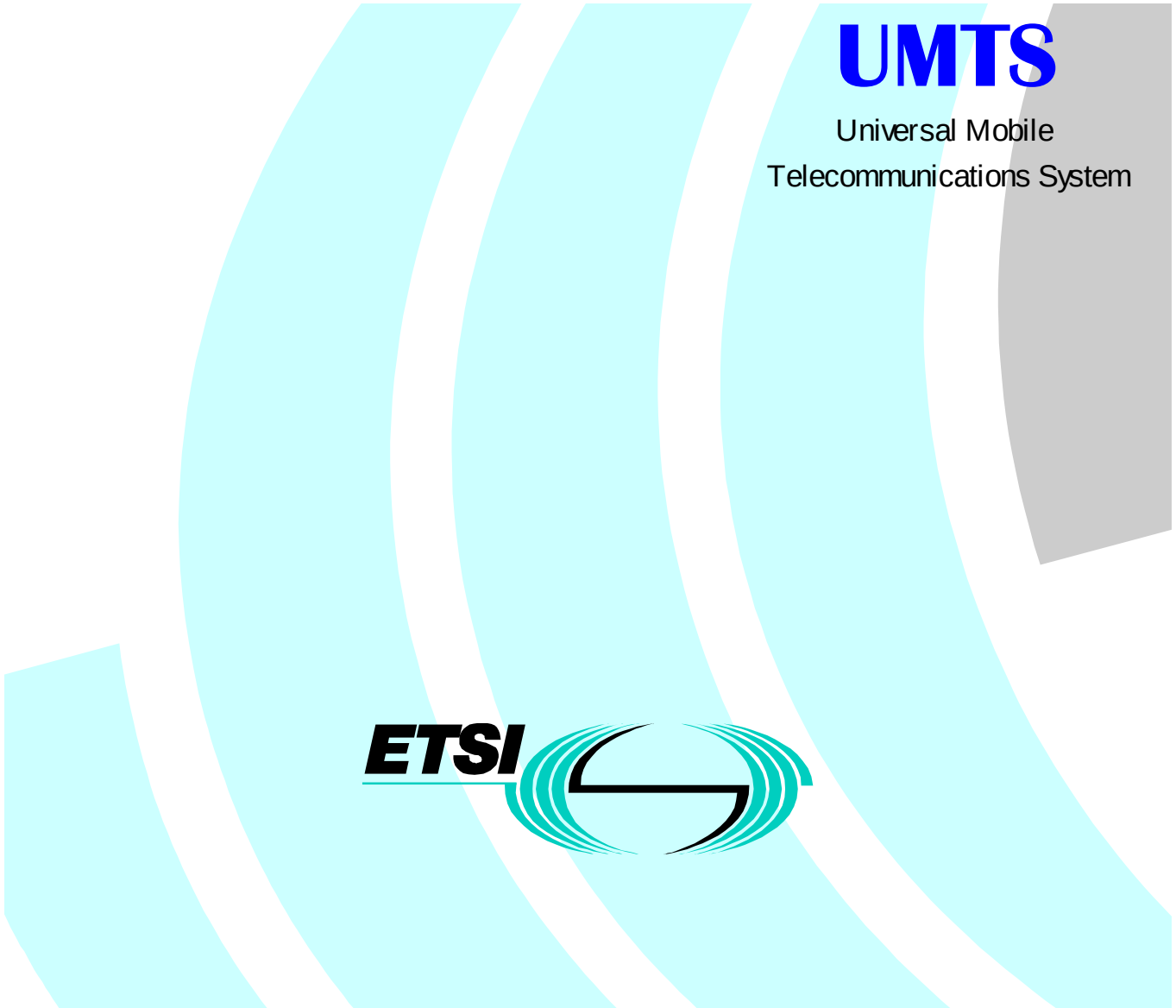
UMTS 33.21 V3.0.0 (1999-02)

Technical Specification

Universal Mobile Telecommunications System (UMTS); Security Requirements (UMTS 33.21 version 3.0.0)



Reference
DTS/SMG-103321U (xxxx.PDF)

Keywords
Universal Mobile Telecommunications System

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
Individual copies of this ETSI deliverable
can be downloaded from
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 Specification has been produced by ETSI Technical Committee Special Mobile Group (SMG), .

The present document contains a list of security requirements for UMTS Phase 1. The security of UMTS Phase 1 shall satisfy the requirements contained in this specification.

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

Version 3.x.y

where:

3 indicates version approved by SMG for UMTS Phase 1

x the second digit is incremented for all changes of substance, 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 specification contains a list of security requirements for UMTS Phase 1. The security of UMTS Phase 1 shall satisfy the requirements contained in this specification. This specification is derived in part from UMTS 33.20 "Security Principles".

As services will not, in general, be standardised, it is difficult to predict their exact nature. Therefore, this specification lists a set of possible security threats and generalised requirements that shall be applicable irrespective of the actual services offered. The list of threats and requirements will need to be maintained as the UMTS system evolves.

The security features that satisfy the requirements listed in this specification are identified in UMTS 33.22 "Security Features", whilst the security mechanisms that implement the identified security features are specified in UMTS 33.23 "Security Mechanisms".

The structure of this technical specification is as follows:

clause 2 lists the references used in this specification;

clause 3 lists the definitions and abbreviations used in this specification;

clause 4 contains the general objectives for UMTS Phase 1 security features;

clause 5 contains the context in which the security features for UMTS Phase 1 are designed;

clause 6 contains a selection of possible security threats to UMTS Phase 1;

clause 7 contains a list of security requirements for UMTS Phase 1.

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 22.00: "Universal Mobile Telecommunications System (UMTS): UMTS Phase 1".

[2] UMTS 22.01: "Universal Mobile Telecommunications System (UMTS): Service aspects; service principles".

[3] UMTS 23.01: "Universal Mobile Telecommunications System (UMTS): General UMTS Architecture".

[4] UMTS 30.01: "Universal Mobile Telecommunications System (UMTS): UMTS Baseline Document; Positions on UMTS agreed by SMG".

[5] UMTS 33.20: "Universal Mobile Telecommunications System (UMTS): Security Principles".

[6] UMTS 33.22: "Universal Mobile Telecommunications System (UMTS): Security Features".

[7] UMTS 33.23: "Universal Mobile Telecommunications System (UMTS): Security Mechanisms".

2.2 Informative references

[8] ETR 331: "Security Techniques Advisory Group (STAG): Definition of User Requirements for Lawful Interception of Telecommunications - Requirements of the Law Enforcement Agencies".

[9] LINK PCP, 3GS3, Technical Report 1: "Security Features for Third Generation Systems". Vodafone; GPT; Royal Holloway, University of London. February 1996.

[10] 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[11] 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the privacy in the telecommunications sector.

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

[13] ISO/IEC 7498-2: 1988, Information Technology - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.

[14] ISO/IEC 10181, Information Technology - Security Frameworks in Open Systems - Part 2: Authentication Framework.

[15] ISO/IEC 11770, Information Technology - Security Techniques - Key Management - Part 1: Framework.

[16] ISO/IEC CD 13888, Information Technology - Security Techniques - Non-repudiation - Part 1: General Model.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this technical specification, the following definitions apply:

Access Control: The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner. (ISO/IEC 7498-2)

Authentication: The provision of assurance of the claimed identity of an entity. (ISO/IEC 10181)

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

Confidentiality: The property of information that it has not been disclosed to unauthorised parties.

Evidence: Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action. (ISO/IEC CD 13888)

Integrity: The property of information that it has not been changed by unauthorised parties.

Key Management: The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy. (ISO/IEC 11770)

Law Enforcement Agency (LEA): An organisation authorised by a lawful authorisation, based on a national law, to receive the results of telecommunication interceptions. (ETR 331)

Lawful Authorisation: Permission granted to an LEA under certain conditions to intercept specified telecommunications and requiring co-operation for a network operator or service provider. Typically this refers to a warrant or order issued by a lawfully authorised body. (ETR 331)

Lawful Interception: The action (based on the law), performed by a network operator or service provider, of making available certain information and providing that information to a Law Enforcement Monitoring Facility. (ETR 331)

Non-Repudiation Service: A security service which counters the threat of repudiation.

Repudiation: Denial by one of the parties involved in a communication of having participated in all or part of the communication. (ISO/IEC 7498-2)

3.2 Abbreviations

For the purposes of this technical specification the following abbreviations apply:

GSM	Global System for Mobile communications
IMEI	International Mobile Equipment Identity
IMT-2000	International Mobile Telecommunications-2000
IMUI	International Mobile User Identity
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunications Union
LEA	Law Enforcement Agency
N-ISDN	Narrowband ISDN
ODMA	Opportunity Driven Multiple Access
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
SIM	Subscriber Identity Module
TD-CDMA	Time Division - Code Division Multiple Access
TMN	Telecommunications Management Network
UICC	UMTS Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
USIM	User Services Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VHE	Virtual Home Environment
W-CDMA	Wideband - Code Division Multiple Access

4 General objectives for UMTS security features

The general objectives for UMTS security features are:

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

b) to ensure that the resources and services provided by serving networks and home environments are adequately protected against misuse or misappropriation;

c) to ensure that the security features standardised are compatible with world-wide availability;

d) to ensure that the security features are adequately standardised to ensure world-wide interoperability and roaming between different serving networks.

e) to ensure that the level of protection afforded to users and providers of services is better than that provided in contemporary fixed and mobile networks (including GSM).

f) to ensure that the implementation of UMTS security features and mechanisms can be extended and enhanced as required by new threats and services.

5 Security context

The purpose of this clause is to describe the context in which the UMTS security features are designed. This specification assumes the system assumptions, network architecture and functional roles given in UMTS 23.01 and UMTS 30.01, the service description given in UMTS 22.01 and the UMTS Phase 1 description given in UMTS 22.00.

In subclause 5.1 the system assumptions that describe UMTS in general and especially those that have a significant bearing on security are listed.

In subclause 5.2 roles that have a significant bearing on security are defined.

In subclause 5.3 various architectural components that have an impact on the design of UMTS security features are defined.

In subclause 5.4 various identities used in UMTS that have an impact on the design of UMTS security features are defined.

In subclause 5.5 data types and groups that are used to help construct security threats and requirements are defined.

5.1 System assumptions

In this subclause UMTS system assumptions that have an impact on the design of UMTS security features are listed. These assumptions are derived from UMTS 30.01, UMTS 22.01 and UMTS 22.00.

5.1.1 Type of services and service management

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

b) UMTS shall allow service creation. It shall allow the creation of innovative services and individualised service profiles and support the ability to download them to users. (UMTS 30.01, UMTS 22.01)

c) UMTS shall support both interactive and distribution services. (UMTS 22.01)

5.1.2 Access to services

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

b) UMTS shall 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. (UMTS 30.01)

5.1.3 Service provision

a) Home environment specific services based on the Virtual Home Environment (VHE) concept shall be provided in UMTS. (UMTS 22.00)

5.1.4 System architecture

a) Only the UMTS Terrestrial Radio Access Network (UTRAN) (including both Wideband - Code Division Multiple Access (W-CDMA) and Time Division - Code Division Multiple Access (TD-CDMA) radio interfaces, and additional Opportunity Driven Multiple Access (ODMA) functionality) is considered to be part of the UMTS access network. Other types of access networks are for further consideration. (UMTS 22.00) (FFS)

b) UMTS shall be provided with a network management architecture based on Telecommunications Management Network (TMN) principles. (UMTS 30.01, UMTS 22.00)

c) UMTS base stations may need to be installed in an uncoordinated manner for private and business applications (to the extent that no frequency planning is necessary and co-existence of licensed and licence-exempt use is anticipated) (UMTS 30.01).

5.1.5 Security management

a) UMTS security shall be based on the use of a physically secure device called a UMTS Integrated Circuit Card (UICC) that can be inserted and removed from terminal equipment. The UICC shall contain one or more applications at least one of which must be a User Services Identity Module (USIM).

b) A USIM contained in a UICC shall be used to represent and identify a user and his association with a home environment in the provision of UMTS services.

c) The USIM shall be developed on the basis of the GSM Phase 2+ Subscriber Identity Module (SIM). (UMTS Subscriber Identity Module 22.00)

d) UMTS terminal equipment shall support GSM Phase 2 and GSM Phase 2+ SIMs as access modules to UMTS networks. UMTS operators shall be able to decide whether or not to accept GSM SIMs as access modules to UMTS services. (UMTS 22.00)

e) Simultaneous activation of multiple USIMs on one terminal equipment is not required in UMTS Phase 1. (UMTS 22.00)

5.1.6 Interworking and compatibility

a) UMTS shall admit the connection of users to other UMTS users and to users of other networks using their respective addressing schemes (e.g., PSTN, N-ISDN, GSM, X.25 and Internet Protocol (IP) networks). (UMTS 22.00)

b) UMTS is planned as a member of the IMT-2000 family. It is intended to support roaming with other members of the International Mobile Telecommunications-2000 (IMT-2000) family based on market need and business viability. The UMTS access system has been specified as a candidate system to the ITU. UMTS shall meet or exceed the essential ITU minimum requirements. (UMTS 22.01)

c) UMTS shall admit the provision of services in an environment of multiple serving networks and home environments, public or private, some of which will be in direct competition. (UMTS 22.01)

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

5.1.7 Charging and billing

a) UMTS shall support the generation of standardised charging records. (UMTS 22.00)

b) UMTS shall support on-line billing. (UMTS 22.00)

c) UMTS shall support the billing of third party value-added services with to concept of one-stop-billing using standardised procedures. (UMTS 22.00)

5.1.8 Supplementary services

a) The specification of supplementary services for UMTS may not within the scope of standardisation. (UMTS 22.01)

b) Support for GSM supplementary services in UMTS is for further study. (UMTS 22.00) FFS

5.2 UMTS roles

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 roles are defined from a security perspective to

enable security threats to be identified and corresponding security requirements to be constructed in a systematic manner. These roles are derived in part from those defined in UMTS 33.20.

It should be noted that these roles represent purely logical entities, and are not intended to reflect actual legal entities, commercial 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 and a serving network. Similarly, a person could be both a subscriber and a user.

5.2.1 User domain

Subscriber: a person or other entity which has an association with a home environment on behalf of one or more users. A subscriber is responsible for the payment of charges to that home environment (which may be before or after service delivery).

User: 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 profile. A user may have limited access to his service profile, in order to read or modify certain service parameters.

Other Party: 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. Such a party is not necessarily a UMTS user. There may exist legal requirements on the protection of such other parties.

5.2.2 Infrastructure domain

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

Home environment responsibilities include the following:

The provision, allocation and management of subscriber accounts, including the allocation and management of subscriber account identifiers, user identities, user numbers and subscription charges. It also includes all billing mechanisms required to bill subscribers for charges and to pay network operators for user charges.

The provision and maintenance of service profiles for users, including the provision and control of access to service profiles by users.

Negotiation with network operators for network capabilities needed to provide 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.

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

Serving network responsibilities fall into five main areas:

The provision and management of radio resources, including the provision and management of any encrypted bearers needed to ensure confidentiality of user traffic

The provision and management of fixed resources, bearer capabilities, connections and routing.

The collection of charging and accounting data and the transfer of such data to home environments, and other network operators.

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

Relay Node: an entity, typically a mobile terminal, relaying packets between a user's terminal and the serving network (e.g. using ODMA functionality).

5.2.3 Non-UMTS infrastructure domain

Non-UMTS network operators: the role that provides telecommunication network resources other than UMTS resources and may be involved in the provision of UMTS services. The security provided by a UMTS network should not depend on other non-UMTS 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.

5.2.4 Off-line parties

Regulators: the role of any body which is authorised to set laws or guidelines governing the provision or use of UMTS services, or UMTS terminal 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.

5.2.5 Intruders

Intruders: 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, serving networks or any other party. An intruder may, for example, attempt to eavesdrop on user traffic, signalling data and/or control data, or attempt to masquerade as a legitimate party in the use, provision or management of UMTS services.

5.3 UMTS architecture

In this subclause various architectural components of the UMTS system that have an impact on the design of UMTS security features are listed.

User Services Identity Module: an application that represents and identifies a user and his association with a home environment in the provision of UMTS services. The USIM contains functions and data needed to identify and authenticate users when UMTS services are accessed. It may also contain a copy of the user profile. The USIM contains the user's International Mobile User Identity (IMUI) and any security parameters which need to be carried by the user. The USIM is always implemented in a removable IC card called the UICC.

UMTS Integrated Circuit Card (UICC): a physically secure device that can be inserted and removed from terminal equipment. It can contain one or more applications one of which must be the USIM.

5.4 UMTS identities

In this subclause various identities used in the UMTS system that have an impact on the design of UMTS security features are listed.

International Mobile User Identity: The IMUI uniquely identifies a user. The IMUI is stored in the USIM and the home environment database; but need not be known to the user or subscriber.

5.5 UMTS data types and data groups

Different types of data will require different types and levels of protection. Therefore, to be able to derive security requirements we must first distinguish the various types of data that can arise in UMTS. The following subclauses list a number of data types and data groups.

5.5.1 UMTS data types

5.5.1.1 User traffic

User traffic: 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.

5.5.1.2 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 and passed among network operators.

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

Location data: This type comprises location data regarding a user (or terminal equipment). Such data is generated by a network operator and passed to the user's home environment (it may or may not be retained by the network operator).

Addressing data: This type comprises data relating to addresses associated with end users (and possibly terminal equipment). Such data is generated by home environments and distributed to users. It is transferred from a user to network operator to initiate a call, and then passed by the network operator to the associated user's home environment.

Identity data: This type comprises data which determines the identity of an entity. The entities of interest are usually users. User identities are generated by the appropriate home environment, and are stored on the home environment's database and on the USIM. User identities may accompany user-related data such as charging, billing, and location data when it is passed between entities.

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

5.5.1.3 Control data

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

Network resource management data: This type comprises data relating to the physical access of a terminal 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 terminals.

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

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

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

5.5.2 UMTS data groups

5.5.2.1 User-related data

User-related data is data which may (collectively or individually) contain information about a user's identity, behaviour or communication patterns. It may include user traffic, charging data, billing data, location data, addressing data, identity data security management data, access control management data and/or service profile data.

6 Security threats

The purpose of this clause is to list a selection of possible security threats to UMTS. This is intended to provide a motivation for the security requirements identified in this specification.

Many classifications of threats are possible. In this clause, threats are categorised according to point of attack. The following points of attack are defined and discussed in the following subclauses:

- threats associated with attacks on the radio interface;
- threats associated with attacks on other parts of the system;
- threats associated with attacks on the terminal and UICC/USIM.

6.1 Threats associated with attacks on the radio interface

The radio interface between the terminal equipment and the serving network represents a significant point of attack in UMTS. The threats associated with attacks on the radio interface are split into the following categories, which are described in the following subclauses:

- unauthorised access to data;
- threats to integrity;
- denial of service.

6.1.1 Unauthorised access to data

T1a **Eavesdropping user traffic:** Intruders may eavesdrop user traffic on the radio interface. In particular relay nodes may eavesdrop user traffic.

T1b **Eavesdropping signalling or control data:** Intruders may eavesdrop signalling data or control data on the radio interface. This may be used to access security management data or other information which may be useful in conducting other attacks on the system.

T1c **Masquerading as a communications participant:** Intruders may masquerade as a network element to intercept user traffic, signalling data or control data on the radio interface. In particular relay nodes may masquerade as a network element.

T1d **Passive traffic analysis:** Intruders may observe the time, rate, length, sources or destinations of messages on the radio interface to obtain access to information. In particular relay nodes may deduce information about the location or activity of a legitimate user.

T1e **Active traffic analysis:** Intruders may actively initiate communications sessions and then obtain access to information through observation of the time, rate, length, sources or destinations of associated messages on the radio interface.

6.1.2 Threats to integrity

T2a **Manipulation of user traffic:** Intruders may modify, insert, replay or delete user traffic on the radio interface. This includes both accidental or deliberate manipulation.

T2b **Manipulation of signalling or control data:** Intruders may modify, insert, replay or delete signalling data or control data on the radio interface. This includes both accidental or deliberate manipulation.

NOTE Replayed data which cannot be decrypted by an intruder may still be used to conduct attacks against the integrity of user traffic, signalling data or control data.

6.1.3 Denial of service

T3a **Physical intervention:** Intruders may prevent user traffic, signalling data or control data from being transmitted on the radio interface by physical means. An example of physical intervention is jamming. Physical intervention may also be conducted by delaying transmissions on the radio interface.

T3b **Protocol intervention:** Intruders may prevent user traffic, signalling data or control data from being transmitted on the radio interface by inducing protocol failures. These protocol failures may themselves be induced by physical means.

T3c **Denial of service by masquerading as a communications participant:** Intruders may deny service to a legitimate user by preventing user traffic, signalling data or control data from being transmitted on the radio interface by masquerading as a network element to intercept and block user traffic, signalling data or control data on the radio interface.

T3d **Relay failure:** An intruder may interrupt the flow of user traffic by failing to relay packets as expected.

6.2 Threats associated with attacks on other parts of the system

Although attacks on the radio interface between the terminal equipment and the serving network represent a significant threat, attacks on other parts of the system may also be conducted. These include attacks on other wireless interfaces, attacks on wired interfaces, and attacks which cannot be attributed to a single interface or point of attack. The threats associated with attacks on other parts of the system are split into the following categories, which are described in the following subclauses:

- unauthorised access to data;
- threats to integrity;
- denial of service;
- repudiation;
- unauthorised access to services.

6.2.1 Unauthorised access to data

T4a **Eavesdropping user traffic:** Intruders may eavesdrop user traffic on any system interface, whether wired or wireless.

T4b **Eavesdropping signalling or control data:** Intruders may eavesdrop signalling data or control data on any system interface, whether wired or wireless. This may be used to access security management data which may be useful in conducting other attacks on the system.

T4c **Masquerading as an intended recipient of data:** Intruders may masquerade as a network element in order to intercept user traffic, signalling data or control data on any system interface, whether wired or wireless.

T4d **Passive traffic analysis:** Intruders may observe the time, rate, length, sources or destinations of messages on any system interface, whether wired or wireless, to obtain access to information.

T4e **Active traffic analysis:** Intruders may actively initiate communications sessions and then obtain access to information through observation of the time, rate, length, sources or destinations of associated messages on any system interface, whether wired or wireless.

T4f **Unauthorised access to data stored by system entities:** Intruders may obtain access to data stored by system entities. Access to system entities may be obtained either locally or remotely, and may involve breaching physical or logical controls.

6.2.2 Threats to integrity

T5a **Manipulation of user traffic:** Intruders may modify, insert, replay or delete user traffic on any system interface, whether wired or wireless. This includes both accidental and deliberate manipulation.

T5b **Manipulation of signalling or control data:** Intruders may modify, insert, replay or delete signalling or control data on any system interface, whether wired or wireless. This includes both accidental and deliberate manipulation.

T5c **Manipulation by masquerading as a communications participant:** Intruders may masquerade as a network element to modify, insert, replay or delete user traffic, signalling data or control data on any system interface, whether wired or wireless.

T5d **Manipulation of applications and/or data downloaded to the terminal or USIM:** Intruders may modify, insert, replay or delete applications and/or data which is downloaded to the terminal or USIM. This includes both accidental and deliberate manipulation.

T5e **Manipulation of the terminal or USIM behaviour by masquerading as the originator of applications and/or data:** Intruders may masquerade as the originator of malicious applications and/or data downloaded to the terminal or USIM.

T5f **Manipulation of data stored by system entities:** Intruders may modify, insert or delete data stored by system entities. Access to system entities may be obtained either locally or remotely, and may involve breaching physical or logical controls.

NOTE Replayed data which cannot be decrypted by an intruder may still be used to conduct attacks against the integrity of user or signalling information.

6.2.3 Denial of service

T6a **Physical intervention:** Intruders may prevent user or signalling traffic from being transmitted on any system interface, whether wired or wireless, by physical means. An example of physical intervention on a wired interface is wire cutting. An example of physical intervention on a wireless interface is jamming. Physical intervention involving interrupting power supplies to transmission equipment may be conducted on both wired and wireless interfaces. Physical intervention may also be conducted by delaying transmissions on a wired or wireless interface.

T6b **Protocol intervention:** Intruders may prevent user or signalling traffic from being transmitted on any system interface, whether wired or wireless, by inducing protocol failures. These protocol failures may themselves be induced by physical means.

T6c **Denial of service by masquerading as a communications participant:** Intruders may deny service to a legitimate user by preventing user traffic, signalling data or control data from being transmitted by masquerading as a network element to intercept and block user traffic, signalling data or control data.

T6d **Resource exhaustion:** Intruders may prevent access to services by other users by deliberately or accidentally overloading system resources.

T6e **Denial of access:** Intruders could prevent access to services by other users due to inadequate access control. One example would be a user being denied access to service because of repeated intentional failed authentication attempts by another entity. Denial of access could also be accidental (user forgetting a PIN), or a side effect of another entity's activities (such as trying to find out the user's PIN).

T6f **Abuse of emergency services:** Intruders may prevent access to services by other users and cause serious disruption to emergency services facilities by abusing the ability to make USIM-less calls to emergency services from UMTS terminals. If such USIM-less calls are permitted then the provider may have no way of preventing the intruder from accessing the service.

6.2.4 Repudiation

T7a **Repudiation of charge:** A user could deny having incurred charges, perhaps through denying attempts to access a service or denying that the service was actually provided.

T7b **Repudiation of user traffic origin:** A user could deny that he sent user traffic received by another user.

T7c **Repudiation of signalling data or control data origin:** An network element could deny that it sent signalling data or control data received by another network element.

T7d **Repudiation of user traffic delivery:** A user could deny that he received user traffic sent by another user.

T7e **Repudiation of signalling data or control data delivery:** An network element could deny that it signalling data or control data sent by another network element.

6.2.5 Unauthorised access to services

T8a **Masquerading as a user:** Intruders may impersonate a user to utilise services authorised for that user. The intruder may have received assistance from other entities such as the serving network, the home environment or even the user himself. The intruder may be acting or have acted as a relay node on behalf of the user.

T8b **Masquerading as a serving network:** Intruders may impersonate a serving network, or part of an serving network's infrastructure, perhaps with the intention of using an authorised user's access attempts to gain access to services himself.

T8c **Masquerading as a home environment:** Intruders may impersonate a home environment perhaps with the intention of obtaining information which enables him to masquerade as a user.

T8d **Misuse of user privileges:** Users may abuse their privileges to gain unauthorised access to services.

T8e **Misuse of serving network privileges:** Serving networks may abuse their privileges to gain unauthorised access to services. The serving network could misuse security management data about a user to masquerade as that user and gain unauthorised access to services.

T8f **Misuse of home environment privileges:** Home environments may abuse their privileges to gain unauthorised access to services. The home environment could misuse security management data about a user to masquerade as that user and gain unauthorised access to services.

T8g **Freeloading:** Intruders may take advantage of relay nodes to obtain a free communications medium.

6.3 Threats associated with attacks on the terminal and UICC/USIM

T9a **Use of a stolen terminal and UICC:** Intruders may use stolen terminals and UICCs to gain unauthorised access to services.

T9b **Use of a borrowed terminal and UICC:** Users who have been given authorisation to use borrowed equipment may misuse their privileges perhaps by exceeding agreed usage limits.

T9c **Use of a stolen terminal:** Users may use a valid USIM with a stolen terminal to access services.

T9d **Use of a non approved or faulty terminal:** Users may use a valid USIM with a non approved or faulty terminal to access services.

T9e **Use of a barred terminal:** Users may use a valid USIM with a barred terminal to access services.

T9f **UICC removal during terminal operation:** Users may remove a UICC during terminal operation and reuse it to access additional services.

T9g **Integrity of data on a terminal:** Intruders may modify, insert or delete applications and/or data stored by the terminal. Access to the terminal may be obtained either locally or remotely, and may involve breaching physical or logical controls.

T9h **Integrity of data on USIM:** Intruders may modify, insert or delete applications and/or data stored by the USIM. Access to the USIM may be obtained either locally or remotely, and may involve breaching physical or logical controls.

T9i **Eavesdropping the UICC-terminal interface:** Intruders may eavesdrop the UICC-terminal interface.

T9j **Masquerading as an intended recipient of data on the UICC-terminal interface:** Intruders may masquerade as a USIM or a terminal in order to intercept data on the UICC-terminal interface.

T9k **Manipulation of data on the UICC-terminal interface:** Intruders may modify, insert, replay or delete user traffic on the UICC-terminal interface. This includes both accidental and deliberate manipulation.

7 Security requirements

The purpose of this clause is to provide a list of security requirements for UMTS. The security requirements form a natural link between the security threats to the system and the corresponding security features supported by the system to counteract these threats. More precisely, requirements can be derived from threats, and then features may be introduced to satisfy these requirements.

The requirements have been defined with reference to the roles played by the various entities involved in UMTS and the relationships between them.

In subclause 7.1 security requirements that benefit users of the UMTS system are listed.

In subclause 7.2 security requirements that benefit providers of the UMTS system are listed.

In subclause 7.3 security requirements that benefit regulators are listed.

7.1 User security requirements

This subclause identifies security requirements that benefit users of the UMTS system. In this respect the requirements are said to be "owned" by users. The requirements are split into the following categories, which are defined in the following subclauses:

- Secure access to UMTS services;
- Protection of user-related transmitted data;
- Protection of user-related stored data;
- End-to-end security.

7.1.1 Secure access to UMTS services

R1a It shall be possible to prevent intruders, including relay nodes, from obtaining unauthorised access to UMTS services by masquerading as authorised users.

R1b It shall be possible to prevent intruders, including relay nodes, from hijacking a service already provided to an user.

R1c It shall not be possible for unjustified charges to be imposed on users.

R1d It shall be possible for users to be able to verify that serving networks are authorised to offer UMTS service on behalf of the user's home environment at the start of, and during, service delivery.

R1e It shall not be possible for simultaneous access to UMTS services by multiple users from the same terminal to jeopardise the security of individual access to UMTS service.

R1f It shall be possible to protect against unauthorised modification of certain signalling data and control data, particularly on radio interfaces.

R1g It shall be possible to protect the confidentiality of certain signalling data and control data, particularly on radio interfaces.

7.1.2 Protection of user-related transmitted data

R2a It shall be possible to protect the confidentiality of user traffic, particularly on radio interfaces, including protection against eavesdropping from relay nodes.

R2b It shall be possible to protect the confidentiality of user identity data, particularly on radio interfaces, including protection against eavesdropping from relay nodes.

R2c It shall be possible to protect the confidentiality of location data about users, particularly on radio interfaces, including protection against eavesdropping from relay nodes.

R2d It shall be possible to protect against the unauthorised disclosure of location data about users participating in a particular UMTS service to other parties participating in the same UMTS service.

R2e It shall be possible to protect against unauthorised modification of user traffic.

R2f It shall be possible for the user to be able to check whether or not his user traffic is protected, particularly on radio interfaces.

NOTE Regarding R2e, the extent to which integrity protection is applied has yet to be determined. There may be a greater requirement for protection of user traffic in data calls rather than for telephony calls, for example.

7.1.3 Protection of user-related stored data

R3a It shall be possible to protect against unauthorised modification of user-related data which is stored or processed by a provider

R3b It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider

R3c It shall be possible to protect against unauthorised modification of user-related data stored in the terminal or in the USIM.

R3d It shall be possible to protect the confidentiality of user-related data stored in the terminal or in the USIM.

NOTE Protection of user-related data has to be realised according to national legislation implementing directives:

97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the privacy in the telecommunications sector.

95/46/EC of the European Parliament and of the Council of 24 October 1995 n the protection of individuals with regard to the processing of personal data and on the free movement of such data.

7.1.4 End-to-end security

R4a It shall be possible for a user acting as a calling party to remain anonymous towards the called party or any party to which the call is forwarded, except for emergency calls.

R4b UMTS shall not preclude the implementation of end-to-end security services over UMTS bearers (including mutual entity authentication between users, user traffic confidentiality, user traffic origin authentication, user

traffic integrity, non repudiation of charging data, non repudiation of user traffic origin and non repudiation of user traffic delivery)

7.2 Provider security requirements

This subclause identifies security requirements that benefit providers of the UMTS system. In this respect the requirements are said to be "owned" by providers. The term "provider" encompasses both home environments and serving networks, however, home environments and serving networks will be specifically named within the requirements, if appropriate.

The requirements are split into the following categories, which are defined in the following subclauses:

- USIM security;
- Terminal security;
- Secure provision of UMTS services;

7.2.1 USIM security

R5a A valid USIM shall be required to access any UMTS service except for emergency calls where the network should be allowed to decide whether or not emergency calls should be permitted without a USIM.

R5b It shall be possible to prevent the use of a particular USIM to access UMTS services.

R5c It shall be possible to control access to a USIM so that it can only be used to access UMTS services by the subscriber to whom it was issued or by users explicitly authorised by that subscriber.

R5d It shall be possible to control access to data in a USIM. For instance, some data may only be accessible by an authorised home environment.

R5e It shall not be possible to access data in a USIM that is only intended to be used within the USIM, e.g. authentication keys and algorithms.

R5f If a UICC contains more than one USIM (to access services from different home environments) then different home environments shall only have access to the USIMs of their own users.

R5g If a UICC contains more than one USIM (to access services from different home environments) then security management data (e.g. authentication information) of each USIM shall be protected independently against unauthorised access and modification.

R5h It shall be possible to control access to, and selection of, USIMs and other non-UMTS applications stored on the same UICC. In particular, it shall be possible to have shared directories between applications where appropriate.

R5i It shall be possible to ensure that the origin and integrity of applications and/or data downloaded to the UICC can be checked. It may also be necessary to ensure that the confidentiality of downloaded applications and/or data can be ensured.

7.2.2 Terminal security

R6a It shall be possible to deter the theft of terminals.

R6b It shall be possible to bar a particular terminal from accessing UMTS services.

R6c It shall be difficult to change the identity of a terminal to circumvent measures taken to bar a particular terminal from accessing UMTS services.

R6d It shall be possible to ensure that the origin and integrity of applications and/or data downloaded to the terminal can be checked. It may also be necessary to ensure that the confidentiality of downloaded applications and/or data can be ensured.

NOTE 1: Does R6a solely rely on the ability to bar stolen terminals?

NOTE 2: How can requirements R6c and R6c be met without a physically and logically secure terminal identity module which can be cryptographically authenticated. Is a difficult-to-manipulate International Mobile Equipment Identity (IMEI) sufficient to deter most terminal fraud?

7.2.3 Secure provision of UMTS services

R7a It shall be possible for providers to authenticate users at the start of, and during, service delivery to prevent intruders (including relay nodes) from obtaining unauthorised access to UMTS services by masquerade or misuse of priorities.

R7b It shall be possible to detect and prevent the fraudulent use of services. Alarms will typically need to be raised to alert providers to security-related events. Audit logs of security related events will also need to be produced.

R7c It shall be possible for a home environment to cause an immediate termination of all services provided to users associated with that home environment.

R7d It shall be possible for the serving network to be able to authenticate the origin of user traffic, signalling data and control data on radio interfaces.

R7e It shall be possible to prevent intruders from restricting the availability of services by logical means.

R7f It shall be possible to prevent intruders from significantly disrupting services by failing to relay packets as expected.

R7g It shall be possible to prevent intruders from abusing legitimate relay nodes to obtain a free communications medium.

NOTE Regarding R7e, preventing intruders from restricting the availability of services by physical means is outside the scope of this specification.

7.3 Regulator requirements

This subclause identifies security requirements that benefit regulators of the UMTS system. In this respect the requirements are said to be "owned" by regulators. The requirements are split into the following categories, which are defined in the following subclauses:

- Lawful interception.

7.3.1 Lawful interception

R8a It shall be possible to monitor and register every interception and every attempted interception, whether lawful or otherwise, in accordance with the national law. This shall apply to devices and/or via interfaces placed by the serving networks or home environments at the disposal of the national law enforcement agencies according to national law, and intended solely for lawful interception purposes

NOTE Lawful interception has to be realised according to national legislation and the requirements given in:

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

ETR 331 Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications - Requirements of the law enforcement agencies..

Annex A (informative): Status of UMTS 33.21

Status of Technical Specification UMTS 33.21; Security requirements		
Version	**Date**	**Comments**
33.20 proposal version 0.6.0	June 1998	Global revision to remove features and mechanisms, and thereby leave a complete list of requirements without reference to features or mechanisms. The requirements have also been re-ordered to ensure that every requirement is owned by an UMTS entity. No additional requirements have been added. Discursive text has been deleted. New threats added based on SMG10 079/98
33.21 version 0.1.0	15 July 1998	Changes made based on comments received on 33.20 proposal 0.6.0. Security context reduced and clarified. Threats categorised according to point of attack. Additional threats from "LINK PCP, 3GS3, Technical Report 1" added. Further subdivision of threats according to type of attack. Temporary clause added for uncategorised threats. Requirements categorised according to two groups of owner: user and provider. Many requirements rewritten in an attempt to improve clarity. Additional requirements from "LINK PCP, 3GS3, Technical Report 1" added. Temporary clause added for uncategorised requirements.
0.1.1	16 July 1998	Editorial changes in compliance with ETSI Drafting rules.
0.1.2	22 July 1998	Minor corrections required because of editorial changes in v0.1.1. Further changes including many based on comments received.
0.1.3	31 July 1998	Major changes based on comments and discussion at SMG10 #3/98.
1.0.0	July 1998	Specification to SMG#27 for information.
1.0.1	5 October 1998	Changes based on decisions made at SMG10 WPC ad hoc #4/98.
1.0.2	19 October 1998	Further changes made based on comments received.
1.0.3	30 October 1998	Changes based on decisions made at SMG10 WPC ad hoc #5/98.
1.0.4	20 November 1998	Changes based on decisions made at SMG10 WPC ad hoc #6/98.
1.1.0	27 January 1999	Minor typographical and editorial changes.
2.0.0	February 1999	version to SMG#28 for approval
3.0.0	February 1999	specification approved by SMG#28
Text and figures: WinWord 6.0 **Stylesheet**: etsiw_70.dot **Rapporteur**: Peter Howard (Vodafone)		

History

Document history		
V3.0.0	February 1999	Unpublished