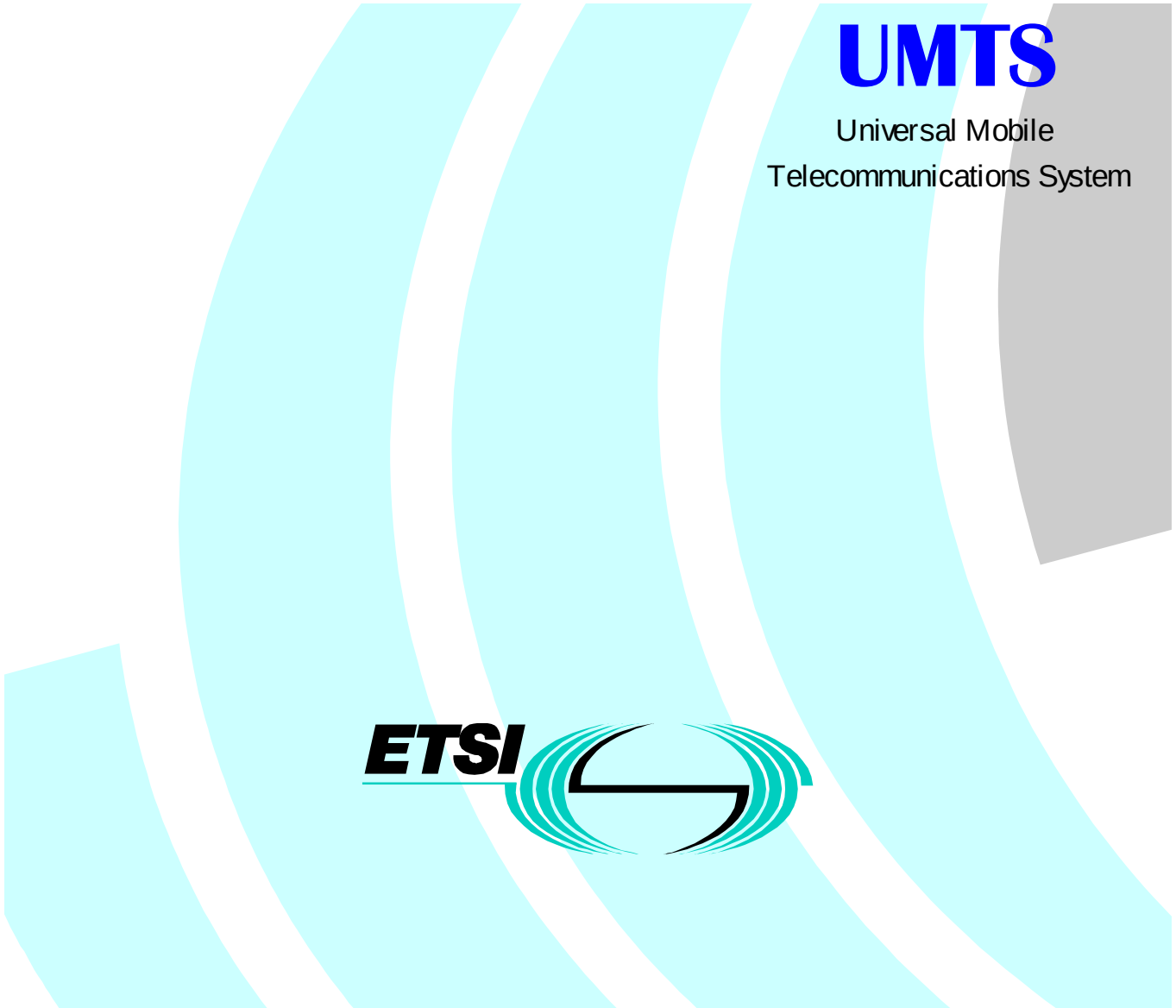
UMTS 33.20 V3.1.0 (1999-02)

Technical Report

Universal Mobile Telecommunications System (UMTS); Security Principles (UMTS 33.20 version 3.1.0)



Reference
DTR/SMG-103320U

Keywords
Universal Mobile Telecommunications System
UMTS SECURITY

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
http://www.etsi.fr
http://www.etsi.org

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This technical report has been produced by the Special Mobile Group (SMG) of the European Telecommunications Standards Institute (ETSI).

This report addresses all aspects of Universal Mobile Telecommunications System (UMTS).

The contents of this report is subject to continuing work within SMG and may change following formal SMG approval. Should SMG modify the contents of this report, it will be re-released by SMG with an identifying change of release date and an increase in version number as follows:

Version 3.x.y

where:

3 indicates UMTS;

x the second digit is incremented for all other types of changes, i.e. technical enhancements, corrections, updates, etc.;

y the third digit is incremented when editorial only changes have been incorporated in the specification.

1 Scope

This technical report addresses all aspects of Universal Mobile Telecommunications System (UMTS) security. It provides a basis for subsequent standardisation in a series of technical specifications.

In clause 4 the general objectives for the provision of security in UMTS are listed.

In clause 5 the context in which the security principles for UMTS are developed is described. First the system assumptions that describe UMTS in general and especially those that have a significant bearing on security are listed. Then, an extended role model is compiled. Besides the typical roles closely involved in service provision, this role model also includes many other roles which: either are of special interest to security (e.g. trusted third parties), must co-operate in order to realise the desired level of security (e.g. manufacturers) or have an interest (regulatory authorities, other party). Further, an overview of the UMTS system architecture is included, as well as an overview of the different data types that exist in UMTS.

In clause 6 the threats to security are listed according to point and nature of attack.

In clause 7 the security requirements with respect to UMTS are listed.

In clause 8 requirements on security features are given and a possible classification of features is presented.

In clause 9 security mechanisms are given that might be used to implement the security features.

Clause 10 is devoted to security management.

Clause 11 is about security devices in general and the User Services Identity Module (USIM) in particular.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative references

[1] UMTS 22.01: “Universal Mobile Telecommunications System (UMTS): Service aspects; service principles”.

[2] UMTS 22.71: “Universal Mobile Telecommunications System (UMTS): Service aspects; automatic establishment of roaming relationships”.

[3] UMTS 30.01: “Universal Mobile Telecommunications System (UMTS): UMTS Baseline document; positions on UMTS agreed by SMG”.

[4] ETR 331 Security Techniques Advisory Group (STAG): “Definition of user requirements for lawful interception of telecommunications - Requirements of the law enforcement agencies”.

[5] ISO/IEC 9798, part 2: "Entity authentication using symmetric techniques".

[6] ISO/IEC 9798, part 3: "Entity authentication using a public key algorithm".

[7] ISO/IEC 9798, part 4: "Entity authentication using non-reversible functions".

[8] ISO/IEC 9798, part 5: "Entity authentication using zero knowledge techniques".

[9] ISO/IEC 9797: “Message authentication codes”.

[10] ISO/IEC 10116: "Modes of operation of an m-bit cipher".

[11] ISO/IEC 10118: "Hash functions, part 1: General".

[12] ISO/IEC 10181: "Security framework standard".

[13] ISO/IEC 11770: "Key management".

[14] ISO/IEC 13888: "Non-repudiation".

[15] ISO 7498-2: "OSI Security Architecture".

[16] Official Journal of the European Communities, 99/C329/01: Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications

2.2 Informative references

[17] LINK PCP, 3GS3, Technical Report 1: “Security Features for Third Generation Systems”. Vodafone; GPT; Royal Holloway, University of London. Feb. 1996.

3 Definitions and abbreviations

3.1 Definitions

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

International Mobile Equipment Identity (IMEI): The IMEI uniquely identifies a mobile equipment. The IMEI is stored in the mobile equipment, for preference in a securely protected module, and at the network side by the terminal manager; it need not be known by the terminal owner.

International Mobile User Identity (IMUI): The IMUI uniquely identifies a user. The IMUI is stored in the International Mobile User Number (USIM) and the home environment database; but need not be known to the user. Although only one IMUI is associated with a particular (logical) user, a person or entity (the physical embodiment of a user) may have more than one (logical) user associated with it. Thus, a person or entity may be associated with more than one IMUI.

International Mobile User Number (IMUN): A user can be reached by using an international mobile user number (IMUN), see UMTS 22.01. This is a diallable number through which the user is addressable and identifiable, irrespective of the UMTS mobile equipment or point of attachment being used.

Smart card: a physical unit that contains a chip and can be inserted and removed from mobile equipment. It can contain one or more applications. A notorious example of an application on a smart card is the User Services Identity Module (USIM).

UPT Application: UMTS shall support Universal Personal Telecommunication (UPT) Phase 2 where the USIM and UPT Phase 2 are realised as distinct applications on the same smart card. This will permit personal mobility between UMTS and fixed networks for UPT users, subject to agreements between UMTS network operators and UPT service providers and between UMTS home environments and fixed network operators.

User Services Identity Module (USIM): an application that represents and identifies a user in the UMTS network. The USIM contains functions and data needed to identify and authenticate the user when UMTS services are accessed, as well as a copy of the user’s user profile. In particular the USIM contains the user’s IMUI and any security parameters that need to be carried by the user. The USIM is always implemented in a smart card.

3.2 Abbreviations

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

APM	Alternative Payment Method
B-ISDN	Broadband ISDN
BS	Base Station
DMO	Direct Mode Operation
GPRS	General Packet Radio System
GSM	Global System for Mobile communications
IMEI	International Mobile Equipment Terminal Identity
IMUI	International Mobile User Identity
IMUN	International Mobile User Number
IMT-2000	International Mobile Telecommunications-2000
IN	Intelligent Network
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunications Union
ME	Mobile Equipment
MS	Mobile Station
PIN	Personal Identification Number
PMR	Private Mobile Radio
PSTN	Public Switched Telephone Network
TMN	Telecommunications Management Network
TTP	Trusted Third Party
UMTS	Universal Mobile Telecommunications System
UPT	Universal Personal Telecommunication
USIM	User Services Identity Module
VASP	Value-Added Service Provider
VHE	Virtual Home Environment

4 General objectives for security

The principal security objectives underlying the provision of UMTS services (for information see LINK PCP, 3GS3, Technical Report 1: “Security Features for Third Generation Systems”. Vodafone; GPT; Royal Holloway, University of London. February 1996) are:

a) to ensure that information generated by or relating to a UMTS user or subscriber is adequately protected against misuse or misappropriation;

b) to ensure that the resources and services provided by a UMTS home environment or network operator are adequately protected against misuse or misappropriation;

c) to ensure that the security features standardized in UMTS are compatible with world-wide availability of UMTS;

d) to ensure that the security features provided by UMTS are adequately standardized to enable secure world-wide interoperability and roaming between different network operators.

Whereby a general guideline should be:

a) to ensure that the level of protection afforded to users and providers of UMTS services should be at least equal to that provided in contemporary fixed networks.

Special attention is drawn to the ability:

a) to ensure that mechanisms are in place for fraud management;

b) to ensure that lawful interception of a users communications be possible in accordance with national law;

c) to ensure that the problem of stolen mobile equipment is adequately addressed;

d) to ensure that emergency services are adequately protected against abuse.

5 Security context

The purpose of this clause is to describe the context in which the UMTS security principles are developed. The security context is described in terms of the following:

a) UMTS system assumptions that are considered to have a significant bearing on the security principles adopted;

b) a role model for UMTS which details the relationships between the various logical parties involved in the use, provision, regulation, administration, etc., of UMTS services;

c) the various types of information considered in UMTS.

5.1 System assumptions

In this subclause the key objectives, requirements and features of UMTS are listed which are considered to have a great impact on the security principles to be adopted for UMTS. These assumptions are based on UMTS 22.01 and UMTS 30.01.

a) Type of services and service management;

UMTS shall support the full range of services from narrow-band (most important: speech) to wide-band (2 Mbit/s as target) based upon an advanced high efficient and flexible radio access scheme (see UMTS 30.01).

UMTS will allow service creation. It will allow the creation of innovative services and individualised user profiles and support the ability to download them to users (see UMTS 22.01 and UMTS 30.01).

b) Access to services;

UMTS is a wireless mobile system. Mobility must include user and terminal mobility to permit roaming. UMTS will allow national and international roaming between networks subject to regulations and inter-operator agreements. These agreements may be set-up statically or dynamically (see UMTS 30.01).

UMTS will accommodate a variety of terminals ranging from those which are small enough to be easily carried on the person to those which are mounted in a vehicle (see UMTS 30.01).

UMTS may support the UPT service concept.

c) Service provision;

UMTS will offer the user the same services using the same interface irrespective the current location of that user; this is referred to as offering the user a Virtual Home Environment (VHE) (see UMTS 22.01 and UMTS 30.01).

UMTS users will have personal user profiles to which they will have direct but limited access.

UMTS will adhere to legal requirements imposed by national authorities e.g. type approval, data protection act.

d) System architecture;

UMTS may support a variety of different radio interfaces, including a satellite segment.

UMTS will support the sequential use of radio interfaces.

UMTS will be provided by an open system architecture based on Intelligent Network (IN) and Telecommunications Management Network (TMN) principles, taking into consideration architectures used in existing mobile networks.

UMTS will support services with a greater range of bit rates. Therefore, cell sizes in UMTS will correspondingly vary over a wider range than in present cellular systems. Moreover, cell/base station technology may exist within, or very close to, user premises.

UMTS base stations can be installed uncoordinated (to the extent that no frequency planning is necessary nor is a licence required for use of the radio spectrum) (see UMTS 30.01).

e) Security management;

UMTS will operate such that security and fraud control originate at all times from the home environment (see UMTS 30.01).

UMTS users will have unique identities.

UMTS mobile equipment may have unique identities.

f) Interworking and compatibility;

UMTS will admit the connection of users to other UMTS users and to users of other telecommunications networks (e.g., Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), Broadband ISDN (B-ISDN) and mobile systems that use direct satellite links).

UMTS is planned as a member of the International Mobile Telecommunications -2000 (IMT-2000) family. It is intended to specify roaming with other members of the IMT-2000 family based on marked need and business viability. It is intended to submit the defined terrestrial radio access system as a candidate to ITU. It will meet or exceed the essential ITU minimum requirements.

UMTS will admit the provision of services in an environment of multiple network operators and home environments, public or private, some of which are in direct competition.

UMTS shall support secure Global Cross-standard Roaming (see UMTS 30.01).

5.2 Role model

This subclause provides a description of the various parties or organisations involved in the use, provision, and regulation of UMTS services and the relationships between them. The descriptions are given purely from a security perspective to enable the security requirements for UMTS to be identified in a systematic manner.

It should be noted that these roles represent purely logical entities, and are not intended to reflect actual legal parties, human beings, or physical machines.

In many cases, some of the parties involved in the provision and use of UMTS will be grouped into a single entity. For example a particular company may act as both a home environment, a serving network and an access network. Similarly, a person could be both a subscriber and a user. The different roles are grouped in four groups (see figure 1).

Off-line group:

- Subscriber
- Regulator
- Type approval agency
- Manufacturer
- Terminal owner

Non-UMTS infrastructure group:

- Non-UMTS network operator
- UPT service provider
- Trusted third party
- Terminal manager

User group:

- User
- UPT user
- Second user

UMTS infrastructure group:

- Home environment
- Serving network
- Access network

- Other Party
- Transport network
- Value-added service provider

Figure 1: Grouping of the UMTS roles

5.2.1 User group

5.2.1.1 User

A user is a person or other entity that has been authorised to use UMTS services by a subscriber. His usage is delimited and described in the user's user profile, by which the subscriber authorises the user the use of some or all of the UMTS services to which he is subscribed. A user may have limited access to his user profile, in order to read or modify certain service parameters.

5.2.1.2 UPT user

A UPT user is a person that has a UPT subscription with a UPT service provider. UPT enables a UPT user to access services via any mobile equipment, irrespective of geographic location and networks utilised. Access to services is based upon a personal UPT number and a set of UPT access and control procedures, typically via a UPT application on a smart card. He has access to services from a UMTS mobile station without the need for additional devices specific to UMTS when a roaming agreement exists between his UPT service provider and a (UMTS) serving network (see also UMTS 22.01).

If the smart card inserted into UMTS mobile equipment provides USIM and UPT applications then precedence shall be given to the USIM application, i.e., the user will register as a UMTS user. If the smart card inserted into the UMTS does not provide a USIM application or the user fails to register as a UMTS user (e.g. the user may not have subscription via a UMTS home environment with whom the access network has an agreement) then the user will register with the UPT service provider, provided the UPT access number or access address identifies a UPT service provider with whom the UMTS access network has an agreement and the user's UPT number or personal user identity identifies the user as having a subscription to the UPT service provider.

5.2.1.3 Second user

A second user a person or entity that is allowed to access services using the user/subscriber/home environment relationship from a user that is not himself. The charges incurred by a second user can either be settled entirely between user, subscriber and second user, or the home environment might provide in a service that averts charges from the subscriber account to a bank account or credit line, associated with the second user.

5.2.1.4 Other party

An other party is a telecommunications user who is either the calling party in a call to a UMTS user, or the called party in a call from a UMTS user.

An other party may have its own security requirements.

5.2.1.5 Third party

A third party denotes an person or entity who is not directly involved with the provision and use of UMTS services but may be affected by them. A third party is not necessarily a UMTS user. A third party will usually, but not always, be a user of telecommunication services. There may be legal requirements on the protection of third parties.

5.2.2 UMTS infrastructure group

5.2.2.1 Home environment

Home environment is 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 commercial agreement established with a subscriber.

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, user devices, subscription charges. It also includes all billing mechanisms required to bill subscribers and second users for user charges and to pay network operators for user charges.

- The provision and maintenance of user profiles for subscribers and associated users, including the provision and control of access to user profiles by users and subscribers.

- Negotiation with network operators for network capabilities needed to provide UMTS 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.

5.2.2.2 Access network

Access network is the role that provides radio resources and local mobility management to support the services offered to the users. Access network capabilities are provided on behalf of home environments, with which the access network has an appropriate agreement, for the benefit of the users associated with those home environments.

Access network responsibilities fall in three 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 collection of charging and accounting data and the transfer of such data to home environments, value added home environment and other network operators.

- The interaction with and provision of facilities for home environments to identify, authenticate, authorise and locate users.

5.2.2.3 Serving network

Serving network is the role that provides fixed capabilities to switch 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 responsibilities fall in four main areas:

- 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, value added home environment and other network operators.

- The interaction with and provision of facilities for home environments to identify, authenticate, authorise and locate users.

- The interaction with and provision of facilities for terminal managers for terminal security management.

NOTE: The term "core network" is also used, it refers to that part of the network that does not belong to the access network.

5.2.2.3 Transport network

Transport network is the role that provides fixed capabilities to route the data generated by the services offered to the users. Transport network capabilities are provided on behalf of home environments, with which the transport network has an appropriate agreement, for the benefit of the users associated with those home environments.

Transport network responsibilities fall in two main areas:

- 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, value added home environment and other network operators.

5.2.2.4 Value-added service provider (VASP)

VASP is the role that provides services other than basic telecommunications service, e.g. content provision or upper layer capabilities, for which additional charges may be incurred. VASPs may send bills directly to the subscriber, or may send bills via the subscriber's home environment.

Editors Note: Do we need to think about the security implications of VASPs? Where is authentication done? Does the home environment do it or does it delegate to the VASP? Note that in the role model in UMTS 22.01 the VASP has (can have) a direct "usage" link to the serving networks. Does this then bypass entirely the home environment?

5.2.3 Non-UMTS infrastructure group

5.2.3.1 Non-UMTS network operators

Non-UMTS network operators is the role that provides telecommunication network resources other than UMTS resources and may be involved in the provision of UMTS services. These networks can act as one of the following:

- *Originating network:* the network from which a call to a UMTS user originates.
- *Intermediate network:* network that may be used to establish connections between UMTS networks.
- *Terminating network:* the network where the call from a UMTS user is terminated.

The security provided by a UMTS network should not depend on other networks, e.g., if security parameters are passed from one UMTS network to another through an intermediate network, then the intermediate network should not be relied upon to maintain the integrity or confidentiality of those parameters.

5.2.3.2 UPT service provider

UPT service provider is the role that has overall responsibility for the provision of a UPT service to UPT users. It is assumed that the UPT service provider is responsible for payment to the UMTS network operators with respect to resources used during the authentication of UPT users and the calls from and to UPT users.

The primary responsibility of a UPT service provider with respect to the service provision in UMTS networks is to negotiate with UMTS network operators for network capabilities needed to provide UPT services to its UPT users, including ensuring that UPT users are properly identified, located, authenticated and authorised to use services before those services are provided to them.

5.2.3.3 Trusted third party (TTP)

It may be necessary to establish trusted third parties for providing:

- directories of home environment, access network, subscriber or user security parameters (e.g. public keys, certificates of public keys);
- trustworthy time-stamps;

- a framework to facilitate roaming agreements between home environments and/or network operators and to set policies governing roaming;
- facilities for the exchange of data related to mobile equipment such as stolen mobile equipment.

Trusted third parties may be hierarchically ordered (e.g. certification authorities).

NOTE: Some functions of the TTPs may be provided by serving networks or home environments.

5.2.3.4 Terminal managers

Terminal managers is the role that has responsibility for UMTS mobile equipment registered in a particular administrative area. As such, a terminal manager is responsible for a set of IMEIs. A terminal manager is also responsible for the provision of resources and the management of data needed to combat the use of stolen, cloned and non type-approved mobile equipment.

NOTE: The need for a terminal manager has not yet been identified for UMTS. If such entities are necessary, then it is likely that the terminal manager will be closely associated with, or become part of, some other entity such as an access network, a core network, or possibly even the terminal manufacturer. For example, a mobile equipment could be registered with a home environment and the role of the terminal manager could then be carried out by the home environment.

5.2.4 Off-line group

5.2.4.1 Subscriber

The subscribers is a person or other entity which has a contractual relationship with a home environment on behalf of one or more users. A subscriber is responsible for payment of charges to that home environment. A subscriber is able to access the user profiles, of its associated users in order to read or modify certain service parameters associated with those users. A subscriber is identified by a unique subscriber account identifier (see UMTS 22.01).

5.2.4.2 Terminal owner

The terminal owner is the owner of mobile equipment capable for providing UMTS services.

5.2.4.3 Regulators

Regulators is the role of any body which is authorised to set laws or guidelines governing the provision or use of UMTS services, or UMTS mobile equipment or networking equipment. Examples of regulators are national governments and their agencies, including law enforcement agencies, national security agencies, export control authorities, etc. The UMTS security features and mechanisms must be such that they do not inhibit the legitimate activities of such organisations.

5.2.4.4 Type approval agencies

Type approval agencies is the role of an organisation which is authorised by a regulator to ensure that the laws and guidelines relating to mobile equipment and networking equipment and UMTS services are complied with. Type approval agencies include certified test houses that conduct type approval testing of mobile equipment. In the context of UMTS security, such bodies may play a role in ensuring that mobile equipment security features are properly implemented.

5.2.4.5 Manufactures

Manufactures is the role of a company that develops, produces and sells mobile equipment and/or networking equipment, hardware as well as software, necessary for the provision of UMTS services.

5.2.5 Intruders

Intruders is the role of a party who attempts to breach the confidentiality, integrity or availability of UMTS, or who otherwise attempts to abuse UMTS in order to compromise services or defraud users, home environments, network

operators or any other party. An intruder may attempt to eavesdrop on user traffic, signalling data and management data, or attempt to masquerade as a legitimate party in the use, provision or management of UMTS services.

5.3 Data types

Different types of data will require different amounts of protection. Therefore, we define the different data types occurring in UMTS service provision:

5.3.1 User data

This type comprises all data transmitted on the end-to-end traffic channel by users to other users. The data could be digital data, voice or any other kind of data generated by the user.

5.3.2 Signalling data

Charging data: This type comprises data relating to charges incurred by users whilst using network resources and services. Such data would normally be generated by core network operators and passed to home environments.

Billing data: This type comprises data relating to charges incurred by subscribers for their subscriptions and users charges. Such data is generated by a home environment (using charging data obtained from network operators and other home environments) and passed to subscribers.

Location data: This type comprises location data regarding a user (or mobile equipment). Such data is generated by a network operator and passed to the user's home environment (it may be retained by the network operators).

Dialling data: This type comprises data relating to diallable numbers associated with users. Such data is generated by home environments and distributed to users. It is transferred from a user to a serving network to initiate a call, and then passed by the serving network to the associated user's home environment.

Identity data: This type comprises data that determines the identity of a network role or network entity. The roles and entities of interest are usually users, subscribers or mobile equipment. *User* and *subscriber identities* are generated by the appropriate home environment, and are held by both the home environment and the user or subscriber respectively. In addition, a user's identity will be held by the appropriate subscriber. *Mobile equipment identities* are generated by the terminal managers (or equipment manufacturer), and are held by both the terminal manager and mobile equipment. User identities may accompany user-related data such as charging, billing, and location when it is passed between entities. Similarly, subscriber identities accompany billing data when it is passed between home environment and subscriber.

Security management data: This type comprises data relating to security management. It includes such data as encryption keys and authentication messages. It may be generated by a third party or by the involved entities themselves.

5.3.3 Control data

Routing data: This type comprises data passed through the network to enable correct routing of calls. Such data will be generated by network operators (using location and dialling data) and passed amongst network operators.

Network resource management data: This type comprises data relating to the physical access of mobile equipment to the network operator and to the physical interface between network operators. Such data is generated by network operators and passed amongst network operators and mobile equipment.

Access control management data: This type comprises data relating to access control to mobile equipment, network resources and user profiles. Such data may include Personal Identification Numbers (PINs) generated by users, and databases of identities generated by network operators. It is generally stored by the generating entity.

Service profile data: This type comprises data regarding the user profiles of users. Such data is generated and passed between a user, the user's subscriber and the subscriber's home environment.

Additional call control data: This type comprises all data needed to set up, maintain, or release a call, other than identity, dialling and routing data. Such data will be generated by users or network operators and passed between users and network operators, or between network operators.

6 Security threats

6.1 Radio interface

6.1.1 Loss of confidentiality

a) Interception by monitoring at a radio interface using a commercial scanner to intercept digital radio interfaces.

b) Interception by monitoring at a radio interface using a scanner that can be built with sufficient knowledge of radio technology and UMTS specifications.

c) Interception by monitoring at a radio interface by a subscriber of the system using his (possibly modified) mobile station to listen to the communications of any channel. For this attack, only a little knowledge is necessary by anybody who has access to a stolen mobile station.

d) Attracting calls from mobiles using entity masquerading as a base station.

e) Test equipment or other device is used as a false base station.

6.1.2 Loss of traffic flow confidentiality

a) Traffic within a network is analysed revealing the rate of messages, the length of the messages, the sender or receiver identities.

b) Traffic within a network is analysed revealing that some messages are sent at a certain time and at a specific interface.

c) The behaviour of a specific (not necessarily known) subscriber is observed. For example, when this subscriber makes calls, which calls are from what location, and to which groups he/she belongs.

d) An attacker links a call to a specific subscriber (for example by calling him/her) and can then link all calls to that subscriber.

6.1.3 Loss of integrity

a) Deletion of parts of the message or file or deletion of the whole message or file by deliberately transmitting on the same channel as the MS.

b) Deletion of parts of the message or file, deletion of the whole message or file, accidentally. When mobile station MS1 is sending to base station BS1 and MS2 is sending to BS2 on the same frequency and time slot and MS1 falls into a radio gap, MS2 is received by BS1. If there is no possibility to distinguish the mobile stations at a very low level, BS1 will handle the data from MS2 as if it were from MS1.

c) An attacker uses his detailed knowledge of system performance to make very accurate modifications to messages or files. When mobile station MS1 is sending to base station BS1 and MS2 is sending to BS2 on the same frequency and time slot and MS1 falls into a radio gap, MS2 is received by BS1. If there is no possibility to distinguish the mobile stations at a very low level, BS1 will handle the data from MS2 as if it were from MS1.

d) Insertion of pre-recorded data and voice signals that have been enciphered and do not need to be understood by the attacker.

e) Receiving the information intended for a user by masquerade as that user (or mobile equipment) by means of replay of data.

6.1.4 Denial of service

a) Denial of service caused an attacker jamming the radio path.

6.2 System infrastructure

6.2.1 Loss of confidentiality

a) Interception by monitoring with a tap on the wire of any system interface and using a commercially available (and possibly modified) protocol analyser to understand the information sent.

b) Interception and/or manipulation of data by accessing all information processed or stored within an entity of the system. This attacker needs physical access to a network node, for example a base station, and good knowledge of the internal working of the system. The attacker is likely to be an insider, such as maintenance or operating personnel.

c) Receiving the information intended for a fixed entity by masquerade as a fixed entity of the system at any of its interfaces. These attacks, by replay of data for example, have the disadvantage that it is necessary to cut existing connections, an operation that might be noticed.

d) Masquerade as a system entity over an interface that is not permanently connected.

6.2.2 Loss of integrity

a) An attacker can use some equipment at any interface of the system to manipulate the data and voice signals being transferred by the interface.

b) Deletion can be carried out, for example by physical action like cutting a wire to an interface.

c) Deletion by manipulation of the data header to reroute the data normally carried by the interface.

d) An insider, such as maintenance engineer with physical access to an entity in the system and good knowledge of the internal working of the system, can manipulate the data or voice signals processed or stored.

e) Masquerading as a system entity (possibly with the help of replay of messages), over an interface that is permanently connected to manipulate the through-going data. Existing connections need to be cut and will be noticed.

f) Masquerading as a system entity (possibly with the help of replay of messages), over an interface that is not permanently connected. This attack may not be immediately noticed.

g) Insertion of the own voice of the attacker for calls in which the communicating parties do not know each other or if the recognition of the voice cannot be guaranteed.

6.2.3 Denial of service

a) Denial of service caused an attacker disconnects a node from the system either by manipulating the system configuration or by physical manipulation (e.g. wire cutting).

b) Denial of service caused by an attacker erasing all messages passing through a specific interface.

c) Denial of service caused by an attacker delaying messages going in one or both directions.

d) Denial of service caused by an attacker, who could be an authorised user, overflowing the system with messages generated by him/herself.

6.2.4 Unauthorised access

a) A legitimate subscriber or operator of the system gathers information about other users for which they do not have authorised access.

b) An attacker can masquerade as another subscriber and execute the access rights of this subscriber to access to prohibited resources, for example access to the system as a whole, or access to specific services.

c) An attacker can use stolen or non-type approved equipment to access prohibited resources.

d) An attacker with sufficient knowledge of the internal working of the system may be able to acquire additional access rights or circumvent access control mechanisms.

e) An attacker might misuse some information he/she got for other purposes, e.g. the network operator or users home environment can misuse some personal data of subscribers

f) An attacker who has borrowed some equipment, e.g. a mobile station, and who is allowed to use this equipment only to a certain extent can nevertheless try to excess the limits.

6.3 Applications

a) Repudiation of delivery where one person sends a message to another person and the message is received by this second person. However, the receiving person then denies the receipt of the message.

b) Repudiation of origin where one person sends a message to another person and the message is received by this second person. However, the sending person then denies having sent the message.

c) New services weaken security of existing network

d) New services have intrinsic security weaknesses

e) Interconnection between UMTS and other networks (e.g. Internet Protocol (IP) based) weakens UMTS security.

f) Specified security algorithms become compromised by advances in cryptanalysis or computing power

6.4 Terminal equipment

a) An attacker can use stolen or non-type approved equipment to access prohibited resources.

b) An attacker with sufficient knowledge of the internal working of the system may be able to acquire additional access rights or circumvent access control mechanisms.

c) An attacker who has borrowed some equipment, e.g. a mobile station, and who is allowed to use this equipment only to a certain extent can nevertheless try to excess the limits.

7 Security requirements

This clause identifies the requirements for security in UMTS. These requirements have been developed from the need to counter the specific threats identified in the previous clause and with reference to the roles played by the various entities involved in UMTS (see subclause 5.2).

As it is difficult to predict the exact nature of the services that will be offered, this clause defines a set of generalised requirements that should be applicable irrespective of the actual service offered. These requirements, and the threats they are intended to address, will need to be continuously reviewed, particularly as experience is gained of future Global System for Mobile communications (GSM) services such as the General Packet Radio Service (GPRS) and the Cordless Telephony System (CTS).

7.1 Confidentiality

7.1.1 Confidentiality of user traffic

a) The confidentiality of user traffic shall be ensured while transmitted over the radio interface between the mobile station and the base station.

b) serving networks can provide an end-to-end user traffic confidentiality service to users, when accompanied with key recovery scheme intended for lawful interception.

c) An end-to-end confidentiality service for user traffic without key recovery scheme can be operated on the network. Access to these services will be determined by regulatory authorities. All functionality and operational control shall be contained entirely within the mobile stations.

d) The confidentiality of user traffic shall be ensured while transmitted over any radio interface between network nodes.

7.1.2 Confidentiality of signalling

a) The confidentiality of signalling shall be ensured while transmitted over the radio interface between the mobile station and the base station. As an exception, some signalling messages may be exchanged during the initial stage of the user authentication protocol before a ciphering key agreement is established. These messages however, may not jeopardise requirement b) to f).

b) At all times the confidentiality of the user identity shall be protected when transmitted over the access interface.

c) At all times the confidentiality of user profile information shall be protected when transmitted over the access interface.

d) At all times the confidentiality of the home environment identity shall be protected when transmitted over the access interface.

e) At all times the confidentiality of the subscriber identity shall be protected when transmitted over the access interface.

f) At all times the confidentiality of location information shall be protected when transmitted over the radio interface.

g) The confidentiality of signalling shall be ensured while transmitted over any radio interface between network nodes.

which yields features such as encryption along network-network microwave links.

h) Home environments can enable end-to-end confidentiality for signalling between home environment and user.

i) Serving networks can enable end-to-end confidentiality for signalling between each other.

j) The possibility for multi-user calls on one terminal must not jeopardise the security of the different calls.

7.2 Integrity

7.2.1 Integrity of user traffic

a) The integrity of user traffic shall be ensured while transmitted over the radio interface between a mobile station and a base station.

b) The user can enable end-to-end user traffic integrity.

c) The integrity of user traffic shall be ensured while transmitted over any interface through radio between network entities.

7.2.2 Integrity of signalling

a) The message authenticity of signalling shall be ensured while transmitted over the radio interface between the mobile system and the access network.

b) The message authenticity of signalling shall be ensured while transmitted over any interface through radio between network nodes.

which yields features such as signatures and checksums along microwave links.

a) Home environments shall be able to enable end-to-end message authenticity for signalling between home environment and user.

b) Serving networks shall be able to enable end-to-end message authenticity for signalling between each other.

7.3 Authentication

7.3.1 User related authentication

a) The home environment shall be able to authenticate the user at connection set-up as well as throughout service delivery.

b) The user shall be able to authenticate the access network identity at any time.

c) Users shall be able to enable end-to-end user authentication.

7.3.2 Infrastructure domain authentication

a) With respect to network-network interfaces across network operator domain borders:

- Any network operator shall be able to authenticate any other network operator.
- Any receiving network operator shall be able to authenticate the source of data throughout the transmission phase when data is sent over fixed network lines between network operator domains.

b) With respect to network-network radio interfaces between nodes of the same network operator:

- Any receiving network node shall be able to authenticate the node identity of the sending network node at connection set-up and that of the data source during the subsequent transmission phase when data is sent over a radio interface.

Figure 2 illustrates the latter two requirements.

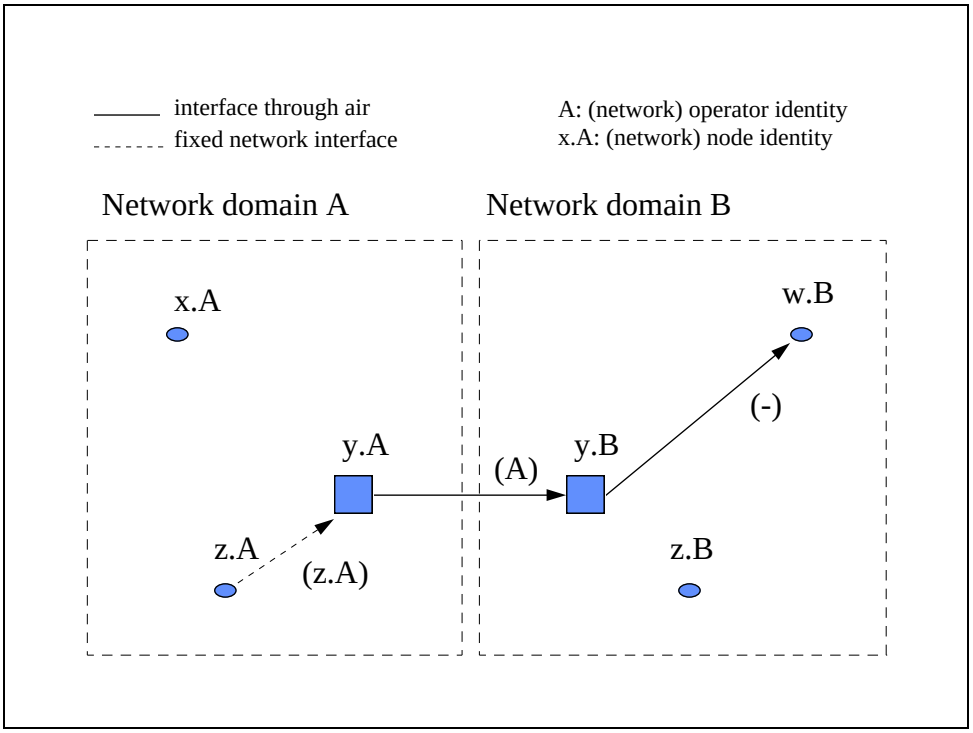


Figure 2: Authentication in network operator domains and across domain borders

NOTE: In figure 2 what is between parenthesis is what is may be authenticated by the other entity. To protect the integrity of over fixed network lines across network operator domain and not of other fixed network lines, is not primarily for any reason that these lines are more vulnerable for tampering. It is more useful since it helps to identify the organisation responsible for losses and malfunctions, and it might come along with a non-repudiation feature implemented on those links anyway. Further steps, allowing the organisation responsible for the malfunction to trace the affected node or link, are at the discretion of that organisation and can be taken from a fraud management point of view.

7.4 Availability

a) Radio channels (particularly control channels) shall be protected against jamming, e.g. by detection and automatic channel re-assignment.

7.5 Access control

a) The subscriber and the user shall have the ability to restrict the usage of the USIM by implementing an access control protocol.

b) Home environment databases containing personal information related to subscribers shall be provided with access control.

c) Terminal manager databases that contain information on ownership of terminal equipment shall be provided with access control.

Examples may be PIN-codes or non-cryptographic user authentication mechanisms.

7.6 Data protection

To allow the home environment to protect information related to persons within his organisation:

a) All forwarding and processing of personal information shall be logged.

To ensure that a USIM information is protected:

b) Data that only has to be used within the USIM, e.g. data for authentication of a user (keys, cryptographic algorithms…) shall not be accessible via the USIM-ME interface.

c) Data that are permanent identities or other values and parameters that are not allowed to be changed, e.g. permanent user identities which must remain fixed for a period of time like IMUI, shall not be accessible by the user. Access control shall be provided for serving network and home environment access.

d) Data that are temporary identities or other information that only are allowed to be changed by the serving network or home environment, e.g. a temporary identity, user profile, services and applications for telecommunication applications and other non-telecommunication applications, shall not be accessible by the user. Access control shall be provided for serving network and home environment access.

To allow the network operator to protect information related to persons according to legal demands:

e) Databases containing personal information shall be provided with access control.

f) All forwarding and processing of personal information shall be logged.

Serving networks as well as users might be concerned about the threat that monitoring the traffic intensity might reveal some information that is not to leak. In order to hide the traffic intensity of the real data, users and network operators having that concern might want to generate dummy traffic that cannot be discerned from meaningful traffic by the transporting network.

g) Users and network operators shall be able to generate dummy traffic that will be transported transparently through the network.

7.7 Anonymity and pseudo-anonymity

a) Users will be able to enable a service that ensures them to remain anonymous towards the second party (called party).

b) Users will be able to restrict exposure of their location information while accessing the UMTS network.

Part of the anonymity concerns of users are addressed also by the access control requirements in subclause 7.5.

7.8 Protection of resources

To allow the network operator to protect the infrastructure of the system:

a) Protection against unauthorised use of services shall be provided.

b) Protection against unauthorised use of radio resources (e.g. misuse of priorities) shall be provided.

c) Databases shall be provided with access controls.

d) The state of every part of the infrastructure shall be made known.

e) Configuration and network management facilities shall be provided with access controls.

f) A fall-back mode of security in case of network degradation shall be provided.

g) Facilities shall be provided for the disabling of mobile equipment.

To allow the users home environment to control the use of services:

h) Facilities for the management of authorisation shall be provided.

i) Facilities for the enforcement of authorisation shall be provided.

To allow the owner of the mobile station to protect his mobile:

j) Stolen or lost mobile stations shall be protected against misuse.

k) Blacklist management system shall be provided.

7.9 Security management

To inform the network operator about status of security within the network:

a) Security relevant information shall be recorded.

b) Security relevant events shall generate alarms.

c) Detection of jamming at the radio interface shall be provided.

d) The network operator shall provide reports on authentication failures to home environments.

To allow the network operators to control the security functions within the network:

e) Security functions shall be customised to users' needs.

f) Security functions shall be adaptable to current situation.

To inform the home environment about status of security within the network, in particular end-to-end security:

g) Security relevant information shall be logged.

To allow the home environment to control end-to-end security:

h) Security functions shall be adaptable to current situation.

To inform the user about status of security within the network, in particular end-to-end security:

i) An indication of security level and state shall be provided to the user.

To allow the user to control end-to-end security:

j) End-to-end security functions shall be selectable and adaptable to current situation.

7.10 Non-repudiation

a) To allow the sender of a message to prove that the message was received by the recipient a non-repudiation of delivery service shall be provided.

b) To allow the recipient of a message to prove that the message was sent by the sender a non-repudiation of origin service shall be provided.

7.11 Charging and billing

To allow a serving network to secure charges towards a home environment:

a) Charging has to be secure, accurate and reliable.

b) If charging is based on the duration of the communication, the beginning and the end of the communication have to be defined, accurate, reliable and incontestable.

c) If charging is based on the amount of transferred information, the calculation has to be defined, accurate, reliable and incontestable.

d) It shall not be possible for the user or for the subscriber to impose charging to another user or another subscriber without consent of the latter.

e) It shall be possible to limit charges incurred by the home environment.

To allow the network operator to secure charges towards other network operators:

f) Other network operators shall be authenticated.

g) Users shall be authenticated.

h) Integrity (and confidentiality) of charging information shall be maintained.

i) Access to user profiles by other network operators shall be logged.

j) It shall be possible to limit charges incurred by the other network operators.

To allow the network operator to check charging by other network operator:

k) Information concerning type and duration of the calls (traffic logs, statistics) shall be secured.

l) The quality of the authentication procedure used by the other network operators shall be checked.

To allow a users home environment to check charging concerning his organisation:

m) Information concerning type and duration of the calls (traffic logs, statistics) shall be secured.

n) The quality of the authentication procedure by network operator shall be checked.

To allow the home environment to secure charges towards subscribers:

o) The type and duration of each call shall be measured.

p) Access to user profiles by users shall be logged.

q) It shall be possible to limit charges incurred by subscribers.

To allow the subscriber to check charging concerning his calls:

r) the users have be informed in forehand about the actual charging principles and rates used (e.g. if the charging is based on duration of communication, amount of transferred information, source or receiver of the information, actual time of day of the communication, other matters that will be charged, etc.).

s) A secure advice of charge service shall be provided.

t) Billing has to be secure, accurate and reliable.

u) The user shall be informed of accumulated charges.

7.12 Lawful interception

a) Every interception and every attempted interception, whether lawful or otherwise shall be monitored and registered in accordance with the national law. This shall apply to devices and/or via interfaces placed by the network operators or home environments at the disposal of the national law enforcement agencies according to national law, and intended solely for lawful interception purposes.

b) Lawful interception has to be realised according to national legislation and the requirements as given in "Official Journal of the European Communities, 99/C329/01: Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications" and in ETR 331.

c) For lawful interception purposes the access network shall know the real user's identity.

7.13 Supplementary services

It is as yet unclear whether the specification of supplementary services for UMTS is within the scope of standardisation. It is possible that merely a framework for the implementation of such services will be provided. Supplementary services must be considered on an individual basis, to assess the risks associated with their implementation and use, and to determine adequate measures to ensure that security is not compromised. For example, international call barring may be

mandatory with certain services (e.g. call forwarding), multiple use of services may be limited (e.g. multiple call forwarding), or services may require multiple USIMs (e.g. multiple registration by a user).

7.14 UPT

Security requirements will arise from the additional services offered by UPT (e.g. remote access, multiple registration), as well as requirements due to the method by which UPT is supported (e.g. additional access control or authentication of UPT users may be necessary).

Many of the services offered by UPT can be viewed in such a way as to relieve the need for additional security requirements. Examples are multiple registration on a mobile equipment and remote registration, both of which can be viewed merely as supplementary services (and in which case the guidelines in subclause 7.13 should be noted). Another example is multiple registration by a user, which, given that distinct USIMs (with distinct IMUIs) are required for each registration, can be viewed simply as registrations by distinct users (the minor problem remains that these distinct users have the same diallable numbers)

7.15 Satellite component

This subclause identifies security issues relating to the satellite component of UMTS. This includes requirements specific to satellites, and requirements for which the nature of the satellite component merely leads to an extension of existing requirements. The UMTS satellite architecture(s) will have an impact on both the UMTS security requirements, and the UMTS security mechanisms.

7.15.1 Access control

The unauthorised use of satellites (as repeaters) is undesirable, because it may reduce, for example, the capacity or QoS, as well as undermining the commercial basis for services. If the threat is deemed sufficiently serious, then action may be required to discourage or prevent it. The extent to which this can be achieved will depend upon the satellite architecture. For example, it may be more difficult to protect satellites having no on-board processing capability.

7.15.2 Denial of service

Deliberate jamming of satellite transmissions may be difficult to prevent. Nevertheless, detection and location of the source of such activity may be possible. Although this is not a satellite specific problem, there may be mechanisms (e.g. user location) used for satellite operation that could assist in combating it. Spread spectrum techniques might also be advantageous. Jamming is not a satellite specific problem, but the associated large scale loss of coverage that could result, may make the threat more serious.

7.15.3 Key distribution

There is a need to protect transmitted data (traffic, signalling, and control) against eavesdropping (this may include inter-satellite traffic). Distribution of encryption keys to satellites may be an issue, although this will depend upon the satellite architecture. For example, if the satellites have on-board processing capability, and data is to be decrypted (and subsequently re-encrypted with different keys) at the satellite, then key distribution to, and amongst satellites is required. Alternatively, if the satellite merely acts as a bent pipe, then no additional key management is likely.

7.15.4 Lawful interception

Many governments will insist upon facilities for lawful interception of all communications, both within their own domains (both incoming and outgoing) and possibly in other domains by agreement with the relevant governments. Numerous requirements will therefore be imposed on the system on a national basis. For example governments may require real-time interception, and prevention of other outside authorities carrying out (unauthorised) interception. There may be difficulties regarding the interception of traffic within the satellite component, particularly if the area served by a ground station can include more than one country, if on-board encryption takes place, or if the system has no ground (switching) station.

7.15.5 Limitation of service domain

In terrestrial systems, the area served by a particular operator can be efficiently limited by physically restricting the location of base stations. Within the satellite component, such restrictions cannot be easily implemented. Thus, the question arises as to whether operators of satellite systems can, or need, to have their service domains limited, e.g. to respect national boundaries. This will depend to some extent on the licensing regime used for operators of such systems. The use of directional antennae and position locating functions may be helpful in this matter.

7.15.6 Impersonation

It is necessary to prevent intruders from impersonating elements of the network. Elements peculiar to the satellite component (e.g. satellites and gateways) may be at risk to such threats. There are a number of issues to consider, such as: are these elements considered part of UMTS, and are they at risk? The need for protection may depend upon the satellite architecture. For example, protection is unlikely to be necessary for "bent-pipe" satellites because they are essentially anonymous.

7.15.7 Location privacy

Information concerning the geographic location of a user may have to be transmitted over the radio path for effective satellite operation. The need for providing confidentiality of such data requires investigation.

7.15.8 Handover

A number of handover scenarios involving satellites are being considered for UMTS. Amongst these are some that depend upon the satellite architecture e.g. handover between satellites. This will have an impact on cryptographic key management, in particular, on the distribution of encryption keys to, and amongst, satellites.

7.15.9 Operation of mechanisms

All security mechanisms employed in UMTS must operate effectively within the satellite component. Factors that may influence the effectiveness of security mechanisms include satellite architecture, transmission quality, transmission speed and position location capability.

7.15.10 Other issues

Issues relating to the transmission links between satellites and ground stations may be outside the scope of UMTS. For example, data may have to be protected when passed over such links (i.e. confidentiality and integrity).

7.16 Private Mobile Radio (PMR) services

It is assumed that PMR type services will be supported by UMTS. A number of requirements will arise that are peculiar to such services.

PMR type services to be supported by UMTS can be considered in two groups:

1 The first group of services provides two way simultaneous multi-point communication between a single calling party and several called parties. This is known as a group call. The mobile users, who form the group, can change rapidly. There is a need for a mobile user to perceive a seamless handover between cells and to be able to enter a group call that is already in progress in the new cell. This requirement results in the need for a secure but rapid means of distributing security parameters such as encryption keys.

2 The second group of services provides communication between a mobile and one or more mobiles in a group. This is known as "direct mode operation" (DMO) and does not involve any form of network infrastructure. This is known as a "single hop DMO call". Repeaters, bridges or gateways, however, may be used in the communication path and these are known as "multiple hop DMO call". It is not yet clear whether DMO will be supported in UMTS.

Both groups of services require security mechanisms that:

a) Provide a secure means of distributing a common key for group calls over the radio interface.

b) Provide a secure means of distributing keys within the fixed infrastructure to the various base stations and to repeaters in the case of direct mode operation.

c) Provide control over synchronisation to allow for late entry to a group call and to determine call priorities.

d) Provide key management for the various mobility scenarios to achieve a seamless handover as perceived by the user.

e) Are transparent to any end to end encryption that may be used by the service at either end.

Many PMR systems are associated with a dispatcher role whose task is to use the radio system to control the organisation's resources. The following requirements have been identified:

To allow the dispatcher to authenticate users:

f) The quality of authentication mechanism used by the home environment shall be checked.

g) The home environment shall provide reports on authentication failures of users.

To allow the dispatcher to authenticate group membership:

h) Group members shall be registered, incl. late entry.

i) Group management tools shall be provided.

j) Dynamic group number reassignment shall be secured.

k) Remote change of parameters in the mobile shall be secured.

To allow the dispatcher to authenticate external connections:

l) Communication partners for outgoing calls shall be authenticated.

m) Communication partners for incoming calls shall be authenticated.

To allow the dispatcher to maintain the confidentiality of communication in his group:

n) Users shall be prevented from bypassing the security functionality.

To allow the dispatcher to maintain the integrity of communication in his group:

o) Users shall be prevented from bypassing the security functionality.

To allow the dispatcher to maintain traffic flow confidentiality within the group:

p) Covert identities for users and user groups shall be provided and managed.

To allow the dispatcher to monitor the traffic and the communication of his group(s):

q) The dispatcher responsible for monitoring or logging of actions shall be authenticated.

r) A facility for recording traffic, including end to end encrypted traffic, shall be provided.

To allow the dispatcher to control the use of services:

s) Facilities for real-time control and enforcement shall be provided.

t) Facilities for barring of incoming and outgoing external calls shall be provided.

u) Facilities for authorisation of calls by dispatcher shall be provided.

v) Facilities for disabling of mobile equipment shall be provided.

To inform the dispatcher about status of security within the network, in particular end-to-end security:

w) Security relevant information shall be logged.

x) Security relevant events shall generate alarms.

To allow the dispatcher to control end-to-end security:

y) Security functions shall be adaptable to current situation.

7.17 Mobile equipment

The following security requirements relate to the use of mobile equipment:

a) Access to a mobile equipment shall be controlled so that it can only be used by the owner, or by a party explicitly authorised by the owner.

b) Privacy of certain data stored in the mobile equipment shall be maintained.

c) Unauthorised modification to certain data stored in the mobile equipment shall be prevented.

d) Mechanisms shall be provided to deter, detect and prevent the use of mobile equipment that is not type approved but is otherwise acceptable for use.

e) The use of mobile equipment identified as being faulty shall be prevented.

f) The use of cloned mobile equipment should be prevented through a combination of adequate type approval and terminal authentication.

g) The IMEI identifies one piece of UMTS equipment and is allocated by the equipment manufacturer. The IMEI must be unique and protected against any unauthorised modification. IMEI interrogation via the radio interface should be carried out using the protection mechanisms of the radio interface.

Although there are clear requirements for the protection of mobile equipment as outlined above, it may be inappropriate to set up a costly infrastructure to provide the necessary security features to protect mobile equipment. In any event, the specification of mechanisms for protecting mobile equipment may lie outside the scope of standardisation.

In order to provide a management structure to enable registration of type approved mobiles, registration of manufactured mobiles, reporting of stolen mobiles, etc., on a national, regional and world-wide basis, it may be necessary to involve roaming administrators in mobile equipment security management. In which case there may well be other security requirements, e.g., securing read/write accesses to databases of type approved mobiles.

7.18 Fraud control

a) To detect intruders and to deter, detect and prevent the use of stolen or cloned mobile equipment mechanisms for the control and management of fraud shall be provided.

b) The service creation process shall included features to deter, detect and prevent the creation of services that may be at risk of fraud.

7.19 Alternative payment methods (APMs)

Within UMTS, secure APMs may be defined, i.e., ways of paying other than the conventional way where a user is billed after he has used services. APMs could be realised with USIMs in the form of prepaid cards or reloadable smart cards.

The payment system may also cater for non-UMTS applications. It could range from being able to pay for low cost services such as public transport and parking, to having full personal banking applications.

Requirements concerning alternative payment methods may include:

a) Subscriber and user information should be protected against disclosure to unauthorised parties.

b) It should be an open system i.e. enable participation of several financial institutes, home environments, retailers and users without the need for a relation of trust between them. Trust is needed between home environment and user, and between home environment and retailer.

c) Anonymous payment to the home environment may be necessary.

d) The user may require some insurance against theft or loss (e.g. a maximum amount may be set).

e) If during a (reload) transaction the connection fails, the procedure must be terminated properly.

7.20 Adaptive mobile equipment

UMTS is expected to utilise adaptive transceivers, enabling mobile equipment to identify and operate over a range of radio interfaces. In particular, the UMTS radio interfaces may differ in frequency and in multiple access principles, especially when the satellite component is taken into account. The required software may be downloaded to mobile equipment via the radio interface or from the USIM. Ensuring the integrity, authenticity and possibly confidentiality of software and any other control data is necessary. Data from the network should be passed (transparently) to the USIM to check integrity and authenticity before being downloaded to the mobile equipment. This avoids security functionality being required in the mobile equipment.

7.21 Strength of mechanisms

a) The security mechanisms of UMTS have to assure confidentiality, integrity and availability of communication.

b) The security mechanisms of UMTS have to be flexible enough to allow improvements, if weak point are found.

c) The strength of security mechanisms of UMTS should be surveyed regularly.

7.22 Direct mode terminals, repeaters and gateways

These may be used to provide:

a) Direct mode communications between two or more mobile equipment e.g. PMR direct mode.

b) Extension of radio coverage into areas with no permanent infrastructure or poor radio network coverage e.g. underground railways.

c) Cordless access to another telecommunications network (e.g. PSTN).

Since the radio infrastructure may take no part in the communication, the following security issues must be addressed:

d) Lack of incentive for any one provider to protect total system as fraudulent traffic will often appear on someone else's network (e.g. PSTN).

e) Costs of mobile equipment to the end user may not be subsidised via network usage charges. Those that are subsidised and intended for use on another network, could be sold at a discount to the usual prices charged for a direct mode, radio repeater of gateway equipment.

f) Lack of central control, possible use of long life static keys and lack of centralised audit will increase the security risk.

Since in many cases, vehicle installations, for example, it will not be possible to secure physically the equipment, the following security issues must be addressed:

g) To operate efficiently for all users who may wish to use it, a gateway/repeater may need to contain all security information for all potential users.

h) To operate the gateway/ repeater may have to decrypt incoming and then encrypt outgoing traffic with clear information present at some point in the equipment. Therefore, end-to-end security services may be required to address this.

8 Security features

This clause provides a classification and generic definition of the security features that are to be supported by UMTS. Individual instances of features will specify which entity or party controls the feature, under what circumstances the feature may be invoked, which entities or parties should be made aware that it has been invoked, which information types are involved, etc.

8.1 Scope of security features

The range of security features defined in this subclause embraces those features required to protect user traffic and user data, those needed to control access to UMTS telecommunications services and networks, those needed to protect signalling and other data transferred between or within networks, those needed to protect stored data and those needed for security management.

Each of the features is assigned to one of the following categories:

- authentication;
- confidentiality;
- anonymity;
- access control;
- integrity;
- non-repudiation;
- supplementary.

8.2 Requirements on security features

This subclause provides a list of requirements on UMTS security features:

a) Those provided for the benefit of UMTS human users should be user friendly, require a minimum of user interaction and, as far as possible, be transparent to the users.

b) If the activation of a security feature provided for the benefit of a customer is controlled by another party, e.g. a network operator, then the customer should be made aware of a failure to activate the feature.

c) Those provided for the benefit of UMTS users should work without any reduction in security when a user roams.

d) They must not affect the privacy of third parties.

e) They should not unduly increase time delays for UMTS procedures.

f) They are compatible with the correct operation of UMTS procedures.

g) They are such that differences in security functionality for terrestrial and satellite components of UMTS can be minimised.

h) They have a minimal impact on the use of radio resources.

i) They are compatible with the use of sequential radio paths.

j) They are compatible with the error characteristics of UMTS radio paths.

k) They are standardised to the extent needed for interoperability and world-wide roaming whilst allowing the maximum freedom for all parties involved in UMTS to set their own security policies.

l) They are compatible with the use of UMTS by UPT users.

m) They must be compatible with regulations governing emergency transmissions. For example, there may be a requirement to transmit in clear during an emergency.

n) They should not impair the proper use of emergency services.

8.3 Classification of security features

8.3.1 Authentication

a) Entity authentication: This feature allows one entity to verify the identity of another.

b) Transmitted data origin authentication: This feature allows the recipient of a message to verify the identity of the originator of the message.

8.3.2 Confidentiality

a) Confidentiality: This feature ensures that data is not made available or disclosed to unauthorised parties.

8.3.3 Anonymity

a) Anonymity: This feature ensures that an entity cannot be identified by unauthorised parties.

8.3.4 Access control

a) Access control to equipment: This feature ensures that entities can only use equipment for which they are authorised.

b) Access control to a service: This feature ensures that entities can only use services for which they are authorised.

c) Access control to data: This feature ensures that entities can only access data for which they are authorised.

NOTE: Distinction will be made in feature c) above between read and write access, in each particular instance.

8.3.5 Integrity

a) Integrity: This feature provides protection of data against manipulation by unauthorised parties.

NOTE: By integrity it is meant the ability to detect modification, not prevent it. Prevention is covered by the feature access control to data.

8.3.6 Non-repudiation

a) Non-repudiation of origin of transmitted data: This feature allows an entity to verify that a transmitted message originated from a specified entity.

b) Non-repudiation of delivery of transmitted data: This feature allows an entity to verify that a transmitted message was received by a specified entity.

c) Non-repudiation of access to data: This feature allows an entity to verify that a specified entity gained access to data.

d) Non-repudiation of access to services: This feature allows an entity to verify that a specified entity gained access to services.

e) Non-repudiation of procedure involvement: This feature allows an entity to verify that a specified entity was involved in a certain procedure.

NOTE: Non-repudiation of origin of transmitted data implies transmitted data origin authentication. It is for further study whether both features are necessary FFS.

8.3.7 Supplementary

a) Support for end-to-end security services: This feature ensures that the home environment/network operator can provide end-to-end security services to particular fixed or mobile users, subject to the availability of additional end-user equipment.

8.4 Feature instance descriptions

Each feature identified in the previous subclause comprises merely a generic statement of the feature. To be of practical use, more detail such as when the feature is used and by which entities, is required. For this reason, a comprehensive list of feature "instances" must be specified.

Particular instances of features are described by specifying the following information:

- involved entities;
- information types;
- requirements addressed;
- when utilised;
- invoking entity;
- notified entities;
- extent of standardisation.

These fields contain the following information respectively.

involved entities: If the feature concerns stored data, this field identifies the entity or entities storing the data. Similarly, if the feature concerns any action to be performed by one or more entities, then this field identifies those entities. If the feature concerns transmitted data, then this field identifies the particular entities involved in the interface over which the data is transmitted.

This field only identifies entities directly involved in the utilisation of the feature. Other entities which may be involved indirectly are identified under the heading "notified entities".

information types: This field lists the information types or groups to which the feature applies. Formal definitions of information types may be found in subclause 6.4. This field may be empty, (e.g. for any instance of feature not involving the protection of data such as "authentication of a user").

requirements addressed: Each feature instance will satisfy, or contribute towards satisfying, one (or more) of the security requirements set out in clause 7. This field identifies the requirements in question. It also explains to what extent the feature satisfies the requirement, and indicates which other feature instances may be required to fully satisfy.

when utilised: This field may indicate which procedures will cause the feature to be invoked (e.g. authentication of a user may be invoked at registration, handover, etc.). Alternatively the instance may be required continuously, (e.g. confidentiality of stored data), or perhaps during all transmissions (e.g. integrity of signalling data).

invoking entity: This field indicates the entity or entities that may invoke the feature instances. A specific entity may be responsible for invoking a feature e.g. the home environment may invoke authentication of a user), whilst in other cases more than one entity could be considered as invoking the feature (e.g. non-repudiation of transmitted data). At least one entity must be identified as the invoking entity each time a feature is utilised (see also "when utilised" above).

The entities listed will usually be one or more of those entities identified under "entity or interface involved".

NOTE: Which entity invokes a feature may depend upon the mechanism used.

notified entities: In addition to the entity or entities directly involved in a feature (see "involved entities" and "invoking entities"), there may be a number of other entities which are notified when the feature is invoked (or if the feature is not invoked when it should be). This field identifies such entities and describes the conditions under which they are notified (e.g. a user may be notified if the integrity of his personal data stored by the home environment is lost).

extent of standardisation: This field examines the extent to which the feature should be standardised. It may indicate, for example, that the mechanism used to implement the feature must be completely standardised to allow global roaming of users (e.g. authentication of users), or perhaps that it required no standardisation at all and could be "vendor specific" (e.g. confidentiality of stored data).

9 Security mechanisms

The purpose of this clause is to specify the security mechanism available for the provision of the security features to be implemented. This clause also specifies how mechanisms should be described. After identifying some general requirements on mechanisms in subclause 9.1, the general approach to selecting mechanisms for UMTS is detailed in subclause 9.2. This is followed by a discussion of the selection criteria in subclause 9.3. Finally, subclause 9.4 describes how mechanisms are presented.

9.1 Requirements on security mechanisms

This subclause provides a list of requirements on UMTS security mechanisms.

a) The security mechanisms should require the minimum of long-distance real-time signalling. For instance, the need for international signalling connections at every location update or call when roaming should be avoided.

b) The security mechanisms should require a minimum of bilateral pre-arrangements between home environments and network operators.

c) The UIM or equivalent security device must always be physically present to make use of any UMTS service and to guarantee the correct functioning of the security mechanisms needed by users.

d) The security mechanisms should include the means to manage cryptographic keys that may need to be exchanged by home environments and network operators.

e) The security mechanisms needed by users should be such that it is easy to distribute and change their cryptographic keys.

f) The security mechanisms should be standardised only to the extent needed for interoperability and roaming.

g) The security mechanisms should support version control management to allow for subsequent upgrading and revision of mechanisms:

   - the UMTS security architecture should provide flexible, adaptable and scaleable security mechanisms such that new security features can be added quickly and cost-effectively in response to new requirements brought about by the introduction of new UMTS services and features;

   - the migration between security mechanisms used to provide a given set of security features should be done such that security is not compromised as a direct result of the migration process.

NOTE 1: Home environments may need to upgrade security mechanisms due to suspected or actual compromise.

NOTE 2: Security mechanisms may need to be upgraded periodically in line with advances in technology.

h) The security mechanisms should include the means to detect and report security violations, and the means to restore the system to a secure state.

i) The security mechanisms should satisfy legal requirements imposed by national authorities e.g. export controls, lawful interception.

9.2 Approach to the selection of security mechanisms

This subclause describes the general approach taken for the selection of UMTS specific mechanisms, and also assigns priorities to the mechanisms. Various approaches exist for realising a particular type of mechanism, and the most common approaches are identified here.

The approaches identified here are (generally) in accordance with the approaches identified by ISO and appropriate references are given in the text.

The priority assigned to a particular mechanism indicates the relative importance of the mechanism to UMTS (i.e. its impact on the secure operation of UMTS). A rating of Primary (P) indicates that failure to use the mechanism could seriously impair secure operation of the system, whilst a rating of Secondary (S) indicates that the consequences are (probably) less severe. A rating of Tertiary (T) indicates that the specification of such mechanisms may be outside the scope of standardisation and need not be addressed. Further subdivision using numerals 1 - 3 accompanies the P or S rating (1 = most important, 3 = least important).

9.2.1 Authentication

Four approaches have been identified for providing authentication mechanisms (see ISO/IEC 9798, parts 2 to 5):

a) symmetric;

b) public key;

c) cryptographic check functions;

d) zero knowledge.

Unless further study dictates otherwise, at least one mechanism will be realised for each of the above approaches.

Mechanisms should, wherever possible, be based on those mechanisms used in current systems.

Mechanisms should incorporate secure key distribution/agreement if necessary.

The authentication mechanisms could be designed that an enhancement to a secure end-to-end protocol comprising end-to-end authentication between users is reachable.

Priorities assigned to authentication are as follows:

P1 Authentication of user to network operator/home environment;

P1 Authentication of home environment/network operator to user;

S1 Authentication between home environments and network operators;

S2 Authentication of terminal to network operator/ terminal manager.

The following list of security characteristics could be realised by the UMTS authentication mechanisms. The list does not claim to be complete or exhaustive. Some of the mentioned security characteristics should be mandatory (marked with an M), others are optional ones (marked with an O). The non-repudiation features could be used for incontestable charging purposes.

e) mutual explicit authentication of user and serving network (M);

f) agreement between user and serving network on a shared secret key K_S with mutual key authentication (M);

g) mutual key confirmation between the user and the serving network (O);

h) mutual assurance of key freshness (O);

i) non-repudiation of the authentication protocol between user and serving network (O);

j) possibility of verification of the mutual authentication by any third party (O);

k) good forward secrecy of the shared session keys (O);

l) confidentiality of the user identity on the radio interface (O);

m) confidentiality of the user identity to the network operator (O);

n) exchange of certified public keys between user and serving network (if an asymmetric scheme is used) (M);

o) exchange of the certified public key from a trusted third party (e.g. a trusted time server) to the user (if an asymmetric scheme is used) (O);

p) no session key agreement between unknown parties (M);

q) data generated by user and/or USIM, delivered to the network operator and/or third party (O):

- non-repudiation of origin, i.e., assurance to the serving network and third party, that the user or USIM has sent data;

- non-repudiation of delivery, i.e., assurance to the USIM or third party, that the serving network knows data;

r) data generated by serving network, delivered to the user, USIM or third party (O):

- non-repudiation of origin, i.e., assurance to the USIM or third party, that the serving network has sent data;

- non-repudiation of delivery, i.e., assurance to the serving network, that user, USIM or other party knows data;

s) a current and secure time-stamp needed to achieve non-repudiation of the authentication protocol can also be used by the USIM and the serving network to check the expiration date of exchanged certificates on public keys (O).

The authentication mechanisms could be split between "new" registration and "current" registration. For a new registration it is possible to combine the authentication mechanism with an online dynamic roaming agreement between home environment and serving network.

9.2.2 Confidentiality

The following approaches have been identified for providing confidentiality mechanisms (see [8–10]):

a) block ciphers (and their various modes of operation) these can be divided into the following categories:

- symmetric;

- asymmetric;

b) stream ciphers.

Mechanisms for confidentiality may depend upon the choice of radio interface(s). Nevertheless, some aspects will be independent of this (e.g. management of cipher keys) and can be studied immediately.

Priorities assigned to confidentiality are as follows:

P2 Confidentiality of user traffic, signalling data, and control data over the radio interface;

P3 Confidentiality of user traffic, signalling data, and control data sent between provider domains;

T Confidentiality of user traffic, signalling data, and control data sent within a provider domain;

T Confidentiality of stored data;

T End-to-end user traffic confidentiality.

9.2.3 Anonymity

Three approaches have been identified for providing anonymity mechanisms:

a) identity confidentiality these can be divided into the following categories:

- symmetric;
- asymmetric;

b) pseudonymous access, e.g. temporary identities;

c) anonymous access.

Priorities assigned to anonymity are as follows:

P3 user anonymity over the radio interface;

T user anonymity over internal network interfaces.

9.2.4 Access control

Six approaches have been identified for providing access control mechanisms:

a) non-cryptographic authentication, these can be further subdivided into:

- personal identification numbers;
- simple challenge - response;

b) biometrics;

c) registration;

d) type approval;

e) barring;

f) auditing;

g) physical means.

Priorities assigned to access control are as follows:

S1 access control to equipment;

T access control to stored data.

9.2.5 Integrity

Four approaches have been identified for providing integrity mechanisms (see ISO/IEC 10118 and ISO/IEC 13888):

a) non-cryptographic integrity (error detection/correction, CRCs);

b) cryptographic check functions;

c) MACs;

d) hash functions.

Priorities assigned to integrity are as follows:

S2 integrity of user traffic, signalling data, and control data over the radio interface;

S2 integrity of user traffic, signalling data, and control data sent between provider domains;

T Integrity of user traffic, signalling data, and control data sent within a provider domain;

T Integrity of stored data;

T End-to-end user traffic integrity.

9.2.6 Non-repudiation

Two approaches have been identified for providing non-repudiation mechanisms (see [11]):

a) symmetric;

b) asymmetric.

Priorities assigned to non-repudiation are as follows:

S3 Non-repudiation of user access to services;

T Non-repudiation of access to stored data;

S3 Non-repudiation of origin and delivery of user traffic.

9.3 Criteria for evaluating security mechanisms

In order to compare different security mechanisms that might be used within UMTS, criteria are needed by which mechanisms can be judged. Given an agreed set of "objective" criteria, a judgement can be made as to which mechanisms are preferable. In this sub-clause such criteria are described.

9.3.1 Security service provision

Fitness for purpose: Most fundamentally, the security mechanisms employed must provide the security services which they are designed to provide. This should be possible to establish using informal arguments.

Security proof: If possible, the fitness of the security mechanisms should be established using formal (mathematical) techniques.

Algorithm maturity and exposure: Long-term existence of a (non-discredited) algorithm in the public domain may be an advantage since it will necessarily have resisted crypto-analytic attack.

Availability of replacements: The availability of similar replacements for a mechanism (in the event of it being discredited or otherwise rendered unusable) is a significant advantage.

9.3.2 Communications overheads

Numbers of messages: All else being equal, security mechanisms are to be preferred which minimise the number of messages that need to be exchanged.

Total lengths of messages: Security provision will inevitably involve transferring additional information across communication links. Clearly, minimising the total amount of such information transfer is desirable.

Message expansion: Apart from one-off overheads, some security mechanisms (e.g. encryption) involve expanding message content by a fixed ratio. Clearly, where bandwidth is at a premium, such as on the radio path, such overheads need to be minimised.

Performance effects: Certain types of security mechanism may degrade the quality of a channel. For example, use of encryption may actually magnify the effects of bit errors, i.e. the channel bit error rate may be increased. It would clearly be desirable to minimise any such impairment of communications channels.

9.3.3 Administration overheads

Key storage: Certain cryptographic algorithms require the storage of relatively large amounts of key material. Mechanisms which minimise key storage may have very significant advantages.

Storage of other security parameters: Use of certain types of security mechanisms will require the storage of other types of information. For example, some authentication mechanisms require communicating parties to store sequence numbers for every other party with which they communicate. Other authentication mechanisms require all "recently received" messages to be stored to detect malicious replays occurring within the tolerance interval for synchronised clocks.

Need for trusted third parties: Some mechanisms may require the participation of a specific trusted third party (either on-line or off-line). For example, authentication mechanisms may require an on-line authentication server, an off-line certification authority or an on-line trusted time server (to provide clock synchronisation).

Involvement of other entities: A mechanism to provide a security feature between two entities may involve further entities. The number of such additional entities should be minimised, and the necessary level of trust in such entities should also be minimised.

9.3.4 Processing and other hardware overheads

Cryptographic algorithm calculation: Many security mechanisms will require entities within the system to perform cryptographic calculations. In some cases, the amount of processing required could have significant cost and/or time delay ramifications (e.g. implementing RSA in a user token). Hence, minimising cryptographic complexity is a desirable goal.

Other computation: For similar reasons, it would be desirable to minimise any other computations relating to the provision of security services.

Special hardware needs: Some mechanisms require the presence of particular functionality at communicating entities. For example, some authentication mechanisms require closely synchronised clocks. Other authentication mechanisms, and some key management mechanisms, require the means to generate either genuine random values or unpredictable pseudo-random numbers. Minimising such requirements would clearly be desirable.

Matching processing requirements: Different security mechanisms distribute processing requirements differently between sets of communicating entities. Ideally, a security mechanism will match the processing requirements to the capabilities available to the various entities. Moreover, different mechanisms have varying proportions of pre-processing, "real-time" processing, and post-processing. For example, one authentication mechanism may allow more pre-processing than another, speeding up an on-line transaction. This "time distribution" of processing requirements must also be taken into account in mechanism choice.

9.3.5 Adherence to international standards

ISO/IEC SC27 Mechanism Standards. Where possible, it would be desirable for the mechanisms employed to adhere to ISO standards produced by ISO/IEC SC27, e.g. ISO/IEC 9798 (authentication mechanisms) parts 2 to 5 and ISO/IEC 11770.

OSI Security Architecture and Security Frameworks. Where relevant it would be desirable for the security mechanisms to be employed in a way conforming with the OSI Security Architecture in ISO 7498-2 and the multi-part security framework standard in ISO/IEC 10181.

9.3.6 Limitations on use

Existence of patents: The existence of patents on a mechanism, whether national, regional or world-wide and whether applied for or granted, can be a significant disadvantage.

Export restrictions: Some mechanisms may be subject to widespread export restrictions. The existence of such restrictions will be a clear disadvantage.

9.4 Presentation of security mechanisms

This specified security mechanisms will be presented under a number of headings in the following way.

Security feature: This identifies the security feature provided by the particular mechanism.

Instance of feature: This identifies the particular instance(s) of the security feature for which the mechanism is provided.

Description of mechanism: This provides a detailed description of the mechanism.

Location of functions: This defines the location of the functions that make up the security mechanism.

Operational procedures: This specifies all the procedures necessary to operate the mechanism.

Management requirements: This describes all the requirements for managing the mechanism and the security parameters associated with the mechanism.

Algorithmic requirements: This defines the requirements for any cryptographic algorithms needed for the mechanism, including the interfaces to the algorithms.

Extent of standardisation: This defines the extent to which the mechanism needs to be standardised.

Justification for choice of mechanism: This gives a brief account of why the particular mechanism was chosen to provide the required security feature.

The method of presentation described above is illustrated by the following hypothetical example.

> **Security feature:** Confidentiality.
>
> **Instance of feature:** Privacy for voice traffic on the radio path.
>
> **Description of security mechanism:** Stream cipher to encrypt voice traffic on the radio path.
>
> **Location of functions:** Terminals and base stations, cipher located within MAC layer.
>
> **Operational procedures:** Cipher started in terminal by error protected command from base station; synchronisation of cipher maintained by using physical layer frame number as message key, etc.
>
> **Management requirements:** Encryption key needs to be established at terminal and base station with transfer between base stations at handover; protected transfer of key to visited networks, etc.
>
> **Algorithm requirements:** Stream cipher, B-bit base key input, M-bit message key input, S-bits of key stream for C channels per message key, etc.
>
> **Extent of standardisation:** Standard algorithms required, but proprietary algorithms may also be supported by special terminals.
>
> **Justification for choice of mechanism:** Voice codec and radio path characteristics demand use of a stream cipher; cipher operation must be compatible with seamless handover; need for international roaming demands a common set of algorithms and identifiers, etc.

10 Management and security

Security management provides the means for a UMTS network operator and/or home environment to create, update, retrieve, and delete information related to the security aspects of UMTS and specifies the mechanisms and other factors needed to manage, or which influence, UMTS security features, the mechanisms used to provide and distribute cryptographic keys, access control management, operation and administration of security mechanisms etc. which are needed by UMTS security mechanisms. Security management is required to provide a level of protection to users and providers of UMTS services which shall be at least equal to that provided in fixed networks.

Security management also provides mechanisms which allow network operators and home environments to perform security administration (e.g. security alarm reporting, secure management of USIMs).

10.1 Management of security features

Management of security is required for all requirements listed in clause section 7. Mechanisms are required to perform the various management procedures associated with the security requirements above.

10.2 Security management requirements

The following requirements can be identified:

a) Security management requirements shall be compatible with the demands of UMTS, including world-wide operation.

b) Security management shall protect UMTS users, users and network operators against intrusion of the network, impersonation of network, home environment and/or user, fraud, misuse and theft.

c) Equipment and network specifications must include and maintain complete technical security profiles which must themselves be kept secure.

Documentation of all types should be appropriately classified according to its sensitivity and protected from unauthorised access. Associated with this is the need for standard formal change control procedures in all applicable environments. All such changes should be reviewed for consequential impact on security and/or functionality.

10.2.1 Event logging

Event logging is a generic term which allows a UMTS home environment and/or network operator to log activities relating to a UMTS user or user. Event logging needs to be under constant review in the light of both technical development and new fraud attacks.

The use of this very general feature by home environment or network operator encompasses security features such as authentication, blacklisting, tracing fraud information gathering etc.

Logs and security management reports should be subject to security measures appropriate to their integrity, sensitivity and availability.

Logs and security management reports may be called upon as legal evidence. As such they are potentially subject to challenge both from attackers and from legal process. They must, therefore, be kept secure in such a way so as not to compromise their integrity and availability.

10.2.2 Fraud management

Mechanisms are required to deter, detect, and prevent fraud (whether logical or physical) occurring through exploitation of system weaknesses, as well as through the use of services with the intention of not paying for them. The management of these mechanisms may require functionality :

a) inside the UMTS network to initiate data collection and the collection of specific monitored events;

b) external to the network to determine whether fraudulent activity or abuse is taking place. This may involve a combination of real time call, mobility and service processing, and non-real time analysis of processing across multiple instances of calls and service invocations from one or more networks;

c) to terminate service(s) to the user when requested by the network operator and/or home environment.

Further details are provide below.

The UMTS architecture must be flexible enough to allow the implementation of mechanisms to combat fraud arising from known actions, but also from unknown actions that may arise in the future. The UMTS architecture should also be sufficiently resilient to resist known and potential fraud attempts that may be attempted against it.

10.2.3 Fraud indicators

Indicators of fraud may be classified into three basic categories. These are shown below with a few examples of each. None of the lists is exhaustive.

a) usage indicators for individual users:

- number of calls originated/terminated in a given time interval;

- total time usage of calls originated/terminated in a given time interval;
- duration of individual originated/terminated calls;

b) mobility indicators for individual users:

- number of distinct cells visited in-call in a given time interval;
- number of distinct location areas visited out-of-call in a given time interval;

c) association indicators, which may or may not be pertinent to individual users:

- higher than expected congestion on the radio interface;
- velocity checks;
- simultaneous and independent use of services by apparently the same user;
- attempts to access services e.g., international calls, to which the user is not entitled.

It is possible to sub-classify certain indicators. For example, the number of international calls rather than the total number of calls may be of primary interest.

10.2.4 Fraud control actions

These include the following for the prevention of fraud:

a) routing certain types of calls e.g. to specific international destinations, via an operator and requiring the user to specify a PIN or other information;

b) limiting the scope of certain services e.g. barring international call forwarding for all users;

c) only offering certain services which are prone to fraudulent activity to a subset of users e.g. call forwarding services;

and for the detection of fraud and subsequent control:

d) analysing genuine user behaviour and setting threshold levels for indicators accordingly;

e) determining rules with respect to which set of indicators must surpass their associated threshold levels for a user to be deemed fraudulent;

f) raising bars for all or a subset of services on users suspected of fraudulent activity;

g) termination of all or a subset of ongoing calls for users suspected of fraudulent activity in home and visited networks (note: this will require co-operation between networks);

h) performing location estimates by triangulation of users suspected of fraudulent activity.

10.2.5 Network security management

a) Measures should be implemented to maintain all aspects of the security of network services, network elements and the communications between them;

b) Regular checks should be made on the integrity of all communications software and transmission protocols. This should include both logical and physical aspects;

c) The use of any specialised telecommunications testing and monitoring equipment on the network should be controlled and monitored for abuse and unintended security breaches.

10.2.6 New services - Impacts on security

The introduction of new services and service requirements on UMTS may impose new and different security management requirements compared to second generation systems, e.g. handover between networks, quality of service management, service creation capabilities etc. Each service needs to be studied in order to assess the management requirements.

10.2.6.1 Interworking

The UMTS security architecture should permit secure interworking between the UMTS network and other networks which may have their own security architectures:

a) where possible the level of protection offered by the UMTS security architecture for a particular UMTS service should not be compromised due to interworking with other networks;

b) if the level of protection offered by the UMTS security architecture for a particular UMTS service is compromised due to interworking with other networks, then the affected UMTS entities should be notified accordingly;

NOTE 1 users should be notified if the level of protection of their user traffic is compromised.

NOTE 2 serving networks should be notified if new threats are discovered. As a result they may need to implement appropriate measures to counter these new threats.

10.2.6.2 Service Creation Concept

a) a structured service creation process should be provided where fraud scenarios can be minimised or prevented;

b) it should be possible for new fraud scenarios to be detected as part of the service creation process;

c) tools should be provided to allow the necessary security features to be incorporated into new services as an integral part of the service creation process.

NOTE 1 Fraud detection rules could be imbedded into a structured service creation process such that new fraud scenarios can be pre-empted.

NOTE 2 Service creation tools could be used to build the necessary security features in order to counter new fraud scenarios.

10.2.6.3 Automatic roaming

a) The UMTS security architecture should allow users to be able to roam on visited networks without the need for a prior agreement between the user's home environment and the serving network operator.

NOTE 1 See UMTS 22.71 "Automatic establishment of roaming relationships".

NOTE 2 Roaming brokers may be used as intermediaries between home environments and network operators to facilitate automatic roaming.

NOTE 3 Automatic roaming may involve security mechanisms which require the support of a trusted key management infrastructure.

11 Requirements on security devices

This clause will identify requirements for the security devices that are needed to provide the UMTS security functions defined in this report.

Three types of device have been identified: the USIM, elements within the UMTS mobile equipment, and network elements controlled by home environments, network operators or mobile equipment managers.

11.1 User Services Identity Module (USIM)

The USIM is the secure module within the UMTS mobile equipment which uniquely identifies the user. The USIM can be either separable from the mobile equipment, e.g. in the form of a smart card, or permanently embedded. The USIM provides non-volatile storage for data, and a secure environment in which to store, execute and verify the results of cryptographic algorithms. External access to the data and functions within the USIM can be controlled in different ways. A conventional method is that using PINs and there are also a number of biometrics techniques which could be used to authenticate the user to particular areas of the USIM.

The level of security of the data stored on the USIM is dependent on the use of the data and the entity controlling it. There will be data which can only be used within the USIM and therefore never accessed from an external source, such as authentication keys and PINs. Other data, such as permanent identities will require access from the mobile equipment but will never be able to be altered or only altered in a controlled manner.

The basic data that will be present on the USIM is:

a) data, that only has to be used within the USIM and therefore never accessed from an external source, e.g. data for authentication of a user (keys, cryptographic algorithm,...);

b) data, that are permanent identities or other values/parameters that are not allowed to be changed, e.g. permanent user identities which must remain fixed for a period of time like IMUI;

c) data that are temporary identities or other information that only are allowed to be changed by the serving network/home environment, e.g. temporary user identities, user profile, services/applications (for telecommunication), other non-telecommunication applications (like electronic purse);

d) data that the user himself has stored on the USIM and is able to change only by the user, e.g. user's PIN for authentication to the USIM, telephone numbers/addresses, abbreviated dialling numbers.

Depending on the different kinds of data there have to be the corresponding security measures to protect the stored information against unauthorised access, modification, manipulation, e.g. with physical/logical techniques in case a) or with logical measures like access rights, PINs or authentication in cases b) to d). Another example: authentication of the home environment is needed if the home environment sends some applications to the USIM or changes the user profile over the radio interface.

It is envisaged that the USIM will be in the form of a micro-processor, and therefore will be able to support substantial functionality.

The USIM will be capable of multitasking, such as sending data from the mobile equipment whilst engaged in a voice call.

If biometrics techniques are used then the logic to support the comparison between the biometrics received and that stored will be required.

The USIM will be able to support the implementation of applications during its lifetime. These applications may be other telecommunications applications like GSM, or non- telecommunications applications, such as an electronic purse. The USIM will be able to securely separate applications, and also if required, be able to support multi-functionality whereby two applications would interact. An example of multi-functionality is the use of an electronic purse for paying for telephone calls in real time.

11.1.1 USIM-ME interface protection

The proposed extensive functionality of USIMs may require significant amounts of sensitive data to pass through the USIM-mobile equipment interface. Therefore, the interface has also to be protected against:

- unauthorised access to the mobile equipment and USIM via the interface;
- manipulation/modification of the interface itself;
- unauthorised access of the data passing the interface;
- manipulation, modification of the data passing the interface.

The protection could be realised by physical and logical security measures.

11.1.2 Presence of USIM/IC card

The USIM realizes the authentication of user towards the network and provides some security features (e.g. encryption) for confidentiality of the user. Authentication is needed for the proof that the home environment/network provider serves the "right" customer with his related access rights. Moreover, some lawful requirements of some countries ask for a clear assignment of customers (e.g. lawful interception). Another lawful requirement in some countries is the "telecommunication secrecy". Here authentication is one measurement. Moreover, authentication is one possibility to guarantee the payment of the "right" customer for the used services. But, charging is not the only reason for authentication (see above).

In addition, the USIM provides some measures for confidentiality e.g. encryption methods/keys. These security measures are important to realise and guarantee the "telecommunication secrecy". However, there could be also some other security methods for other applications e.g. electronic banking. Which features are needed depends on the service application and the access rights and profile of a user, so that it is easier if authentication and security features are together on one entity.

So the USIM/IC card should be physically present in order to make use of any services apart from emergency calls. Free services cannot be an exception to this rule, as the identification of the user (achieved by authentication of the USIM) is not only required for charging purposes, but for routing (of mobile terminating calls), lawful interception purposes, and to deter abuse of free services (for instance, by a denial of service attack).

Where the user need not be authenticated to be the called party, or where the user is the called party and the calling party has accepted all call charges, services could be provided by the user “call forwarding” the desired services to the target terminal, assuming that the target terminal contains a USIM that can be authenticated for service delivery (this USIM could be an integral USIM in the terminal). The requirement for a USIM to be present in the target terminal cannot be relaxed:

- because the target terminal needs to be identifiable by the network for routing purposes;
- because the target user may need to be identified by law enforcement agencies;
- because allowing reception of services without USIM authentication represents a degradation in UMTS security.

At least it should be configurable which service application needs the presence of the USIM/IC card.

11.1.3 USIM/IC card as an application, multiple application, multiple subscription

If an IC card provides more than one application and more than one service application should be used at the same time then the following requirements have to be fulfilled:

- it must be possible to configure for each service application if an application can be used twice in parallel over several mobile equipment;
- the different application must not influence each other;
- security related data (authentication information/security features/measures) of each application has to be protected against unauthorised access;
- security related data has to be protected against unauthorised modification/manipulation;
- if security related data has to be sent to the mobile equipment see above.

If an IC card provides more than one subscription (access services from different home environments) then the following requirements have to be fulfilled:

- the different home environments are only allowed to have access on their own user profiles, no access to the "foreign" user profiles should be allowed;

- security related information (authentication information/security features/measures) of each user profile has to be protected against unauthorised access;

- security related information (authentication information/security features/measures) of each user profile has to be protected against unauthorised modification/manipulation.

11.2 Mobile equipment

The mobile equipment may be required to permanently store sensitive data such as an ME identity, and type approval information, as well as cryptographic algorithms. Temporary storage of additional data such as cryptographic session keys and authentication data may also be necessary. Protection of this data against unauthorised reading or modification will be required. In particular it may be necessary to protect cryptographic algorithms against being read, and to protect ME identities against modification. Physical measures (e.g. tamperproof modules) will be necessary to protect permanently stored data.

In the case of an integrated USIM, the protection afforded to data within the USIM or ME should be independent.

11.3 Network security elements

Numerous security functions will be carried out in the network. This could include the generation of authentication parameters, session keys, and temporary identities, as well as encryption, verification (integrity and authentication), storage and checking of identities, location data etc. Generally the network elements have to be protected against unauthorised access, modification and manipulation/destruction, especially that one realising security (providing authentication algorithms, secret identity keys,...).

Annex A (Informative): Status of UMTS 33.20

Status of Technical Report UMTS 33.20		
Date	**Version**	**Comments**
June 1996	09.01 v 2.5.0	approved by SMG SG
June 1996	09.01 v3.0.0	approved by SMG for endorsement by SMG 5
November 1997	33.20 draft 1	Revised after review by SMG10-WPC and renumbered as UMTS 33.20
February 1998	33.20 draft 2	Revised during SMG10 Plenary 4 to 6 February 1998 (Draft 2)
March 1998	33.20 draft 3	Revised after SMG10 4th- 6th Feb. Worcester, to include GSM security issues from plenary through contributions for 7.1 (AW), 7.2.11 (HR) 11.2.4 (PH); (
March 1998	33.20 draft 3a	New text added on repeaters/gateways in 7.3.11(CB) and USIM (RS) in sect 13.1
March 1998	33.20 v0.4.0	Draft 3a cleaned-up by SMG-PN and all revision marks accepted. Document still contains several editor's notes. References to other UMTS specifications (out of date) and ITU-T specifications have to be checked and corrected. Version to SMG10 Lund for further consideration.
April 1998	33.20 v0.5.0	Global revision as agreed upon at the SMG10-meeting in Lund, including revision in view of 98P103, 98P104, 98P105; revision of scope (removal of clauses features and mechanisms and authentication framework for inclusion in new document), up-to-date list of references and abbreviations, editorial changes
June 1998	33.20 v0.6.0	Document based on v0.5.0, used as a starting point for 33.21.
July 1998	33.20 v0.6.1	Re-inclusion of removed parts from version 0.5.0, ordering of the security threats, adaptation on the subclause on the presence of the USIM in clause 11 and redrafting in view of the ETSI drafting rules.
July 1998	33.20 v0.6.2	Minor corrections.
July 1998	CR 33.20-001	To SMG#27 for approval as CR 33.20-001: as replacement of already "approved" version 3.0.0.
February 1999	3.1.0	CR 33.20-001 (replacement of version 3.0.0) approved by SMG#28
Text and figures: WinWord 6.0 **Stylesheet**: etsiw_70.dot **Rapporteur**: Colin Blanchard		

History

Document history		
V3.1.0	February 1999	