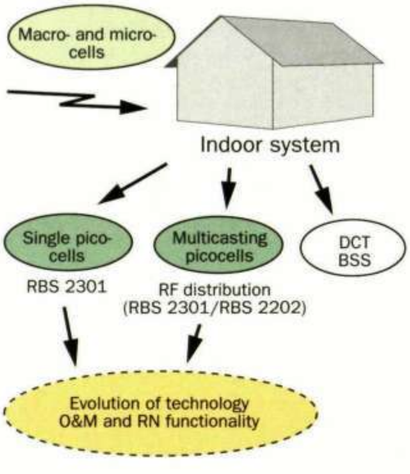


Fig. 13
To improve coverage, operators tend to install more and more base stations, shrinking the radius of each existing cell. Ericsson's compact micro-RBS (RBS 2301) serves cell sites as small as 100-300 metres in diameter. The micro-RBS has a volume of approximately 30 litres (7.926 US gallon) and offers 15 traffic channels.

Fig. 14
Ericsson has a wide range of competitive solutions for efficient indoor coverage.



in addition offers indoor coverage (picocells).

Efficient microcellular technology

The necessity for smaller cell sizes to enhance capacity also implies increasing the number of base transceiver stations (BTS). Consequently, BTSs must be extremely cost-effective. Ericsson's new micro-RBS cuts site costs by up to 70 per cent and is very easy to install and maintain.

Microcellular networks also require high-capacity base station controllers, which can handle hundreds of cells and BTSs in complex hierarchical layers. High-capacity BSCs also reduce the overall BSC site costs, as well as the signalling load on the mobile switching centre.

To increase flexibility, a variety of MSC-BSC-BTS transmission solutions are offered, including fibre, copper and microwave.

Improved coverage

To increase the number of subscribers, and thus competitiveness, PCS operators need virtually complete population coverage out of doors. But, they also need new solutions for specific indoor coverage.

Ericsson solutions to providing better coverage include low-noise amplifiers (LNA) close to the antenna masthead, an arrangement that extends cell ranges. LNAs improve the uplink sensitivity of the base station, thus widening the coverage area of the base station.

Future solutions include adaptive multi-beam antennas, which reduce the number of base stations considerably, thus greatly reducing operator costs for infrastructure, sites and maintenance.

For indoor applications, there are two main driving forces: efficiency for the operator, and mobility for the end user. The successful introduction of indoor solutions is based on low infrastructure costs for operators, and competitive call and subscription charges for users.

For business users, enhanced data services – combined with cost-effective indoor coverage – are crucial components of a competitive network offering. By means of new developments, Ericsson supports improved indoor access. Micro-BTSs, and distributed multicasting (pico) radio heads, increase indoor capacity as well as coverage.

Ericsson indoor solutions cover residential, business and public environments. PCS, in combination with digital cordless telephony (DCT), intelligent network and/or PBX applications, paves the way for cost-effective implementation of indoor coverage.

In the long-term, PCS 1900 may be offered as a PBX replacement solution for small businesses.

Improved voice quality

Cellular users are increasingly demanding PSTN-like levels of voice quality. The use of voice-controlled – or at least voice-based – value-added services, such as telephone banking and automated information services, also infers requirements for better intrinsic voice quality.

To meet that requirement, the PCS 13 kbit/s full-rate vocoder is now being enhanced. The new enhanced full-rate (EFR) coder comprises the latest advances in algorithm research and speech coding – offering wireline-like speech quality at the level of 32 kbit/s adaptive differential pulse code modulation (ADPCM) "land line".

Advanced data services

The market demand for higher data rates is one of the main driving forces in the future wireless market. The current PCS specifications provide access to both circuit- and packet-switched networks, via circuit-switched connections over the radio interface.

At present, Ericsson is actively contributing to the standardisation of GSM Phase 2+, which encapsulates a wide range of wireless data applications to be implemented in the PCS 1900 system.

Today's data transfer rate of 9.6 kbit/s (supporting fax, e-mail, voice/fax mail, PC file transfer and short message service) will be expanded to 19.2, 28.8, and even 64 kbit/s in the near future.

The first step will be to introduce high-speed circuit-switched data (HSCSD) solutions which enable users to access two time slots instead of one – thus doubling the data capability.

The second step will be to introduce bandwidth-on-demand (as a built-in capability of HSCSD). By dynamically allocating up to eight time slots for each single data call (64 kbit/s; the full PCS bandwidth), new services can be offered, such as high-speed multimedia access, videoconferencing and CD-quality sound.

With the HSCSD high-speed data capacity, graphics-heavy World Wide Web pages can in principle be downloaded as easily and quickly as via a terrestrial connection.

In this way, PCS networks will be fully competitive with the transmission speeds offered in wireline networks (through ISDN or leased line connections).

Packet data services

As the use of specially-targeted data services for mobile users is expected to increase, there will be a need to improve the efficiency of the utilisation of scarce radio resources. In order to provide means for several users to share the same radio path, general packet radio services (GPRS) are now being standardised as a set of new flexible data services.

With GPRS, the spectrum is used only when the user is ready to send. When there is no data to be transmitted, the spectrum is free to be used for another call.

GPRS will complement existing circuit-switched data services and offer efficient utilisation of both spectrum and network resources, as well as fast response time for users.

The new packet data services will offer point-to-point connectionless services, providing TCP/IP connectivity to external LANs and the Internet, as well as point-to-point connection-oriented X.25 capabilities.

Furthermore, a set of point-to-multipoint broadcast and group call services is also being defined.

In addition, the GPRS packet-switched data capability will permit operators to offer flexible tariff options, especially for customers planning for high-volume usage of Internet services.

GSM evolution to multimedia

Data communications bit rate / Application	Single slot 9.6 kbit/s	Double slot 19.2 kbit/s	Multiple slot 76.8 kbit/s
Simultaneous voice & data	Half rate + 4.8 kbit/s	Full rate + 9.6 kbit/s	Full rate + 76.2 kbit/s
HiFi music/ voice	Wireline quality with enhanced full-rate coder	HiFi quality voice	HiFi quality voice and music
Multimedia/ video	Still pictures, animations	Animations, video	Video conferencing

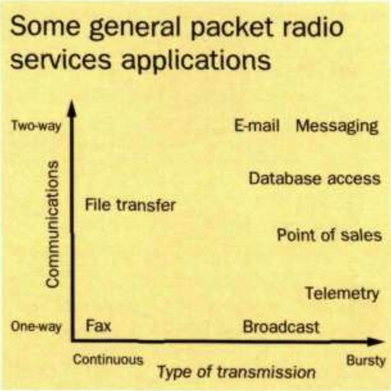
Fig. 15
By introducing multiple-slot techniques, bit rates are increased and multimedia applications can be offered.

Fig. 16
Mobile data communications provide access to a variety of networks and advanced data services.

Conclusion

The growing emergence of a mass-consumer market for personal communications services has coincided with the worldwide trend towards the deregulation of telecom markets and the ongoing rapid march of advancing technology. It was under these conditions that Ericsson developed its PCS 1900 system for personal communications services. Based on the well-proven and almost universally-accepted GSM standard, the PCS 1900 system offers the telecom operator a reliable, efficient and cost-effective service that can be easily integrated into existing communication networks of all types.

Supported by Ericsson's global research and development resources, the PCS 1900 system is constantly being developed and enhanced to ensure that it continues to lead the way to the communications networks of the future.



Some general packet radio services applications

Fig. 17
General packet radio services (GPRS) are evolving towards two-way communications and bursty transmission services.

A choice of system implementations for the service control point

Rob Eubanks, Marko Hentilä and Thomas Larsson

As more and more new services are integrated into intelligent networks, the role of service control points (SCP) grows in importance. The Ericsson SCP-T, which is based on a telecom-purpose computer (TPC), has gained a solid reputation amongst network operators for its robustness, reliability, performance, and compatibility. Now, Ericsson expand their product portfolio for network intelligence platforms with the SCP-G, an SCP developed on a general-purpose computer (GPC).

The authors describe how the Ericsson SCP-G – a product that incorporates the best features of its companion, the SCP-T – significantly broadens operators' choice and freedom in designing their network systems.

The Ericsson SCP

Thanks to several key features in the Ericsson SCP, operators who choose it are able to benefit from a number of its key attributes.

Because Ericsson designed the SCP to comply with the globally-accepted IN standard ETSI Core INAP CS-1 – which is functionally compatible with ITU-T Capability Set 1 (CS-1) Recommendations – the Ericsson SCP can be used in various network environments.

Ericsson's programming technique for network intelligence services is SIBScript. Originally pioneered by Ericsson in the mid-1980s, SIBScript is based on a concept of service-independent building blocks (SIBs). The SIBScript architecture permits new IN services to be introduced into the network without disturbing or interrupting service or operations.

The Ericsson SCP is a robust solution whose design draws heavily on experiences won in developing fault tolerance in the AXE. What's more, because SIBs are thoroughly pre-tested telephony functions, their use further minimises faults in design and verification, as well as in the deployment of services. SIBScript also includes far-reaching support for handling the various and sometimes unexpected call events that occur in telecom networks.

Experience

Ericsson have extensive experience of using general-purpose computers (GPC) in telecom networks for real-time applications. For example, Ericsson's telecommunications management platform, TMOS, of which SMAS is the application for IN service management and creation, is based on general-purpose computers. TMOS-related development was first started in 1989. Ericsson also use general-purpose computers for real-time applications in the service data point (SDP), which was first introduced in early 1995. Today, the SDP is running successfully in several IN networks

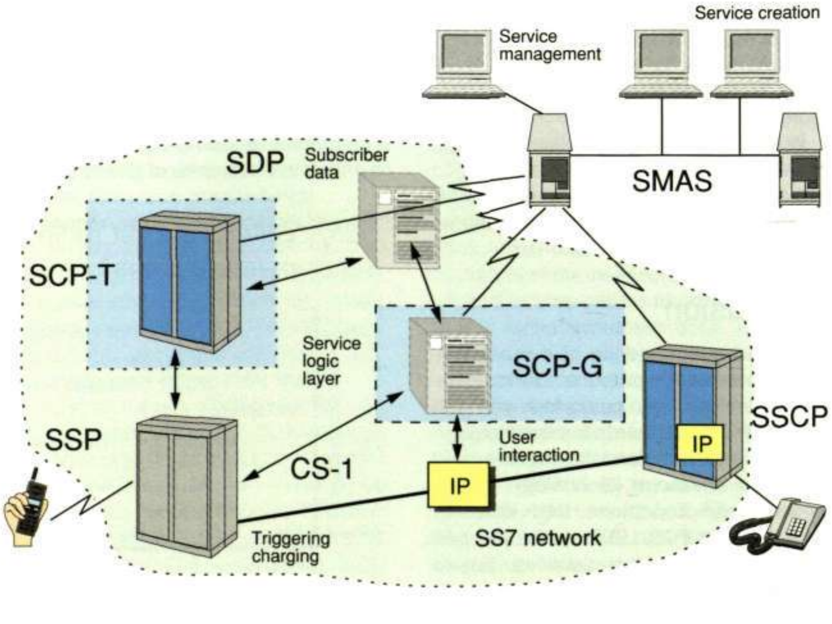


Fig. 1
SCP-G offers a choice of system platform for the IN applications.

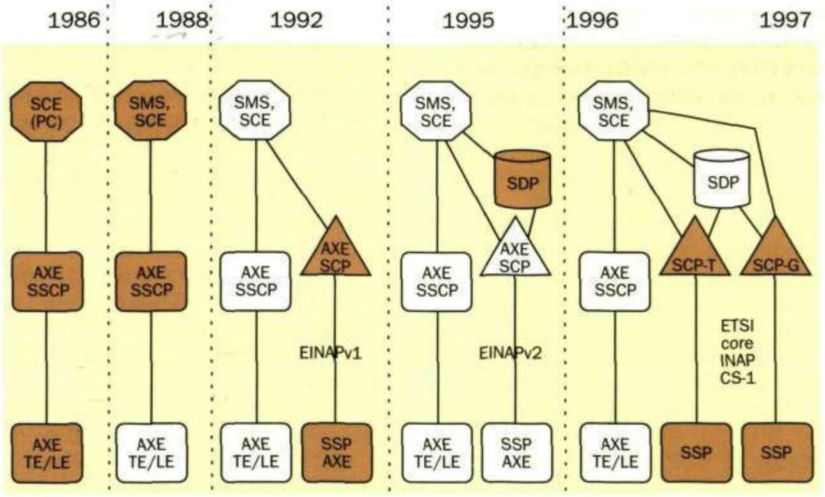


Fig. 2
Ericsson's IN evolution – today the most widespread IN platform, with 59 customers in 29 countries (Sept 96).

around the world. The SCP-G is based on the same platform architecture as the SDP.

SCP-G characteristics

An SCP-G is vital to operators who require open systems and third-party software. Likewise, an SCP-G addresses operators' demands for scaleability.

As seen from Fig. 3, subscriber management, service creation, service management, service applications and service execution are identical in both versions of the SCP. Indeed, when Ericsson designed the SCP-G, they did their utmost to apply the most attractive characteristics of their well-proven SCP-T.

Reliability

The SCP-T platform, which has AXE's well-proven built-in fault tolerance, and which is optimised for telecommunications, consists of a computer – the APZ control system – and the APT switching system, which includes the real-time IN application platform: service script interpreter (SSI).

Due to its nature, the hardware platform for the general-purpose computer is not as fault-tolerant as its telecom counterpart. Nonetheless, considerable efforts were invested into the development of the SCP-G to ensure high availability, and to produce a telecom network node whose robustness and reliability matches that of most other telecommu-

Subscriber management	Subscriber installation, removal, subscription handling Generic service adapter, Application programming I / Fs	
Service creation & management	Service installation, modification, removal, upgrade Graphical user interface in service creation environment	
Service applications	Cellular VPN, Universal Personal Telecommunications,.. Service independent building blocks, SIBScript	
Service execution	Service control functionality Service script interpreter (SSI)	"Custom" SIB/API
System services, "middleware"	ETSI CORE INAP CS-1	
	SS7, TCAP, EINAP, CS-1 MTP, INM, ...	SS7, TCAP, CS-1 SNAP, TCP/IP...
Operating system	APZ 212 10, APZ 212 20, ...	UNIX-versions, (NT), ...
System hardware	Telecom-purpose computer	General-purpose computer

Fig. 3
Network Intelligence™ open choice solution for the SCP.

Table 1

Year	1998	1999	2000	2001	2002	2003
TPS minimum	750	1,000	1,500	2,250	3,000	4,500
TPS	1,000	1,600	2,500	4,000	6,400	10,000
TPS maximum	1,500	2,700	4,860	8,750	15,750	28,000

Box A
Abbreviations

API	Application programming interface
ATM	Asynchronous transfer mode
B-ISDN	Broadband integrated services digital network
CAMEL	Customised application for mobile-enhanced logic
CORBA	Common object request broker architecture
CPU	Central processing unit
CS-1	Capability Set 1
CS-1+	Additions to CS-1
CTM	Cordless terminal mobility
EINAP	Ericsson intelligent network application protocol
FMC	Fixed mobile convergence
FPLMTS	Future public land mobile telephone system
IN	Intelligent network
INM	IN management interface
IP	Intelligent peripheral
IT	Information technology
NI	Network Intelligence™
NP	Number portability
MTP	Message transfer protocol
RAM	Random access memory
SCE	Service creation environment
SCP-T	Telecom purpose computer-based SCP
SCP-G	General purpose computer-based SCP
SCSI	Small computer standard interface
SDP	Service data point
SIB	Service independent building block
SMAS	Ericsson's service management system (TMOS family)
SMS	Service management system
SNAP	Service node application system
SS7	Signalling system 7
SSCP	Service switching and control point
SSI	Service script interpreter
SSP	Service switching point
TCAP	Transaction capabilities application protocol
TINA	Telecommunications information network architecture
UMTS	Universal mobile telephony system (3rd-generation mobile)
UPT	Universal personal telecommunications service
VPN	Virtual private network service
WIN	Wireless IN

nications network products.

High availability is a built-in feature of the SCP-G, which has no single point-of-failure. The SCP-G hardware is duplicated, and hot-standby functionality is provided by in-house middleware, known as the service node application platform (SNAP).

Performance

The SCP-G application is designed to be portable, thereby ensuring competitive price/performance, by enabling the use of the very latest in hardware and software technology. Generally speaking, suppliers of both types of platform (GPC and TPC) are expected to double the capacity of their products every 15-24 months.

Based on general trends to date, where computing capacity has been increased by 200% every 18 months, a reference value for transactions per second (TPS) was extrapolated from Table 1. The nominal reference value for the year 1998 is 1,000 TPS, which should be compared with the year 2003, where 10 times as much capacity is forecasted. A more conservative minimum value predicts that capacity will increase by 200% every two years (instead of every 18 months), whereas a more optimistic maximum value predicts that significant technological breakthroughs will follow one after another at 15-month intervals (200% increase in capacity every 15 months).

Portability

The same service creation environment (SCE) is used for both the SCP-T and the SCP-G, greatly facilitating service design, since the services can be ported directly from one platform implementation to the other. Since redesign – which puts a heavy constraint on time – is essentially eliminated when both types of node are used in the same network, tremendous savings are gained. Portability also allows end-users to employ the same interface in both systems – another source of savings since only one set of customer service procedures and sales or promotional materials is needed for both the SCP-T and the SCP-G. Similarly, because the same management system, SMAS, can be used to handle both types of node, service management and updates are greatly simplified.

Third-party software

Because the SCP is available on a general-purpose computer, it is open to third-party software. Thus, new SIB-type functionality can be created in familiar programming environments, such as C++. Also, commercially available programs, such as credit-card authentication algorithms, can easily be added to IN services using the same mechanism.

An API ("custom SIB"), which has been developed to maintain integrity in the network, creates a firewall between third-party software applications and the service script interpreter, see Fig. 4.

Software development through object-oriented languages facilitates interworking with management and information systems. The UPT and number portability services, which share similar functionality, and which will affect the global numbering plan and needs for capacity in similarly dramatic ways, make the most of the SCP-G's power and expandability.

Open solutions

NI/Open™, Ericsson's openness for network intelligence solutions, is fully incorporated into the SCP product array. Designers of the SCP-G created it to be as independent as possible of UNIX and other hardware.

This independent design gives operators a choice of operating system, workstation vendor, and design language of third-party services. Thus, operators can mix and match the SCP-T and the SCP-G, with accompanying portability and shared service management, in the same network. This open design, which is unique to the telecommunications industry, draws on Ericsson's long history of supplying state-of-the-art solutions.

Software scaleability

The SCP-G system is a suitable choice for both very large subscription volume applications and small pilot or experimental applications. Hence, the SCP-G complements the capacity range of Ericsson's SCP-T and SDP. The SCP-G is also well-suited to a "pay-as-you-grow" strategy.

Because it is inherently scaleable, adaptable and flexible, the SCP-G can support very large numbers of subscribers. UNIX-based software can run each powerful new generation of hardware, fully utilising advances in processing power, storage capacity and retrieval time.

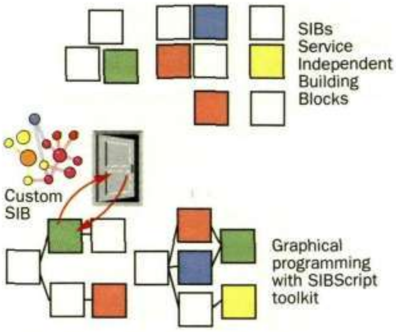


Fig. 4
"CUSTOM SIB" – a brand-new option for adding external applications.

SCP-G architecture

The first implementation of the SCP-G consists of a Sybase relational database management system and a general-purpose computer platform (currently, HP9000 UNIX servers).

The ITU-T Capability Set One (CS-1) Recommendations include the standard ETSI Core INAP CS-1 interface between the SSP and the SCP. Ericsson support the entire specification in its first release ("100% of 100%"). By means of additional messages ("CS-1+"), the SCP-G is also able to communicate with an external service data point (SDP) during service execution. CS-1+ is an extension of the CS-1 recommendations.

Hardware scaleability

The hardware can be adapted for a variety of configurations:

- number of servers (functional processors), and number of CPUs in each server;
- amount of RAM;
- amount of disk space;
- number of SS7 links.

The service control functionality (SCF) executes service logic, which is made up of service independent building blocks. The SCF conforms to the service script interpreter (SSI) concept.

The service control functions of the SCP-G may physically be distributed amongst multiple processors, or they may reside on a single processor. Each type of function generally has two instances: one in a primary mode and another in a secondary mode (for example, SCF-primary and SCF-secondary, see Figure 5). Primary functions are active and execute traffic. Under normal conditions, the secondary function is also active on another processor. Should a processor that contains the primary function fail, then the corresponding secondary function becomes primary.

Middleware

The service node application platform (SNAP) contains support for high availability. The process monitor is responsible for sending out a heartbeat to each process in the system. Should a given process fail to respond after three con-

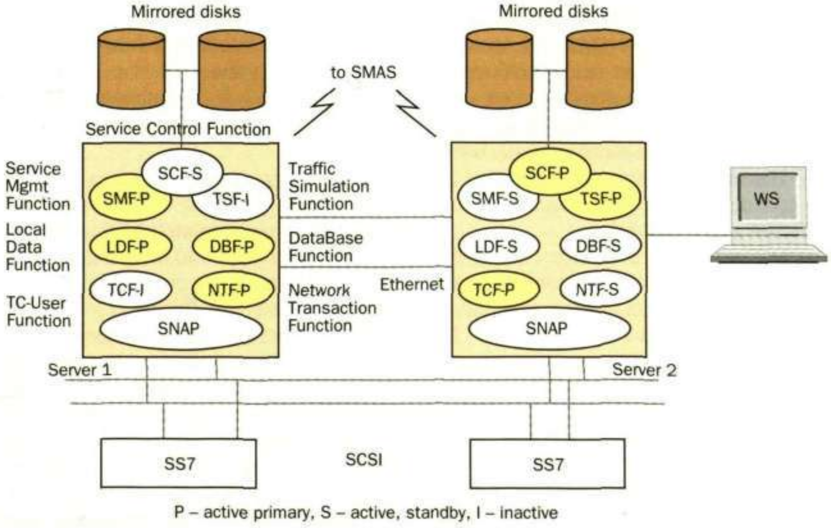


Fig. 5
SCP-G low-end two-server configuration.

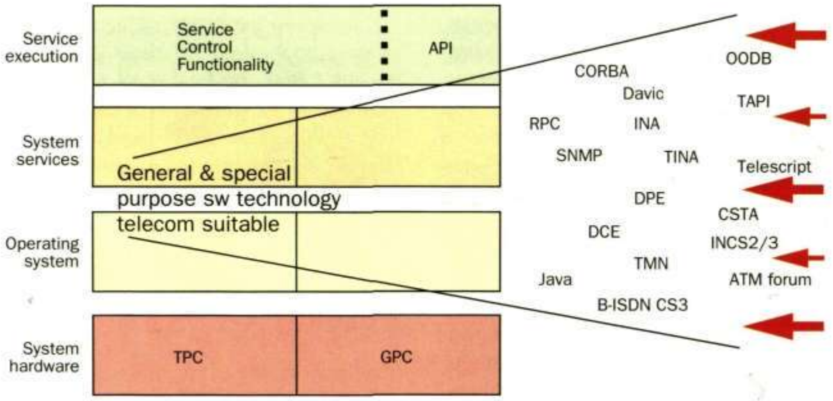


Fig. 6
Ericsson's SCP platforms – merging the best standards and industrial trends.

secutive calls, then the process monitor considers the process to be dead. The process monitor's next course of action, which is invoked by its configuration file, might include restarting the process, switching over to another process ("hot stand-by"), or starting a different version of the process.

Another important middleware subsystem is the network transaction function (NTF), which is an SS7 subsystem. This system, of which the TC-user is a subsystem, is prepared to handle multiple TC users in order to allow multiple protocols.

SCF-SMF communication

Like the SCP-T, the SCP-G is managed by an SMAS system. By means of the standard UNIX transmission control protocol and Internet protocol (TCP/IP) connection, a binary Ethernet or an X.25 interface allows SMAS to communicate with the SCP-G. The SMAS interface is used to install, replace, remove, and fetch SCP-G service and subscription data.

SCF-SDF communication

The SCP accesses a service data point (SDP), which is a network element used to hold large amounts of subscriber data, via Ericsson CS-1 extensions to SS7/TCAP. The SCP-G may also access an SDP by means of a TCP/IP connection.

Interfaces (to external databases and IT systems)

SCP-G services (or an SCP-T that is connected to an SDP) can access various databases, such as corporate credit-card databases or a network operator's billing system. The SCP-G platform supports a range of interfaces commonly used in such applications.

Redundancy

To eliminate instances of single point-of-failure, redundant sets of hardware are used, including:

- multiple functional processors;
- dual local area network (LAN) interfaces between processors;
- multiple SS7 interface units connected to two processors by means of independent small computer standard interfaces (SCSIs);
- two sets of mirrored application disks controlled by independent processors over independent SCSIs;
- multiple links to SMAS from two functional processors.

Similarly, network redundancy can be built up using a mated-pair configuration.

Management system

The SCP-G incorporates the Ericsson service script concept into its design. SMAS allows services to be created from Ericsson's feature-rich SIBs. Moreover, if desired, new "custom SIBs" can be constructed in C++, or from other add-ons. Because the service creation part of SMAS is the same for both the SCP-G and the SCP-T, the CS-1 service scripts can be ported between the two systems. The SCP-G system is meant to be flexible, allowing operators to use third-party software in it. To maintain system integrity when third-party software is used, a firewall separates all third-party software from the SIBs.

Vision

A great deal of work has gone into creating standards for integrating B-ISDN into the IN model, and IN controls of broadband connections are expected to become available in the near future. Features of this kind could be facilitated by CORBA-based and TINA-like distributed-processing environments, which represent a natural path of evolution for the SCP-G.

Today, Ericsson are actively involved in developing IN-mobile architectures (NP, CTM, CAMEL, WIN, FMC, UMTS, UPT, FPLMTS), "service brokers", "intelligent terminals" and "intelligent agents", "server – client architecture", and "personal assistants", in order to lead development, and to create "de facto" standards for the telecommunications industry. One example worth mentioning in greater detail is a UPT service running over an ISDN-LAN/ATM gateway to a conventional computer, which permits voice signals to be sent via a TCP/IP connection over the LAN. Another area of focus is the World Wide Web, and the opportunities it offers for giving end-users greater control via the Internet.

The use of object-oriented languages in software development will facilitate interworking with management and information systems, which implies that the number of calls with an IN component involved will increase. In turn, as the number of IN-related calls increases, the demand for available storage capacity and processing power in the SCP-G will also increase.

This is part of Ericsson's visionary Network Intelligence™ concept, that expands IN for the 21st century.

Customer choice

Today, customers have a choice of platforms, meaning that solutions can be designed to match specific customer requirements and needs. The SCP-T and the SCP-G have different characteristics, and which system platform a customer chooses depends on the particular situation and usage.

However, regardless of which Ericsson platform operators choose, Ericsson's leading role in the field of IN will ensure that operators always get the best solution for profitable business.

Conclusion

In areas where telecommunications have been deregulated, and competition is permitted amongst rival operators, a primary feature that sets one operator apart from the next is the services they provide. The platform for providing services is the intelligent network, of which the heart is the service control point (SCP).

As long as services continue to play a vital role in determining an operator's success, operators will continue to add new services to their systems, implying that the role of the SCP will take on ever-increasing proportions of importance. Thus, an operator's choice of SCPs can be a key factor of his success. With the release of the SCP-G, Ericsson's already strong stable of SCPs becomes stronger than ever.

The SCP-G draws upon the features that made the SCP-T a success, including service-independent building blocks (robustness), fault-tolerance (reliability), and compatibility with a variety of network environments, while bringing such new elements into play as choice amongst platforms (telecom-purpose computer vs. general-purpose computer), acceptance of third-party software, the ability to port services to or from an SCP-T, and increased scaleability of hardware and software configurations.

To the operator, this all boils down to greater choice and flexibility – telecom vs. general-purpose computer platform; standard vs. third-party software; full-size vs. scaled-down system, and so on. Armed with a choice, operators can match solutions to each specific need, and make a direct impact on their bottom line.

Box B
Trademarks

Ericsson Review

Vol.73, 1996

Contents 1996

Access Technologies

Mobile Communication Systems

Mobile Communication Technologies

Network Operation & Maintenance

Power & Cooling Systems

Miscellaneous

Telefonaktiebolaget L M Ericsson
S-126 25 Stockholm, Sweden
Tele: +46 8 7190000
Fax: +46 8 6812710

ISSN 0014-0171
Ljungföretagen, Örebro 1996