3GPP TS 21.133 V4.1.0 (2001-12)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Security Threats and Requirements
(Release 4)

Keywords
Security, Threats, Requirements

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

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

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This specification takes notice of the Security Principles and Objectives as set out in [1]. It contains an evaluation of perceived threats to 3GPP and produces subsequently a list of security requirements to address these threats.

As teleservices and applications will not, in general, be standardised, it is difficult to predict their exact nature. Therefore, this specification considers all security threats and aims at listing generic security requirements that shall be applicable irrespective of the actual services offered. The list of threats and requirements may however need to be updated as the 3GPP system evolves.

The threat analysis performed relies to a large extent on previous experiences with 2G systems, in particular GSM, and takes into account known problems from that area.

The security requirements listed in this specification shall be used as input for the choice of security features and the design of the 3GPP security architecture as specified in [2].

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 a reference to the general objectives for 3G security;

clause 5 contains an overview of the context in which the security architecture of 3G is designed;

clause 6 contains a list of identified security threats to 3G, and gives some results from the threat analyses that have been performed;

clause 7 contains an overview of the risk assessment resulting from the threat analyses performed

clause 8 contains the resulting list of security requirements for 3G and indicates how these requirements relate to the threats and the security objectives .

Finally, Annex A gives some more detailed information on threats and risks connected to so called false base station attacks.

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 33.120: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Principles and Objectives".

[2] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

Baseline documents:

3GPP s3-99003: UMTS 33.21, version 2.0.0: "Security requirements".

3GPP s3-99016: ARIB, Requirements and Objectives for 3G Mobile Services and System, Annex 8 - Security Design Principles.

ETSI SMG10 99C019: Countermeasures to active attacks on the radio access link.

[3] ETSI ETR 332: "Security Techniques Advisory Group; Security requirements capture".

[4] ETSI ETR 331: "Definition of user Requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".

[5] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

[6] ISO/IEC 10181-2: "Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems".

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

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

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

[10] UMTS 22.21: "Universal Mobile Telecommunications System (UMTS): Virtual Home Environment".

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

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

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

[14] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

3 Definitions and Abbreviations

3.1 Definitions

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

Access Control: The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner [5].

Authentication: The provision of assurance of the claimed identity of an entity [6].

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.

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 [7].

Law Enforcement Agency (LEA): An organisation authorised by a lawful authorisation, based on a national law, to receive the results of telecommunication interceptions [4].

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 [4].

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 [4].

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 [5].

3.2 Abbreviations

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

GSM	Global System for Mobile communications
HE	Home Environment
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
N-ISDN	Narrowband ISDN
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
SIM	Subscriber Identity Module
SN	Serving Network
TD-CDMA	Time Division - Code Division Multiple Access
TMN	Telecommunications Management Network
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UPT	Universal Personal Telecommunication
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 3G security features

The general objectives for 3G security features have been stated as [1]:

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 (There shall be at least one ciphering algorithm that can be exported on a world-wide basis (in accordance with the Wassenaar agreement));

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;

f) to ensure that the implementation of 3G security features and mechanisms can be extended and enhanced as required by new threats and services.

Furthermore it has been agreed that the basic security features employed in 2G systems will be retained, or where needed enhanced. These include:

- subscriber authentication,
- radio interface encryption,
- subscriber identity confidentiality,
- use of removable subscriber module,
- secure application layer channel between subscriber module and home network,
- transparency of security features,
- minimised need for trust between HE and SN.

In some instances, 3G will need to be equipped with stronger or more flexible security mechanisms than those which were designed for GSM, due to new or increased threats. These will be treated in the threat analysis.

Mechanisms to combating fraud in roaming situations should be included in the 3G specifications from the start.

Mechanisms for lawful interception under authorisation should be included in 3G specifications from the start.

5 Security context

The purpose of this clause is to describe the context in which the 3G security features are designed. This specification assumes the system assumptions, network architecture and functional roles given in UMTS 23.01 [11] and UMTS 30.01 [12], the service description given in UMTS 22.01 [9] and the UMTS Phase 1 description given in UMTS 22.00 [8].

In subclause 5.1 the system assumptions that describe 3G 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 3G security features are defined.

In subclause 5.4 various identities used in 3G that have an impact on the design of 3G security features are defined.

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

5.1 System assumptions

In this subclause 3G system assumptions that have an impact on the design of 3G security features are listed. These assumptions are derived from UMTS 30.01 [12], UMTS 22.01 [9] and UMTS 22.00 [8].

5.1.1 Type of services and service management

a) 3G 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. [12]

b) 3G shall allow service creation. It shall allow the creation of innovative services and individualised service profiles and support the ability to download these services to users. [9] [12]

c) 3G shall support both interactive and distribution services. [9]

5.1.2 Access to services

a) 3G is a wireless mobile system. Mobility must include user and terminal mobility to permit roaming. 3G shall allow national and international roaming between networks subject to regulations and inter-operator agreements. These agreements may be set-up statically or dynamically. [12]

b) 3G 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. [12]

5.1.3 Service provision

a) Home environment specific services based on the VHE concept shall be provided in 3G. [8] [10]

5.1.4 System architecture

a) The UTRAN (including both W-CDMA and TD-CDMA radio interfaces) is considered to be part of the 3G access network. Other types of access networks (e.g. fixed wireline access) are also to be considered. [8]

b) Standardised protocols for operation, administration and maintenance of 3G shall be defined in co-operation with ETSI TMN. [30.01, 22.00]

c) 3G 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) [12].

5.1.5 Security management

a) 3G security shall be based on the use of a physically secure device i.e. a UICC, as defined in [14], that can be inserted and removed from terminal equipment. This UICC shall contain one or more applications at least one of which must be a 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 3G services.

c) The USIM shall be developed on the basis of the phase 2+ GSM SIM. [8]

d) 3G terminal equipment shall support GSM phase 2 and phase 2+ SIMs as access modules to 3G networks. This will result in security being limited in extent and quality to GSM level. For this reason 3G operators shall be able to decide whether or not to accept GSM SIMs as access modules to 3G services. [8]

e) Simultaneous activation of multiple USIMs on one terminal equipment is not required in 3G phase 1. [8]

5.1.6 Interworking and compatibility

a) 3G shall admit the connection of users to other 3G users and shall support interworking with other networks (e.g., PSTN, N-ISDN, GSM, X.25 and IP networks). [8]

b) 3G is planned as a member of the IMT-2000 family. It is intended to support roaming with other members of the IMT-2000 family based on market need and business viability. The 3G access system has been specified as a candidate system to the ITU. 3G shall meet or exceed the essential ITU minimum requirements. [9]

c) 3G 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. [9]

d) 3G shall support secure Global Cross-standard Roaming. [12]

5.1.7 Charging and billing

a) 3G shall support the generation of standardised charging records. [8]

b) 3G shall support on-line billing. [8]

c) 3G shall support the billing of third party value-added services with the concept of one-stop-billing using standardised procedures. [8]

5.1.8 Supplementary services

a) The specification of supplementary services for 3G may not be within the scope of standardisation. [9]

b) Support for GSM supplementary services in 3G is for further study. [8]

5.2 3G roles

This subclause provides a description of the various parties or organisations involved in the use, provision, and regulation of 3G 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 [13].

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 3G 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, i.e. pre-pay or subscription).

User: a person or other entity that has been authorised to use 3G services by a subscriber. His usage is delimited and described in the user's service 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 3G user, or the called party in a call from a 3G user. Such a party is not necessarily a 3G 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 3G services to its users, including off-line agreements to allow service provision, and on-line interaction to ensure that users are properly identified, located, authenticated and authorised to use services before those services are provided to them.

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 four main areas:

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

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

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

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

Value Added Service Provider (VASP): A subscriber may subscribe to services also from a VASP that may not have any association with the Home Environment of that subscriber, although the VASP would use (parts of) the services of the subscriber's Home Environment to offer the subscriber access to the VASP services. VASP is defined in UMTS 22.21 on Virtual Home Environment.

5.2.3 Non-3G infrastructure domain

Non-3G network operators: the role that provides telecommunication network resources other than 3G resources and may be involved in the provision of 3G services. The security provided by a 3G network should not depend on other non-3G networks, e.g., if security parameters are passed from one 3G 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.

NOTE: The GSM/3G interworking on terminal and/or SIM basis is not clear yet.

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 3G services, or 3G 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 3G 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 3G, or who otherwise attempts to abuse 3G 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 3G services.

5.3 3G architecture

In this subclause various architectural components of the 3G system that have an impact on the design of 3G security features are listed.

User Services Identity Module (USIM): an application that represents and identifies a user and his association with a home environment in the provision of 3G services. The USIM contains functions and data needed to identify and authenticate users when 3G services are accessed. It may also contain a copy of the user's service profile. It may also provide other security features. The USIM contains the user's 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.

5.4 3G identities

In this subclause various identities used in the 3G system that have an impact on the design of 3G 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 3G 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 3G. The following subclauses list a number of data types and data groups.

5.5.1 3G 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 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 3G data groups

5.5.2.1 User-related data

User-related data includes user traffic, charging data, billing data, location data, addressing data, identity data, security management data, access control management data and service profile data.

6 Security threats

The purpose of this clause is to list possible security threats to the 3G system, detailing what the threats achieve, how they are carried out and where in the system they could occur.

It is possible to classify security threats in many different ways. In this clause threats in the following categories have been considered.

Unauthorised access to sensitive data (violation of confidentiality)

- **Eavesdropping:** An intruder intercepts messages without detection.
- **Masquerading:** An intruder hoaxes an authorised user into believing that they are the legitimate system to obtain confidential information from the user; or an intruder hoaxes a legitimate system into believing that they are an authorised user to obtain system service or confidential information.
- **Traffic analysis:** An intruder observes the time, rate, length, source, and destination of messages to determine a user's location or to learn whether an important business transaction is taking place.
- **Browsing:** An intruder searches data storage for sensitive information.
- **Leakage:** An intruder obtains sensitive information by exploiting processes with legitimate access to the data.

- **Inference:** An intruder observes a reaction from a system by sending a query or signal to the system. For example, an intruder 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.

Unauthorised manipulation of sensitive data (Violation of integrity)

- **Manipulation of messages:** Messages may be deliberately modified, inserted, replayed, or deleted by an intruder

Disturbing or misusing network services (leading to denial of service or reduced availability)

- **Intervention:** An intruder may prevent an authorised user from using a service by jamming the user's traffic, signalling, or control data.
- **Resource exhaustion:** An intruder may prevent an authorised user from using a service by overloading the service.
- **Misuse of privileges:** A user or a serving network may exploit their privileges to obtain unauthorised services or information.
- **Abuse of services:** An intruder may abuse some special service or facility to gain an advantage or to cause disruption to the network.

Repudiation: A user or a network denies actions that have taken place.

Unauthorised access to services

- Intruders can access services by masquerading as users or network entities.
- Users or network entities can get unauthorised access to services by misusing their access rights.

A number of security threats in these categories are subsequently treated in the remainder of this clause according to the following points of attack:

- Radio interface;
- Other part of the system;
- Terminals and UICC/USIM.

Note also that Annex A gives some extra information as regards threats connected to active attacks on the radio interface. The threats treated in annex A are incorporated in the following lists.

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 3G. 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;
- unauthorised access to services.

6.1.1 Unauthorised access to data

T1a **Eavesdropping user traffic:** Intruders may eavesdrop user traffic on the radio interface.

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 active 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.

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.

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 attacks

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

T3b **Protocol intervention:** Intruders may prevent user traffic, signalling data or control data from being transmitted on the radio interface by inducing specific 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.

6.1.4 Unauthorised access to services

T4a **Masquerading as another user:** An intruder may masquerade as another user towards the network. The intruder first masquerades as a base station towards the user, then hijacks his connection after authentication has been performed.

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

T5a **Eavesdropping user traffic:** Intruders may eavesdrop user traffic on any system interface, whether wired or wireless.

T5b **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.

T5c **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.

T5d **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.

T5e **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.

T5f **Compromise of location information:** Legitimate user of a 3G service may receive unintended information about other users locations through (analysis of) the normal signalling or voice prompts received at call set up.

6.2.2 Threats to integrity

T6a **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.

T6b **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.

T6c **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.

T6d **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.

T6e **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.

T6f **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.

6.2.3 Denial of service attacks

T7a **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.

T7b **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.

T7c **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.

T7d **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 3G 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

T8a **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.

T8b **Repudiation of user traffic origin:** A user could deny that he sent user traffic.

T8c **Repudiation of user traffic delivery:** A user could deny that he received user traffic.

6.2.5 Unauthorised access to services

T9a **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.

T9b **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.

T9c **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.

T9d **Misuse of user privileges:** Users may abuse their privileges to gain unauthorised access to services or to simply intensively use their subscriptions without any intent to pay.

T9e **Misuse of serving network privileges:** Serving networks may abuse their privileges to gain unauthorised access to services. The serving network could e.g. misuse authentication data for a user to allow an accomplice to masquerade as that user or just falsify charging records to gain extra revenues from the home environment.

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

T10a **Use of a stolen terminal and UICC:** Intruders may use stolen terminals and UICCs to gain unauthorised access to services.

T10b **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.

T10c **Use of a stolen terminal:** Users may use a valid USIM with a stolen terminal to access services.

T10d **Manipulation of the identity of the terminal:** Users may modify the IMEI of a terminal and use a valid USIM with it to access services.

T10e **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.

T10f **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.

T10g **Eavesdropping the UICC-terminal interface:** Intruders may eavesdrop the UICC-terminal interface.

T10h **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.

T10i **Manipulation of data on the UICC-terminal interface:** Intruders may modify, insert, replay or delete user traffic on the UICC-terminal interface.

T10j **Confidentiality of certain user data in the terminal or in the UICC/USIM:** Intruders may wish to access personal user data stored by the user in the terminal or UICC, e.g. telephone books.

T10k **Confidentiality of authentication data in the UICC/USIM:** Intruders may wish to access authentication data stored by the service provider, e.g. authentication key.

7 Risk Assessment

7.1 Evaluation of threats

Threats have been analysed and evaluated as regards the combined likelihood of occurrence and severity of impact. The threat analysis and the assessment of risks has followed the procedure outlined in ETSI Technical Report ETR 332 [3]. Extensive use has been made of the collected experiences of operators of first generation (analogue) systems and second generation (especially GSM) systems as regards current and envisaged threats to mobile systems. Note that this evaluation normally emanates from the situation as it is before any security mechanisms have been applied, whereas in some cases threats relate also to the situation where GSM-like security mechanisms have been assumed.

The evaluation results are given here as a list of threats evaluated as being of major or medium (significant) impact. Major threats are indicated, other threats listed are assumed to be medium impact.

7.1.1 Threats evaluated to be of major or medium value.

T1a **Eavesdropping user traffic:** Intruders may eavesdrop user traffic on the radio interface. (MAJOR)

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 active 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. (MAJOR)

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. (MAJOR)

T4a **Masquerading as another user:** An intruder may masquerade as another user towards the network.. The intruder first masquerades as a base station towards the user, then hijacks his connection after authentication has been performed.

T5b **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.

T6e **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.

T9a **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. (MAJOR)

T9b **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.

T9d **Misuse of user privileges:** Users may abuse their privileges to gain unauthorised access to services or to simply intensively use their subscriptions without any intent to pay. (MAJOR)

T10a **Use of a stolen terminal and UICC:** Intruders may use stolen terminals and UICCs to gain unauthorised access to services. (MAJOR)

T10c **Use of a stolen terminal:** Users may use a valid USIM with a stolen terminal to access services. (MAJOR)

T10d **Manipulation of the identity of the terminal:** Users may modify the IMEI of a terminal and use a valid USIM with it to access services. (MAJOR)

T10e **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.

T10f **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.

T10k **Confidentiality of authentication data in the UICC/USIM:** Intruders may wish to access authentication data stored by the service provider, e.g. authentication key. (MAJOR)

7.2 Results of threat analysis

Not surprisingly, as the experience from operating mobile systems has shown, most of the significant threats can be categorised into a small number of groups:

Masquerading: as other users to gain unauthorised access to services (i.e. charged to another user's account),

Eavesdropping: which may lead to compromise of user data traffic confidentiality, or of call-related information like dialled numbers, location data, etc.

Subscription fraud: where subscribers exploit the services with heavy usage without any intention to pay.

What is new is the acknowledgement of threats which exploit more sophisticated, active attacks to achieve the eavesdropping or masquerading (see Annex A). These may involve attacks which involve the manipulation of signalling

traffic on the radio interface and attacks where the intruder masquerades as a radio base station. Furthermore, attention is now not only focused on radio interface attacks, but also on other part of the system.

8 Security Requirements

8.1 Requirements derived from threat analysis

This subclause gives a complete list of security requirements as derived from the threat analysis. They have not been ordered according to risk evaluation values. The threat or threats directly leading to the requirement or connected to the requirement are given in brackets for each entry.

8.1.1 Requirements on security of 3GPP services

8.1.1.1 Requirements on secure service access

R1a A valid USIM shall be required to access any 3G service except for emergency calls where the network should be allowed to decide whether or not emergency calls should be permitted without a USIM. (T7d, T9a,d)

R1b It shall be possible to prevent intruders from obtaining unauthorised access to 3G services by masquerading as authorised users. (T4a, T9a,c)

R1c It shall be possible for users to be able to verify that serving networks are authorised to offer 3G services on behalf of the user's home environment at the start of, and during, service delivery. (T1c,e, T3c, T4a, T9b,c)

8.1.1.2 Requirements on secure service provision

R2a It shall be possible for service providers to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorised access to 3G services by masquerade or misuse of priorities. (T4a, T8a, T9a,d)

R2b 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. (T8a,b,c, T9d,e, T10a,b)

R2c It shall be possible to prevent the use of a particular USIM to access 3G services. (T9a,d, T10a)

R2d It shall be possible for a home environment to cause an immediate termination of all services provided to certain users, also those offered by serving networks. (T9a,d, T10a,b)

R2e 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. (T8a,b,c, T9c)

Note: It is assumed that user traffic contains sufficient redundancy such that a stream cipher provides a basic level of data origin authentication on the radio interfaces and that, if that is not sufficient and additional measures are required, the application should be aware and measures should be implemented at the application layer.

R2f It shall be possible to prevent intruders from restricting the availability of services by logical means. (T3b,c, T7e)

R2g There shall be a secure infrastructure between network operators, designed such that the need for HE trust in the SN for security functionality is minimised.

8.1.2 Requirements on system integrity

R3a It shall be possible to protect against unauthorised modification of user traffic. (T2a, T6a,c, T7b,c)

Note: It is assumed that user traffic contains sufficient redundancy such that a stream cipher provides a basic level of data integrity protection on the radio interfaces and that, if that is not sufficient and additional measures are required, the application should be aware and measures should be implemented at the application layer.

R3b It shall be possible to protect against unauthorised modification of certain signalling data and control data, particularly on radio interfaces. (T2b, T3b,c, T6b,c, T7a,b,c)

R3c It shall be possible to protect against unauthorised modification of user-related data downloaded to or stored in the terminal or in the USIM. (T6d,e, T6c, T10f,i)

R3d It shall be possible to protect against unauthorised modification of user-related data which is stored or processed by a provider. (T6c,f)

R3e It shall be possible to ensure that the origin and integrity of applications and/or data downloaded to the terminal and/or the UICC can be checked. It may also be necessary to ensure the confidentiality of downloaded applications and/or data. (T6c,d,e,f, T10e,f,i)

R3f It shall be possible to ensure the origin, integrity and freshness of authentication data, particularly of the cipher key on the radio interface. (T1a,b, T2b, T5c, T6c)

R3g It shall be possible to secure infrastructure between operators. (T5a,b,c, T6a,b,c, T7a,b,c, T9b,c)

8.1.3 Requirements on protection of personal data

8.1.3.1 Security of user-related transmitted data

R4a It shall be possible to protect the confidentiality of certain signalling data and control data, particularly on radio interfaces. (T1b,d, T5b,c,d)

R4b It shall be possible to protect the confidentiality of user traffic, particularly on radio interfaces. (T1a, T5a)

R4c It shall be possible to protect the confidentiality of user identity data, particularly on radio interfaces. (T1b,d, T3b, T5b,c,d,e)

R4d It shall be possible to protect the confidentiality of location data about users, particularly on radio interfaces. (T1b, T3b, T5b,c,d,e)

R4e It shall be possible to protect against the unwanted disclosure of location data for a user participating in a particular 3G service to other parties participating in the same 3G service. (T5f)

R4f It shall be possible for the user to check whether or not his user traffic and his call related information is confidentiality protected. This should require minimal user activity. (T1a,b)

8.1.3.2 Security of user-related stored data

R5a It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider. (T5c,e)

R5b It shall be possible to protect the confidentiality of user-related data stored by the user in the terminal or in the USIM. (T10h,j)

8.1.4 Requirements on the terminal/USIM

8.1.4.1 USIM Security

R6a It shall be possible to control access to a USIM so that it can only be used to access 3G services by the subscriber to whom it was issued or by users explicitly authorised by that subscriber. (T10a, g)

R6b 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. (T10h,j, k)

R6c 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. (T10h,k)

8.1.4.2 Terminal Security

R7a It shall be possible to deter the theft of terminals. (T10a,c,d)

R7b It shall be possible to bar a particular terminal from accessing 3G services. (T10a,c,d)

R7c It shall be difficult to change the identity of a terminal to circumvent measures taken to bar a particular terminal from accessing 3G services. (T10a,c,d)

8.2 External requirements

8.2.1 Regulator requirements

8.2.1.1 Lawful interception

R8a It shall be possible for law enforcement agencies to monitor and intercept every call and call attempt, and other service or call related user actions, in accordance with national laws. 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. (Derived from Security Principles and Objectives [1]).

Annex A (Informative): Threats linked to active attacks on the radio access link

The success of digital mobile communication systems leads to a larger interest for fraudsters, especially as the opportunities for attacking other systems are dwindling. Thus, it can be expected that there will be more investment by the fraudster on more complex equipment which may lead to new active attacks becoming more of a concern. This annex focuses on active attacks in which an attacker manipulates signalling on the radio interface or masquerades as a network element in order to mount various forms of attack (so called "False Base Station" attacks).

This annex analyses a number of threats related to these types of attacks. Extensive analyses have been made of these and similar threats in the baseline document "Countermeasures to active attacks on the radio access link" (see references).

A.1 User identity catching

- **Active identity catching**

An intruder may spoof a serving network and send a request for the permanent user identity to a targeted user to capture his permanent identity in clear text.

A.2 Suppression of encryption between target and intruder

An intruder may succeed in disabling encryption on the radio interface by several means.

The intruder may masquerade completely as a serving network. The intruder can either use a man-in-the-middle attack by establishing two connections, one to the user and one to a valid serving network (relaying data with or without modifications between a user and a valid serving network) or just masquerade as a serving network without establishing a link to a real network. In any case, the intruder may be able to suppress encryption between the user and himself by sending the appropriate signalling messages.

Alternatively, the intruder may just manipulate the signalling messages by which the user and serving network agree on their ciphering capabilities to create an incompatibility that will prevent ciphering from being established.

The threats following these actions are described below:

- **Eavesdropping of a genuine call.**

Once encryption is disabled, the intruder can capture signalling and user traffic.

- **Answering a mobile originated call.**

When the target attempts to make a call, the intruder relays the messages between the target and the true network until after authentication is completed. The intruder cuts the connection with the true network suppresses encryption and proceeds to set up the call as a new call (to any suitable network) and under the intruder's own full control.

A.3 Compromise of authentication data

Authentication data can get compromised, either during its transport between the home environment and the serving network, or by unauthorised access to databases.

- **Forcing use of a compromised cipher key**

The intruder obtains a sample of authentication data and uses it to convince the user that he is connected to a proper serving network, and forces the use of a compromised cipher key. The intruder may force the repeated use of the same authentication data to ensure the same encryption key will be used for many calls. Leads to continuous eavesdropping.

- **Impersonating the user**

The intruder obtains a sample of authentication data and uses it to impersonate a user towards the serving network. Masquerading as a base station towards the serving network (or eavesdropping on such a connection) could be used to obtain valid authentication data for this attack.

- **Reusing authentication data**

The intruder forces the repeated use of the same authentication data. Weaknesses in the efficiency of the encryption protection may be exploited either for cipher cryptanalysis or protocol attacks.

A.4 Hijacking of services

The goal of these attacks is to access mobile communication services on the target's account.

- **Hijacking services for outgoing calls**

While the target camps on the false base station, the intruder pages the target for an incoming call. The user then initiates the call set-up procedure, which the intruder allows to occur between the serving network and the target, modifying the signalling elements such that to the serving network it appears as if the target wants to set-up a mobile originated call. After authentication the intruder releases the target, and subsequently uses the connection to make fraudulent calls on the target's subscription.

This could be possible if the network does not enable encryption, or if the intruder can disable encryption (as in A.2) or if the intruder has access to the cipher key (as in A.3).

- **Hijacking incoming calls**

While the target camps on the false base station, an associate of the intruder makes a call to the target's number. The intruder allows call set-up between target and serving network. After authentication the intruder releases the target, and subsequently uses the connection to answer the call made by his associate. The target will have to pay for the roaming leg.

This works either if the network does not enable encryption, or if the intruder can disable encryption (as in A.2) or if the intruder has access to the cipher key (as in A.3).

Annex B:
Change history

Change history						
TSG SA#	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
SP-03	21.133	2.0.0			3.0.0	Approved at SA#3
SP-06	21.133	3.0.0	001		3.1.0	Integrity of user data
SP-14	21.133	4.0.0	003	Rel-4	4.1.0	Definition of UICC (Also some minor editorial cleaning as per 3GPP editing decisions made since version 4.0.0)