UMTS Security Awareness

© UMTS Forum, 2003

This report has been produced by the UMTS Forum, an association of telecommunications operators, manufacturers and regulators .The UMTS Forum comprises of IT and media industries interested in broadband mobile multimedia that are active both in Europe and other parts of the world and who share the vision of UMTS (Universal Mobile Telecommunications System). These are key industry members of the Forum and have contributed significantly to this report. In terms of a technology platform UMTS will move mobile communications forward from today's environment to the Information Society incorporating third generation mobile services that will deliver speech, data, pictures, graphics, video communication and other wide-band information direct to people on the move. UMTS UTRA (Universal Terrestrial Radio Access) is a member of the IMT-2000 family of standards.
This report has been generated by one of the UMTS Forum Working Groups, the Information and Communication Technologies Group (ICTG), which addresses the main services and applications enables for the introduction of UMTS / Third Generation.
Report 30 is one of the family members of UMTS Forum reports that deal with the regulatory framework and the vision for UMTS. Other outputs from the Forum cover technical aspects, economic conditions, and licensing issues.
The views, conclusions and detailed recommendations expressed in this Report are purely those found and expressed during the work of creating this document and exempts National Administrations who are UMTS Forum members from being bound to them.

The following UMTS Forum members contributed in the preparation of this report:

Ecaterina Ganga ecaterina.ganga@siemens.com

John Whitehead John.whitehead@seri.co.uk

Roberto Sannion Roberto.sannino@st.com

Jorge Pereira Jorge.Pereira@cec.eu.int

Bosco Fernandes bosco.fernandes@siemens.com

All comments received from BT, Telia and Alcatel were incoroporated.

First edition, revision 2.8

Copyright © UMTS Forum, 2001. All rights reserved. Reproductions of this publication in part for non-commercial use are allowed if the source is stated. For other use, please contact the UMTS Forum Secretariat, Russell Square House, 10-12 Russell Square, London WC1B 5EE, UK; Telephone +44 20 7331 2020.
Web: www.umts-forum.org
All possible care has been taken to assure that the information in this report is accurate. However, no warranty of any kind can be given with regard to this material. The UMTS Forum shall not be liable for any errors contained in the report or for incidental consequential damages in connection with the use of the material.

Table of Contents

1. EXECUTIVE SUMMARY 1

2. INTRODUCTION 3

2.1 THIS REPORT 3
2.1.1 Risks and Threat analysis 3
2.1.2 Where must security measures be applied? 6
2.1.3 What resources need protection? 6
2.1.4 How should security be deployed? 7
2.2 SECURITY LEVELS 7
2.3 SCALABLE TO MEET SECURITY ISSUES 8

3. GENERAL ARCHITECTURE OVERVIEW GSM/UMTS 10

3.1 GSM 10
3.1.1 Security limits of 2G 10
3.1.2 Elements to be retained from 2G security 11
3.2 UMTS 12
3.2.1 Access network security: user access security 14
3.2.2 Network Security: network Domains 14
3.3 SPECIAL CONSIDERATION FOR THE IMS 15
3.3.1 IMS Domain Security 15
3.4 SECURITY IMPLEMENTATIONS 21
3.4.1 Virtual Private Network (VPN) 21
3.4.2 Internet 24
3.4.3 WLAN security 25

4. SECURITY AND PRIVACY WITH IP 28

4.1 BACKGROUND 28
4.2 CURRENT SECURITY AND PRIVACY ISSUES 28
4.3 SECURITY WITH IPV4 28
4.4 SECURITY WITH IPV6 28
4.5 PRIVACY 29
4.6 IMPLICATIONS OF SECURITY ABOVE THE TRANSPORT LAYER. 29
4.6 APPLICATIONS 30
4.7 NETWORK MANAGEMENT & BILLING 30
4.8 END-TO-END SECURITY INFRASTRUCTURE 30
4.9 INTERMEDIATE SECURITY INFRASTRUCTURE 31

5. SECURITY TECHNOLOGIES 32

5.1 INFRASTRUCTURE 32
5.1.1 Public Key Infrastructure (PKI) 32
5.2 FIREWALLS 33
5.3 CRYPTOGRAPHY 34
5.3.1 Symmetric Private Key Cryptography 34
5.4 PROTOCOLS 35
5.4.1 IPSec 35
5.4.2 IPSec, NATs and Firewalls 36
5.4.3 Automated key exchange with IKE 36
5.4.4 Limits and unsuitability's of IPSec 37
5.4.5 Protocol overhead of IPSec 37
5.4.6 IPSec requires special HW 37
5.4.7 IKE authenticates nodes, not people 38
5.4.8 IPSec and IKE do not prevent DoS attacks 38
5.4.9 IPSec does not provide application-layer end-to-end security 38
5.5 TRANSPORT LAYER SECURITY (TLS) 39
5.5.1 WTLS Wireless Transport Layer Security Protocol 39

5.6 PAP (PASSWORD AUTHENTICATION PROTOCOL) 39
5.7 XML (TRUSTED ENVIRONMENT) 39
5.7 INTRUSION DETECTION SYSTEMS (IDS) 40

6. TOOLS 41

6.1 AAA (AUTHORISATION, AUTHENTICATION AND ACCOUNTING) 41
6.2 CERTIFICATES 41
6.3 DRM 41

7. TERMINAL 43

7.1 TEMINAL VIRUS 43
7.2 PERSONAL TRUSTED DEVICE (PTD) 44
7.3 VIRUS 44
7.4 BIOMETRIC BASICS 44
7.5 SMART CARDS 46

8. PRIVACY (PRIVACY) 47

8.1 P3P-PLATFORM FOR PRIVACY PREFERENCES 47
8.2 LOCATION BASED SERVICES 47

9. SECURITY IN 3G CELLULAR NETWORKS 49

9.1 3GPP SPECIFICATIONS ON UMTS SECURITY 50
9.2 UMTS SECURITY PRINCIPLES AND OBJECTIVES 50
9.3 SECURITY ARCHITECTURE, FEATURES AND MECHANISMS 50
9.4 NETWORK ACCESS SECURITY (I) MECHANISMS 53
9.4.1 Use of temporary identities 54
9.4.2 Radio access network encryption 55
9.4.3 Signalling integrity provided inside UTRAN 55
9.5 NETWORK DOMAIN SECURITY (II) 55
9.5.1 MAP Application Layer Security (Release 4) 56
9.5.2 IP Network layer security 57
9.6 USER DOMAIN SECURITY (III) 60
9.6.1 3GPP User domain security features 61
9.6.2 3GPP User domain security mechanisms 61
9.6.3 The security mechanisms for USIM: 62
9.7 APPLICATION DOMAIN SECURITY (IV) 62
9.7.1 3GPP Application Domain Security Features 62
9.8 VISIBILITY AND CONFIGURABILITY OF SECURITY (V) 63

10. FEATURES AND REQUIREMENTS NOT COVERED BY STANDARD MECHANISMS 64

10.1 NETWORK ACCESS DOMAIN 64
10.1.1 Requirements to the network: 64
10.1.2 Requirement to the terminal: 64
10.1.3 Requirement to Operation and Maintenance: 64
10.2 NETWORK DOMAIN 64
10.3 USER DOMAIN 65
10.4 APPLICATION DOMAIN 65
10.5 CONCLUSIONS ON STANDARDISATION 65

11. FRAUD 67

11.1 CURRENT SITUATION 67
11.2 CONSEQUENCES 68

12. SERVICES AND APPLICATIONS 69

12.1 ARTS ASSOCIATION FOR RETAIL TECHNOLOGY STANDARDS 70
12.2 MET MOBILE ELECTRONIC TRANSACTIONS 71
12.3 MOBEY GLOBAL MOBILE PAYMENT STANDARDS 71
12.4 MOBILE PAYMENTS FORUM 72

13. REGULATORY ISSUES FOR SECURITY 74

13.1 LAWFUL INTERCEPTION 74
13.2 REGIONS (USIM) 75
13.3 PRIVACY 75

DEFINITIONS 76

ANNEX A ABBREVIATIONS AND GLOSSARY 78

ANNEX B BIBLIOGRAPHY 89

List of Figures

Figure 2.2 Security levels in an UMTS network 8
Figure 3.0 Security Architecture 13
Figure 3.2 OSI in comparison to Cellular Implementation 15
Figure 3.3.1 IMS Security Architecture 17
Figure 3.3.2 Security relations between IMS and NDS/IP 18
Figure 3.3.3 Security relations within IMS and adjacent Networks 19
Figure 3.4 Different Network Security implementation 21
Figure 3.4.1 Generic configuration and examples of protocols for a secured VPN 23
Figure 3.4.2 End-to-End security in IPv6 versus IPv4 24
Figure 5.1.1 Secured applications using a public key infrastructure 33
Figure 9.3 Overview of the security architecture 51
Figure 9.3.1 Mobile Equipment registration and connection in UMTS 53
Figure 9.4.1 Mutual authentication of the user and network 54
Figure 9.5 IPSEC protecting the IP based UMTS network 60
Figure 11.1 Fraud 67
Figure 12.0 e-Commerce 69

1. EXECUTIVE SUMMARY

During the last few years, the numbers of wireless users accessing data networks have surpassed the number of fixed line users. As mass adoption of connected mobile devices ensues with the ongoing development and implementation of 2.5 and 3G networks, there is an increasingly heated competition to provide compelling user applications and services. While performance and efficiency have obvious implications when it comes to application or user acceptance, strong security remains paramount to ensuring consumer adoption as well as business success. Efficient mobile security is a critical catalyst for the widespread adoption of the wireless Internet.

First-generation wireless security architectures leveraged corporate security infrastructures that were originally designed for resource-rich computers. While these technologies are acceptable in the enterprise, they are unacceptable in the home. Ad hoc wireless networks demand sophisticated security to support today's increasingly robust user-compelling applications.

Security is very large and important, and always has a costs implication. The question that follows, is how secure does it need to be? How much are operators willing to spend on security? In this context, many features that are necessary to meet the basic security requirements can be reused to fulfil end-to-end security requirements of users on application level. The Internet has really given life to the legends of hackers who can break into pretty much any computer system and change or even destroy the content. The interesting part is that the Internet in itself is not the problem, and that eavesdropping of traffic is much more cumbersome, but still the blame for the fraud is on the network in lots of media. One of the more common mistakes that one can make when implementing security solutions is sub-optimising one part and neglecting another.

Wireless security represents the joint effort of several parties, including mobile device vendors, mobile equipment manufacturers, security vendors, wireless operators, systems integrators and consultants, the enterprise itself and ultimately, the end user. Without customer confidence, applications such as m-commerce and corporate access to confidential data simply will not take off. Email is probably the biggest single threat to business existence if it is not managed effectively and perhaps needs to be one of the key elements of a security policy. The problems range from efficient and effective cryptographic algorithms to e-commerce protocols and from secure thin clients such as smart cards to intellectual property protection. Clearly, the problem may require a different solution depending on the environment it is targeted for: a different protocol and/or algorithm etc.

Security needs broad level involvement and not unless all measures have been put in place no network is 100 percent secure. The tools and technology to stop crime are known and available, yet administrators are so overwhelmed with day-to-day IT chores that they don’t have the time for healthy security practices. What is efficient and yet practical will be based on individual judgement in finding the right solution. Absolute security is absolutely impractical.

The analysis of the work carried out in this Report, led to a debate of different point of attacks in a cellular network bearing in mind that one needs to ”Secure the users to secure the enterprise”. Security involves the perception and making the user feel safe.

While the 3G standards define many security aspects of the 3G wireless networks and include areas such as network security, smart cards, fraud detection, algorithms and

lawful interception, operators will individually look at some of most important issues that need attention.

Since, the standards bodies have addressed a number of security issues scattered in a number of different specifications, this Report gives a summary on what exist and what and where there is yet space for something to be done.

Even so, where networks have taken the right technical and strategic decisions, security risks will always remain, this report therefore helps understand the impact and typical wireless security threats and how much of security is needed in 3G (also legacy 2G and WLAN) networks. It should be added here that security should be understood as a process. It is not something that is bought/implemented once and that's it. Security needs permanent updating, monitoring and re-action. Internal security is still the biggest threat says most studies. They are likely to be more serious than external attacks for a number of reasons. Insiders already have access to the organization's network and data; the company has already invested in them some basic level of trust; they know what the secrets are and where to find them; they may have motivation to harm the company either directly or indirectly; and it is virtually impossible to prevent a determined insider from stealing data or information.

Mobile and Wireless Security's "best" practices that ensure success are designed to avoid unnecessary risks, clearly assign responsibilities and reward appropriate employee behaviour.

2. INTRODUCTION

In today's turbulent times, it is vital that "security" solutions are implemented to protect networks from within-as well as from the outside world. Ensuring adequate security and to quantify the benefits of security solutions is a very difficult task and the question that does very frequently get asked is how much of security is enough? The reality is that a compromise between security, usability and cost is normally implemented.

2.1 This Report

Security concerns are among the key obstacles to the full-scale peer-to-peer wireless networks. As wireless communication devices become increasingly ubiquitous and the value of information travelling wirelessly increases, the implementation of security architecture is ever more important. Growth in wireless security market will be fuelled as complacency and lack of security awareness gives way to growing recognition of the value of precautionary measures to safeguard corporate information. Robust security must be implemented so employees will be able to access sensitive corporate information with minimal risk. Wireless security represents the joint efforts of several parties, including mobile device vendors, mobile equipment manufacturers, security vendors, wireless operators, systems integrators and consultants, the enterprise itself and, ultimately, the end-user.

More specifically, this report concentrates on the following elements, which are of concern to the network operators and manufacturers deploying UMTS / 3G networks:

- Network
- User device
- Content
- Service provider
- Applications

It also generates a number of questions to promote an understanding of the level of security and where it needs to be implemented.

Threats related to the persons, buildings, corporate and institutions (bank etc.) are beyond the scope of this report and have not been considered. Along with concern for employees, companies are paying more attention to threats against the infrastructure that drives so much of modern business.

2.1.1 Risks and Threat analysis

Normally, there are two dimensions to security that need attention the safeguard of the user's privacy and the safeguard of the integrity of the information. As indicated in the introduction, increasingly people are using networks such as the Internet for on-line banking, shopping, and many other applications. The generic term used is e-commerce or m-commerce when using a mobile network. This often involves the transfer of sensitive information such as credit card details over the network. Hence to support this type of networked transaction, a number of security techniques have been

developed which, when combined together, provide a high level of confidence that any information relating to the transaction is received at the other end unchanged.

Therefore, in summary the concern one has is that the information received from the network:

- Has not been altered in any way-integrity;
- Has not been intercepted and read by anyone and is not stored in an insecure way such that it is not exposed to theft later on either-privacy/secrecy;
- Has come from an authorised sender-authentication;
- Has proof that the stated sender initiated the transaction-non-repudiation.

Secrecy and integrity could be achieved by means of data encryption and data authentication while entity authentication and non-repudiation require the exchange of a set of (encrypted) messages and procedures between the two communicating parties. Using encryption and data integrity protection mechanisms solve a part of the problem, it introduces a lot of other problems- it becomes impossible for intermediaries to insert information into the profile.

But even while using other services in a network one gives out a lot of information about him/herself; which also gives rise to concern that this personal information is not misused. These are for example Location and presence.

Nevertheless, there are a variety of possible security threats that need to be considered while looking at what level of security in needed in the different delivery elements of a network. Standardisation deals with some of these and looks at what the possible threats could be how they could be carried out and where in the system they could occur.[1]

The following list a few:

Violation of confidentiality (unauthorised access to sensitive data)

Unauthorised access to sensitive data by an intruder may happen. The intruder might intercept messages or access confidential data sources. In particular, intruders might gain access to users-related (transmitted or stored) data.

- Eavesdropping /listening: An intruder intercepts messages without detection and can identify and remove the protocol control information at the head of each message, leaving the message contents. The message contents, including passwords and other sensitive information, can then be interpreted.

- Masquerading: An intruder pretends to be a legitimate system entity in order to obtain confidential information. He can use a recorded message sequence to generate a new sequence.

- Traffic analysis: An intruder observes the time, rate, length, source, and destination of messages and to combine these pieces of information (for e.g. to determine a user's location or to learn whether an important business transaction is taking place).

[1] Source: 3GPP TS 21.133

- **Browsing**: An intruder searches data storage for sensitive information.

Violation of integrity (unauthorised manipulation of sensitive data): Messages may be deliberately modified, inserted, replayed, or deleted by an intruder.

Fraud

- **Repudiation:** A user or a network denies actions that have taken place (e.g. subscribers exploit the services with heavy usage without any intention to pay, subscribers deny having sent/received traffic).

- **Fraud related to the accessibility of sensitive data sources** (banking fraud, fiscal fraud, transactions fraud etc.)

- **Misuse of privileges:** A user or person may exploit their privileges to obtain unauthorised services or information.

- **Abuse of services:** An intruder may abuse some special service or facility to gain an advantage or steal a service.

- **Unauthorised use** of resources: Users may abuse their privileges to gain unauthorised access to services or to intensively use their subscriptions without intention to pay.

Denial of Service: Intruders may perform active attacks by disturbing or misusing network services preventing user or signalling traffic from being transmitted on any system interface, whether wired or wireless.

- **Intervention:** An intruder may prevent an authorised user from using a service by jamming the user's traffic, signalling, or control data. E.g. calls might be unlawfully diverted to some other destination.

- **Resource exhaustion:** An intruder may prevent an authorised user from using a service by overloading the service.

- **Abuse of services:** An intruder may abuse some special service or facility to gain an advantage or to cause disruption to the network.

Economic Loss is related to all the risk categories of this paragraph.

Theft of:

- **Identification** An intruder might try to obtain system service or confidential information using the stolen identity co-ordinates (*masquerading*) and behaving as an authorised user.

- **Documents / Information** Active attacks can be performed against sensitive information sources (unauthorised access to data stored by system entities, passive traffic analysis)

- **Theft** of data in terms of Intellectual property.

Trust: Reliability of data (authenticity of the data originator, integrity of the data contents) is endangered by the possibility that an intruder masquerades as another user towards the network or masquerades as a serving network.

Who are you? Use of a stolen terminal, with or without UICC/USIM calls for integrity of data on a terminal. Intruders may modify, insert or delete applications and/or data stored by the terminal or on UICC/USIM.

Unauthorised use of resources: Users may abuse their privileges to gain unauthorised access to perform active attacks by intensively using the network, generating lack of resources.

Viruses: Converging of mobile devices and wireless networking lead to a focus change for virus writers (today they concentrate on the widest spread PC operating systems), as mobility/ always-on connectivity of 3G devices offer viruses a faster and larger impact on the global network.

Globalisation hugely increases the number of access points and data sources, and consequently creating the above-mentioned risks.

Creating bills for the third party without getting any benefit himself.

2.1.2 Where must security measures be applied?

In order to avoid or diminish the risks described in 1.1.1, security mechanisms have to be provided at the following network points:

- Data storage (server, network, device, removable memory)
- Device / terminal
- Network

  -Access Network

  -Core Network
- Applications

2.1.3 What resources need protection?

Another key element of a successful security implementation is to identify what has to be protected by security mechanisms:

- Information (what can be accepted, what can be given, authenticity)

  -Personal

  -Corporate

  -Business
- e-money (e-balances, e-wallet, e-cash)
- Rights (Intellectual Propriety knowledge, personal rights, rights to use)
- Usage of resources (network capacity, applications, etc.)

2.1.4 How should security be deployed?

The list below summarises the security technologies currently available and where they should be applied:

- Firewalls
- Biometrics
- Intruder detection systems
- DRM (Digital Rights Management)
- PKI (Public Key Infrastructure)
- Security Protocols
- Physical security (tamper proof)
- P3P (Platform for Privacy Preferences)
- Encryption
- Fraud Management
- Virus detection /Antivirus mechanisms

The above are specific to different network points or in some cases could be used in different product/entities as listed below:

Access:

-Physical

-Networks

-Data

-Applications

-AAA (Authorisation & Authentication Accounting)

-AuC (Authentication Centre)

-HLR/VLR (Home/Visitor Location Register/SGSN)

-EIR (Equipment Identification Register) and CEIR

2.2 Security Levels

This section indicates that security has to be considered at the different network levels, going from the physical up to the application level, as shown in the following figure.

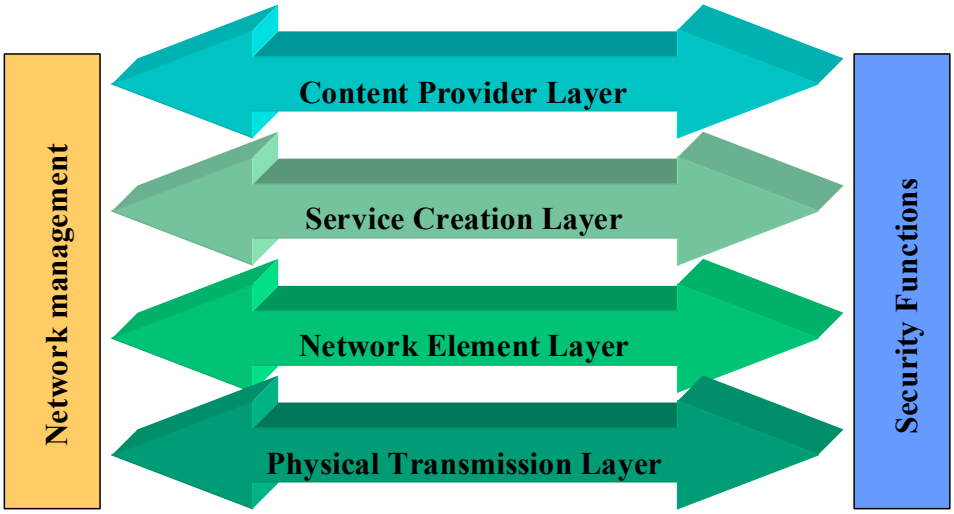


Figure 2.2 Security levels in an UMTS network

The physical transmission layer security refers mainly to the security protocols that typically offer a secure communication channel. In general, the protocols offer the security services as authentication of communication partners, confidentiality and integrity. Today there are several standardisation activities for security protocols. One of the drawbacks of adding a security protocol is the increased bandwidth consumption on the protected channel. This reflects mainly overhead in signalling in case of integrity protection but not necessarily with encryption where the same amount of data outputs an encrypted message of the same length. Nevertheless, the need for key management and computational overhead are probably at least as severe problems as bandwidth increase.

Security at the network element layer implies securing connections inside and between UMTS networks. Security gateways and firewalls are secure network elements; which may offer confidentiality, authentication, integrity and access control. Their cost has to be taken into account.

Security issues at the upper layers of service and content providers are largely independent of the structure of the UMTS network itself, but nevertheless they play an important role in the overall security of the system. More costly infrastructure, as PKI (Public Key infrastructure) could be used for generation, distribution and revoking of cryptographic keys or certificates.

So security functions can be added at one or more different network levels and is generally realised in networks, end systems and applications in parallel.

However, this impacts on the overall network architecture and network management and could be a penalty in terms of policy, costs and performance.

2.3 Scalable to meet Security Issues

Security systems have to have the capability of dealing with vastly different levels of users wanting to access systems. Scalability is at the centre of this requirement, security systems at whatever point in the network, have to quickly and efficiently

perform their function without causing the users any delay. This has to be balanced against providing the level of security required by the operator or provider of the service the user is accessing.

The use of distributed architecture within wireless portals and other wireless Internet sites provides the ability to deal with wide variation in the number of users accessing the service. Distributed architecture also allows access to all the necessary information suppliers from whichever area e.g. AAA or product supplier. The security elements similarly have to be scaleable, this requirement is more difficult to achieve. Each part of the distributed system, which may not be within the service provider's domain, has to guarantee to provide the necessary level of security, AAA and scalability when the systems are accessed.

When deploying wireless security, it is important to consider all elements involved in order to implement true end-to-end security across the whole network. A point (one hop only) solution is simply not good enough. More important, the solutions deployed should be interoperable and scalable as vulnerable points are likely to multiply.

As cellular wireless systems become used for application which require strong security mechanisms to protect personal data or data for e-commerce, consideration has to given to the capability of security mechanism to be scaleable to deal with high volumes of users at peak periods. Security has to be proportional to the both the subscriber base and network elements installed.

The security mechanism also has to minimise the number of 'turns' in communication between the wireless device and the security mechanism in order to reduce both the time taken and the cost of processing for the subscriber. E.g. a signature of a message should fit in the same message.

Cellular devices have limitation both the capacity to store, process data and execute the security mechanism, which also contributes to time problems. Where as subscribers have to consider the cost element for what they see as data not being relevant part of service which they want to use. Subscribers also have concerns about the time taken to gain access through security mechanism particularly in peak usage periods.

3. GENERAL ARCHITECTURE OVERVIEW GSM/UMTS

3.1 GSM

Mobile telecommunication networks, including the current 2nd generation GSM networks, were regarded as closed systems. They usually operate not easily available protocol stacks and signalling protocols where hardware is expensive, and use lines that are not easily accessible for the public. This is not any more the situation for GPRS and 3rd generation mobile networks, since these networks already base parts of their signalling and data communication, for voice as well as for user traffic, on IP transport.

Anyway, GSM was designed to offer a whole lot of security. Its prime goal was to be as secure as the fixed networks to which it would be connected. The utilisation of advanced cryptographic methods was one of the main advantages of the 2G digital systems (with respect to the analogue first generation). As GSM (and other 2G systems) grew successful and wide spread, both the usefulness and limitations of its security features became more evident.

For example, one GSM security limitations is that protection against so-called “active attacks”, which involved somebody who has the required equipment to impersonate a legitimate network element, was not addressed.

The security features for GSM were mainly reduced to:

- User authentication
- Radio interface encryption
- User identity and location confidentiality

The concept was to protect the user against someone, who knew the user’s IMSI (International Mobile Subscriber Identity), from misusing this information to track the location of the user or to identify calls made to or from that user by eavesdropping on the radio path.

3.1.1 Security limits of 2G

GSM does not offer a solution against the following:

- Active attacks using false base stations,
- Encryption keys (used for radio interface ciphering) and authentication data are transmitted in clear between and within networks;
- Encryption does not extend far enough towards the core network (resulting in the clear text transmission of user and signalling data across interfaces between network elements e.g. in GSM, from the BTS to the BSC, GPRS is an expectation;
- Encryption may sometimes be switched off (e.g. because some countries may not allow it) without any indication to the user;
- Some parts of the security architecture are kept secret (e.g. the cryptographic

algorithms) and therefore not reliable on the long term (global secrets sooner or later are revealed);

- As technology advances and attackers have better tools, cryptographic Keys could become vulnerable to massive attacks (when someone tries all the keys until one matches);
- Data integrity is not provided - data integrity defeats certain false base station attacks and, in the absence of encryption, provides protection against channel hijack;
- The IMEI (International Mobile Equipment Identifier) is an unsecured identity and should be treated as such;
- Fraud and LI (Lawful Interception) were not considered in the **design phase** of second-generation systems but as afterthoughts to the main design work;
- There is no HE (Home Environment) knowledge or control of how an SN (Serving Network) uses authentication parameters for HE subscribers roaming in that SN;
- Second generation systems do not have the flexibility to upgrade and improve security functionality over time.
- Going trough legacy networks lowers the global security level[2]

Some GSM security limitations were left on purpose, as it was estimated that the additional cost of the enhancements would be major than the deriving risks.

Due to a different environment and applications, a similar comparison led to a different conclusion for the UMTS case and countermeasures for the perceived weaknesses of GSM were developed.

3.1.2 Elements to be retained from 2G security

3G security retains (and in some cases develops) the following security elements of second-generation systems:

- Authentication of subscribers for service access[3];
- Radio interface encryption[4];
- Subscriber identity confidentiality on the radio interface;
- The SIM as a **removable**, **hardware** security module that is manageable by network operators and independent of the terminal as regards its security functionality;

[2] Point 10) added by UMTSF ICTG

[3] Conditions regarding the option of authentication and its relationship to encryption was planned to be tightened;

[4] The strength of the encryption was planned to be greater than that used in second generation systems (the strength is a combination of key length and algorithm design), in order to meet the threat posed by the increased computing power available to those attempting crypto-analysis of the radio interface encryption;

- SIM application toolkit security features providing a secure application layer channel between the SIM and a home network server;
- The operation of security features is independent of the user[5];
- Home Environment (HE) trust in the Serving Network (SN) for security functionality is minimised.

3.2 UMTS

UMTS, as a mobile technology, benefits from the GSM legacy in terms of protection mechanisms on the radio path. Moreover, some of the limits of the GSM protection mechanisms are eliminated by the enhancements introduced in UMTS.

However, what substantially changes in UMTS is a consequence of the business model that envisages more than one player. Content providers, Service providers, Carrier providers and subscribers have to transfer each other very sensitive information. Sensitive data transfer between parties involved in the business represents a potential security risk.

On the other hand, the added value of 3G mobile systems is mainly in the variety of new services deriving from the adoption of the above-mentioned business model.

All the new services that will need to be secured cannot be listed at the time of writing. However, the environment in which these services are likely to be developed can be described. 3G security has to secure this environment.

The environment in which new services will be developed can be characterised by but not limited to the following aspects:

There will be new and different providers of services. For example: content providers, data service providers, HLR (Home Location Register) only service providers;

3G mobile systems will be positioned as the preferred means of communications for users. They will be preferable to fixed line systems;

There will be a variety of prepaid and pay-as-you-go services, which may be in some markets, the rule rather than the exception. A long-term subscription between the user and a network operator may not be the paradigm;

There will be increased control for the user over their service profile, which they might manage over the Internet and over the capabilities of their terminal it will be possible to download new services and functions. This could mean that there will be active attacks on users (In active attacks, equipment is used to impersonate parts of the network to actively cause lapses in security. In passive attacks, the attacker is outside the system and listens in, hoping security lapses will occur). This is something we have not seen yet and may surprise a number of people.

Non-voice services will be as important as, or more important than, voice services;

The terminal will be used as a platform for e-commerce and other applications. Multi-application smart cards where the USIM is one application among many can be used

[5] The user does not have to do anything for the security features to be in operation; greater user visibility of the operation of security features will be provided to the user;

with the terminal. The smart card and terminal will support environments such as Java to allow this. The terminal may support personal authentication of the user using biometric methods.

Therefore, the protection of the information on the radio path is not sufficient anymore.

Security in a mobile network covers a wide range of possible issues affecting the supply of and payments for services. In UMTS, there are many ways in which threats and security issues like these should be considered possible between the network elements caused by:

- Mutual authentication between the user and the network.
- Signalling integrity protection within the RAN.
- Encryption of user data in the RAN and over the air interface.
- Use of temporary identifiers.

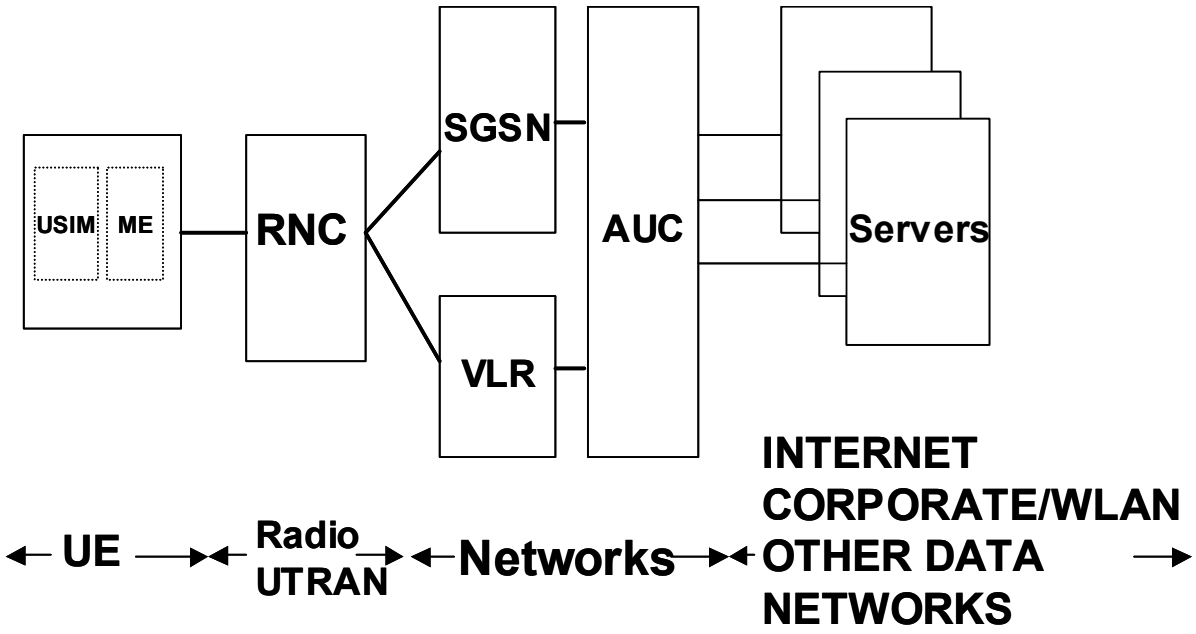


Figure 3.0 Security Architecture

UMTS standardisation is driven by 3GPP, whereas IETF is the standardisation organisation body that drives all IP (related) activities. 3GPP adopts the IETF recommendations (RFC's) with respect to the definition of the IP part of the future UMTS network. Applications are seen to be out of scope by 3GPP. Mobile applications are addressed by OMA, W3C, OASIS etc. As a result security-related Standards for Inter-working between the Application Level and Network Domain level are not sufficient and incomplete. As a conclusion, one could say that the inter-working between Application Domain Security and Network Domain Security is not completely defined and therefore operator's requirements are not fully met. This

reflects in especially the IP parts of the network but also other Enterprise and Third party networks that provide applications and content.

Active network solutions have been opposed to many of the problems caused by the increasing heterogeneity of the Internet. These systems allow nodes within the network to process data passing through in several ways, allowing code from various sources to run on routers introduces numerous security concerns that have been addressed by research into safe languages, restricted execution environments, and other related areas. However, little attention has been paid to an even more critical question: the effect on end-to-end security of active flow manipulation.

In addition, security has to be considered also on the:

- Terminal
- Software
- Personal

3.2.1 Access network security: user access security

The communication on the radio path prior to call set-up is a broadcast (Broadcast and Random Channel, however the protocol only assumes that a certain type of information can be transmitted on a link) between different elements of the Network and as such open to attacks. It is only after the mutual authentication of the user and network that a secure connection is formed.

The following are the most important interfaces:

-Secure user access to UMTS networks (AAA)

-Security of the connection

3.2.2 Network Security: network Domains

Within the network there are several areas that need to be considered:

-Security inside an UMTS network

-Security between networks that are controlled by different mobile operators/ISP's

-Security between the Corporate Networks and the UMTS Network

-Security between the Internet and the UMTS Network

Two main mechanisms are to be considered (advantages/drawbacks):

-Link-by-link protection

-End-to-end

If we consider the security in the network implemented according to the OSI (Open System Interconnection) model, we find that each layer has its own level for security.

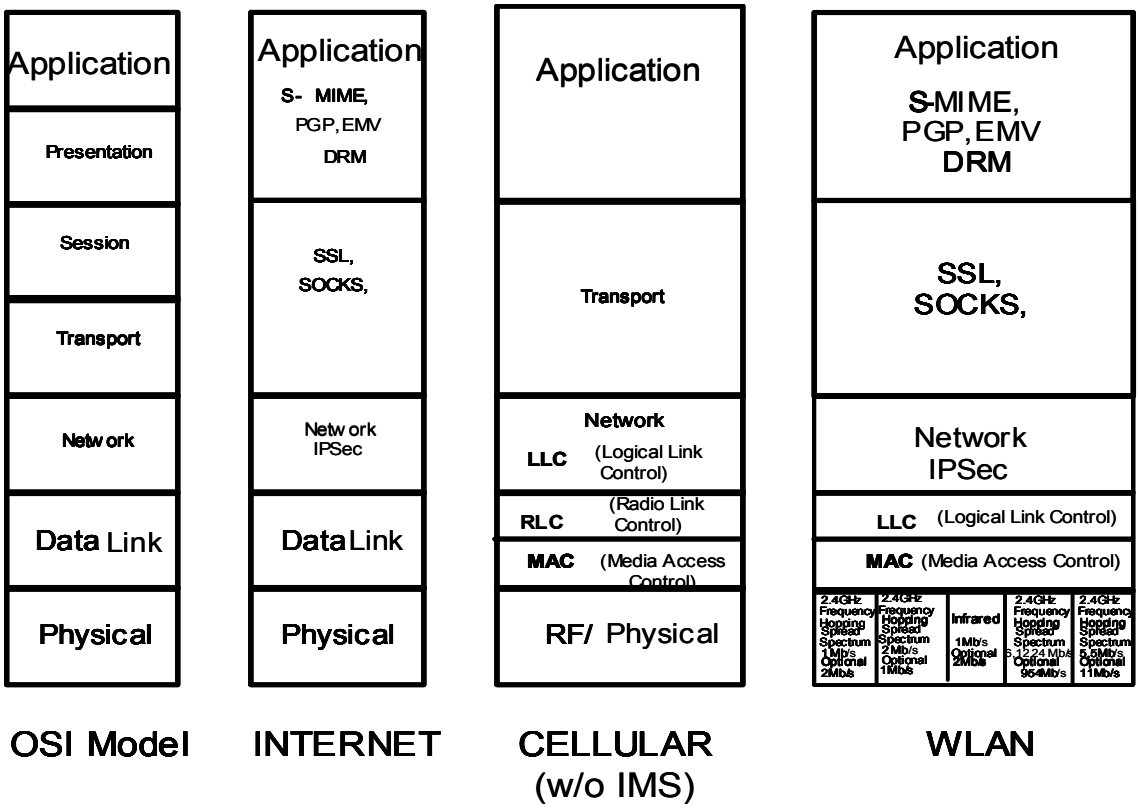


Figure 3.2 OSI in comparison to Cellular Implementation

Note that when security in the network is implemented according to the OSI model one speaks of end-to-end security in the higher OSI layers. This is also valid in IPsec (network layer) where one can also speak of end-to-end security between the devices and link-to-link (hop-by-hop) encryption along the communications path until it reaches its destination. In Cellular and other networks the level of security procedures are a little different.

3.3 Special Consideration for the IMS

3.3.1 IMS Domain Security

The IMS (IP Multimedia Subsystem) will be introduced in 3GPP UMTS Release 5 as an enhancement of the PS domain supporting IP Multimedia Services and includes the collection of signalling and bearer related network elements.

It offers Multimedia Calls, Session and Service Control, which are mainly based on the IETF SIP protocol (RFC2543).

Compared with GSM, IMS offers a decentralised architecture (single functions in single entities). Furthermore, IMS enables PLMN operators to offer their subscribers multimedia services based on and built upon Internet applications, services and protocols.

IMS also tries to achieve **access independence**. For this reason interface specification should be conform as far as possible to IETF standards. IMS offers a platform to integrate new-sophisticated services, which can be developed by the PLMN operators.

It also should be mentioned that the **IMS Domain is used to transport signalling traffic**.

User traffic (Media Streams) and signalling traffic are considered independently but it is clear that the IMS can actively influence the QoS for media streams (negotiation phase during a call setup)[6].

Development of the IMS core network itself involves the provision of several new platforms[7]:

Given the concept of IMS, it cannot be assigned to a single security area (Access, Network Domain, Application Domain, etc.)

Therefore, this section is exclusively dedicated to the standardised security features, which are applied for IMS. Most of the issues regarding Access Security and Network Domain Security are covered in the following subsections.

[6] Only the MRFP (Media Resource Function protocol) that is responsible for media mixing is fit in the user traffic path.

[7] The **Call State Control Function (CSCF**) manages the SIP session establishment and call control and forms the link to the **SIP Application Server (AS**).

The **Policy Control Function (PCF**) manages the Quality of Service policy.

The **Multimedia Resource Function (MRF)** controls the multi-party conferencing features of SIP. A **Media Gateway Control Function (MGCF)** together with a **Transport Signaling Gateway (TSGW)** perform a similar function in the mobile domain to the soft switch in a VoIP network, i.e. they enable inter-working with ISDN-based circuit switched networks including inter-working between IP addresses and E.164 numbering schemes.

The **Home Subscriber Server (HSS**) is the packet (GPRS) equivalent of the HLR in GSM and carries through from 2.5G/3G into IMS.

In addition, an MSC server could be added, which is another form of soft switch enabling this same all-IP packet switched core network to deliver GSM circuit switched services via a 2G or 3G RAN to conventional mobile terminals.

The IMS network and SIP call control place new requirements for the Telecom Management system (shown as **OAM – Operations Administration & Maintenance**) including charging applications. Terminal Management is also required as part of the OAM, in order to provide customer care for the User Equipment (UE) which will have the capability for downloadable applications.

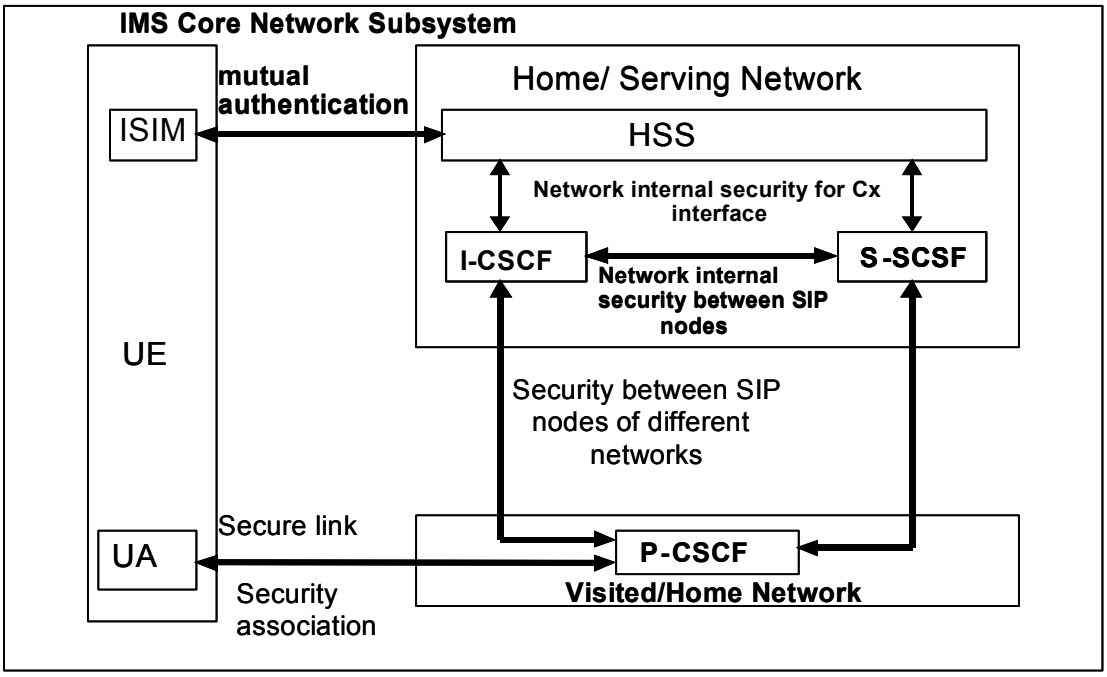


Figure 3.3.1 IMS Security Architecture

The above figure is affiliated to the security relations as defined in TS33.203, which is relevant for IMS. The IMS Authentication and Key Agreement process provides mutual authentication between ISIM[8] and HSS[9]. It is based on the same principles as the UMTS Authentication and Key Agreement (AKA) procedure.[10]

A secure link and a security association should be provided between user agent and P-CSCF[11]. Furthermore, security associations between SIP nodes as well as for the Cx interface between HSS and SIP nodes should be provided.

The IMS security mechanisms are independent from those of the CS and PS domain of the UMTS. It is still argued whether the ISIM is sitting in the same physical UICC card or as a separate one.

[8] The IMS Subscriber Identity Module defined from 3GPP Release 5 requires a separate SIM application called ISIM. Amongst other things, it stores the authentication and encryption parameters (integrity IK and encryption keys CK) used on the higher IMS application layer between the IMS and the terminal on the ME not in the ISIM after the ISIM has calculated them. In other words a terminal has to authenticate itself twice in order to run IMS services, once to the mobile network and once to the IMS.

[9] HSS, the Home Subscriber Server, replaces HLR and AuC, acting as the master database for users and providing for user security. In addition, it extends its control function to the IMS and provides for user IP addressing.

[10] The Authentication and Key Agreement (AKA) is a procedure for mutual authentication of the user and the network. Furthermore, the AKA procedure establishes keys for confidentiality and integrity protection on the network and the USIM. There are two AKA procedures – the UMTS AKA for CS and PS domain and the IMS AKA for the IM Subsystem. The names of these keys are confusingly similar to 3G AKA.

[11] The Call Session Control Function (CSCF) manages the SIP session establishment and call control. In the current 3GPP architecture referred to here, the CSCF also incorporates the Policy Control Function (PCF), which manages the Quality of Service policy. The CSCF can have three roles. The Proxy CSCF (**P-CSCF**) is the first contact point from a mobile into the IMS. The Serving CSCF (**S-CSCF**) actually handles the session states in the network and in the Interrogating CSCF (**I-CSCF**) is the contact point for connections destined to a subscriber of the network.

Authentication parameters are carried out by an Application layer protocol i.e. 3GPP SIP. This mechanism is similar to the existing UMTS AKA (Authentication and Key Agreement, refer to [TS33.203]). Compared to UMTS AKA the ISIM (IM Services Identity Module) is responsible for storing the security parameters like SQN, long term Key, CK and IK stored in the ME rather than the ISIM during a session.

This is also reflected in TS33.210.

In R5 the ISIM application shall require the presence of a USIM application on the same UICC. This shall not preclude the possibility in later releases of having an ISIM in a UICC that does not contain a USIM.

The following picture gives an overview of the existing IMS Security Network Architecture and the different security associations within this system according to the current standardisation activities of 3GPP[12].

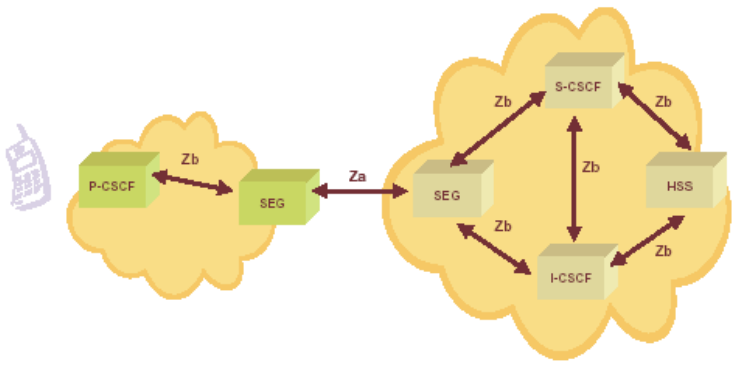


Figure 3.3.2 Security relations between IMS and NDS/IP

3GPP Security requirements relevant for IMS Core Network according to 33.210 (Network Domain Security) are as follows:

- Inbound and Outbound Signalling traffic between different PLMNs shall be conveyed securely through Security Gateways (SEG[13]). A network might have more than one SEG.

[12] 3GPP SA3.

Please note, the reference points as depicted do not comprise all IMS Zb interfaces. The following table gives an overview of all IMS Inter-domain signaling interfaces (Za), which have to be interconnected to a SEG (Security Gateway). The detailed description of the interfaces can be found below:

Mb	Interface between P-CSCF and GGSN
Mw	Interface between CSCF and CSCF of different operators e.g. between P-CSCF (visited) and I-CSCF (home). Please note the interface between CSCFs of the same IMS domain is also called Mw
Mk	Interface between two operators BGCFs
Mm	Interface between CSCF and other non-IMS IP Network. Please note this interface will not be standardized within Release 5 time schedule
Gi	Interface between MRF-P and GGSN is part of Release 5 but there's no detailed protocol specification available
Mc	Interface between MGCF an MGW. If these entities belonged to different Domains the interface is an Inter domain Interface

[13] The Security Gateway (SEG) provides security protection for the IP-based control plane signaling between networks.

- Za Security Interface between two SEG of different Security Domains
- Zb Security Interface between SEG and NE or between NE and NE of the same Security domain
- IPsec ESP protocol (according to RFC2406) shall be supported
- Tunnel Mode (according RFC2401) shall be applied
- Support of AES (Advanced Encryption Standard) Ciphering[14]

The following picture gives a rough overview of the security relations, which can occur in an IMS network (i.e. the shown relations are not exhaustive). They're affiliated to the general security requirements of TS33.210 as described above:

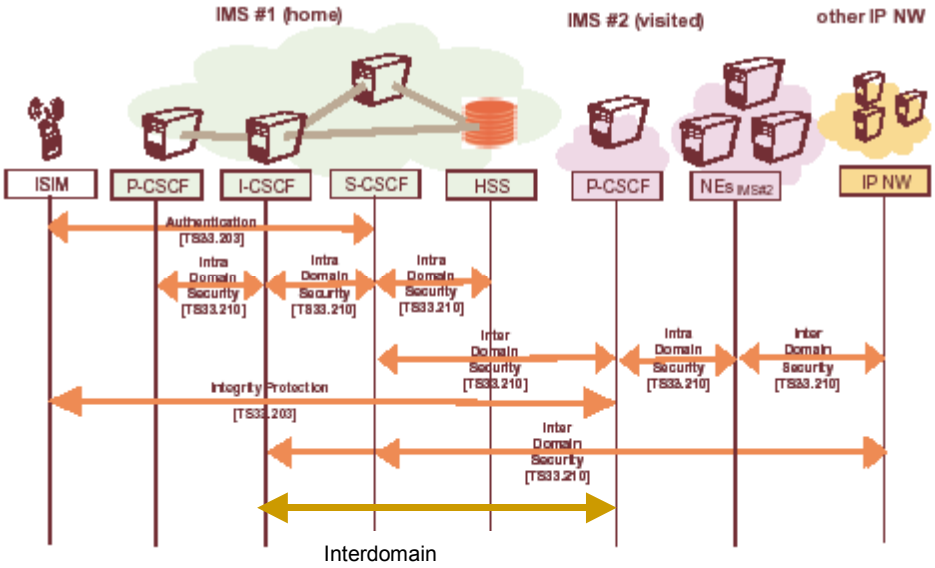


Figure 3.3.3 Security relations within IMS and adjacent Networks

Intra Domain Security is optional and left to the operator's choice.

In case of using pre-shared keys between n different domains you will need (n) (n-1) / 2 number of keys. As from one operator's point of view, only (n-1) keys are needed (the keys shared with its partners.

In case of asymmetric keys the number can be reduced to 2n (n Public Keys and n Private Keys). From one domain operator's viewpoint, it manages its own key pair and has a copy of (n-1) public keys of the (n-1) other domains.

A hybrid solution can also be envisioned where asymmetric and pre-shared keys respectively are only partially used?

Please note that in a real operator's network several S-CSCFs, I-CSCFs and maybe several HSS can be expected, which would increase the number of

[14] For Authentication AES_MAC and ESP_HMAC_SHA-1 shall be supported

security relations.

If all entities reside at the same location (Intranet) the effort of key-exchange and therefore a key distribution concept might not have to be supported.

As mentioned above, IMS is a pure Signalling Network based on SIP.

The only dependency between IMS and the transport plane is that the transport plane shall ensure the QoS of the media streams between the calling and the called party, negotiated via IMS. Furthermore, it also can be envisioned? that an IMS Network operator possesses its own transport plane.

From a standardisation perspective integrity protection and confidentiality protection in the core Network are currently not mandated for bearer traffic. The overhead for small IP packets (application dependent), which have to be secured by IPsec, is considerable high.

3.4 Security Implementations

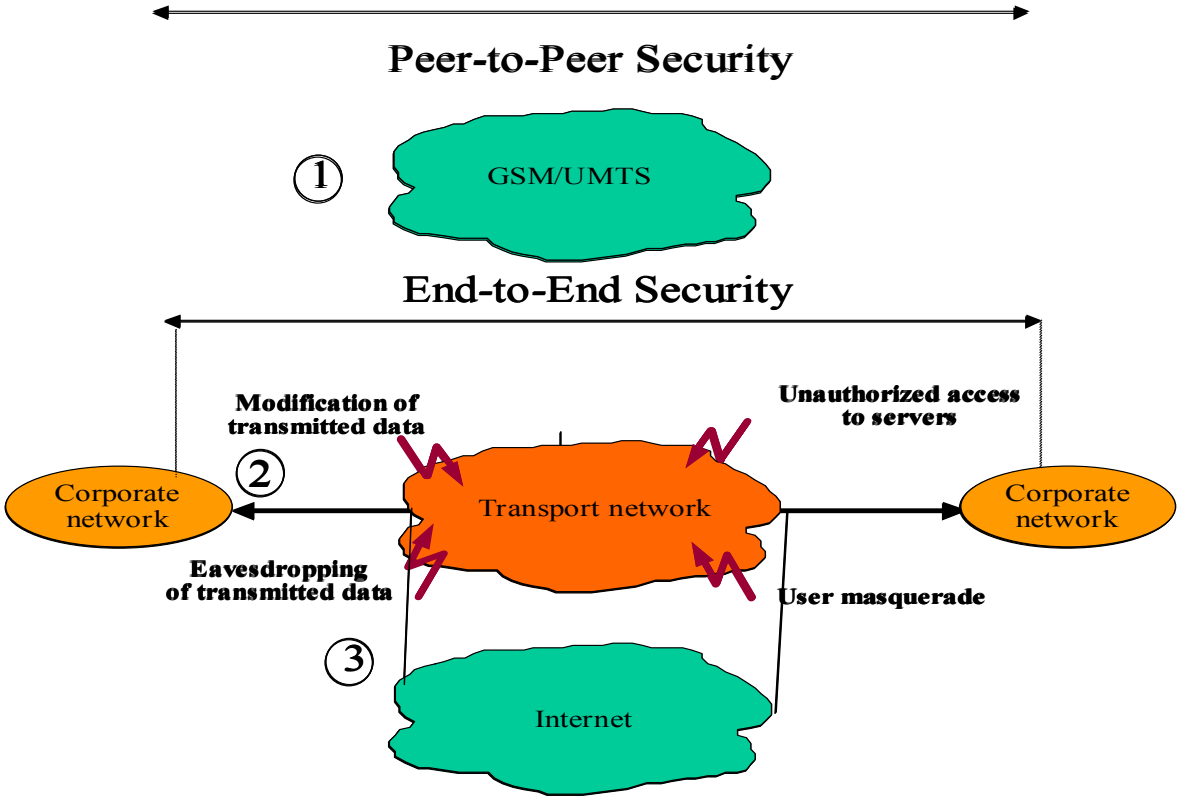


Figure 3.4 Different Network Security implementation

There are three types of networks that need to be addressed:

1. Public PLMN (Public Land Mobile Network)

2. Corporate LAN or Wireless LAN

3. Internet (a world wide public network)

3.4.1 Virtual Private Network (VPN)

A key element of secure networking is the proper design and configuration oof virtual private networks (VPNs). VPNs were originally conceived to address network security issues such as authentication, confidentiality, and integrity in fixed networks. Nevertheless, the increased user/device mobility and the new emerging integration trend between mobile and fixed networks have introduced a whole new realm of security concerns not previously foreseen. VPNs are deployed following two general schemes: the first is based on customer premises equipment, where the communicating endpoints negotiate and apply security; the second pertains to a network-based approached, where the VPN functionality is out sourced to the network operator or service provider. Currently, GPRS supports static VPN deployment between the border gateway of the GPRS core network and remote corporate security gateway. This means that VPNs are realized under certain circumstances, and cannot satisfy the new emerging security requirements introduced by mobile Internet. Furthermore, this security scheme permits the flow of unprotected data over the

GPRS backbone, exposing them to various attacks.

A VPN usually consists of the following interacting parties

- **VPN Router**: VPN Router (e.g. access router, remote access server, firewall) provides the WAN interface (on the public network side), routing functionality and filtering and are end points of the VPN-tunnel.
- **Remote Client**: Remote Clients provide remote access capabilities, e.g. for teleworkers, to a corporate network via the public network.
- **Domain Name System (DNS):** This server has the task to map Domain Names to IP addresses. This enables locating of IP nodes even if IP addresses dynamically change.
- **Public-Key Infrastructure (PKI):** It has to provide the generation, management, and distribution of so-called public-key certificates, which are used as vehicles for the distribution of the public keys and to bind these public keys to a genuine identity of their owner. Certificates are revoked too in case if they are stolen or forged and published in a certificate revocation list (CRL).
- **Policy Server**: VPNs require a security policy database specifying which security rules will be applied, e.g. encryption yes or no. An important policy function for VPNs is AAA (Authentication, Authorisation and Accounting).
- **VPN Manager:** The classical management applications (fault detection and resolution, configuration management, performance management, accounting, security management) are also important for VPNs.
- To be able to build up secure VPNs the communication between the involved parties (VPN Router, Remote client, DNS, PKI, Policy Server and VPN Manager) must be secured properly.

The VPN Tunnel should provide confidentiality, integrity and authentication.

The security protocol IPSec will play a dominant role for securing VPN tunnels.

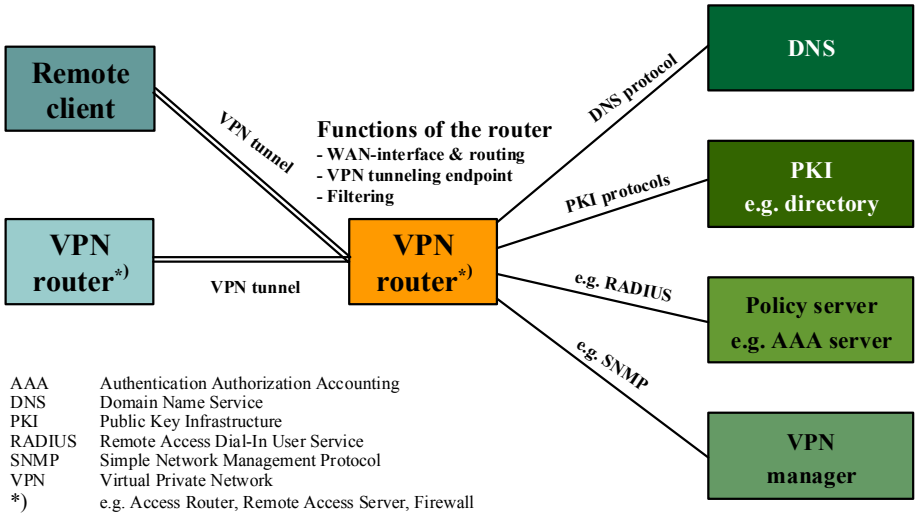


Figure 3.4.1 Generic configuration and examples of protocols for a secured VPN

VPN is commonly defined as a routed link between two or more points across a heterogeneous network topology with various degrees of security that ensure privacy for all parties. VPN provides a solution to a problem especially where the end-to-end security is broken.

The main advantages of using VPN's are:

- Increased security (coverage)
- Protection from inside attacks faster reaction to new security threats
- Enables mobility (people and devices) as well as truly distributed organisations
- Enables security as a service- both external and internal

A VPN has also disadvantages e.g. a VPN cannot protect session set up signalling e.g. information used for routing, and should a network operator trust the terminal/user to secure information that the network operator relies on for billing (There are well known over billing/channel hijack attacks which VPN cannot counter). Also, this puts the burden on the user to manage the VPN; some users would prefer (and trust) the operator to take responsibility for this, even if this means hop-by-hop security across networks.

A Virtual Private Network (VPN) is an emulation of a private network using public networks.

VPN can provide permanent interconnection of multiple sites or dynamic dial-in capability and can include the connection of external partners to an internal network (extranet scenario).

IP-based VPNs use IP as network layer protocol at the VPN peers (VPN router, remote client).

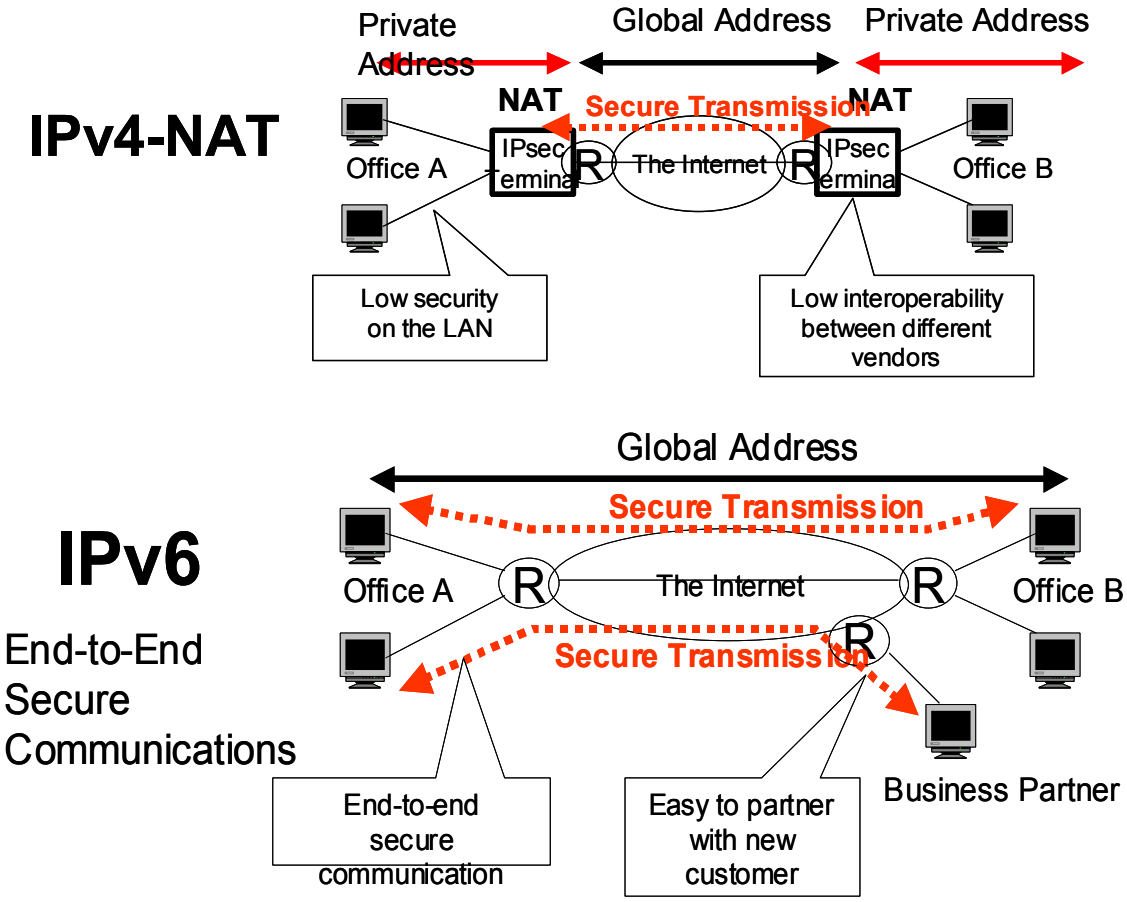


Figure 3.4.2 End-to-End security in IPv6 versus IPv4

The IPv4-NAT situation is better scalable than the architecture underneath when using pre-shared keys for entity authentication. Moreover, such a drawing better belongs to the section discussing the advantages of IPv6.

3.4.2 Internet

The Internet today provides generic communications infrastructure for packet-based communications. Several edge networks that carry both business and non-business oriented traffic communicate with each other via this public infrastructure. This public infrastructure deploys IPv4 for its network functions. IPv4 inherently lacks security. The design that is still in use today was considered a prototype that would be redesigned and extended over time. Two fundamental observations concerning security can be still identified:

- Many protocols base their security on the assumed authenticity of IP addresses and port numbers. Based on the assumption that there are networks connected to the Internet that are entirely controlled by their respective user group, we must not anticipate that any element in an IP packet is secure or cannot be read or modified. This implies that we must not trust an IP sender address or port number (not any other element in the IP or transport

header).

- Most (applications, protocols, in most cases) that use a user identification and password authentication mechanism, transmit the password in clear text or in a form that can easily decoded, such as Base 64. One-time password mechanisms or challenge/ response mechanisms are seldom used, although some standards have been developed to protected password/credential exchanges. This implies that security flaws in one of the lower protocol layers, which enable an attacker to read the data in transmission can be used to attack application programs and user accounts (i.e. the application layer).

3.4.3 WLAN security

While the WLAN industry prepares itself for a golden future, the issue of security looks like becoming a major concern. New issues encountered are highlighted by independent investigators are as follows:

- Weaknesses in the data-scrambling technique used in the 802.11b standard. The encryption approach used by the privacy standard 802.11 was badly flawed and that no matter how long an encryption key was used, it could easily be broken.

- Simple fixes to the protocol may be difficult to achieve.

- In many cases however, corporate users very often incorrectly configure WLAN, so that the wireless access points were actually inside a company's security firewall leaving the entire network and its services vulnerable to attack.

- Wired equivalent protocol (WEP), which in theory makes it difficult to access someone's wireless network without authorisation, or to passively eavesdrop on communications, most WLAN are not using WEP or have set the encryption keys to one of several well-known default values.

WLANs created by the Institute of Electrical and Electronics Engineers Inc. (IEEE), which uses Direct Sequence Spread Spectrum (DSSS) modulation for its physical layer. DSSS itself provides a security mechanism on the radio path: in order to monitor Direct Sequence systems, the receiver must be synchronised with the code used, otherwise all that would be detected would be background noise.

In addition to this, two other mechanisms are used:

- Network authentication: each user in a WLAN has an identity which is stored in each AP (Access Point); before a user can log into the network, his or her identity must be matched against the list in the AP.

- Encryption of the transmitted traffic: the used encryption technique is called WEP (Wired Equivalent Privacy) algorithm, which is standardised within the IEEE 802.11b.

Traditional WLAN security includes the use of:

- Service Set Identifiers (SSIDs)[15]

[15] An SSID is a common network name for the devices in a WLAN subsystem; it serves to logically segment that subsystem. An SSID prevents access by any client device that does not have the SSID.

- Open or shared-key authentication[16]
- Static WEP keys [17]
- Optional Media Access Control (MAC) authentication.[18]

A combination of them offers a good level of protection, but each element can be compromised.

The innumerable accounts of Wired Equivalent Privacy's (WEP) weaknesses are well known and that there are widely available script-kiddie-level tools, such as Air Snort, that can quickly crack WEP encryption. Besides, fewer than half of the networks have WEP enabled, much less IPsec or some other measure that might be safe from third graders.

Since wireless networks are practically always installed inside the firewall, so whatever protections the firewall provides are moot if an intruder comes in wirelessly. It's bad enough if a war-dialling intruder finds an unprotected dial-in port and gets inside your firewall. An 802.11b-based intruder may be connected at 11Mbits/sec, not 56Kbits/sec. There are most likely two causes for this state of affairs, beyond the network managers who don't care if anyone in a quarter-mile radius can access their networks, and those forced to install a wireless network without effective security despite their objections. First, many people underestimate the distance over which 802.11b radio signals can be picked up. Second, many wireless networks are being set up informally by users who don't know or care what WEP is or what a firewall blocks out.

Currently installed WLAN security is not sufficient for the enterprise organisation, while it could be acceptable for very small businesses, or those that do not entrust mission-

---

By default, however, an AP broadcasts its SSID in its beacon. Even if broadcasting of the SSID is turned off, an intruder or hacker can detect the SSID through sniffing.

[16] The 802.11 standard, supports two means of client authentication: open and shared-key authentication. Open authentication involves little more than supplying the correct SSID. With shared-key authentication, the AP sends the client device a challenge text packet that the client must then encrypt with the correct WEP key and return to the access point. If the client has the wrong key or no key, authentication will fail and the client will not be allowed to associate with the access point. Shared-key authentication is not considered secure, because a hacker who detects both the clear-text challenge and the same challenge encrypted with a WEP key can decipher the WEP key. With open authentication, even if a client can complete authentication and associate with an AP, the use of WEP prevents the client from sending data to and receiving data from the AP, unless the client has the correct WEP key.

[17] Another type of key that is often used, but is not considered secure, is a "static" WEP key. A static WEP key is a key composed of either 40 or 128 bits that is statically defined by the network administrator on the AP and all clients that communicate with the AP. When static WEP keys are used, a network administrator must perform the time-consuming task of entering the same keys on every device in the WLAN. If a device that uses static WEP keys is lost or stolen, the possessor of the stolen device can access the WLAN. An administrator won't be able to detect that an unauthorized user has infiltrated the WLAN, until and unless the theft is reported. The administrator must then change the WEP key on every device that uses the same static WEP key used by the missing device. In a large enterprise WLAN with hundreds or even thousands of users, this can be a daunting task. Worse still, if a static WEP key is deciphered through a tool (like AirSnort), the administrator has no way of knowing that the key has been compromised by a hacker.

[18] Some WLAN vendors support authentication based on the physical address, or MAC address, of the client Network Interface Card (NIC). An access point will allow association by a client only if that client's MAC address matches an address in an authentication table used by the access point. But MAC authentication is an inadequate security measure, because MAC addresses can be forged, or a NIC can be lost or stolen.

critical data to their WLAN networks.

Therefore, IEEE 802.11i Task group is currently focussed on enhancing the standard's security features by using standard 802.1x[19], which provides mutual authentication procedures (to be negotiated[20]between the client and the authentication server) and dynamic per-user, per-session WEP keys. Several 802.1x authentication types exist, each providing a different approach to authentication while relying on the same framework and the Extensible Authentication Protocol (EAP) for communication between a client and an AP.

3GPP/WLAN inter-working will be included in 3GPP from Release 6, which focuses on a simple WLAN bearer. From release 7 on, WLAN should be able to provide session continuity with UMTS, so WLAN should offer the same security level as UMTS.

[19] The IEEE has adopted 802.1X as a new standard for authentication on wired and wireless networks; 802.1x was demonstrated in November 2000, while EAP-SIM/802.1X was first demonstrated in February 2002.

[20] Clear, WEP, TKIP (Temporal Key Integrity Protocol), AES

4. SECURITY AND PRIVACY WITH IP

4.1 Background

The Internet today provides generic communication infrastructure for packet-based communications. Several edge networks that carry both business and non-business oriented traffic communicate with each other via this public infrastructure. This public infrastructure deploys IPv4 for its network functions. IPv4 inherently lacks security. There have been a variety of exploits on end systems due to the protocol design as well as implementation problems resulting in substantial loss of revenues. IPsec [RFC2401] supplements IPv4 for the security needs at the network layer. IPv6 the new version of the IP, as part of its basic design has security integrated into the network layer. It is the same IPSec that is integrated into IPv6.

The security needs addressed by the IPSec Server the data privacy and integrity needs of the data in transit across the Internet in addition to providing authenticity of the data. Traditionally, the term security addresses *privacy, authentication, integrity* and *secrecy*.

IPSec provides for these needs. Consequently, IPv6 provides for these needs. Such needs are a critical requirement for enterprises that use the Internet or Internet like infrastructures for their day-to-day business.

IPv6 is expected to re-enable peer-to-peer applications. Security will therefore play a very natal role in sustaining this attribute.

4.2 Current Security and Privacy Issues

Hosts and devices on IPv4 networks are subjected to various attacks such as identity impersonation (referred to as spoofing), loss of privacy, loss of data integrity, communications monitoring, and denial-of-service. Such attacks are the result of discovering exploits that emerge from the implementation of protocols and applications.

While the objective of introducing security mechanisms in IPv6 is to ensure data privacy and authenticity, the mere usage of these security mechanisms may not render the end-to-end communications fully secure, forever. However, the framework provided by IPSec is generic enough to allow a change in the security mechanisms without a major change in the framework.

4.3 Security with IPv4

IPv4 has no security mechanism inbuilt into the protocol by design. IPv4 is used in conjunction with IPSec to provide security at the network layer. The use of IPSec has resulted in tunnelled traffic for Virtual Private Network (VPN) implementations. VPNs have become popular due to the technical and economical benefits that accrue when the edge networks use a public Internet infrastructure, instead of setting up a captive network infrastructure, to interconnect and communicate privately.

4.4 Security with IPv6

IPSec is mandated and integrated into the protocol. Every implementation of IPv6 is

expected to support IPSec as part of the protocol. IPSec implementation in IPv6 is achieved by means of two optional extension headers (ESP & AH) and cryptographic key management. Using these extension headers in different combinations can provide some or all of the security services such as data integrity, authenticity, confidentiality, and protection against spoofing and session replays. These secure services are provided using symmetric/asymmetric key mechanisms. Hence, there is a need for security key management framework [ISAKMP] [IKE] [IKEv2] to make an end-to-end secure communication truly happen. Therefore, a Public key Infrastructure (PKI) is required for wide scale deployment of security infrastructure across the Internet. Note that UMTS makes use IPv6 and IPsec, without the need for a PKI e.g. SIP in 3GPP IMS uses IPsec, with session keys derived from a symmetric key K in the ISIM.

The PKI will function as an authoritative source for certified keys of hosts and services on the Internet and somewhat similar operationally to the DNS service [BIND]. There is no accepted standard for PKI and therefore a lack of deployed PKI mainly because of the perceived complexity and cost.

Current day implementations use static key allocations and often do a manual exchange of keys.

4.5 Privacy

While privacy of the data in transit is assured, the privacy of a network layer session (defined as set of IP datagram's for the duration of communication between two end hosts) depends on the choice of the mode of transfer-tunnel mode/transport mode. A local IPv6 peer's packet destined to a remote peer is encapsulated in an IPv6 packet generated at the local network's tunnel end point. With the payload of the tunnel's packet encrypted, the traffic between the local and the remote peer is completely hidden. Given the fact that the session between the peers occurred is completely hidden from an intruder on the tunnel, the session can be deemed as private. In contract, using transport mode will ensure that the data transferred is private but will not hide the fact that the session between two endpoints occurred.

In many instances, a constant 64-bit interface identifier is used to form a global IPv6 address (stateless address auto configuration). In the event secure transfers are not used (tunnel mode/ transport mode) the IPv6 source and destination addresses are visible, rending the fact that an immediate snoopers can notice the occurrence of the session itself. In cases where the devices move between networks, it then becomes possible to track the movement of the device and hence the sessions it participates in. This is considered a serious threat to privacy, especially for mobile/wireless users. RFC 3041 is proposed as a solution to this. This solution involves the use of a pseudo random number as an interface identifier that changes over time, to generate an IPv6 address. This would make it difficult for the intruders to detect or track a given device.

4.6 Implications of security above the transport layer.

All end-to-end (the two end points) security models today inherently imply security above the transport layer. The use of SSL, PGP, S/MME and similar mechanisms at the applications layer secure the data in transit and perhaps authenticate the peer application. Additionally, link layer security mechanisms ensure privacy on the physical communications link, hop-by-hop. IPsec in IPv6 implies security at the network layer.

It complements the security mechanisms at the other layers and does not eliminate the need for them e.g. application layer cannot protect session set up signalling e.g. A and B party numbers, APN's used for routing and would a network operator trust the terminal/user to secure information that the network operator relies on for billing. However, network layer security cannot necessarily protect the user data i.e. the user may not trust “a chain” of network operators to maintain security on each and every link or may consider potential access to the data by a specific operator as a threat e.g. a business rival.

With IPSec in IPv6, applications can choose to use the network layer security. This implies that applications that do not want to use the security features of IPv6 can still work on IPv6 infrastructure.

4.6 Applications

Business applications such as e-commerce, m-commerce applications, e-business applications etc., will benefit the most by taking advantage of the IPv6 security infrastructure.

Since IPsec (i.e. security at network layer) alone does not give a complete response to security threats in end-to-end m/e-commerce applications, which always use specific application-level security mechanisms.

They can authenticate and secure all the transactions by using the various secure services provided.

Peer-to-peer applications are based on a many-to-many model as opposed to the one-to-many model of the client-server applications. End-to-end security is a key requirement for peer-to-peer applications such as VoIP, video conferencing etc. Deployment of IPv6 will enable such end-to-end security mechanisms over the public Internet.

Home networking is gaining momentum. Typically, the home needs to be connected to the public Internet to enable access away from home. It is very critical to secure data to and from these home networks. IPv6 (with the IPSec support) will be the favoured network protocol for such home networks.

4.7 Network Management & Billing

Network management data is collected to analyse and monitor the traffic across the network. This information is strategic to decision makers in the corporate and hence the need to secure such data. On the other hand, from the service provider perspective billing data collected to bill subscribers for the services provided is very critical. This data needs to be absolutely secure and authentic, else it would result in inappropriate billing and revenue losses. IPv6 security fits the need here.

4.8 End-to-end security infrastructure

To ensure that every end-to-end session is private in the real sense of the word, a large support infrastructure to support security is required. A public key infrastructure (PKI), much like the existing DNS service, with the objective of providing certified public keys for every potential IPv6 host is required. An IPv6 host that intends to communicate securely with a remote host will require to have the latter’s public key to begin a secure communications. Such a service requires to be made available.

4.9 Intermediate security infrastructure

Firewalls are intermediate systems used to restrict access based on several parameters such as source IP, destination IP, port information etc. In case of applications employing IPSec to provide end –to-end security, this information will be encrypted and hence may not permit typical firewall functions. Therefore, there can be two possible scenarios evolving:

Firewalls still functions as perimeter security devices and hosts behind the firewall arm themselves with *Intrusion Detection Systems* so that they complement the perimeter security.

Current Intrusion Detection Systems may not be fast enough to prevent exploitation of “one shot” messages used in GSM/3G e.g. certain MAP messages carried over IP, that remove service from specific customers or large groups of customers.

Firewalls are completely replaced and every host is responsible for its security.

This assumes that the threat is interception/manipulation on the link between the hosts (IPSec is good at addressing this). What if the system administrator goes “rogue” or the application on the host is compromised e.g. IPSec will not help.

Business applications will benefit the most from the IPv6 security infrastructure as they can secure the data and authenticate the clients as well as the client applications. Clearly, the integration of security and privacy mechanisms into the basic protocol will prove advantageous and provide a hitherto inexperienced advantage-an authenticated originator!

5. SECURITY TECHNOLOGIES

UMTS relevant security mechanisms are mainly standardised by 3GPP and IETF (IPSec, TLS etc.). Beside this it is important to consider also, those network functions that are part of an operator's UMTS network while being outside the scope of 3GPP standardisation (e.g. Routers, DHCP Server etc.) Particularly the increasing use of IP-based protocols and applications in mobile networks exposes those to additional threats, and opens up possible new security gaps.

5.1 Infrastructure

5.1.1 Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is an electronic security technology, which uses a pair of (converse) cryptographic keys:

- Private key- this is unique to its owner/user, and is used to open/decrypt messages sent to him/her in confidence over the PKI infrastructure. The owner/holder can also use the key to digitally sign his/her messages before sending them over the Internet or Network. These digital signatures play the same role as hand written signatures in the real world, enabling the authentication of parties in online communications and non-repudiation.

- Public key-This is the converse of the private key, and is made available to everyone via a public directory. Note that the security required to protect this public key from substitution by an intruder who wants to forge a users signature, is far from trivial, despite what the textbooks say. Certificates are just the start. Anyone wishing to send messages to third party in confidence should use the intended recipient's public key. In PKI-based e-communications and transactions, the sender accesses the public directory to find the intended recipient's public key and then uses this to encrypt the message. As only the recipient's private key-which is known only to the recipient- will be able to decrypt this message, true confidentially is ensured during online transmission.

Another important application of PKI technology is to exchange securely shared secrets that can in turn be used to protect communications between the two entities.

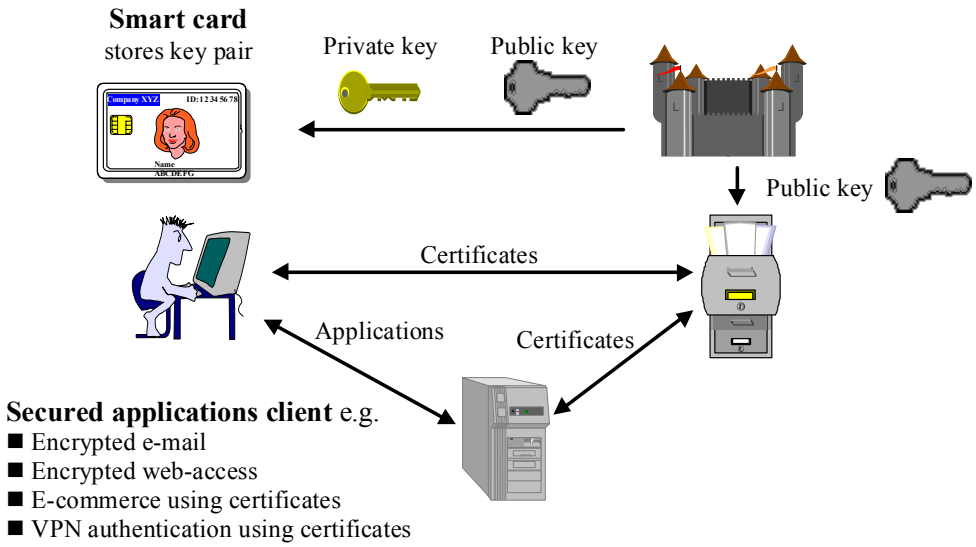


Figure 5.1.1 Secured applications using a public key infrastructure

Secured applications using a public key infrastructure protect the assets of a company in today's networked world.

Inversely, when a private key holder wants to authenticate himself/herself online-say to make a payment- he/she can sign the message digitally using his/her private key. The recipient can validate the signature using the sender's public key.

In practice, such authentication is achieved using digital certificates- digital identity certificates, issued by an independent, trusted third party, which assumes the role of Certificates Authority. When issuing digital certificates to potential users of a PKI-based infrastructure, the CA signs each one digitally using its own private key. This serves as its rubberstamping of each individual user's identity, and provides the authentication needed for e-transactions between two parties who do not know each other. Effectively, both parties take the word of the trusted third party in relation to the authenticity of their e-business/e-commerce counterpart. A hierarchy of CAs can be used and/or different CAs can cross-certify each other.

A variety of PKI deployment types are available to businesses today, such as in-house PKIs, out-sourced PKIs and certificate authority (CA) services provided by trusted third parties (TTP). One needs to work out which of these solutions suits his business needs best and at what cost. A good PKI should be invisible to its end users.

5.2 Firewalls

Firewalls are common mechanism to guard against security threats in the Internet. In addition, in corporate environments these can be seen as a device that separates and protects your network, in most cases, from the Internet. It can restrict traffic to only what is acceptable and allows monitoring so you can see what is happening. Firewalls enforce a security policy by establishing a single point for security decisions to be made. They also limit exposure to the Internet, and allow you to log traffic.

Firewalls can't do many things. They can't protect against malicious insiders. If someone wants to copy your data onto a disk and walk out with it, the best firewall known can do nothing about it. Similarly, firewalls can't protect connections that don't pass through them. If someone has a dial out modem, there is nothing the firewall can do to protect this connection. In addition, perhaps most important, firewalls can't set themselves up. All firewalls need some measure of configuration, log analysis and up-dating and all networks are slightly different. A misconfigured firewall may give you an illusion of security, which might entice you to act as if you're protected when you really aren't.

Prior to the explosive growth of e-commerce, firewalls were sufficient for most part. It was possible to configure a single firewall to prevent unauthorized traffic coming into your company because the rule was simple: No traffic is allowed into your corporate site, unless that traffic originated from within the inbound response, granting it permission to enter the network. This is known as a stateful inspection firewall. However, that traffic model has changed. A single firewall no longer can protect today's corporate environment. An electronic presence is imperative in business today, and we now encourage external traffic to come into our networks. They come to purchase our products, to access our services; and to see our marketing messages.

A single firewall is no longer considered sufficient. Multiple firewalls are required and

the rationale is three-fold:

- Different *types* of firewalls (proxy vs. stateful inspection) can offer better protection. It becomes exponentially more difficult for a hacker to get through multiple types of firewalls.

- Using multiple firewalls from different vendor's offer enhanced protection. No two vendors could possibly design and implement their firewall code (software) exactly the same way. By taking advantage of that fact, you are enhancing perimeter security.

- The third reason for using multiple firewalls addresses performance and scalability issues: More boxes translate into more horsepower. Not only use the firewalls in single file, but multiples of them in parallel to manage the workload. Then Firewall load balancers typically are used to evenly share the traffic amongst the firewalls.

5.3 Cryptography

5.3.1 Symmetric Private Key Cryptography

Shared Secret Symmetric Key Cryptography plays a vital role in securing telecommunications and digital transactions. This is especially true for devices with constrained memory and minimal processing power: smart cards, USB tokens, PDA's, cell phones, MP3 players, etc. Faster, smaller and more efficient cryptographic algorithms, scalable from tiny devices to high-end machines, are needed.

AES is expected to replace Data Encryption Standard (DES) algorithm and supports key lengths of 128, 192 and 256 bits. IETF (RFC 3268) promotes the use of AES as add-on to the TLS protocol (Transport Layer Security) for forward secrecy.

Besides AES there are many other cryptographic algorithms that are not described in this report but can be found in different literature.

Examples include Rivest-Shamir-Adleman (RSA), and Elliptical curve algorithms.

At the algorithmic front, the cryptographic community is celebrating the establishment of the Advanced Encryption Standard (AES), which replaces the DES at the top of the symmetric algorithms.

Cryptography becomes an inevitable part of our life in the new millennium. Indeed, cryptographic security is a keystone for the Internet, for electronic payment, e-commerce, and mobile commerce.

RSA keys supports 1024 and 2048 bits, but public key is problematic for radio transmission system e.g. appending a 40 bit-signalling message with a 2048 bit signature and the need for the SIM to do 2^{2048} operations. Nevertheless, Elliptic Curve Cryptography can reduce the length of the key needed and the number of processing operations needed.

The RSA still remains a very popular and widely used public-key crypto-algorithm. However, due to their superior characteristics, crypto-systems based on elliptic curves have become a serious competitor for RSA. Asymmetric cryptography is characterised by its specific use of keys: Each participant of an asymmetric crypto-system is endowed with a pair of keys - a private key and a public key. The security of such a

system is based on the difficulty of computing the private key from the corresponding public key. In all currently known asymmetric crypto-systems, this task is related to a mathematical problem that is assumed to be very difficult to solve. The main achievements of asymmetric cryptography are “Creation of digital signatures”.

5.4 Protocols

5.4.1 IPSec

The IETF IP Security Protocol Working Group (IPSec) developed a security framework to protect client protocols of IP at the network layer, providing cryptographic security services that flexibly support combinations of authentication, integrity, access control, and confidentiality. The major specifications were completed in November 1998. Since then, the IPSec framework has gained wide acceptance as the standard solution for setting up secure IP communication, e.g. in VPN scenarios. For any fully conformant IPv6 implementation, support for IPSec authentication header (AH) and encrypting security payload (ESP) is mandatory.

Therefore, IPSec (IP Security) is a collection of inter-operating standards to provide IP level security between communicating entities. It incorporates a number of mechanisms to provide authentication, data integrity and confidentiality but does not mandate particular algorithms, (which algorithms to use can be negotiated but some algorithms are mandatory to implement (required by the IETF standard) or key management policies.

Highlights of the standards are:

- Communicating entities negotiate and maintain a security association (SA), which defines how security issues are to be managed between the entities.

- The resources (processing/memory) required negotiating and maintaining a security association may be taxing on the phone architecture and may only be feasible on a ‘higher end’ phone;

- A centralized element in a telephony network topology (a call-manager/MGC in a stimulus architecture or a gate-keeper in a functional architecture) could be heavily burdened in maintaining a large number of security associations. This could be catastrophic in a system initialisation or fail-over scenario when a large number of endpoints could be trying to negotiate security associations simultaneously;

- Depending on where the security associations are maintained, end-to-end traffic may traverse several security associations each with its own decrypt/encrypt pair, which may increase communication latency;

- IPsec tunnels are mostly terminated on the NAT box. In this case there is no problem. In tunnel mode the outer addresses are in the clear (not encrypted). Problems arise (among other things) when the IP header (including the addresses) is integrity protected. The NAT cannot change addresses because then the MAC would not be correct anymore. Port numbers can be encrypted. NAT is typically more of an issue for transport mode. In tunnel mode configuration environments, the NAT is usually located jointly with the IPsec tunnel endpoint so that this is not an issue. It should be also noted that not only encryption is an issue to NAT but also authentication/integrity as it prevents any change to the packet content (which typically contain port

numbers, IP addresses, checksums based on IP addresses).

The most common application of IPSec is to run "secure IP tunnels" between hosts, remote hosts or gateways. IPSec ESP tunnels are the basic building block of many of today's IP VPN solutions.

The notion "IPSec" is often used to denote the protocol securing these IP communications. However, IPSec is not a single protocol, but a complete protocol suite instead, defining different protocols that provide for different services.

Currently IPSec is the most widespread solution to transparently secure IP traffic. For a variety of scenarios and network configurations, IPSec is an easy solution but several IPSec usage limitations exist. These originate from the scope of the IPSec specifications, as well as from conflicts with other IP-based protocols and mechanisms.

5.4.2 IPSec, NATs and Firewalls

In the IP world, devices that operate between the sender and the receiver of an IP packet are often called "middle boxes". These consist of firewalls and NAT (network address translation) devices as common entities in today's network infrastructure. Without special care of the configuration of both IPSec and such middle boxes, conflicts between these instances are most likely to occur.

For integrating IPSec into existing network architecture it is important to keep in mind that ESP encryption "scrambles" the upper layer protocol headers. Therefore, it is not possible to read header information of protocol layers above IP, e.g. the TCP port of ESP encrypted packets, which is normally required by firewalls. Current firewall products usually offer IPSec support and therefore combine the benefits of both technologies in case an IPSec tunnel endpoint is located at the firewall itself.

It is a well-known fact that IPSec conflicts with NAT devices. Despite the major efforts in the IETF to solve this problem, the protocols simply have conflicting goals.

While both IPSec ESP and AH protect the IP packet payload against modifications, IKE creates a challenge as it uses the IP address as entity identification in its payload.

NAT's modify IP header parameters and possibly also TCP headers; intermediate NAT devices usually break IPSec integrity protection. These facts should be considered carefully when designing an IP network infrastructure using both IPSec and NAT.

However, these properties relate to the most general scenario for IPSec with an arbitrary infrastructure between the IPSec peers. IPSec running between gateways of two security domains usually do not conflict with NATs or Firewalls, as the gateways are likely to include and harmonize such functionality.

5.4.3 Automated key exchange with IKE

ESP and AH use symmetric cryptographic mechanisms to secure IP traffic, which means they require secret keys, shared between the peers. One main reason for dynamic key exchange protocols is that such shared secret keys should be changed frequently, e.g. after a few hours.

In addition to pure key exchange, it is necessary to dynamically agree on several parameters, like the algorithms to be used. Any key exchange protocol for IPSec must be able to negotiate SAs instead of session keys only. As a key exchange protocol must secure its own negotiation process, it requires keys for itself. These are usually long-term keys different from the IPSec SAs to be negotiated.

For the dynamic negotiation of security associations IPSec uses the Internet key exchange (IKE) protocol [IETF2409] as the default mechanism. However, IKE does not have to be used. E.g. SIP in 3GPP IMS uses IPsec with session keys derived from a symmetric key K in the ISIM.

IKE defines exchanges consisting of a fixed number of messages and runs them over UDP. Both peers may initiate IKE exchanges.

All the different exchanges can be assigned to two protocol phases. IKE phase 1 creates a secure authenticated channel between the IKE peers. The security of phase 1 is based on long-term keys. IKE phase 2, which runs through this secure channel, is used to create the IPSec SAs required for AH and ESP.

The two-phase design mainly follows performance aspects. Phase 2 can be executed very quickly, and repeatedly, over the same secure channel established in phase 1.

For phase 1, IKE uses an authenticated Diffie-Hellman key agreement mechanism. The standard currently defines four different methods to authenticate the IKE peers. However, only two of them are used in practice (digital signature and pre-shared key). All these exchanges can be run either in main mode, requiring six messages, or in aggressive mode, requiring only three messages. Only main mode offers a limited protection against denial-of-service attacks by adding cookies to the messages.

Currently the IETF is defining IKEv2 .

5.4.4 Limits and unsuitability's of IPSec

IPSec / IKE provide a flexible framework for securing information flows over IP; however one has to bear in mind the various prerequisites and restrictions. For a number of deployment scenarios there are solutions that are better suited to address the particular security issues. Some important points of concern are discussed in this section.

5.4.5 Protocol overhead of IPSec

IPSec requires additional bandwidth, which might be considerable, compared to the original unsecured packet flow, depending on the average length of the packets. For the IPSec ESP mechanism used in tunnel mode, a new IP header has to be added as well as an ESP header and trailer which adds an overhead of at least 30 bytes, but probably of 60 bytes and more. In case of a comparable average packet size (e.g. non-multiplexed VoIP packets are typically of size 75 bytes), the bandwidth requirements might even double due to the use of IPSec. For larger average packet sizes, this overhead decreases however accordingly (e.g. for multiplexed VoIP packets, i.e. RTPmux). In summary, one has to be aware of the additional resource requirements for security.

5.4.6 IPSec requires special HW

The IPSec encryption processes need considerable resources inside the network

elements. For wire speed performance, special purpose hardware has in general to be deployed, which corresponds to additional costs. For any particular case, there is a trade-off between the deployments of IPSec over public connections vs. private network connections without the need for IPSec. This might not necessarily be the case on client platforms that only handle their own encryption/decryption traffic.

5.4.7 IKE authenticates nodes, not people

IKE is suited for automated authentication of network elements, but it does not specify methods for the authentication of persons to administrational terminals or NEs, e.g. via keywords or biometrical properties. For human user authentication, a number of different authentication solutions exist. Note that support of legacy authentication mechanisms for human users are supported in many products thanks to the (non-IETF-officially-approved) xauth mechanism that fits into IKE. IKEv2 tries to support legacy authentication mechanisms to authenticate users.

5.4.8 IPSec and IKE do not prevent DoS attacks

IPSec / IKE deal with a number of attacks on the network E.g. replay, spoofing and man-in-the-middle attacks. Denial-of-Service attacks, where a network element is confronted with a large number of service requests, are generally regarded as very hard to be countered. Like other security protocols, IPSec cannot provide full protection from DoS, but IKE offers only means for a limited DoS protection. In addition, IPSec is not meant for providing packet filtering or any Firewall functionality.

However, it is quite common to operate IPSec together with firewalls at the network border, and most firewall products offer some IPSec support.

5.4.9 IPSec does not provide application-layer end-to-end security

IPSec (/ IKE) operate on the network layer. As such, the protocols are not in general suited for end-to-end security. In particular, if different transport mechanisms (The term “transport” in IETF sense refers to TCP/UDP layer of the stack (layer 4). PPP is layer 2. IPsec is layer 3.5 and using different layer 2 protocols (e.g. PPP one end and WLAN or UMTS on the other end) does not prevent you from using IPsec end-to-end.)are deployed on the way (e.g. PPP or GSM) for end-to-end security, a mechanism is required which operates on (or above) the transport layer. The most common example for a layer-4 security mechanism is Transport Layer Security (TLS). A common application of TLS is for example HTTP (HTTPS). As opposed to IPSec, TLS is able to secure a particular application, identified by the TCP session. TLS does, however, not work for UDP based protocols like DNS, L2TP, or PPTP. It can therefore not be deployed for VPNs or VoIP (as far as the latter is transported over RTP – UDP).

Secure transport of emails has to be performed on layer 7, since emails are delivered to email servers or gateways, which are basically application programs. Since there is no connection set up between sender and receiver, the recipient cannot authenticate himself to the sender using the challenge response procedures of IKE phase I. Furthermore, the used keys and encryption mechanisms cannot be negotiated between both, as is the case during IKE phase I between NEs. All the required information has to be part of the message containing the email. For the purpose of secure email delivery, asymmetric cryptographic schemes exist which operate on layer 7, like PGP or S/MIME.

5.5 Transport Layer Security (TLS)

An Internet standard called TLS has been developed from SSL (Secure Socket Layer).

SSL was designed by Netscape Communications Corporation to provide privacy and reliability between two communicating applications at the Internet session layer. SSL used public key-encryption to exchange a session key between client and server. The key is used to encrypt the http (Hypertext transfer protocol) transaction. Each transaction uses a different session key.

5.5.1 WTLS Wireless Transport Layer Security Protocol

IETF has been working on a second version of TLS that incorporates the features required for wireless environments, hence making WTLS unnecessary (as TLS version 2).

WTLS is based upon the industry standard transport level security protocol (TLS); formally know as Secure Sockets Layer (SSL) and to secure the transport layer in Terminals. WTLS was designed so as to adapt TLS to the perceived specific constraints of (narrowband) wireless networks like GSM. A clearer distinction should be made between WTLS and WIM, as these are two different things.

Similar to private keys in the Wireless Identity Module (WIM) is used for the application layer to authenticate the user. The user would enter a pin number to authenticate themselves with the WIM. WTLS is the binary form of TLS to reduce the overhead. “WAP GAP” i.e. if the WAP Gateway is in the operator network, decrypts WTLS and re-encrypts to TLS. One solution is to put the WAP gateway on the Service Providers site but WAP 2.0 now offers TLS end to end

5.6 PAP (Password Authentication Protocol)

PAP is a simple procedure for a peer (usually a host, or router) to establish its identity using a 2-way handshake. This operation is performed upon initial link establishment. Once the link Establishment phase is complete, an ID/Password pair is repeatedly sent by the peer to the authenticator (the node that is responsible for verifying the operation) until authentication is acknowledged or the connection is terminated.

PAP is not intended to be a strong authentication procedure, and all passwords and IDs are sent across the link in the clear. The nodes have no protection against monitoring, or security attacks. Then why use it? RFC 1334 states that it is most appropriately used where a plain text password must be available to simulate a login at a remote host. In such use, this method provides a similar level of security to the conventional user login at the remote host.

5.7 XML (Trusted Environment)

XML transaction security could be seen as a machine-to-machine validation of complex trust hierarchies added that complex XML security technology already exists, although demand for it has not yet materialised. At the moment, nobody really needs to do that however; a need will arise in the future. The implementation and experimentation is happening before the standard takes shape. IT security is in its awkward adolescence. Some parts are mature; some are in their infancy. Everything else is somewhere in between. That's where we are now. Work is on going (incl.

standards) that has developed to provide security features within XML.

Instead, XML will serve as the basis for the next phase of secure e-commerce transactions, analysts predict. Although XML security will retain the issue of trusting signers, it will deal with transactions as if they were documents, allowing companies to send purchase orders and checks via e-mail. This is a very big change, that'll be what fuels business-to-business commerce.

5.7 Intrusion Detection Systems (IDS)

An intrusion detection system contains three fundamental parts:

- Data Collection: e.g. system log data from hosts, measurements of transported data-volume;
- Data Analysis: look for typical attack patterns (e.g. TCP SYN flooding) or in general for anomalies in the traffic;
- Visualization of the analysis result so that the OAM team can decide about subsequent actions;

Intrusion detection can and should be performed host-based, e.g. evaluating the system log data. Other alternatives are network intrusion detection systems that monitor and analyse traffic in a certain sub-network. The networks IDSs are invisible for all the other entities in the network (i.e. they cannot be addressed by any other device except for the OAM network). Their main function is to analyse the traffic in the subnet preferably in real-time and notify the operator on any potentially critical observation. Current Intrusion Detection Systems may not be fast enough prevent exploitation of “one shot” messages used in GSM/3G e.g. certain MAP messages carried over IP, that remove service from specific customers or large groups of customers.

Meaningful locations for a network IDS in the MNO network are:

- The Data Management Centre
- At the Gi router
- Optionally in sub-domains (IMS, etc.)

There are number of IDS products available on the market today. Nevertheless, many organizations are investigating Intrusion Prevention Systems (IPS) instead. An IPS has the ability to block attacks in real time. Where traditional IDSs passively monitor traffic by sniffing packets off a switch port, IPSs sit inline and actively intercept and forward packets. Through inline deployment, IPSs can drop packets or deny connections based on policy settings. Traditional IDs have limited response mechanisms, such as resetting TCP connections or requesting a firewall rule change.

6. TOOLS

6.1 AAA (Authorisation, Authentication and Accounting)

Authentication is this process of proving someone's or something's claimed identity. Authentication usually involves challenging a person to prove that he has physical possession of something e.g. a smart card or that he has knowledge of something e.g. password. Authentication protocols define the message flows by which this challenge and response re sent and received by the parties being authenticated.

6.2 Certificates

A certificate basically consists of the *Certification Authorities* **(CA**) digital signature on the public key together with the owner identity, thereby linking the two together in an unambiguous way. The structure of digital certificates has been standardised by the ITU X.509 standard [X509]. In order to verify a certificate the CA's public key is needed, thereby creating an identical authentication problem. The CA's public key can be certified by another CA etc., but in the end you need to receive the public key of some CA, usually called the root CA, out-of-band in a secure way, an various solutions can be imagined for that purpose. However, there is a problem in this design. What happens if a CA issues a certificate but does not properly check the identity of the owner, or worse, what happens if a CA deliberately issues a certificate to someone with a false owner identity? Furthermore, what happens if a private key with a corresponding public-key certificate is leaked to the public domain by accident, or worse, by intent? Such events could lead to systems and users making totally wrong assumptions about identities in computer networks. Clearly, CAs must be trusted to be honest and to do their job properly and users must be trusted to protect their private keys. Trust management includes methods for assessing policies regarding issuance and handling of public-key certificates and for determining whether CAs and users adhere to these policies.

Digital certificates and PKIs represent an attempt to mimic real-world human assessment of identity and trustworthiness in an automated and mechanical fashion, but present implementations are based on a very limited trust model making them inadequate as a general tool for trust assessment and decision-making.

6.3 DRM

Digital Rights Management standards (DRM) are a significant catalyst—and barrier—for the future of custom content delivery. Essentially, DRM protects ownership/copyright of electronic content by restricting what actions an authorised recipient may take. From a content owner's point of view, the irresistible appeal of DRM is its ability to restrict access according to a set of conditions known as business rules. Files can be programmed to allow, or not allow, anything from copying and sharing to playback on various devices, depending on a given user's license.

A Digital rights Management (DRM) system has to support the following fundamental functions:

- Persistent protection of the content
- Key management

- Authentication of users and devices
- Description of usage rules
- Enforcement and execution of the above

Applications that interact with DRM systems must be tamper-resistant. If content providers are to use a particular DRM system, they must have confidence that there is not a single point of weakness that can destroy the effectiveness of the entire deployment of that DRM system. This means that every implementation and rendering application running within the environment that will handle a particular bit-stream must be certified to be compliant and robust with the DRM system specification.

If end-to-end systems are to be used for the widely varying types of applications expected for UMTS the digital rights management systems used must be very flexible, extensible and intuitive. For example the “right” should be associated with individual, not the device. DRM standards lack, most of the existing DRM technology is proprietary.

Note that DRM technology alone can never provide a 100% full proof solution. DRM technology needs to be endorsed by appropriate legislation. A lot of lobbying around this legislation has been going on and still continues.

OMA is currently working on a DRM Standard that needs to be approved and implemented in the Networks and Devices. Nevertheless, out of the current knowledge a DRM standard could be years away and until the debate is settled, no carrier could run an open peer-to-peer network unless it would be willing to track every file traveling across its pipes. Until than the Operators will try to run closed networks with select content. After the DRM debate is finally settled, the network can be opened to all content, using digital signatures encoded in copyrighted files to determine when and how much royalty is collected.

7. TERMINAL

Mobile devices, networks, and applications maintain strict performance and size requirements with which legacy security technology simply cannot comply. Public key technology is clearly required to meet the security and scalability requirements of the open systems' applications that will drive demand for wireless data services.

The mobile equipment has a strong personal character since the user always carries it with him or her, and can use it everywhere and at any time. It is therefore reasonable to expect that the mobile equipment can be positioned as a Personal Trusted Device. “The Mobey Forum” promotes the personal nature of the mobile device since it offers the following opportunities:

- To enforce a multi-channel security approach, i.e. to use the mobile equipment as a trusted device to establish a secure connection to access services over other channels. For example, authentication to an Internet service (e.g. login or transaction confirmation) can be sent from the mobile equipment to the PC through a local connection (e.g. Bluetooth) or through a remote connection (e.g. GSM). This functionality, if it turns out that proximity payments with mobile equipment is a viable approach, would become prominent.

- To provide a user-friendly and secure solution for the storage of sensitive authentication data (e.g. private keys, certificates). When applicable, sensitive data should be stored in a tamper resistant device.

Even if the mobile equipment will probably play an important role as a Personal Trusted Device, other complementary approaches could be possible.

Security mechanisms are usually optional according to standards (e.g. WAP standards). As a consequence, there is no unified set of security features implemented in the mobile phones available today on the market. MeXE defined these security features for GSM and 3G handsets, but no terminal manufacturer/ operator has required these specifications to be implemented, and the MeXE work is considered “dead”. It does require manufactures to agree a “Local PKI” which may have been part of the problem.

Whilst not taking a stand on the implementation techniques, there is a clear need to define the minimum set of security requirements that mobile manufacturers should adopt when developing devices intended to support secure mobile commerce transactions.

Peer-to-peer is highlighting a point-to-point capability and assuming that this is allowed in the future a need for, protection is needed because sharing of files is allowed under full peer-to peer example, Device to Device gaming.

Security is as weak as the weakest link. Especially I mean that the obvious tamper proof device [U]Sim has to rely on what the terminal is feeding in and it never is sure what messages are *really* sent out by the terminal.

7.1 Teminal Virus

Today’s viruses address mainly PCs and corporate computer environment. The

targets are the (most common) operating systems, as a virus writer's goal is to achieve the largest number of infections in the fastest time.

As mobile devices and wireless networking are converging, virus writers could change focus.

SMS and GPRS always-on connections could provide valid mechanisms for infection spread.

Almost every user feature in today's digital mobile phone has an impact in terms of security, and a large part of this is driven by software execution in the phone. In addition, we expect a phone to operate at all times; indeed there are regulatory obligations that require the ability to make emergency calls at any time (providing the battery has enough power and there is network coverage at the location of the mobile phone). This must be reflected in the design of both the hardware and the software.

In the more distant future not only will software download (Soft Define Radio) be targeted, but also dynamic reconfiguration of the hardware will be addressed, so that the result is that best suited to the user requirements. The consequences of moving to this type of system are enormous. The security checking procedures in the downloaded software, and in the supporting software system and environment, will need very high security requirements. Mobile Phones are vulnerable to Computer viruses. The problem emerges when the user resets the phone and then turns the phone on and off in quick succession. This disables the software in-built security capability.

7.2 Personal Trusted Device (PTD)

The mobile phone is rapidly evolving into much more than a wireless telephone; its transforming into a Personal Trusted Device (PTD), with the ability to handle a wide variety of services and applications such as Banking, payments, ticketing, and secure access based applications.

7.3 Virus

A Virus is a piece of code that copies itself into a program, and executes when the program runs. It then may duplicate itself and the reproduction infects other programs. The reproduction may not occur immediately. It might not manifest itself until it is triggered by some kind of an event, as examples a date base etc. A virus may also modify other programs. The damage of a virus may only be irritating, such as the execution of superfluous code, that degrades a system's performance, but a virus usually does damage. Indeed, some people define a virus as a program that causes the loss or contamination of data, or some other re-source. Can the loss of operating efficiency be classified as damaging? Of course, but the damage is relative. A virus may be difficult to detect or find. They may even get rid of themselves at some point.

7.4 Biometric Basics

Things you can carry, such as keys or ID badges, can be lost, stolen or duplicated. But you need to secure the biometric profile e.g. fingerprint template from substitution/ copying and more importantly the "signature" that is sent from the end user device to the network from substitution/replay. How is this protection provided? It is encrypted with a user specific key, so it does not replace SIM cards digital certificates etc

The same goes for things that you know, such as passwords or personal ID numbers. However, biometrics relies on who you are; on one of any number of unique characteristics that you can't lose or forget.

Most biometric systems can be set to varying degrees of security, which gives you some flexibility to determine access levels. Increasing security in biometric systems sometimes makes them more restrictive, resulting in an increased false rejection rate.

The net effect of false rejection rates is usually nothing more than inconvenience. However, if security is set too low, the false acceptance rate might increase, which turns out to be potentially far more serious because it involves an unauthorized person gaining access to protected resources.

The main drawback of using most biometric systems -- other than that they are often expensive is that they sacrifice some measure of personal privacy for the sake of convenience. To verify your face, finger or iris, you must have some personal information on file in the verifying system; personal data that can be stolen or made public.

Nevertheless, biometric systems are becoming increasingly popular, both as standalone security systems and as added security on top of traditional pass wording systems, largely because they are convenient. You can easily forget a password, but you'll never forget your face, finger or eye and this is part of what troubles me about biometric technology.

Fingerprint recognition requires that a template of your fingerprint actually be present in the system to verify your access. If you want to pass as somebody else, presumably you'd need to either have that person's finger with you or change the template residing in the system that verifies your print.

Breaking into a system and replacing a legitimate print with your own is not easy to do unless the system's security is poor to begin with. However, while biometric proponents stress the strength of their proprietary technologies and of biometric security in general no system is ever completely secure. And if your fingerprint, voiceprint or iris template falls into the wrong hands, you'll be hard pressed to get a new set of fingers, a new voice or a new eye.

One could compare all computer security is like putting a wooden stake in front of your house and hoping that trespassers will run into it. Contrary to what many biometric proponents would have us believe that biometric security outclasses traditional forms of security all biometric systems are, in the end, merely another form of computer security with its own set of strengths and weaknesses.

Biometrics effectively trades some amount of privacy and cost effectiveness for ultimate convenience and these systems are certainly no less secure than standard pass wording systems. Nevertheless, biometrics seems to be where the industry is headed.

Aside from their Orwellian connotations, biometrics systems offer an enormous amount of convenience to users. And, in the present political climate, it is hard to counter the argument that we should adopt biometric systems as additional layers of security on top of traditional pass wording systems at least until privacy questions arise e.g. Thumb, Finger, voice authentication etc.

7.5 Smart Cards

Smart cards are rapidly gaining acceptance as a means of addressing the requirement for systems that can accurately and securely verify a person's identity and rights. Smart cards include an embedded chip (either a microcontroller with internal memory or a memory-only chip), contain the tools necessary for security applications, and are available with both contact and contact-less interfaces to readers. Properly implemented, a smart card-based identity verification system provides a robust barrier to unauthorized access.

8. PRIVACY (PRIVACY)

8.1 P3P-Platform for Privacy Preferences

The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium, is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Web sites they visit. At its most basic level, P3P is a standardised set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P enabled browsers can "read" this snapshot automatically and compare it to the consumers own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form that users can understand, and, most importantly, enables users to act on what they see.

8.2 Location Based Services

One of the most important enabling services will be Location based services. However, there are concerns regarding privacy. Suppose you call the emergency service, triggering an automatic location service sending your position to the rescue squad, but within a few minutes besides an ambulance also the local reporters appears. Alternatively, you use your new phone to call up location-specific information, such as maps or traffic updates, or to locate a nearby restaurant, and when you get home your wife/ husband, or a blackmailer, is aware that you were not in London but in Paris. These and many other examples show that there is a need to securely gather and transfer location information for location services, protecting the privacy of the individuals involved. Indeed, privacy concerns are as long-term impediment to the success of e-business ventures and in particular of location dependent value added services. The IETF “geopriv” working Group main task is to assess the authorisation, integrity and privacy requirements that must be met in order to transfer location information, or authorise the release or representation of such information through an agent. Currently, using existing formats but enhancing fields a “Location Object” is being defined. This will include a data format incorporating fields with cryptographic checksums or encrypted contents, to ensure that the security and privacy methods are available to diverse location-aware applications. Besides the security mechanisms used within the object, a list of requirements for the embedding protocol that transports the geopriv Location Object will be specified. The goal is that this combined specification (embedded Location Object and transport protocol requirements) will have a broad applicability and will be mandatory for all IETF implementation of location-aware protocols, in particular for the SIP SOS (Emergency call) or http/html.

The combination of these elements should provide a service capable of transferring geographic location information in a private and secure fashion, including the option of denying transfer or revealing what time zone the target is in, but not what city or reducing the resolution or precision of location information provided.

Although in this framework a most important role is played by user-controlled policies, which describe the permissions given by the user to treat his privacy requirement, that is the conditions under which location information may be released to whom, the policies themselves are probably out-of scope for geopriv. In scope of the working

group is the authentication of requestors and responders or proxies, the authentication of policies.

3GPP and the Location Information Forum (LIF) now part of Open Mobile Alliance (OMA) also define policy-controlled privacy information for location services. Compared to them, geopriv searches a more general solution, rather long-term, providing more flexibility and applicability in more contexts, for value-added services and chains of services and probably for later use in 3GPP in all-IP networks.

9. SECURITY IN 3G CELLULAR NETWORKS

3GPP and IETF bodies mainly standardize UMTS relevant security mechanisms. Beside this, we also have to consider those network functionalities that are part of an operator's UMTS network while being outside the scope of 3GPP standardization (e.g. **Routers**, **DHCP** Server etc.).

3GPP has carried on its work in defining and working on the Security issues for UMTS / 3G (see Chapter 5).

For example, the UMTS new access security features described by the 3GPP specification (summarized in section 5.2.1.) are:

- Entity authentication of the user to the network and network to the user (with operator-specific algorithms);
- Use of temporary identities (in both CS and PS domains);
- Enhanced encryption of communication on the radio and protection of the signalling integrity on the radio access network (with cryptographic algorithms publicly available).

But 3rd generation mobile networks will include also the packet-switched (PS) domain that basically offers packet-switched IP-based services to the mobile user. These packet-switched services are based on GPRS (General Packet Radio Services) and are already upgrading second-generation GSM networks with packet-switched services. In an upcoming version of UMTS networks, called release 5, an IP based multimedia subsystem will additionally be included providing VoIP, instant messaging and other services.

The main difference between IP and, for example, SS7 transport is that in contrast to complex SS7 technology, an IP stack is part of every personal computer and PDA operating system, and will be part of any mobile phone soon. IP is easily accessible, everywhere.

An increasing part of mobile core networks will be IP-based, supporting IP-based services. And an increasing part of the IP traffic in mobile core networks will have to traverse lines that are not so "closed" any more.

For a long time, the development of Internet technologies was based on the premise of unhindered exchange of information. The resulting network structures are very flexible and decentralised: It is easy to connect further computers to the Internet, and the range of possibilities for everybody to develop and make use of new applications is essentially unlimited. These properties made possible the rapid growth of the Internet, but on the other hand allow for misuse due to the lack of controlling instances. It is well known that the Internet protocol itself does not offer any security in terms of authentication, integrity or confidentiality, and it is well known that the Internet Engineering Task Force (IETF) spends more and more effort on security issues. Thus, it is clear that security means for the IP-based parts of mobile core networks are an important prerequisite for the economic success of UMTS.

The most common and most generic solution to apply strong

Security to IP-based traffic is the IP security framework (IPSec), specified by the **IETF**

and chosen by 3GPP to provide core network security (see chapter 5.2.2). Assuming that the threat is interception/manipulation on the link between the hosts (IPSec is good at addressing this). What if the system administrator goes “rogue” or the application on the host is compromised than IPSec will not help here.

9.1 3GPP specifications on UMTS security

The UMTS relevant security aspects standardisation happens in several bodies, in particular in ITU, 3GPP, and IETF. Unfortunately, the architecture and security requirements of the system are different in different standardisation bodies.

In this chapter, we will have a look to 3GPP specification and its relationship with IETF.

The 3GPP is responsible for standardising the UMTS Mobile Network. Due to the fact that IP based Mobile Networks become more and more important, 3GPP also tries to consider these new influences. Therefore, the 3GPP standardisation body intends to reuse the existing security protocol as defined by IETF in order to avoid the development of new mobile specific protocols.

In case of 3GPP specific adaptations of IETF standards for a UMTS Mobile Networks 3GPP is supposed to bring forward these modifications to IETF.

9.2 UMTS Security principles and objectives

The general objectives for 3G security features have been stated as[21] to ensure:

- Adequate protection against misuse and misappropriation of:

  - Information generated or relating to an user;

  - Resources and services provided by Serving Networks (SE) and Home Environments (HE);

- Features standardised provide worldwide:

  - Availability (at least one ciphering algorithm should be exportable on a world-wide basis[22]);

  - Interoperability and roaming between different serving networks;

- The level of protection of users and providers is better than that provided in contemporary fixed and mobile networks;

- The implementation of 3G security features and mechanisms can be extended and enhanced as required by new threats and services.

9.3 Security architecture, features and mechanisms[23]

The figure below gives an overview of the 3G-security architecture from the 3GPP

[21] From 3GPP TS 21.133
[22] In accordance with the Wassermann agreement;
[23] From 3GPP TS 33.102

recommendations point of view:

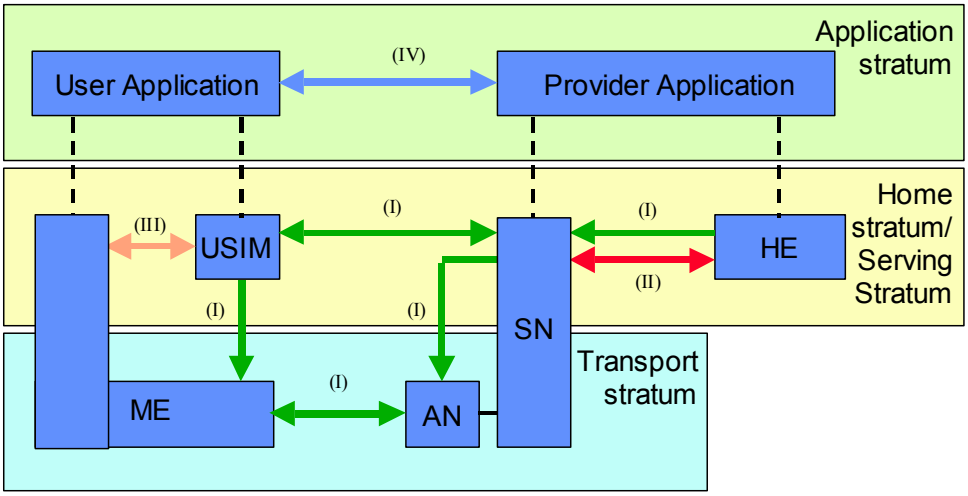


Figure 9.3 Overview of the security architecture

To see how Security works in 3GPP we have to match the 3G Security Architecture with the UMTS Network Domains, also defined by 3GPP.

Some of the security topics are not domain specific but depend strongly on the functional flow. Therefore, 3GPP looks at typical service functional flows. The following strata can be identified within UMTS (see TS 23.101):

– Application stratum

– Home stratum

– Serving stratum

– Transport stratum

These Strata are the bases for the UMTS Security Architecture.

Five security feature groups are defined. Each of these feature groups meets certain threats and accomplishes certain security objectives:

- Network access security (I): the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;

  - User identity confidentiality (user identity and location confidentiality, user non trace- ability)

  - Entity authentication (user and network authentication)

  - Confidentiality (cipher algorithm agreement, cipher key agreement, confidentiality of user data, confidentiality of signalling data)

  - Data integrity (integrity algorithm agreement, integrity key agreement, data integrity and origin authentication of signalling

data)

- Mobile equipment identification

- Network domain security (II): the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wire line network;

- User domain security (III): the set of security features that secure access to mobile stations;

  - User-to-USIM authentication

  - USIM-Terminal Link

- Application domain security (IV): the set of security features that enable applications in the user and in the provider domain to securely exchange messages;

  - Secure messaging between the USIM and the network

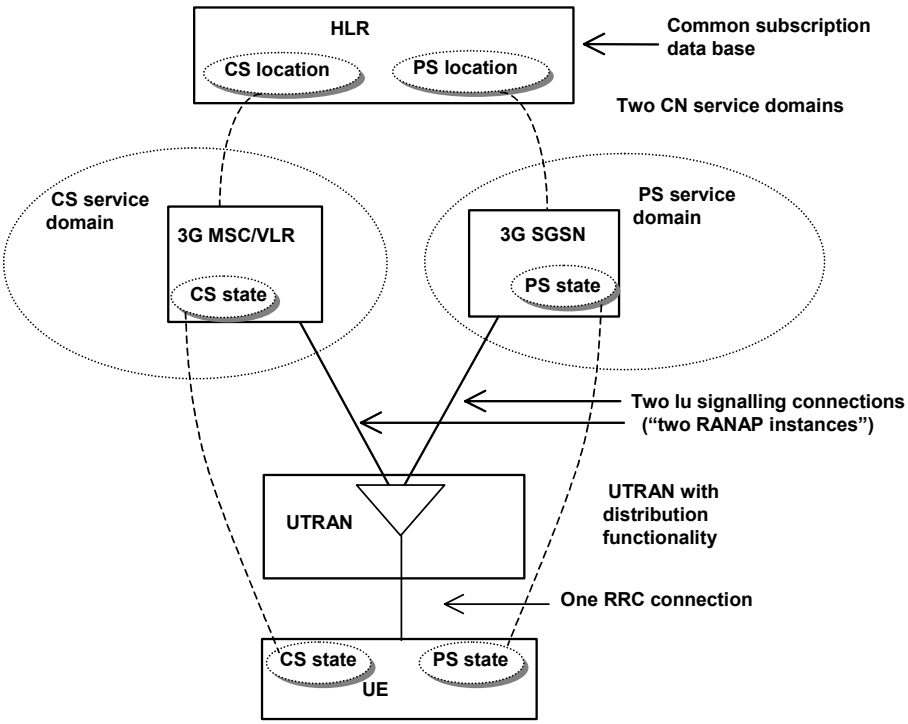
- Visibility and configurability of security (V): the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

  - Visibility

  - Configurability

The following figure gives an overview of the Mobile Equipment (ME) registration and connection principles within UMTS with a CS service domain and a PS service domain.

As in GSM/GPRS, user (temporary) identification, authentication and key agreement will take place independently in each service domain.



(source: TS 23.121 [4] – Figure 4-8)

Figure 9.3.1 Mobile Equipment registration and connection in UMTS

9.4 Network access security (I) mechanisms

Mutual authentication of the user/network and related cryptography:

The involved entities are the Home network (HN), the Serving network (SN) and the Terminal (USIM). The mutual authentication mechanism is based on two parameters shared between terminal (USIM) and Home Network's database Authentication Centre (AuC): a static master key (K)[24] and a dynamic sequence number (SQN).

Serving network (SN) checks the subscriber's identity (as in GSM): the permanent or temporary identity (IMSI or TMSI) of the subscriber is transmitted to VLR/SGSN[25], which then send an authentication request to the Authentication Centre in the HN.

Using the one-way functions f_i (which are easy to compute and difficult to invert), the master key K, a Sequence Number SQN[26] and a random bit string RAND, the Authentication Centre AuC generates an Authentication Vector (containing parameters RAND, AUTN, XRES, CK, IK) as described in fig. 5.2-1.

Using a similar computation, the terminal checks if the Serving Network is a legitimate network by verifying if the parameter AUTN was really generated in AuC. This check performed by the terminal is a new UMTS feature.

[24] The master key K is 128 bits long; it is never transferred out of USIM and AuC.

[25] Mobility management functions for CS and PS domains are independent of each other and consequently authentication vectors are sent to and used independently by VLR and SGSN.

[26] Sequence Numbers are in increasing order, to prove to the user that the Authentication vector is "fresh", i.e. it was not used before.

As they are used only in the USIM and AuC, which are both, controlled by the same operator, the algorithms f1-f5 can be operator specific. An example set of algorithms (called MILENAGE) is presented in 3GPP specification TS 35.206.

According to the Authentication and Key Agreement (AKA) mechanism for UMTS, temporary keys 128 bits long[27] for encryption and integrity check (CK, IK) are derived in AuC from the master key during authentication and sent to VLR/SGSN and later further to RNC. The same temporary keys CK and IK are computed in the USIM (terminal side).

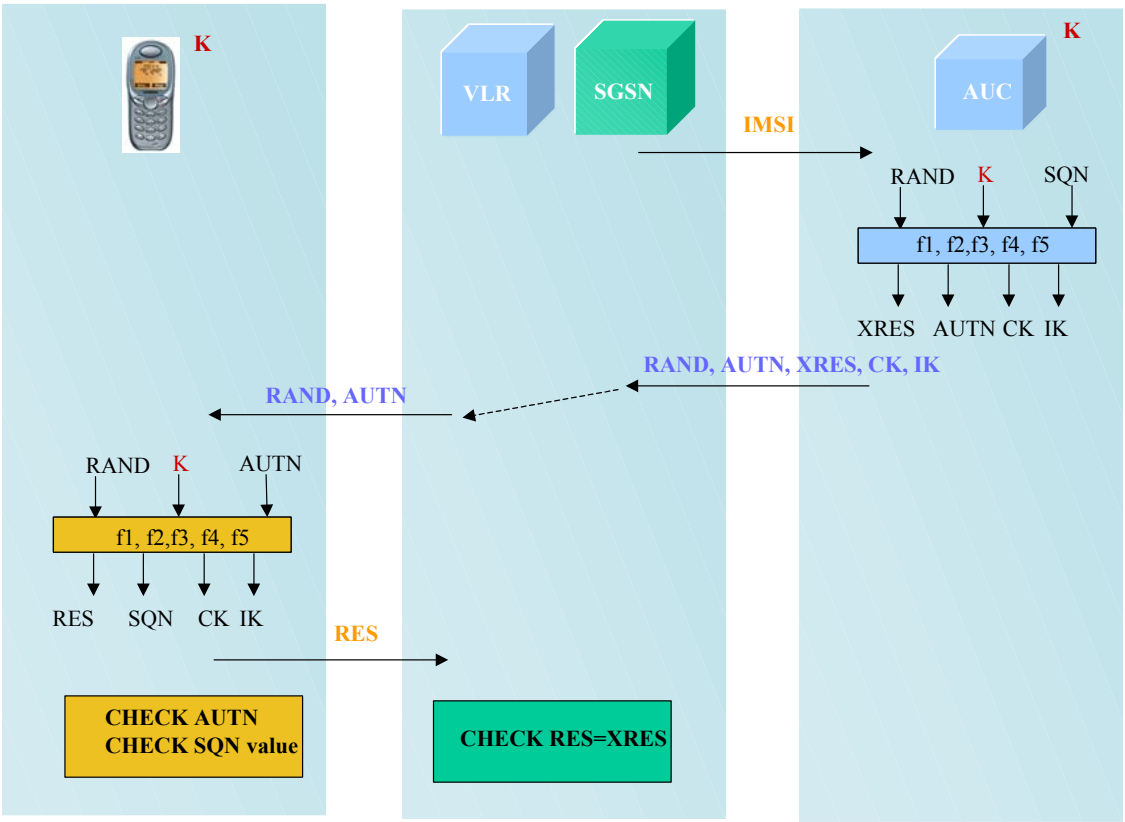


Figure 9.4.1 Mutual authentication of the user and network

9.4.1 Use of temporary identities

The identification of the user in UTRAN is done mainly by temporary identities (TMSI in the CS domain and P-TMSI in the PS domain). The permanent identity (IMSI) used only for the first user identification by the network, and this is the only case when confidentiality of the user's identity is not protected.

Allocated temporary identities are transferred by the serving network (VLR or SGSN) to the terminal while encryption is active. The mechanism offers a good protection level, but not complete (especially against active attacks).

[27] GSM keys were 64 bit long

9.4.2 Radio access network encryption

The encryption takes place in the terminal and RNC, after the mutual authentication is performed.

According to the 3GPP specification, there is only one encryption algorithm (named f8), based on the cipher key CK obtained during the authentication phase in USIM and AuC. The cipher key has to be transferred from AuC to RNC.

Algorithm f8 is publicly available and specified by 3GPP TS 35.201. The encryption mechanism is based on a block cipher concept named KASUMI[28] and described in the 3GPP specification TS 35.202.[29]

The encryption/decryption is still an optional mechanism in UMTS!

9.4.3 Signalling integrity provided inside UTRAN

UMTS provides an authentication mechanism for individual control messages, in order to ensure the identities of the communicating parties also after the mutual authentication phase.

Integrity protection (i.e. authentication of control messages) is applied between terminal and RNC, by the means of the integrity key IK obtained during the authentication phase in USIM and AuC. IK as well as CK are then transferred to RNC.

The integrity protection algorithm is called f9. It is based on the KASUMI mechanism as f8.

The integrity protection is not applied to all messages (messages sent before integrity key is in place are not protected).

9.5 Network domain security (II)

Network domain security is defined in TS33.102 as 'the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wire line network'.

This definition is explicitly limited to signalling data, 3GPP does neither mandate nor recommend any security features for the protection of user data.

As mentioned earlier, one of the weaknesses of the GSM security architecture is the consequence of the unprotected transmission of authentication data between networks[30]. This happened because it was a common feeling that communication on SS7 networks needed less protection as only a small number of large institutions have access to them.

For the UMTS networks benefit, security of SS7-based networks is enhanced in release 4, as a specific security mechanism is developed for the MAP protocol, called MAPSEC and providing confidentiality and integrity protection.

[28] KASUMI block cipher concept is based on the block cipher MISTY from Mitsubishi
[29] KASUMI transforms a 64-bit input into a 64-bit output under the control of the 128-bit cipher key CK.
[30] Cipher keys used to protect traffic on the radio interface are transmitted in clear between networks. And even when we get the ciphering one still has to rely on the roaming partner…

Moreover, in future releases the UMTS core network structure will evolve and IP will become the dominant protocol.[31] The IPSEC protocol will provide confidentiality and integrity of communication on the IP layer.

Therefore, 3GPP specification for network domain security covers two major areas:

- MAP application layer security (Release 4)
- IP network layer security (Release 5)

The critical issue is the key management, i.e. the generation, exchange and distribution of the keys used by the confidentiality and integrity algorithms.

The key management for MAPSEC is planned to be provided by techniques similar to those used for IPSEC, using a certain set of parameters called Security Associations (SAs), negotiated trough the Internet Key Exchange (IKE) protocol before confidentiality and integrity mechanisms[32] are applied.

An SA logically describes a secure connection between peers (e.g. two IPSEC peers) and contains:

- Encryption and authentication keys
- Information about the used algorithm
- Lifetime of the keys
- Lifetime of the SA
- A sequence number (to protect against replay attacks)

IKE permits the secure exchange of secret keys over an insecure channel, as it is based on the concept of public key cryptography. As the authentication of the parties that run IKE need long-term keys, these can be exchanged manually or through Public Key Infrastructure.

9.5.1 MAP Application Layer Security (Release 4)

The Mobile Application Part (MAP) is specified in TS 29.002. [33]

MAP application layer security is specified in TS 33.200 and aims to protect the

[31] 'For native IP based protocols, security shall be provided at the network layer' (TS 33.210). Within the 3GPP architecture, the relevant interfaces are Gn/Gp, and Gi, as well as the interfaces to and within the IMS (Go, etc.).

[32] As ESP and AH in IPSEC;

[33] In the PO domain, MAP is used for the communication between SGSN and HLR (Gr interface), between SGSN and EIR (Gf interface), between SGSN and (G) MSC (Gs and Gd interface), and between GGSN and HLR (Gc) interface. The protocol stack for those interfaces is MAP over TCAP over SCCP over MTP. If optional IP transport is used, the MTP layer is replaced by M3UA over SCTP over IP. However, network entities do not know what transport technology is used along the path of a MAP message. Hence, security solutions purely relying on secure IP transport are not sufficient.

confidentiality and integrity of MAP operations. Three different protection modes are supported:

- Protection Mode 0: No protection
- Protection Mode 1[34]: Integrity & Authenticity
- Protection Mode 2[35]: Confidentiality & Integrity & Authenticity

MAPSEC will support different encryption and integrity algorithms. So far, only AES with 128 bit keys is assigned as being mandatory. A selective protection of MAP messages is possible through the definition of message-specific protection profiles. Since the final destination of the MAP message is not known at the origin, no distinction between inter-domain and intra-domain traffic can be made, and equal protection has to be applied to both traffic types.

MAP Security management means:

- The initial exchange of MAPSEC keys
- The policies for renewal of MAPSEC Security Associations (SAs)
- The trigger events and procedures for withdrawal of SAs
- The decision about applied protection mode (and whether fallback to Mode 0 is allowed)

See Appendix of TS33.200 for more information on the decision about key lengths, algorithms and SA expiry times (hard expiries for incoming traffic while outgoing traffic is subject to soft expiries, i.e. if no other SA is available, the expired SA will still be used.

Inter-domain security associations and inter-domain key management are subject to roaming agreements and need to be investigated further in future.

At the start of the (intra- or inter-domain) communication between two network elements, the initiating NE checks its Security Policy Database (SPD) whether MAPSEC is mandated by the security policies. If yes, the NE checks the Security Association Database (SAD) for an existing, applicable SA. The SAD contains the keys, algorithms, and expiration time and protection profiles for each existing SA[36]. An automatic key management (using a Key Administration Centre) is currently still planned as Rel. 5 feature, although a decision about moving it to Rel. 6 is still pending

9.5.2 IP Network layer security

IPSEC is standardised by IETF (Internet Engineering task force). It consists of several RFC's and it is a mandatory part of IPv6, while in IPv4 IPSEC can be used as an optional add-on mechanism.

[34] The clear text of the MAP payload is concatenated with a message authentication code (MAC-M) of mandatory length 32bits. The MAC-M covers the security header as well as the MAP payload.

[35] The encrypted payload is concatenated with the MAC-M covering the security header and the encrypted payload. The length of the cipher text will be identical to the length of the original payload. The length of the MAC-M is mandatory to be 32bits.

[36] See the normative Annex B of TS33.200 for a detailed message flow.

As already mentioned, UMTS networks will include a packet-switched (PS) domain as the IP-based part of the core network. Obviously, the security requirements for these core network parts differ for each interface and for each layer of the IP stack.

To establish a basic, common security framework 3GPP has mandated the use of IPSec for specific parts of UMTS Release 5 core networks, and has specified IPSec as optional for other parts. With these prerequisites, it is possible to provide a basic protection level that ensures security for the most vulnerable parts of the operator's core network signalling on the one hand, and allows each operator to individually apply additional security means, if necessary.

The main IPSEC components are: Authentication Header (AH), Encapsulation Security Payload (ESP) and Internet Key Exchange (IKE).

ESP provides both confidentiality and integrity to IP packets, while AH provides only integrity. This redundancy was generated by the restriction of exporting confidentiality mechanisms in some countries (restrictions largely dropped now days, with the consequent importance increase of ESP). ESP has two operating modes:

- Transport mode

Everything in an IP packet is encrypted, except for IP header; an ESP header is added, containing information about the SA in use; a MAC (Message Authentication Code) is calculated over the entire packet except the IP header, and added at the end

- Tunnel mode

A new IP header is added; then the same operations of the transport mode are applied, with the consequent protection of the original IP header

Both AH and ESP need keys, which can be found in the Security Associations (SAs).

The preferred method for UMTS core network control messages is to use ESP in tunnel mode between security gateways (middle nodes), as using the transport mode implies that communicating network elements have to know each other's IP address and have to implement the complete IPSEC functionality.

3GPP (TS 33.210) recommends protecting IP based signalling traffic in a hop-by-hop manner using IPSEC Security Associations (SAs).

There is difference between intra-domain and inter-domain traffic. For signalling traffic within a security domain, IPSEC support is optional.[37]. Therefore, an operator is able to adjust security in a fine-grained way. The possible choices are:

- No IPsec, in case security is already provided by other means, or is not required.

- IPsec between specific entities only, e.g. providing secure tunnels between

[37] Inter-domain traffic between two network elements in the same security domain can be optionally protected by IPSEC. Inter-domain traffic has to be routed through Security Gateways (SEGs). The inter-domain interface between two security gateways in different security domains is called Za . Intra-domain traffic between two network elements (NEs) in the same security domain can either be transmitted without any security mechanisms, or optionally IPSEC SAs on the so-called Zb interface can be used. NEs may establish Security Associations as needed towards a SEG or another NE in the same domain (optional Zb interface, NE-NE or NE-SEG). All signaling traffic to other domains has to be routed through SEGs, which implement the Za interface (SEG-SEG).

different sites of the same core network, i.e. within the same security domain.

- IPSEC protecting the complete core network internally.

3GPP mandates to use certain IPsec features for message protection and key management.[38]

The granularity of IPsec associations depends on the operator's policy with respect to how many different security feature combinations should be supported simultaneously for the communication between two NEs or two SEGs[39].

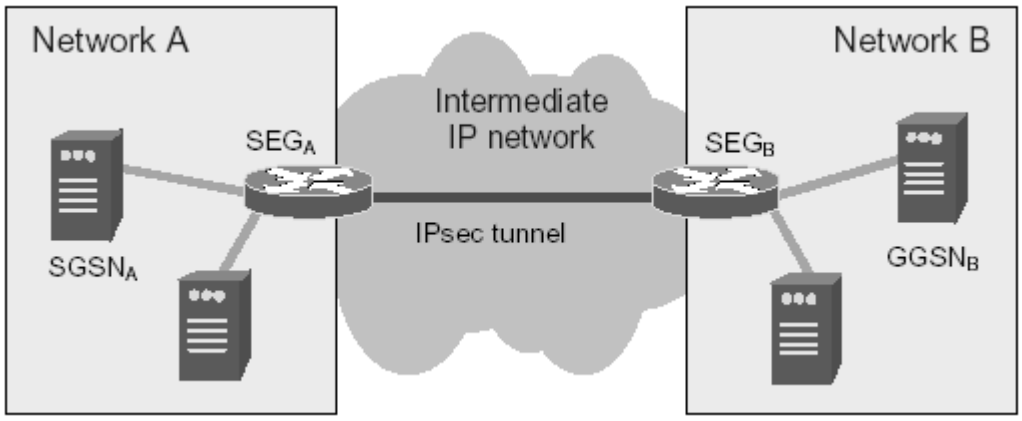
The figure below gives an impression of the configuration between two security domains owned by different operators. An ESP tunnel between SEGA and SEGB must protect signalling running between SGSNA and GGSNB. Additionally, the network operators can decide to protect traffic internally, e.g. between SGSNA and SEGA within network A.

For each bi-directional connection, at least three SAs are necessary.[40] However, using a larger number of SAs increases the vulnerability for traffic flow analysis. The set-up of security associations is controlled by policies stored in (local or centralised) Security Policy Databases (SPD). The NE maintains a list of active SAs together with their parameters in a Security Association Database (SAD). The message flows for the set-up of IPSec SAs are in principle similar to the MAPSEC case.

[38] 3GPP mandates to use the following IPSEC features for message protection and key management:
- ESP must be used for inter-domain control plane traffic;
- Integrity protection/message authentication together with anti-replay protection must always be used.
- Tunnel mode must be supported (for inter-domain communication, this is the only mode applicable)
- If confidentiality is supported, AES encryption is a mandatory cryptographic algorithm
- HMAC_SHA1 and AES MAC must be supported for authentication.
- Internet Key Exchange (IKE, RFC2407-2409) must be used for negotiation of IPSEC SAs., with the following IKE Phase 1 features supported:
  - Pre-shared secrets for authentication
  - Only Main Mode and Fully Qualified Domain Names
  - Mandatory support of AES in CBC mode for confidentiality
  - SHA-1 support for integrity/message authentication

[39] SEG (Security Gateway) operate at the border of each security domain, respectively. SEG functionality could be imagined as an IPSEC box, co-located with a GSN at the network border (and with a border gateway), or as a firewall with built-in IPSEC.

[40] One for key management (ISKMP) and two associations for each direction of the message flows. Additional associations can be used in order to provide other feature combinations (with/without confidentiality, different encryption/authentication algorithm, etc.).



(source Siemens Mobile Communications)

Figure 9.5 IPSEC protecting the IP based UMTS network

Security Gateways (SEGs): Borders between security domains (Za interface) are protected by one or more Security Gateways (SEGs) whose responsibility is to enforce security policies for inter-working between network domains. This may include filtering policies and firewall functionality. Only SEGs shall engage in direct communication with entities in other security domains. The number of SEGs depends on the operator's need to (1) differentiate between externally reachable destinations; (2) support load balancing/sharing; (3) avoid single points of failure. SEGs can be integrated with other UMTS entities (e.g. in the GGSN), however those integrated SEGs should then be exclusively used for traffic from the co-located network entity. No other traffic should be routed through such an integrated SEG.

Requirements on SEGs:

- SEGs shall be physically secured
- SEGs shall offer capabilities for secure storage of long-term keys (e.g. for IKE authentication)
- SEGs will maintain logically separate SAD and SPD databases for each interface.

9.6 User domain security (III)

The User Domain security features are described in 3GPP TS 33.102 as '*the set of security features that secure access from and to mobile stations*'. A key goal in this domain is to minimize the damage and fraud that can occur when a handset is stolen.

TS 21.101 introduce an architectural split of the User Equipment Domain in two parts: the Mobile Equipment Domain (ME) and the User Services Identity Module Domain (USIM).

- Mobile Equipment Domain: The Mobile Equipment performs radio transmission and contains applications. The mobile equipment may be further sub-divided into several entities, e.g. the Mobile Termination, MT which performs the radio transmission and related functions, and the Terminal Equipment, TE which contains the end-to-end application or (e.g. laptop connected to a mobile

phone).

- USIM Domain: In a security context, the USIM (User Services Identity Module) is responsible for performing UMTS subscriber and network authentication and key agreement according to TS 21.133. It should be capable of performing GSM authentication and key agreement to enable the subscriber to roam easily into a GSM Radio Access Network.

The USIM contains data and procedures, which unambiguously and securely identify itself.

These functions are typically embedded in a stand-alone smart card. This device is associated to a given user, and as such, allows to identify this user regardless of the ME he uses.

9.6.1 3GPP User domain security features

The following user domain, security features have been identified by 3GPP (TS 33.102)

- User-to-USIM Authentication

USIM has to authenticate the user before letting him get access to USIM information. The authentication is performed trough a PIN number, known to the user and stored securely in the USIM. The implementation mechanism is described in TS 31.101.

- USIM-Terminal Link

The terminal has to be used only by an authorised USIM, so if the terminal is stolen it cannot be used with another USIM. The mechanism of USIM-terminal authentication is described in TS 22.022.

- USIM personalisation.

USIM personalisation is an anti-theft feature. When a ME is USIM personalised to a particular SIM it will refuse to operate with any other USIM. Hence, if the ME is stolen the thief will not be able to use it with another USIM.

9.6.2 3GPP User domain security mechanisms

TS 33.103 and TS 33.102 describe the security mechanisms for the user domain network elements:

The security mechanisms for UE:

- User identity confidentiality (UIC_{UE}): conventional mechanism for user identity confidentiality (between user and serving network)[41]

- Data confidentiality (DC_{UE}): mechanism for data confidentiality of user and

[41] This mechanism allows the identification of a user on the radio access link by means of a temporary mobile subscriber identity (TMSI/P-TMSI). A TMSI /P-TMSI has local significance only in the location area or routing area in which the user is registered. Outside that area it should be an accompanied by an appropriate Location Area Identification (LAI) or Routing Area Identification (RAI) in order to avoid ambiguities. The association between the permanent and temporary user identities is kept by the Visited Location Register (VLR/SGSN) in which the user is registered.

signalling data[42]

- Data integrity (DI_{UE}): The mechanism for data integrity of signalling data

9.6.3 The security mechanisms for USIM:

Authentication and key agreement (AKA_{USIM}): The purpose of this procedure is to authenticate the user and establish a new pair of cipher and integrity keys between the VLR/SGSN and the USIM. During the authentication, the USIM verifies the freshness of the authentication vector that is used.

9.7 Application domain security (IV)

The 3GPP specification TS 33.102 defines Application Domain security as “the set of security features that enable applications in the user and in the provider domain to securely exchange messages”.

It will provide the capability to the exchange of secured packets between an entity in a 3G or GSM PLMN and an entity in the UICC. Secured Packets contain application messages to which certain mechanisms according to 3GPP TS 22.048 have been applied. Application messages are commands or data exchanged between an application resident in or behind the 3G or GSM PLMN and on the UICC. The Sending/Receiving Entity in the 3G or GSM PLMN and the UICC are responsible for applying the security mechanisms to the application messages and thus turning them into Secured Packets.

9.7.1 3GPP Application Domain Security Features

The following application domain security features are defined in TS 33.102: Secure messaging between the USIM and the network.

Secure messaging as currently defined in TS 33.102 will provide a secure channel for the transmission of messages between the USIM and a network server.

USIM Application Toolkit, as specified in TS 31.111, provides the capability for operators or third party providers to create applications, which are resident on the USIM (similar to SIM Application Toolkit in GSM).

There exists a need to secure messages, which are transferred over the network to applications on the USIM, with the level of security chosen by the network operator or the application provider. Security features for USIM Application Toolkit are implemented by means of the mechanisms described in TS 22.048.

3GPP Application Domain Security Mechanisms

3GPP defined security mechanisms on the transport layer for (U) SIM Application Toolkit. Some of the security mechanisms fulfil more than one security requirement. The features provided in TS 22.048 to ensure security of messages are:

[42] User data and some signalling information elements are considered sensitive and must be confidentiality protected. To ensure identity confidentiality, the temporary user identity (P-) TMSI must be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it. These needs for a protected mode of transmission are fulfilled by a confidentiality function, which is applied on dedicated channels between the ME and the RNC.

- Authentication mechanisms
  - Cryptographic Checksum
  - Digital Signature
- Message integrity mechanisms
  - Redundancy Check
  - Cryptographic Checksum
  - Digital Signature
- Replay detection and sequence integrity mechanisms
  - Simple Counter
  - A counter included in the calculation of the Cryptographic Checksum
  - A counter included in the calculation of the Digital Signature
- Proof of receipt mechanisms
  - Unsecured acknowledgement
  - Acknowledgement included in the calculation of the Cryptographic Checksum
  - Acknowledgement included in the calculation of the Digital Signature
- Message confidentiality mechanisms
  - Encryption mechanism

The only one defined application security mechanisms in TS 33.102 is Mobile IP security. The introduction of Mobile IP functionality for end users in 3G has no influence on the security architecture for 3G. Mobile IP terminals may be equipped with security functionality independent of the 3G-network access security in order to allow security functions outside the 3G networks. 3G networks, supporting Mobile IP services, should support its inherent security functionality.

9.8 Visibility and configurability of Security (V)

The specification refers to the capability for the user to see if an incoming call is ciphered, to cipher his outgoing calls and to refuse enciphered calls. Work is still in progress in 3GPP. But it has been agreed that the feature in place in GSM, “an encryption status indicator” on the phone will be carried over to 3G. The operator decides which customers they want to have this feature, by setting a flag on their SIM card during personalisation.

10. FEATURES AND REQUIREMENTS NOT COVERED BY STANDARD MECHANISMS

10.1 Network access domain

This chapter summarises the access security features and requirements from 3GPP and from the customer, which are not covered by the current standard methods.

10.1.1 Requirements to the network:

- o There is no special mechanism specified to provide user identity and user location confidentiality for IMS users.
- o Protection against unauthorised modification of user traffic on the radio interface
- o The serving network should be able to authenticate the origin of user traffic on the radio interface.
- o Prevention of restricting the availability of services by inducing certain protocol
- o Failures

10.1.2 Requirement to the terminal:

- o The user should be able to check, whether his user traffic and call related information is confidentiality protected or not.

10.1.3 Requirement to Operation and Maintenance:

- o Detection and prevention of fraudulent use of services. Raise alarms to alert providers to security-related events. Generation of audit logs of all security related events.

10.2 Network domain

The mandatory 3GPP mechanisms only cover data integrity and data origin authentication for inter-domain signalling traffic.

Confidentiality and protection against replay attacks as well as protection against traffic flow analysis are recommended options in the 3GPP solutions. Hence, 3GPP standardization currently only covers the first four requirements for inter-node communication.

Furthermore, the application of the security mechanisms in 3GPP is limited to signalling traffic, and only the protection of inter-domain signalling traffic is mandatory in 3GPP. Hence, the 3GPP mechanisms by itself do not provide a complete network domain security solution.

It is not within 3GPP's intention to standardise implementation details of individual nodes.

Furthermore, network design and also the communication between the network

entities that are required for IP transport on the Gn and Gi interface are not in the scope of 3GPP.

In summary, 3GPP does not cover the following sets of requirements:

- All requirements dealing with the protection of network
- Requirements for inter-node communication of user-data traffic (future activities in 3GPP are possible).
- Requirements for inter-node communication of network entities outside the scope of 3GPP (IP routers, switches, DNS Server, etc.).
- Requirements on network design

Furthermore, the mechanisms for the IPSec SAs on the Za and Zb interfaces, as well as for the MAPsec SAs on the Zf interface still leave several implementation-specific options:

- Location of the security gateways
- Strategies for SA set-up
- Strategies for security feature selection for SAs
- Implementation of optional Zb interface

10.3 User domain

User domain security is well specified within 3GPP and determines the security functions to be implemented in great detail.

10.4 Application domain

The mandatory 3GPP mechanisms only cover secure messaging between the USIM and the access network. The set of security features that enable applications in the provider domain to securely exchange messages are not covered within 3GPP.

10.5 Conclusions on standardisation

UMTS security is very much determined by 3GPP and IETF (IPSEC) standardisation bodies.

Upcoming decisions may e.g. be whether integrity should say " Security protection as specified by Network Domain Security (NDS/IP or NDS/MAP)" as it is more than just integrity.

Protection will become mandatory for IMS core network communication, whether PKI will be used and whether a protocol will be standardised allowing users to retrieve certificates Make the distinction between 1) PKI for NDS which is relatively simple as only roaming partners need to be involved and 2) the horrendous problem of 800 million- 1.2 billion end users. This second aspect is being addressed by Work item in 3GPP as "Bootstrapping of application security from 3G AKA and support for subscriber certificates". Emphasise that this does not replace authentication/

encryption key derivation by the symmetric key on SIM card. It is there to support applications that need non-repudiation, which can only be provided by true “digital signatures” i.e. one and only one party has the private key. It will be used only when the overhead (especially signalling on the radio interface, but also more general issues) on the transaction can be justified from their network operators, e.g. for digital signatures.

For UMTS the UICC will be the physical card and the SIM becomes a software application/subscription on the UICC for accessing GSM networks. The equivalent application for accessing 3G networks is called a USIM, and for accessing an IMS service, the application is an ISIM. There may be more than one of each application on a UICC, which give access to networks and services from different operators (access independence). Alternatively, conversion functions may be resident on the UICC and used where the networks / services are provided by the same operator/ trusted partner.

As there are functional entities in UMTS Networks, that are not UMTS specific, they are not handled in the above-mentioned bodies. Functional entities and their security features have to be identified in order to fill these (supposed) gaps.

The investigations performed showed that Network Access Security and User Authentication are well defined by standardisation activities, so those areas do not provide a major gap.

Differing to this, application related security functions are only well standardised for some basic authentication functions in the Mobile Equipment, and for a small number of selected generic applications.

Apart from those, the area of application domain security contains a number of security gaps, particularly in the area of the support of 3rd party applications and in the area of the inter-working of application domain security and network domain security.

In a similar way, security standardisation in the network domain only covers selected aspects, and various major gaps can be identified, particularly related to the inter-domain communication and the inter-working with the fixed Internet.

11. FRAUD

Where do you start when securing your business :

- Telecoms policy.
- E-commerce/ allowing more flexibility.

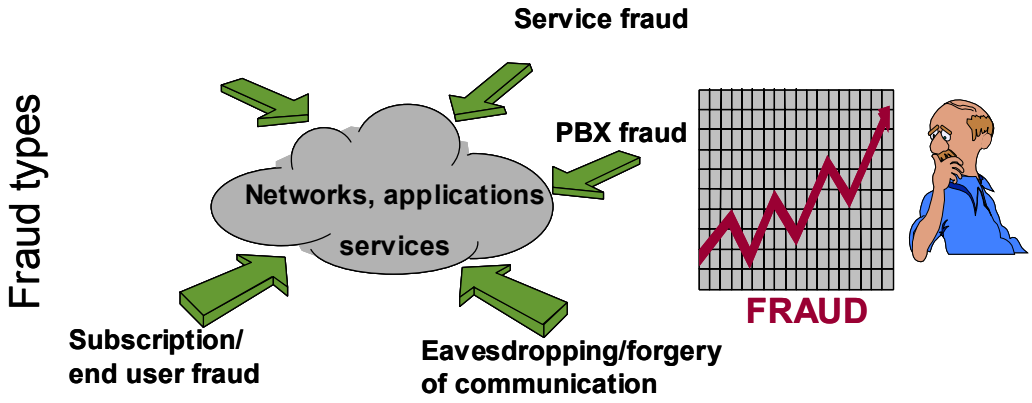


Figure 11.1 Fraud

Providers loose on average 2% of service revenues (i.e. billions of US $). With falling toll profits fraud protection becomes crucial.

11.1 Current situation

Fraud is the usage of networks, applications, or services without the intention to pay charged fees. Therefore, Subscribers, network providers, and services providers are concerned. Fraud is an issue in all networks: fixed, mobile, business, enterprise, carrier and Internet. Today's main fraud focus is on traditional voice networks but e.g. e-commerce via Internet will also become a primary target for fraud.

Today no exact fraud rates are available because in general, providers do not publish fraud figures and the distinction between bad debt and fraud is difficult. However, there are several studies giving an idea about the order of magnitude in which fraud occurs.

Fraud is done by insiders (provider staff), by outsiders and/or combinations. The most typical types of fraud are:

- Subscription/end user fraud: e.g. false identities or stolen ID

- Eavesdropping and forgery: e.g. eavesdropping of static passwords or PIN
- Value added services fraud: e.g. abuse of PRS (Premium Rate Service)
- Network management fraud: e.g. manipulation of sensible billing data
- Misuse of PBX features: e.g. DISA (Direct Inward System Access)
- The biggest risk for many operators actually is the roaming fraud. It takes time before CDR transferred back home (because they are not delivered in time by the respected roaming partners). This is also 'hard money' compared with 'soft money' in fraud concerning our own network.

The goal of fraudsters is single personal benefit as well as organized criminal business e.g. selling cloned Devices or abusing PRS.

11.2 Consequences

Because of fierce competition in telecommunication markets with falling tolls, adequate fraud management becomes more and more important.

Telecommunications industry realized fraud as an issue and established forums like TUFF (Telecommunications UK Fraud Forum), ETNO (European Telecom Network Operators' Association), FIINA (Forum for International Irregular Network Access), CFCA (Communication Fraud Control Association). These organizations share information about typical fraud cases to prevent spreading between providers and to combat fraud e.g. with common blacklists to identify bad guys.

There is a need for adequate solutions for overall fraud management covering the providers' current network infrastructure, applications/services and organizational/ technical aspects.

12. SERVICES AND APPLICATIONS

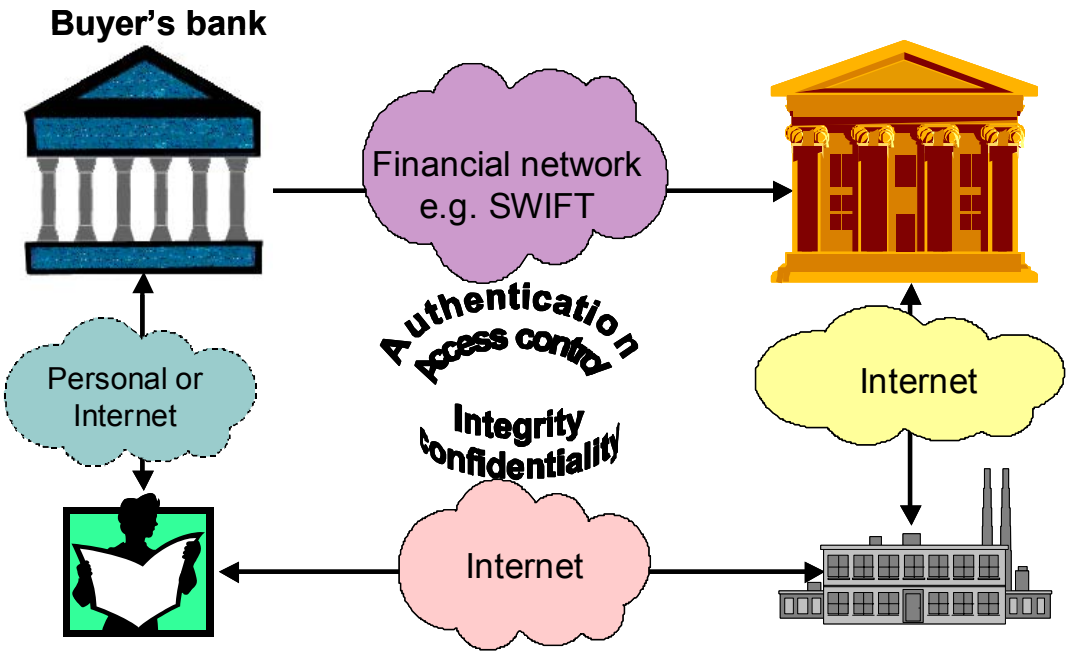


Figure 12.0 e-Commerce

All processes between buyer, vendor and banks have to be protected with security features against any kind of attack or illegal misuse by a third party.

The transfer of money over network requires special security solutions; ordering goods over a network requires additionally trust between all parties to get what they ought to get. In a typical e-commerce scenario 4 parties are involved, the buyer, the retailer and the banks of the buyer and of the vendor. If we assume that there is well-established relationship between the buyer and his bank as well as between the vendor and his bank, this does not exist between buyer and vendor especially for the first time.

Lack of mutual trust between business partners is given e.g. by:

- Is my business partner real and reliable?
- Is the offer, i.e. delivering of goods, real and reliable
- Is the order correct?
- Can the orders and transactions be transmitted confidentially?
- Are the orders and transactions non-reputable?

To give the e-commerce partners a certain level of mutual trust different of security features can be used, e.g.:

- Authentication

- Integrity
- Digital signature
- Encryption
- Non-repudiation

A security infrastructure combined with security components, e.g. smart card or Internet security protocols are available and more and more banks are testing e-commerce solutions or mobile e-commerce solutions.

12.1 ARTS Association for Retail technology standards

The Association for Retail Technology Standards (ARTS) of the National Retail Federation is a retailer-driven membership organization dedicated to creating an open environment where both retailers and technology vendors work together to create international retail technology standards. For further information look-up http://www.nrf-arts.org/

ARTS is a separate council within the NRF governed by a council of retailers and technology solution providers. Current council members can be reviewed on the Council Page.

Established in 1993, ARTS strives to ensure that technology works to enhance a retailer's ability to implement store-level business solutions, and to develop True Open Systems Standards that:

- Provide for Cost Effective Integrated Application Solutions that Protect Investment
- Allow "Best of Breed" Hardware and Software Components that will require minimal interfacing.
- Enable the Utilization of Hardware and Software Technology at the Rate it develops
- Create a global system of retail technology standards through a series of common interfaces.

To date, ARTS has developed two standards of significance: the Retail Data Model and Unified Point of Service (UnifiedPOS). The standard Data Model contains all the data definitions required to develop the computer applications required to operate a modern retailing business. The Model ranges from POS transaction processing through Customer Relationship Marketing (CRM). The Model was developed in four layers.

- Scope Document - describes in business language the retailing enterprise and the functions that have to be supported by computerized applications to achieve success.
- Business Process Relationships - relates data requirements to the specific retailing applications.

- Logical Data Relationships - explains through diagrams the relationships between business functions and the data components. These relationship diagrams save thousands of hours in developing applications.

- Data Definitions - of the more than 2,500 elements of data to ensure that the developers whether vendor or your internal staff completely understand the business application.

Benefits of the ARTS Data Model

The Model has saved retailers a significant amount of time and dollars in developing their computer based applications.

Marks and Spencer, Toys-r-Us and Boscov's have achieved excellent results using the ARTS data model. The original purpose of the Model was to allow retailers to select applications from vendors whose applications were developed using the Model. This enabled best of breed selection with greatly reduced interface costs and rapid implementation. Unlimited Solutions, H B International and PEC are examples of POS vendors that have developed to the Model allowing their retail customers to benefit from best of breed selection. For more information on the Data Model, click here: Explore our Standards.

Benefits of UnifiedPOS

UnifiedPOS, Unified Point of Service is a device interface standard that allows retailers to add new devices to sales floor terminals with minimal, if any, program change. UnifiedPOS links together two specific vendor implementations, JavaPOS and OPOS under one common API specification creating one architectural structure. UnifiedPOS allows retailers choice and provides vendors increased sales opportunities. Products that are compliant with UnifiedPOS, whether JavaPOS or OPOS can be combined within the same application.

12.2 MeT mobile electronic transactions

The MeT Initiative was formed to foster coherent growth of the mobile e-business market. It aims to ensure that applications using secure transactions are developed with a consistent user experience across multiple phones, access technologies and usage scenarios.

The Personal Trusted Device (PTD) of MeT's conception is designed for the broadest applicability to security-conscious purposes, including banking, payment, ticketing and corporate identification and authentication

12.3 Mobey Global Mobile Payment Standards

Security is a prerequisite for the success of mobile commerce. The identification of technical and organisational measures to ensure the establishment of a trust relationship between a mobile user and his or her communication partner is an essential issue. This requires on one hand a widely accepted trust infrastructure (Wireless PKI) at national and global level. It necessitates on the other hand that the mobile equipment fulfils high security requirements to position it as trusted personal equipment.

The fundamentals of the banking industry are built on trust and security. For this

reason, Financial Institutions have recognized early on the need for them to play an active role in the design and the operation of Public Key Infrastructure. The way that this issue is addressed has to take in account the different national contexts, however the strategic requirements are identical:

- Technical requirements: Financial applications need a high security level. This concerns the cytological mechanisms (for example encryption and signature algorithm, key generation, key length, etc.) as well as the hardware components (e.g. tamper resistant storage of private keys).

- Organisational requirements: The quality of security mechanisms also depends on factors, which are not of a technical nature. For example, the user registration process is one of the essential factors determining the quality of digital certificates to be used for mobile financial transactions.

- Legal requirements: Secure transactions (e.g. with digitally signed content) must be binding for the transaction partners.

These necessary legal frameworks as well as the legal liability of the parties involved in a mobile transaction are of central importance.

For this reason, it appears to be important that Financial Institutions are directly involved in the “trust-interface” with their customers. This means that the design and the operation of the Wireless PKI, as far as financial applications (e.g. payment

Services) are concerned; have to be fully integrated with the traditional relationship that Financial Institutions maintain with their customers.

Therefore, it is highly desirable, if not necessary, for the success of Wireless PKI that Financial Institutions take an active and decisive role in the design and operation of processes including:

- User registration and certificate issuance for financial applications (e.g. payment services, mobile banking)

- Co-ordination with other mobile commerce players and bodies

- Co-ordination and, whenever it makes sense, integration of the Wireless PKI in existing or emerging Internet PKI initiatives at national or global level

In conclusion, a successful acceptance of the Wireless PKI necessitates strong co-operation between Financial Institutions and other service providers, technology providers and network operators. This is the only way to ensure a “win-win” case for every party involved in mobile commerce.

For further information look-up: www.mobeyforum.org.

12.4 Mobile Payments Forum

The Mobile Payment Forum is a cross-industry organization launched in November 2001 to create a framework for standardized, secure and authenticated mobile payments, based on payment card accounts. The Forum intends to quickly and efficiently acts as the bridge between the mobile and financial industries to accelerate the maturity of the mobile marketplace.

Membership in the Forum includes organizations involved in initiating, processing and delivering mobile payments: telecommunications operators, payment card companies, financial institutions, device manufacturers, merchants, content providers and software and hardware infrastructure vendors.

Their mission is to combine and leverage the expertise of key participants in the mobile communications and payment card industries to create a foundation for standardized technology and functionality for secure, payment account-based mobile commerce.

In accomplishing this they intend to:

- Expand the global market for m-commerce
- Simplify the consumer payment experience
- Collaborate on future directions for mobile commerce

For further information look-up: www.mobilepaymentforum.org.

13. REGULATORY ISSUES FOR SECURITY

This Report only highlights a few regulatory issues but not in great detail. The UMTSF has a regulatory working group that deals with such issues and as such will respond to such matters whenever needed.

Legal and regulatory issues are increasingly dictating the security solutions, which vendors and services providers offer.

Three key points must be understood concerning the implications of legal and regulatory issues in security in analysing the impact of legal and regulatory issues and how they influence eSecurity.

- The vendor that proactively assists financial services institutions in complying with privacy legislation will be far more successful in the Security software business in the financial services space than those who do not;

- Security software companies should send a clear message to healthcare organisations that failure to comply with acts such as HIPAA privacy and security standards will result in losses in both monetary and reputational interests;

- Security software companies should use the EU Data Privacy Directive as a benchmark for future security solutions pending final passage of HIPAA security rules.

In Mobile Networks, Legal authorities require the possibility to intercept connections, the emergency services need to know where precisely the SOS calls come from etc. These and other technical solutions have to be seen with respect to the legal requirement for data protection.

13.1 Lawful interception

The target in security is to encrypt information in order to get it available only to the entitled receiver.

At the same time, there are many countries where local authorities and laws set limits for encryption and consequently limiting the network security level. Moreover, the local regulations may set a requirement that the authorities have a way of access to sensitive information and subscriber observation, so the authorities should have a chance of monitoring data traffic and listen to the calls, both Packet and Circuit Switched.

In GSM, such an arrangement was added on top of the existing system afterwards. In 3G, it was taken into account from the beginning.

Lawful interception consists of:

- Interception equipment and functionality

- Mediation devices

- Available interception information

Lawful Interception describes the possibility of realization for legal interception, as required by governments. Within this document, we will discuss the basic principles of LI for a deeper understanding we refer to the respective standardization documents (see 3GPP TS 33.106 to 33.108).

Description there is divided into three parts:

- Lawful Interception Requirements (TS 33.106)
- Lawful Interception Architecture and Functions (TS 33.107)
- Handover Interface for Lawful Interception (TS 33.108)

13.2 Regions (USIM)

The different regions around the world USIM could be subject to national interpretation.

13.3 Privacy

Normally, all data collected in a network are of private nature, having to be handled according to the governmental regulations for data Security. Regulations for Privacy and Payment related data are country dependent.

Privacy with respect to telecommunication covers all data that is personalised. This holds not only for name, address and so on, but also for communication related data like destination address and of course all billing relevant data. The country specific laws regulate what operators and service providers have to consider when collecting this kind of data.

In general, one can only use data collected for telecommunication purposes. Use of this kind of data without prior agreement from the user is not permitted (lawful Interception is of higher Priority).

Under discussion is the use of data for localisation of users. In the case of emergency calls, this is very helpful, but otherwise services that address the supervision of people are discussed very controversial in different countries. Currently, no final solution is available on a country individual base.

The EC has adopted a communication to the Council and European Parliament focusing on the next generation Internet and the priorities for action towards migrating to the new Internet protocol IPv6. Furthermore, a new Directive (2002/58/EC) on “processing of personal data and protection of privacy in the electronic communication sector” exist. The Data Protection Directive is part of a package of proposals for initiatives that will form the future regulatory framework for electronic communications networks and services. The new Directive aims to adapt and update the existing Data Protection Telecommunications Directive (97/66/EC) to take account of technological developments. However, it is not well understood how this policy and the underlying Internet technology can be brought into alignment.

Definitions[43]

For the purposes of the present document, the following definitions apply:

Access Control: The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.

Access Independence:" IMS will operate end to end across any bearer including GPRS, WLAN, ADSL and the IMS operator can be independent of the operator of the bearer network and will not necessarily trust that operator to maintain the security of the bearer or to have access to IMS security keys.

Availability: Network and services shall be available whenever needed. It should distinguish between entity authentication and data authentication.

Authentication: The provision of assurance of the claimed identity of an entity.

Cloning: The process of changing the identity of one entity to that of an entity of the same type, so that there are two entities of the same type with the same identity.

Confidentiality: The property of information that it has not been disclosed to unauthorised parties. Only sender and receiver shall be able to read the transferred data.

Certificate: A data structure employing a digital signature, usually issued by a CA, to tie the user data to the public key in a way that cannot be counterfeited. The data structure makes it clear which CA has provided the signature.

Integrity: The property of information that unauthorised parties has not changed it. The user wants to be sure that the data have not been changed on the way from the sender to the receiver.

Key Management: The administration and use of the generation, registration, certification, de-registration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

Law Enforcement Agency (LEA): An organisation authorised by a lawful authorisation, based on a national law, to receive the results of telecommunication interceptions.

Lawful Authorisation: Permission granted to an LEA under certain conditions to intercept specified telecommunications and requiring co-operation for a network operator or service provider. Typically, this refers to a warrant or order issued by a lawfully authorised body.

Lawful Interception: The action (based on the law), performed by a network operator or service provider, of making available certain information and providing that information to a Law Enforcement Monitoring Facility.

Legal requirements: Country specific legal security requirements shall be met. These may call for a weaker security.

[43] From 3GPP TS 21.133 v4.1.0 (2001-12)

Non-Repudiation Service: A security service, which counters the threat of repudiation. A user can't deny having used a certain service. It should also cover the fact that the service provider cannot deny having provided a certain service at some point in time or received something from the user.

Network Protection: The network shall be protected against intrusion, DoS attacks, etc. I would classify DoS prevention under the item “Availability” (first item in list)

Repudiation: Denial by one of the parties involved in a communication of having participated in all or part of the communication.

Home Environment: the role that has overall responsibility for the provision of a service or set of services to users associated with a subscription because of the association with a subscriber. [44]

Serving Network: the role that provides radio resources, mobility management and fixed capabilities to switch, route and handle the services offered to the users. Serving network capabilities are provided on behalf of home environments, with which the serving network has an appropriate agreement, for the benefit of the users associated with those home environments. Serving network capabilities in this context include access network capabilities; a separate access network role is not defined.[45]

Standard compliance: 3GPP and IETF There are also other standardization bodies that are involved with topics described in this paper, e.g. OMA, W3C.

[44] Home environment responsibilities include the following:

- The provision, allocation and management of subscriber accounts, including the allocation and management of subscriber account identifiers, user identities, user numbers and subscription charges. It also includes all billing mechanisms required to bill subscribers for charges and to pay network operators for user charges.
- The provision and maintenance of service profiles for users, including the provision and control of access to service profiles by users.
- Negotiation with network operators for network capabilities needed to provide 3G services to its users, including off-line agreements to allow service provision, and on-line interaction to ensure that users are properly identified, located, authenticated and authorised to use services before those services are provided to them.

[45] Serving network responsibilities fall into four main areas:

- The provision and management of radio resources, including the provision and management of any encrypted bearers needed to ensure confidentiality of user traffic
- The provision and management of fixed resources, bearer capabilities, connections and routing.
- The collection of charging and accounting data and the transfer of such data to home environments, and other network operators.
- The interaction with and provision of facilities for home environments to identify, authenticate, authorise and locate users

Annex A Abbreviations and Glossary

Abbreviation	Meaning	Explanation
2G	Second Generation	Generic name for second-generation networks, for example GSM.
2G+	Second Generation enhanced	Name given to 2G networks enhanced with GPRS or EDGE.
3G	Third Generation	Generic name for third generation mobile networks.
3GPP	Third Generation Partnership Project	A co-operation between regional standards bodies to ensure global inter-working.
AAA	Authentication Authorisation Accounting	A system in IP-based networking to control what resources users have access to and to keep track of the activity of users over a network. AAA services often require a server that is dedicated to providing the three services. RADIUS is an example of an AAA service.
AES	Advanced Encryption Standard	a symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.
AH	Authentication Header	A connectionless security protocol component of IPSec; use symmetric cryptography mechanisms;
AKA	Authentication and Key Agreement	A procedure for mutual authentication of the user and the network in GSM/UMTS
AN	Access Network	
AuC	Authentication Centre	GSM/UMTS network element that manages the authentication or encryption information associated with individual subscribers.
AV	Authentication Vector	
B2B	Business to Business	Term used to identify a business-to-business transaction.
B2C	Business to Consumer	Term used to identify a business to consumer transaction.
BTS	Base Transceiver System	The central radio transmitter/receiver that maintains communications with a mobile radio telephone within a given range.

Abbreviation	Meaning	Explanation
CA	Certification Authority	A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.
CK	Cipher key	A 128 bit key used for the radio access network encryption
CN	Core Network	Physical infrastructure linking wireless base stations. Predominantly circuit-switched, core networks will increasingly become packet-switched.
CS	Circuit Switched	A type of communications in which a dedicated channel (or *circuit*) is established for the duration of a transmission. Circuit-switching networks are sometimes called *connection-oriented* networks.
e-Commerce	Electronic Commerce	Term used to describe transactions that take place on-line where the buyer and seller are remote from each other.
ESP	Encapsulating Security Payload	A connectionless security protocol component of IPSec; use symmetric cryptography mechanisms;
ETSI	European Telecommunications Standards Institute	One of the standards body for Europe.
GGSN	Gateway GPRS Support Node	
GPRS	General Packet Radio Service	Technique used to upgrade current TDMA mobile networks. Allows a subscriber to gain up to eight 14.4 kbit/s channels. Also introduces packet switching.
GSM	Global System for Mobile communications	The most popular standard for 2G mobile networks.

Abbreviation	Meaning	Explanation
HE	Home Environment	The role that has overall responsibility for the provision of a service or set of services to users associated with a subscription because of the association with a subscriber.
HLR	Home Location Register	The functional unit responsible for managing mobile subscribers. Two types of information reside in the HLR: subscriber information and part of the mobile information that allow incoming calls to be routed to the mobile subscriber. The HLR stores the IMSI, MS ISDN number, VLR address, and subscriber data on supplementary services.
ID	Identification	
IETF	Internet Engineering Task Force	An engineering and protocol standards body that develops and specifies protocols and Internet standards, generally in the network layer and above.
IK	Integrity Key	A 128 bit key used for the radio access network messages integrity protection
IKE	Internet Key Exchange	A IETF specified protocol for the dynamic negotiation of Security Associations; IKE permits the secure exchange of secret keys over an insecure channel, as it is based on the concept of public key cryptography
IMEI	International Mobile Equipment Identifier	An identification number assigned to GSM/UMTS mobile stations that uniquely identify each one. It is a serial number that contains a type approval code, final assembly code and serial number.
i-mode		Proprietary HTML-based mobile information service offered by NTT DoCoMo in Japan. The i-mode service is similar to WAP.
IMSI	International Mobile Subscriber Identity	A unique number assigned to a mobile station at the time of service subscription. It contains a mobile country code, a mobile network code, mobile subscriber identification number, and a national mobile subscriber identity.
IMT-2000	International Mobile Telecommunications	ITU initiative for a global standardised 3G wireless networks.
IP	Internet Protocol	The dominant network layer protocol used with the TCP/IP protocol suite.

Abbreviation	Meaning	Explanation
IPSec	**IP Sec**urity	A set of protocols developed by the IETF to support secure exchange of packets at the IP layer
IPv4	Internet Protocol version 4	The version of IP in common use today.
IPv6	Internet Protocol version 6	The emerging standard, which aims to rectify some of the problems, seen with IPv4, not least the address space.
LI	Lawful Interception	The action (based on the law) performed by a network operator or service provider, of making available certain information and providing that information to a Law Enforcement Monitoring Facility.
MAP	Mobile Application Part	A protocol using the lower level layers of the SS7 protocol stack (TCAP, SCCP and MTP) for communication between the various registers and other MSCs.
m-commerce	Mobile Commerce	Similar to e-commerce but the term is usually applied to the emerging transaction activity in mobile networks.
ME	Mobile Equipment	The term used to describe the customer terminal in a UMTS network.
MExE	Mobile Execution Environment	
MSC	Mobile Switching Centre	The location providing the mobile switching function in a second-generation network wireless network. The MSC switches all calls between the mobile and the PSTN and other mobiles

Abbreviation	Meaning	Explanation
NAT	**N**etwork **A**ddress **T**ranslation	An Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A *NAT box* located where the LAN meets the Internet makes all necessary IP address translations. NAT serves three main purposes: - Provides a type of firewall by hiding internal IP addresses - Enables a company to use more internal IP addresses. Since they're used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations. Allows a company to combine multiple ISDN connections into a single Internet connection.
OAM	Operation and Maintenance	
PAP	Password Authentication Protocol	The most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. The Basic Authentication feature built into the HTTP protocol uses PAP. The main weakness of PAP is that both the username and password are transmitted "in the clear" -- that is, in an unencrypted form.
PDA	Personal Digital Assistant	
PDN	Packet Data Network	
PKI	Public Key Infrastructure	A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in a transaction

Abbreviation	Meaning	Explanation
PS	Packet Switched	Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message. Most Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies. Note, however, that although packet switching is essentially connectionless, a packet switching network can be made connection-oriented by using a higher-level protocol. TCP, for example, makes IP networks connection-oriented.
PSTN	Public Switched Telephone Network	Standard domestic and commercial phone service
P3P	**P**latform for **P**rivacy **P**references	A specification that will allow users' Web browsers to automatically understand Web sites' privacy practices. Privacy policies will be embedded in the code of a Web site. Browsers will read the policy, and then, automatically provide certain information to specific sites based on the preferences set by the users. For instance, if the site is an e-commerce site, the browser will automatically provide shipping info. If the site is requesting demographic info, then the browser will know to provide it anonymously. The P3P specification was developed by the W3C P3P Syntax, Harmonization, and Protocol Working Groups, including W3C Member organizations and experts in the field of Web privacy. P3P is based on W3C specifications that have already been established, including HTTP, XML and Resource Description Framework (RDF).

Abbreviation	Meaning	Explanation
RADIUS	**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice	An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.
Release 5	Release from 3GPP	Term applied to the group of specifications due to be released in early 2002, which will concentrate on the core network. Also known as Version 5.
Release 99	Release from 3GPP	Term applied to the group of specifications forming the first phase of release specifications by 3GPP mainly concentrating on the radio access network.
SA	Security Association	A set of parameters negotiated trough the Internet Key Exchange (IKE) protocol before confidentiality and integrity mechanisms are applied. An SA logically describes a secure connection between peers (e.g. two IPSEC peers) and contains: encryption and authentication keys, information about the used algorithm, lifetime of the keys, lifetime of the SA and a sequence number (to protect against replay attacks)
SAT	SIM Application Toolkit	
SEG	Security Gateway	
SGSN	Serving GPRS Supporting Node	
SN	Serving Network	

Abbreviation	Meaning	Explanation
SIM	Subscriber Identity Module	A small printed circuit board that must be inserted in any GSM-based mobile phone when signing on as a subscriber. It contains subscriber details, security information and memory for a personal directory of numbers. A Subscriber Identity Module is a card commonly used in a GSM phone. The card holds a microchip that stores information and encrypts voice and data transmissions, making it close to impossible to listen in on calls. The SIM card also stores data that identifies the caller to the network service provider.
SIP	Session Initiation Protocol	A signalling protocol for Internet conferencing and telephony. SIP was developed within the IETF MMUSIC (Multiparty Multimedia Session Control) working group, with work proceeding in the IETF SIP working group.
SLA	Service Level Agreement	A contract between an Application Service Provider and the end user, which stipulates and commits the ASP to a required level of service. An SLA should contain a specified level of service, support options, enforcement or penalty provisions for services not provided, a guaranteed level of system performance as relates to downtime or uptime, a specified level of customer support and what software or hardware will be provided and for what fee.
SLP	Service Location Protocol	An emerging Internet standard for automatic resource discovery on IP networks.
SPD	Security Policy Database	

Abbreviation	Meaning	Explanation
SSL	Secure Socket Layer	A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Both Netscape and Explorer support SSL, and many web sites use the protocol to obtain confidential user information, such as credit card numbers. SSL has been approved by the IETF as a standard
SS7	Signalling System No. 7	International standard protocol defined for open signalling in the digital public switched network. It is based on a 64 kbps channel and allows for information transfer for call control, database and billing management, and for maintenance functions
TCP	Transmission Control Protocol	A transport layer protocol that offers connection-oriented, reliable stream services between two hosts. This is the primary transport protocol used by TCP/IP applications.
TE	Terminal Equipment	
TLS	Transport Layer Security	
TMSI	Temporary Mobile Subscriber Identity	
UE	User Equipment	

Abbreviation	Meaning	Explanation
UICC	Universal Integrated Circuit Card	Make the distinction between 1) PKI for NDS, which is relatively simple, as only roaming partners need to be involved, and 2) the horrendous problem of 800 million- 1.2 billion end users. This second aspect is being addressed by Work item in 3GPP as "Bootstrapping of application security from 3G AKA and support for subscriber certificates". Emphasise that this does not replace authentication/ encryption key derivation by the symmetric key on SIM card. It is there to support applications that need non-repudiation, which can only be provided by true "digital signatures" i.e. one and only one party has the private key. It will be used only when the overhead (especially signalling on the radio interface, but also more general issues) on the transaction can be justified. Page: 87 [0] Blanchard: Need to state that for UMTS the UICC will be the physical card and the SIM becomes a software application/subscription on the UICC for accessing GSM networks. The equivalent application for accessing 3G networks is called a USIM, and for accessing an IMS service, the application is an ISIM. There may be more than one of each application on a UICC, which give access to networks and services from different operators (access independence). Alternatively, conversion functions may be resident on the UICC and used where the same operator/ trusted partner provides the networks/ services.
UMTS	Universal Mobile Telecommunications System	UMTS is a modular system that incorporates several technologies that realise the convergence of existing and future mobile and fixed networks, including the Internet. The UMTS concept embraces also all applications and services that can be offered to the end-user. UMTS is a member of the IMT-2000 family of systems. .
UMTS Forum	Cross industry body	Non-profit, independent forum that gives guidance to standards and other bodies in terms of market requirements and issues to be solved to allow for a smooth deployment of UMTS. UMTS Forum's "Extended Vision" embraces all elements of the value chain beyond the standards (specified by 3GPP/ETSI) for 3G mobile networks.

Abbreviation	Meaning	Explanation
USIM	Universal Subscriber Identity Module	The module that identifies, and is unique to, the mobile subscriber.
VoIP	Voice over IP	The generic term used to describe the techniques used to carry voice traffic over IP.
VPN	Virtual Private Network	Is an emulation of a private network using public networks
WLAN	Wireless Local Area Network	A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.
WEP	**W**ired **E**quivalent **P**rivacy	A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

Table 1: Abbreviations and Glossary

Annex B Bibliography

[1] UMTS Forum Report No. 1: "A Regulatory Framework for UMTS", October 1998.

[2] UMTS Forum Report No. 2: "The Path towards UMTS Technologies for the Information Society", October 1998.

[3] UMTS Forum Report No. 3: "The impact of licence cost levels on the UMTS business case", October 1998.

[4] UMTS Forum Report No. 4: "Considerations of Licensing Conditions for UMTS Network Operations", October 1998.

[5] UMTS Forum Report No. 5: "Minimum spectrum demand per public terrestrial UMTS operator in the initial phase", September 1998.

[6] UMTS Forum Report No. 6: "UMTS/IMT-2000 Spectrum", December 1998.

[7] UMTS Forum Report No. 7: "Report on Candidate Extension Bands for UMTS/IMT-2000 Terrestrial Component", March 1999.

[8] "UMTS Market Forecast Study", Final Report for EC DG XIII, Analysys/Intercai.

[9] Including Annex A-B, February 1997.

[10] "Global Circulation of IMT-2000 Terminals", ERC Report 60, September 1998.

[11] UMTS Forum Report No. 8: "The Future Mobile Market", March 1999.

[12] UMTS Forum Report No. 9: "The UMTS Third Generation Market – Structuring the Service Revenue Opportunities", October 2000.

[13] UMTS Forum Report No. 10: "Shaping the Mobile Multimedia Future", October 2000.

[14] UMTS Forum Report No. 11: "The UMTS Third Generation Market – Structuring the Service Revenue Opportunities", October 2000.

[15] UMTS Forum Report No. 12: "Naming,Addressing and Indentification Issues for UMTS", February 2001.

[16] UMTS Forum Report No. 13: "The UMTS Third Generation Market –Phase II", April 2001.

[17] UMTS Forum Report No. 14: "Support of Third Generation Services using UMTS in a Converging Network Environment", February 2002.

[18] UMTS Forum Report No. 15: "Key Components for 3G Devices", January 2002.

[19] UMTS Forum Report No. 16: "3G Portal Study", November 2001.

[20] UMTS Forum Report No. 17: "The UMTS Third Generation Market Study Update", December 2001.

[21] UMTS Forum Report No. 18: "UMTS 3G Market Forecasts", February 2002.

[22] UMTS Forum Report No. 19: "Benefits and Drawbacks of Introducing a Dedicated Top Level Domain within the UMTS Environment", March 2002.

[23] UMTS Forum Report No. 20: "IMS Service Vision for 3G Markets", May 2002.

[24] UMTS Forum Report No. 21: "Charging, Billing and Payments Views on 3G Business Models", July 2002.

[25] UMTS Forum Report No. 22: “Impact and Opportunity: Public Wireless LANs and 3G Business Revenues”, July 2002.

[26] UMTS Forum Report No. 23: “A Harmonized Frequency Solution for Early Implementation of UMTS/IMT-2000 in Central and South American Countries, July 2002

[27] UMTS Forum Report No. 25: “WLAN Spectrum Report”, updated May 2003

[28] UMTS Forum Report No. 26: “Social Shaping of UMTS- Preparing the 3G Customer”, January 2003

[29] UMTS Forum Report No. 27: “Strategic Considerations for IMS-the 3G Evolution”, January 2003

[30] UMTS Forum Report No. 28: “Relative Assessment of UMTS TDD and WLAN technologies”, March 2003

- Ref: Prof. Mike Walker
- UMTS Security, K.Boman,G. Horn,P.Howard and V.Niemi “Electronics & Communication Engineering Journal”, October 2002.
- 3GPP TS 21.102 V4.3.0 3rd Generation mobile systems Release 4 specifications (Release 4)
- 3GPP TS 21.133 V4.1.0 3G Security; Security Threats and Requirements (Release 4) 23
- 3GPP TS 23.101 V4.0.0 General UMTS Architecture (Release 4)
- 3GPP TS 33.102 V4.3.0 3G Security; Security Architecture (Release 4)
- 3GPP TS 33.120 V4.0.0 3G Security; Security Principles and Objectives (Release 4)
- 3GPP TS 21.103 V1.1.0 3rd Generation mobile systems Release 5 specifications (Release 5)
- 3GPP TS 23.002 V5.5.0 Network Architecture (Release 5)
- 3GPP TS 23.228 V5.3.0 IP Multimedia Subsystem (IMS); Stage 2 (Release 5)
- 3GPP TS 33.203 V1.1.0 Access security for IP-based services (Release 5)
- 3GPP TR 33.900 V1.4.0 A Guide to 3rd Generation Security The importance of TR 33.900, and the importance of risk assessment and network/service specific security design, really need to be stressed in the report. Experience shows that it is pointless standardising security when suppliers argue about whether a feature is “mandatory for implementation by the supplier and optional for use by the operator” and when operators argue that they can procure a cheaper system, integrate more legacy systems, provision more customers if they turn security off. Perhaps some anonymous case studies of how not to do it would be useful e.g. turning GPRS security off to get more traffic through an SGSN and building prepay ”value” into handsets etc. Seems unfair to single out the IEEE and WLAN.