LINK Personal Communications Programme

Third Generation Mobile Telecommunications Systems Security Studies

Technical Report 1:

Security Features for Third Generation Systems

Final Version

14 February 1996

Communications Security and Advanced Development Group,
Vodafone Ltd.

Telecommunications Systems Group,
GPT Ltd.

Information Security Group,
Royal Holloway, University of London.

Document Release

Document:

Technical Report 1:
Security Features for Third Generation Systems
(Final Version)

Responsible Partner:

Vodafone Ltd.

Contributors:

Ms. Marion Borman (GPT)
Dr. Jason Brown (Vodafone)
Dr. Liqun Chen (RHUL)
Mr. Peter Creteau (GPT)
Dr. Raymond Forbes (GPT)
Dr. Dieter Gollmann (RHUL)
Mr. Yong-Fei Han (RHUL)
Dr. Nigel Jefferies (Vodafone)
Prof. Christopher Mitchell (RHUL)
Prof. Michael Walker (Vodafone)
Dr. Dale Youngs (Vodafone)

Approved for Distribution:

.... Dr. Nigel Jefferies
(Responsible Partner Manager)

.... Prof. Michael Walker
(Project Liaison Officer)

Contents

Executive Summary

This report is the third and final published version of the first deliverable from the DTI/EPSRC LINK Personal Communications Programme project *`Security Studies for Third Generation Mobile Telecommunications Systems'*.

Since the start of the project in February 1993 there has been considerable activity in standardising third generation mobile systems, both within ETSI SMG5 (UMTS) and ITU Task Group 8/1 (FPLMTS). In that time we have seen the emergence from these bodies of draft recommendations for security features in both UMTS and FPLMTS. This activity within the standards bodies, to a large extent, shaped and dictated the direction of the project during its first year. Conversely, as this report shows, the results of the work undertaken by the project have had a significant effect on the standards work, in particular on the draft ETSI report on security features for UMTS [*Security principles for the UMTS*, ETSI DTR/SMG-50901], and particularly during the second year of the project.

The key objectives of the project may be summarised as follows:

- to identify the range and type of security features which third generation systems may be expected to support;
- to propose detailed guidelines on the classes of mechanisms that could be used to provide the identified security features;
- to define the infrastructure needed for the provision, operation and management of the security features:
- to assess the extent to which the security features, mechanisms and infrastructure elements need to be standardised.

This report is concerned with the first of these objectives. It is the third and final version of a report which will consider in detail the requirements for security features in the next generation of mobile telecommunications systems, and the extent to which these features should be the subject of standardisation.

This version of the report differs from its predecessor in the following ways. First, Section 5 on `Security Threats' has been updated in the following ways. A brief description of the new security threats posed by the evolution of second generation systems and in particular GSM has been added. More text on the topic of multiple user registration on a terminal and its relation to call forwarding appears, and the description of security threats specific to the satellite component of UMTS has been updated. In Section 7, a new section on standardization guidelines for security features has been created to reflect the importance of this topic. Section 9 from version 2 on `Future Directions' has been deleted as it is believed that the project has met all its goals. Appendix B from version 2 on `Operational Environments for UMTS' has been transferred to the final version of Technical report 3: Security Architecture for Third generation Systems [F2].

The report begins, in Section 2, with the objectives for security in third generation systems - what are the security features supposed to achieve? Although some very `high level' objectives are given, to really answer the question it is first necessary to understand the context in which it is being asked. This security context is the subject of Sections 3 and 4. It is considered in terms of role models and functional models - the players and what they do, the system and what it does. As well as clarifying the objectives for security, the security context also provides the basis for a threat analysis - the subject of Section 5. Security requirements to meet the security objectives and counter the security threats are examined in Section 6, and a set of security features to address these requirements is proposed in Section 7. Section 8 addresses the completeness of the threats, requirements and features identified in this report.

The report is a detailed description of the approach taken by the project, of the results obtained and the conclusions reached. Moreover, the results of the research reported here have had a significant impact on the standards bodies, in particular on the work of ETSI SMG5. The reader should regard this report as a `snapshot' of the current situation, a situation which reflects the changing standardisation picture.

Michael Walker

Vodafone Limited, 14th February 1996

1 Introduction

The aim of this report is to provide a complete description of the security features to be supported by third-generation mobile telecommunication systems (3GS). It will consider terminal features, air-interface features, supplementary features and network features, with the latter including the features necessary within a single network and those necessary for secure interoperation between different networks. It addresses the following:

1. The security context, including role models, functional models, and involved entities and interfaces.

2. An analysis of the potential threats to third-generation systems.

3. The identification of security requirements.

4. The specification and classification of security features.

One motivation for producing a report such as this is to provide a stable foundation for designing secure third-generation systems. A further objective is to identify those features which are either unsupported in current systems, or are supported using mechanisms inappropriate for use in future systems. Hence, the report motivates the study of security mechanisms for use in future systems.

We follow a systematic approach in defining security features. First we motivate our study by identifying some fundamental security objectives. Then, we establish the necessary context for the security features by establishing generic role and functional entities for third-generation systems. Following this, a threat analysis is carried out to establish where the system is open to abuse. From these threats, a set of security requirements is derived. Finally, a number of security features are conceived to satisfy these requirements.

We describe below the structure of this document in more detail, describing the contents of each section in turn.

First, in Section 2, to motivate our work, we identify a set of basic *security objectives* for third generation systems. This comprises a number of global security objectives, as well as requirements on the management of security.

Having set these objectives, we describe the setting for our investigation. In Section 3 we propose a *role model* enabling us to distinguish between the various logical entities involved, whilst in Section 4 we set out a corresponding *functional model* and identify various *operational environments* and *physical realisations* that may be expected for 3GS. This section has been updated continuously during the project to keep abreast of the developing role and functional models in standards bodies.

Having established the context for security, the next step is to evaluate the *security threats* to the system. This is given in Section 5, which begins with a discussion of threats to existing second generation systems, followed by a list of threats to third generation systems.

Having a list of threats, and bearing in mind the security objectives, we can produce a set of *security requirements* for 3GS. Such a set, which has been revised continuously during the project, is given in Section 6.

Section 7 includes a list of *security features* which. We have proposed a method for describing security features, and given example instances. Guidelines for the standardization of security features have also been given.

We have compared and contrasted our results with those appearing in standards documents throughout this report. In addition, in Section 8, we attempt to verify that the security features proposed meet all the established requirements and threats.

A comprehensive bibliography of the evolving standards for 3GS is given in Section 9, which includes all references made in this report, and Section 10 comprises an exhaustive list of abbreviations used.

Three appendices are attached. Two of these contain background information: Appendix A which describes the IN functional entities proposed for UMTS and Appendix B listing services proposed for UMTS. Appendix C contains the document history.

2 Security Objectives

2.1 Introduction

This section provides the motivation for our study of security for third generation systems. It comprises a number of fundamental security objectives upon which, along with the subsequent threat analysis of Section 5, the security requirements for third generation systems will be built.

Section 2.2 lists a number of security objectives that any well defined telecommunications system should be expected to attain. These are fairly general in nature and are intended to provide a global perspective on what we expect from a secure third generation telecommunications system.

In Section 2.3 we define a number of requirements for secure management. These are requirements on the secure management of the system, which are not specific to third-generation systems, but form a `baseline' for security management, without which more system-specific features are a waste of time. They should be provided, for instance, by a secure TMN.

2.2 Global Security Objectives

The principle objectives for security within third generation systems are:

1. To ensure that information generated by or relating to a user or subscriber is adequately protected against misuse or misappropriation.

2. To ensure that the resources and services provided by a service provider or network operator are adequately protected against misuse or misappropriation.

3. To ensure that the security features standardised are compatible with world-wide availability.

4. To ensure that the security features provided are adequately standardised to enable secure world-wide interoperability and roaming between different network operators.

As a measure of adequacy of the security features, the level of protection afforded to users and providers of services should be at least equal to that provided in contemporary fixed networks.

In [A19], two additional global security requirements are noted, to ensure that fraud management is possible, and to allow lawful interception. However, both these are particular instances of the more general requirements already given.

2.3 Requirements for Secure Management

The basic requirements for secure management are as follows:

1. Management of security keys within and between network operators/service providers should be secure and easy to handle.

2. Security keys and access devices distributed to users should be easily and securely managed and updated.

3. Service providers should be able to restore subscription data relating to users or subscribers upon failure.

4. The service provider should have secure mechanisms to record events associated with users or subscribers.

5. Mechanisms should be in place to enable the management of fraud.

3 Security Context: Role Model

3.1 Introduction

To describe a telecommunications system adequately, it is necessary to discriminate in some way between the various types of activity taking place. Such an approach leads to the creation of logical `entities' with distinct roles to play. These roles therefore represent a collection of related activities. They are not intended to distinguish functional entities. Indeed, it is quite likely that the activities of a role may be split between several functional entities or that one functional entity may take on activities belonging to more than one role.

What is important, especially from a security perspective, is that all responsibilities and benefits associated with activities within the system can be assigned to the various roles.

The object of Section 3.2 is to describe a generic role model suitable for third generation mobile telecommunication systems. We use a structured approach based on dividing the responsibility for various activities into specific areas, then dividing these areas further, eventually arriving at a number of specific entities each responsible for a single type of network activity.

We begin by considering a division into three general types of activity:

1. *Call time activity*. This covers all activity occurring when the system is utilised.

2. *Supporting activity*. This covers those activities relating to creation, upkeep and management of the system.

3. *Activity considered to be `external' to the system.* This covers a number of activities required for a complete description of the system, but which lie outside the scope of the preceding areas.

A subsection of Section 3.2 is devoted to each of the above areas. These subsections begin with a breakdown of the activity considered into more specific areas, and then a description of responsibilities in these areas, given in terms of the roles played by logical entities. It is important to note that the lists of activities and responsibilities are concerned only with security-related events; as such they are not necessarily exhaustive. We remark that the classification used in ETSI/SMG5 for UMTS is by division into customer and provider type roles.

Section 3.3 concludes the discussion of roles with a brief look at standardisation activities within UMTS and FPLMTS. We assess the impact of our work on the standardisation process, as well as noting the (current) distinctions between our views and those of the standards organisations.

3.2 Role Model

3.2.1 Call Time Activity

Whilst a network is in use, a number of key activities are performed. The responsibility for each of these can be assigned to one of four areas: Network Operation, Service Provision, Usage, and Management. The following subsections describe these in more detail, by identifying them with one or more logical entities.

Network Operation

Network Operator
An entity that:
1. provides the network capabilities to support particular services;
2. allows Users, using appropriate terminals, to gain access to the network in order to be able to use the services.

Note:

a. Network Operators can be further categorised into public or private.
b. The role of Network Operator can be separated into the component roles defined in 1) and 2) above. We refer to these as the *Network Provider* and *Access Provider* respectively.

Service Provision

Service Provider
An entity that is:
1. responsible for the provision of particular services, and the associated database management.

Note:
a. A Service Provider is also referred to as a Service Operator.
b. Service Providers can be subdivided into categories corresponding to the services provided, for instance, telecommunication services and value-added services.
c. Service Providers can be further categorised into public, private, or value added.

Usage

User
An entity that is:
1. authorised by a Subscriber to use particular services subscribed to by the Subscriber.

Note:
a. A User is also referred to as an End-User.
b. The user encompasses the physical entities/devices of *Access Device* and *Terminal*.

Other Party
An entity:
1. that is a user of services, but not necessarily of the system in question.

Note:
a. This could, for example, be the calling party in a call to a User, or the called party in a call from a User.

Management

Clearing House
An entity that:
1. is responsible for collecting and distributing data such as billing data, and (possibly) user authentication data, between Network Operators and Service Providers.

Terminal Manager
An entity that:
1. is responsible for collecting and distributing data such as equipment identity data, and (possibly) equipment authentication data, between Network Operators and Service Providers.

Note:
a. This role was introduced primarily to combat the use of stolen, cloned, and non-type approved terminals.

3.2.2 Supporting Activity

In addition to the primary activities involved in the utilisation of a network, as described in the previous subsection, there are also activities relating to the maintenance and management of all aspects of the system. These can be assigned to one of three areas: Service Creation and Implementation, Equipment Design and Manufacture, and Management. The following paragraphs describe in more detail the activities assigned to these areas by identifying them with one or more logical entities.

Service Creation and Implementation

Service Designer
An entity that is:
1. responsible for the design of network services.

Service Modifier
An entity that is:
1. responsible for the modification, customisation and upgrading of existing network services.

Note:
a. This entity could be acting, for example, on behalf of a service provider, subscriber, or user.

Building Block Creator
An entity that is:
1. responsible for the creation of high level reusable functions to be used by the Service Designer and Service Modifier to produce complete services.

Special Resource Provider
An entity that:
1. provides specialised resources to network operators, service providers, and users.

Note:
a. Resources might be databases or voice recognition hardware.

Equipment Design and Manufacture

Access device Manufacturer
An entity that is:
1. responsible for the design and manufacture of access devices.

Terminal Manufacturer
An entity that is:
1. responsible for the manufacture of terminal equipment.

User Interface Designer
An entity that is:
1. responsible for the design of user interfaces.

Management

Administrator
An entity that:
1. creates a framework to enable Service Providers and Network Operators to make roaming agreements with other Service Providers and Network Operators;
2. defines, monitors and enforces a policy for service provision (incorporating the role sometimes referred to as that of a Security Administrator).

Note:
a. An administrator may also be referred to as a Roaming Administrator.

Service Vendor
An entity that is:
1. responsible for negotiating with Service Providers for services on behalf of subscribers;
2. responsible for negotiating with Network Operators for the provision of network capabilities associated with services;

3. responsible for the provision and maintenance of subscriptions to Subscribers.

Subscriber
An entity that:
1. has a contractual relationship with a Service Vendor, on behalf of one or more Users;
2. is responsible for charges incurred to that Service Vendor;

3.2.3 External Activity

The previous two subsections were concerned with fairly concrete activities that are required for the upkeep and utilisation of a network. This subsection describes a number of areas where the activities are less well defined, and whose effect on the system is of a more peripheral nature. The areas we consider are: System Abuse, Regulation, and Other Indirect Activities.

System Abuse

Intruder
An entity:
1. that abuses the network infrastructure or services provided on the network.

Regulation

Regulator
An entity that is:
1. responsible for setting out laws and guidelines governing service provision and use;
2. responsible for ensuring that all entities comply with these requirements.

Type Approval Authority
An entity that:
1. tests and type-approves terminal equipment, subject to the rules laid down by the Regulator and possibly the Administrator.

Indirect

Third Party
An entity that is:
1. not directly involved with the provision and use of services, but may affect, or be affected by them.

Note:
a. There may be legal requirements on the protection of such parties.

3.3 Contributions to Standardisation

There is at present much activity directed towards the development of standards for the next generation of mobile telecommunications systems. As such, this subsection can provide no more than a snapshot of the current status of standardisation and the perceived impact of our work.

3.3.1 Roles Within UMTS

The ETSI group SMG5 has been assigned responsibility for defining the Universal Mobile Telecommunication System (UMTS). Contributions made to SMG5 have had a significant effect on the role model adopted for UMTS. Indeed, the first attempt to define a complete and formal role model for UMTS, carried out by the security working group within SMG5, was based on the role model developed within the 3GS3 project. Service creation and implementation, as well as equipment design and manufacture roles were deemed to be superfluous to SMG5 at the time and hence were omitted from the UMTS model. The current UMTS role model as defined in SMG 50901 (Version 2.2.0) still closely resembles the original. Moreover, it appears to be fairly stable, and may be adopted within UMTS by working groups other than the security group.

The UMTS role model provides a description of the various parties or organisations involved in the use, provision, regulation, etc, of UMTS services and the relationships between them. The descriptions, which are generally more detailed than those given in Subsection 3.2, are tailored to enable the security requirements for UMTS to be identified in a systematic manner. Unlike our classification, the UMTS roles are classified in the following manner:

Customers

Subscribers, Users, Other Party, Third Party, UPT User.

Providers

Service Providers, UMTS Network Operators, Access Providers, Other Network Operators, Terminal Managers, UPT Service Providers.

In addition to these primary roles there are secondary roles classified under the following headings: Regulators and Type Approval Agencies, Roaming Administrators, Miscellaneous Parties, Intruders, Owner.

The first point to note is that some changes in terminology have occurred (Network Operator becomes Network Provider), some roles have been combined (Regulator and type approval agency), and other roles have been separated (Network Provider and Access Provider).

Probably the most important difference between the UMTS role model and our role model lies in the degree of detail of the models. In addition to the fact mentioned above that UMTS roles are described in greater depth than our roles, UMTS also distinguishes specific varieties of certain roles. For example UPT has its own users and service providers. It also defines other network operators to be network operators outside UMTS.

3.3.2 Roles for FPLMTS

ITU-R TG8/1 is the task group of Study Group 8 that is currently responsible for defining the Future Public Land Mobile Telecommunications System (FPLMTS). It has (at present) made limited progress in developing a complete and coherent role model for FPLMTS. Nevertheless, definitions of various logical entities can be found scattered throughout the recommendations. Perhaps the most complete list of roles appears in the security principles document M.1078 [B13]. It comprises the following roles:

> user, mobile terminal, subscriber, home service provider, visited service provider, network operator, terminal manager, transit operator, access provider, other network operator, other user, intruder, UPT user, UPT subscriber, UPT service provider.

No attempt has as yet been made to classify these roles in any way, nor, it seems, has any attempt been made to check the consistency of the definitions. For example, the meaning of the terms `home' and `visited' when applied to service providers is unclear.

4 Security Context: Functional Model and Environments

4.1 Introduction

It is very likely that IN principles will be adopted for the modelling and implementation of third generation systems. Therefore work has been based on the IN functional model. At the time this work was undertaken, the IN functional model was the original ETSI model as proposed by SMG5/NA6. Since then, the model has progressed in ITU SG 11 although the general principles remain unchanged.

Section 4.2 reviews the currently agreed generic IN functional model, uses this to describe an access model for third generation systems, and finally shows how the generic functional model can be mapped to the role model described in the previous section.

Section 4.3 considers operational environments and physical realisations of third generation systems. A study of the various operational environments is necessary in view of the fact that these have a direct bearing on the requirements that must be addressed. Nevertheless, because this subject is itself of merely peripheral interest, a detailed discussion is not considered here. Instead UMTS is used as an example.

To get a realistic view of the operational requirements on the system, and in particular on security, the functional model must be mapped into the physical network architecture realisations. In Section 4.3 a typical realisation is described.

Section 4.4 briefly considers the services which third generation systems will be expected to support, and also defines a comprehensive set of information types necessary to describe the system operation fully.

There will be system requirements that have a significant impact on the architecture of the system, and hence indirectly on the security that is required. To conclude the setting of a context for our study then, in Section 4.5 a number of system requirements deemed to be relevant to security are listed.

4.2 Functional Model

The generic Intelligent Network (IN) functional model is shown in Figure 1. It depicts the types of functional entities required to provide services irrespective of environment (microcells, macrocells, satellite spots, etc.). The model also shows the relationship between these functional entities. Full descriptions of the functional entities may be found in Appendix A.

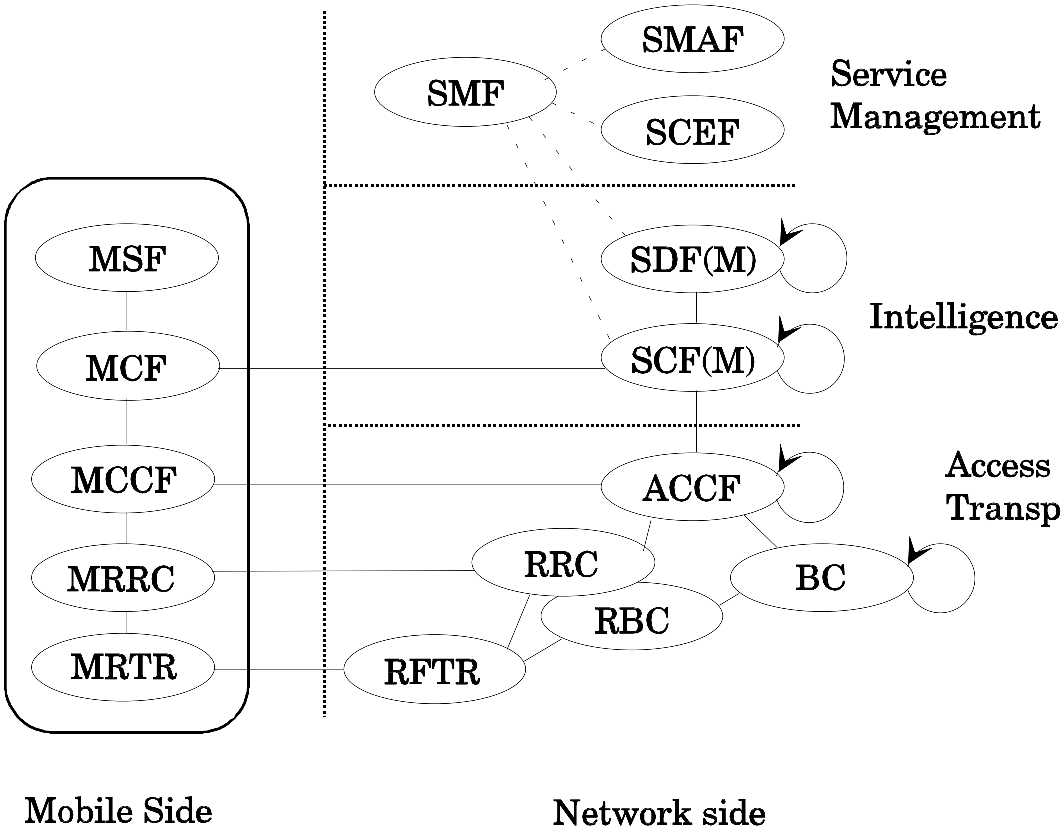

Figure 1: Generic Functional Model

In a specific network, several functional entities of the same type may exist. However, in the basic functional model, each functional entity type is shown only once. A relationship between two functional entities of the same type is shown as a "relation loop" starting and ending in the same functional entity. The peer to peer relationships between functional entities is fully elaborated in the general functional model, Figure 2.

The functional entities are grouped into three classes:

Service Management
Includes functions related to service creation, service provision, customer control capabilities, and support for the administration, coordination and control of a data base;

Intelligence
Includes functions related to service logic and service control (e.g. mobility management functions);

Access and Transport
Includes functions related to access, call and bearer control (e.g. radio resource management).

In the model, a distinction has also been made between functions residing at the mobile side of the radio interface and the functions residing at the network side of the radio interface. The functions at the mobile side together form the functionalities required at the access (mobile) side of the system (e.g. paging response, initial access, authentication, channel coding, ciphering, etc).

The purpose of the functional model, in relation to the security studies, is to understand the likely functional allocation to likely physical implementations. Thereby illustrating the potential risks, and possible sitings of security functions to circumvent the threats.

4.2.1 General functional model

In Figure 2 the general functional model is shown illustrating the interconnection of different logical network entities across different networks. These entities have different significance:

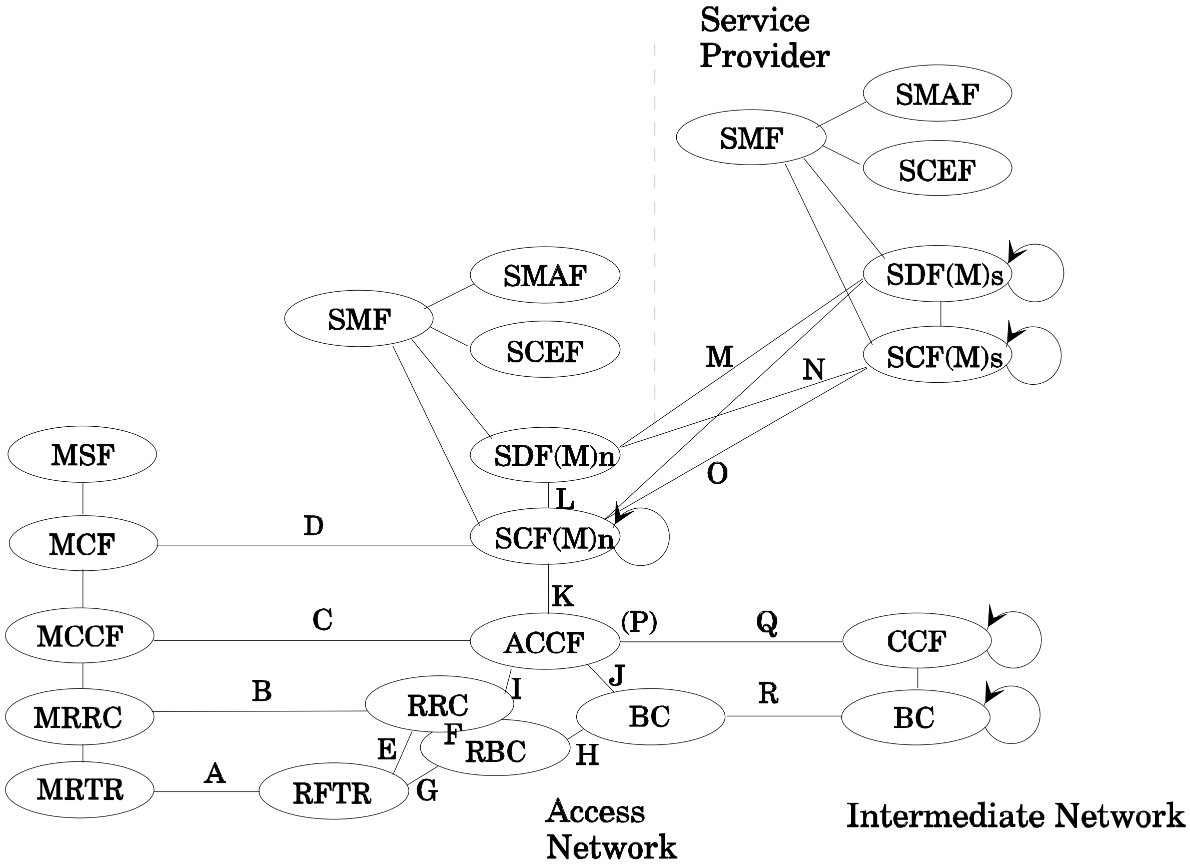

Figure 2: IN Access Model

Access Network
This is the serving network as seen for a mobile originated call. The service control parts of the network are shown with subscript "n", i.e. SDF(M)n and SCF(M)n.

Service provider
This is the service provider of the mobile subscriber. The service control parts of that service provider are shown with the subscript "s", i.e. SDF(M)s and SCF(M)s.

Intermediate network
The intermediate network is used only for routing and establishment of the bearer connection between the originating and the destination networks. In this network, the combination of CCF and BC merely indicate the capability of this network to route and switch a bearer connection and has no significance on the functional architecture of that network (PSTN, ISDN, etc.).

Note that although shown as belonging to different networks, the functional entities belonging to the access network, the service providers and the intermediate network could as well be seen as functional entities located in different parts of the same network.

The direct relationship and the interconnection of the sets of database functions (SDF(M)) and service control functions (SCF(M)) include a number of options resulting in different requirements for the split of functionality (and service logic) between networks and their respective databases (SDF(M)) and control functions (SCF(M)).

Figure 2 also identifies the functional relationships between the different functional entities. Each has a distinct label A - V, although this document is not directly concerned with these relationships.

The purpose of illustrating the different allocation of functionality across different interfaces in differing networks is to better understand the responsibilities and potential allocation of security functionality on network boundaries. This also results in understanding which interfaces may be securely opened between operators and which interfaces must be restricted for internal use by a single network operator.

4.2.2 Mapping of functional Entities

This section allocates the standard functional entities, described in Appendix A, into groups for allocation into the enterprise roles described in Section 3. To fully understand the use and meaning of the terms and abbreviations used here reference to Appendix A is essential.

Figure 3 shows how the functional entities can be logically grouped together to provide a mapping to the logical roles and their corresponding physical realisations defined in Section 3.2.

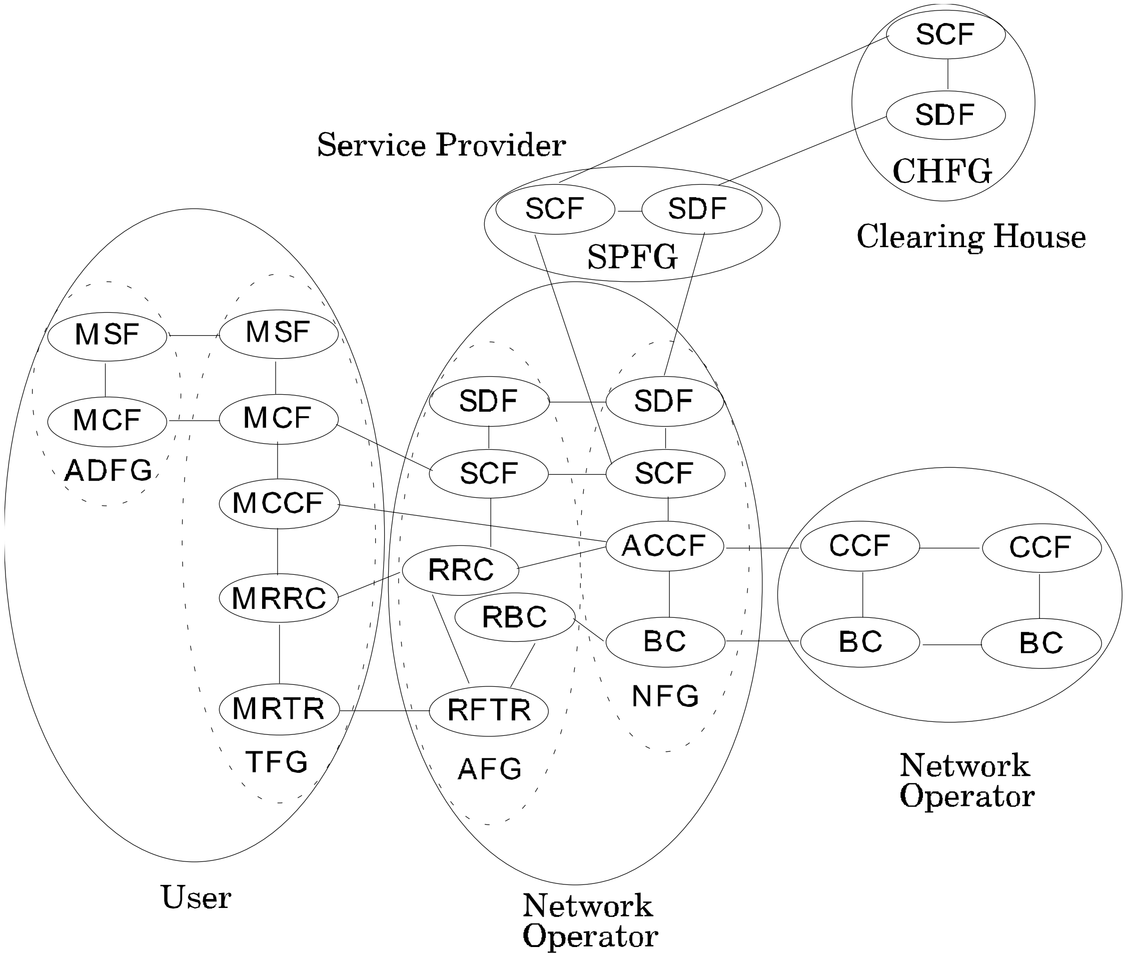

Figure 3: Logical Mapping of Functional Entities

These logical groupings are as follows:

ADFG - Access Device Function Group

The combined functionalities of the Access device MSF and MCF.

TFG - Terminal Function Group
The combined functionalities of the Mobile Terminal Equipment MSF, MCF, MCCF, MRRC and MRTR.

AFG - Access Function Group
The combined functionalities of the access provider including RFTR, RBC, RRC; and possible ACCF, SCF and SDF, for private systems offering public user access; in the network side.

NFG - Network Function Group
The combined functionalities of the public network including possible RFTR, RBC, RRC to support direct or indirect radio access; and ACCF, SCF, SDF and SMF in the network side.

SPFG - Service Provider Function Group
The combined functionalities of the SCF, SDF and SMF used for provision and management of the service, with special responsibility as a billing authority outside of the immediate network resources.

CHFG - Clearing House Function Group
The combined functionalities of the SCF, SDF and SMF used for arbitration of the service, with responsibility for accounting apportionment, and security management (algorithms, keys), approval, etc...

4.3 Operational Environments and Physical Realisations

4.3.1 Operational Environments

The operational environment has a direct bearing on the security requirements that must be addressed. UMTS has been used here as an example.

The support of the UMTS service environment results in a set of considerations and service features which can be found in Technical Report 3: Security Architecture for Third Generation Systems [F2]. This includes interworking with the services of existing networks and support of personal mobility. The UMTS operational environment is depicted in Figure 4, illustrating the likely physical realisations to support different access situations.

4.3.2 Physical Realisations

To get a realistic view of the operational requirements the functional model described in Section 4.2 must be mapped into the physical network architecture. Typically, one such realisation may be as shown in Figure 4.

In such a physical realisation the Service Control Point (SCP) and Service Data Point (SDP) are the physical realisations of the IN functions to support the mobility functions and mobile user data respectively. The local exchange must detect and provide trigger functions (the SSF functionality) in order to route the signalling to the SCP. In particular, the mobility functions which must be supported by the system may involve the following sets of functions or procedures:

(mobile) service/call set-up & release;
location updating;
handover;
registration/deregistration;
authentication;
paging.

The interaction between the mobility functions is represented through the design of information flow charts. Support for the above mentioned procedures across systems (e.g. between operators) can add further requirements for signalling between mobility functions (security services such as encoding and authentication being an example) which may be reflected in the information flows for each procedure. Hence, it is envisaged that consideration is given to physical architectures, functional allocation, and alternative information flows (functional interactions).

These comparisons should highlight some of the potential risk areas resulting from the realization of reference points by physical implementations.

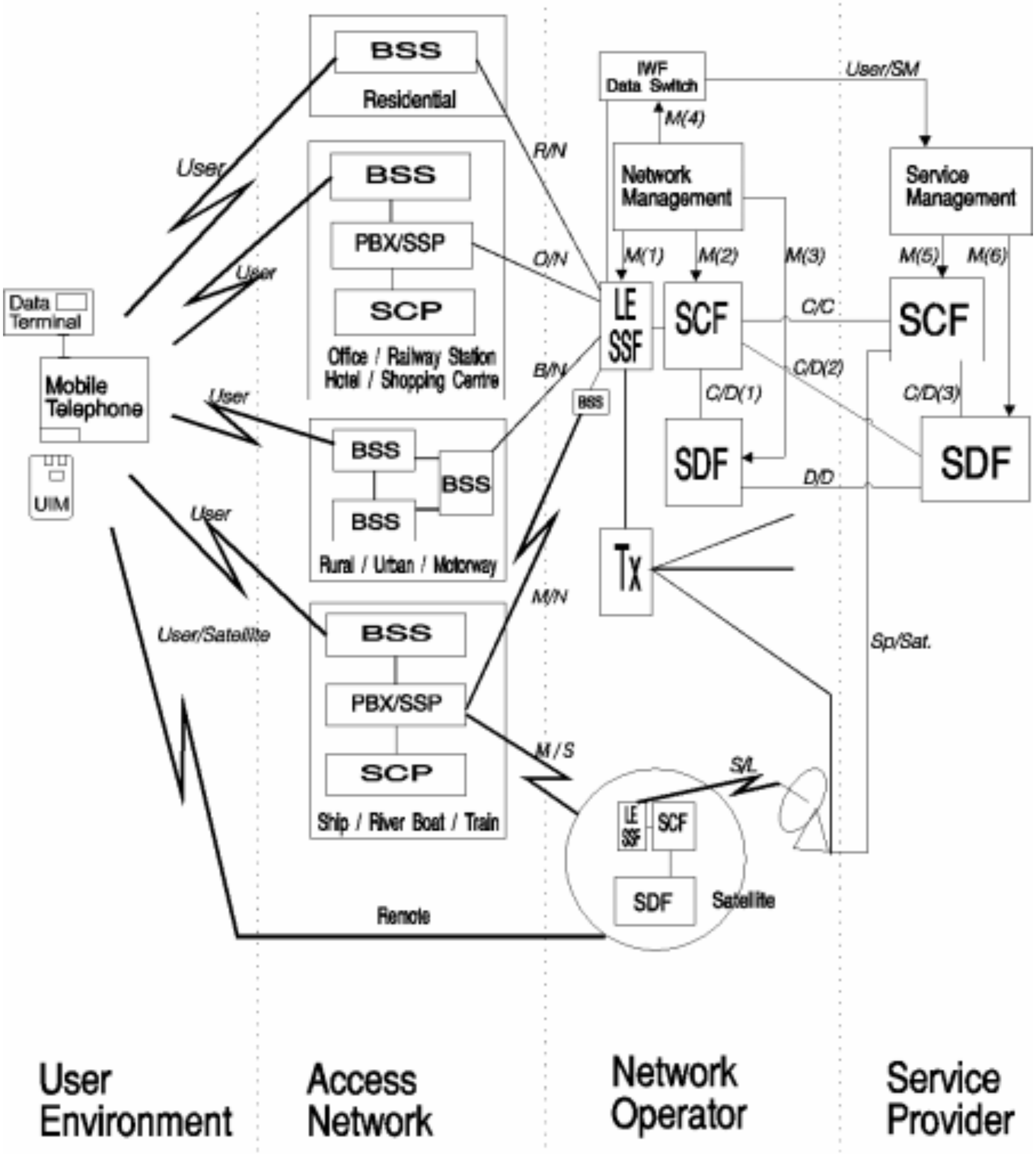

Figure 4: UMTS Operational Environment

4.4 Services and Information types

4.4.1 Services

Compiling a thorough list of services to be supported by third generation systems is outside the scope of this project. Nevertheless, consideration of the requirements imposed on security through the support of particular services is an important subject to study. Appendix B is a list of services considered to be supported by UMTS. This list is taken directly from [A11]. It is not claimed to be exhaustive.

4.4.2 Information Types and Groups

Different types of information will need differing amounts of protection, when stored or transmitted. To model these security requirements the information is allocated a type and grouped into categories dependent on its sensitivity. The following is a list of these types and categories.

Information types

User Traffic
This type comprises all information transmitted on the end-to-end traffic channel by Users to other Users. The information could be digital data, voice, or any other form of transmitted data.

Charging
This type comprises information relating to charges incurred by Users whilst using network resources and services. Such information would normally be generated by Network operators and passed to and amongst Service Providers.

Billing
This type comprises information relating to charges incurred by Subscribers for their subscriptions and Users charges. Such information is generated by a Service Provider (using charging information obtained from Network Operators and other Service Providers) and passed to Subscribers.

Location
This type comprises location information regarding a User (or Terminal). Such information is generated by a network operator and passed to the User's Service Provider (it may or may not be retained by the Network operator).

Dialling
This type comprises information relating to diallable numbers associated with Users (and possibly Terminals). Such data is generated by Service Providers 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 Service Provider.

Routing
This type comprises information passed through the network to enable correct routing of calls. Such information will be generated by Service Providers or Network Operators (using location and dialling information) and passed amongst Network Operators.

Network Resource Management
This type comprises information relating to the physical access of a Terminal to the Network Operator (or Access Provider), and physical interface between Network Operators. Such data is generated by Network Operators and passed amongst Network Operators and Terminals.

Identity
This type comprises information which determines the identity of an entity. The entities of interest are usually Users, Subscribers, or Terminals, but all entities have identities. User and Subscriber identities are generated by the appropriate Service Provider, and are held by both the Service Provider and the User or Subscriber respectively. In addition, a User's identity will be held by the appropriate Subscriber. Terminal identities are generated by the Terminal Manager (or Equipment Manufacturer), and are held by both the Terminal Manager and Terminal. Identities are transmitted from Users and Terminals to Network Operators whenever registration or access to services is attempted. User identities also

accompany User-related data such as charging, billing, and location when it is passed between entities. Similarly, Subscriber identities accompany billing data when it is passed between Service Provider and Subscriber.

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

Service Profile
This type comprises information regarding the service profiles of Users. Such data is generated and passed between Users, the User's Subscriber, and the Subscriber's Service Provider.

Access Control Management
This type comprises information relating to the access control of entities to Terminals, Network Resources, and Service Profiles. Such data includes PINs generated by users, and databases of identities generated by Service Providers, Network Operators, and Service Providers. It is generally stored by the generating entity.

Information Groups

In addition to the specific types of information described above, these types are further categorised into groups to simplify the threat analysis on the data's integrity and confidentiality. These groupings are as follows:

User Traffic
User Traffic.

Signalling Data
Charging, Billing, Location, Dialling, Identity, Security Management.

Control Data
Routing, Network Resource Management, Access Control Management, Service Profile.

Stored Data
Any information type whilst being stored in some manner.

Transmitted Data
Any information type whilst being transmitted in some manner.

4.5 System Requirements Relevant to Security

This section identifies a number of system requirements deemed to be relevant to security.

1. Third-generation systems will support the provision of services in an environment containing multiple network operators and service providers, both public and private, some of which are in direct competition.

2. Subscribers and users will expect to have direct access to their personal service profiles.

3. The necessary support will be provided for end-to-end security services between particular fixed or mobile users.

4. The system will be provided by an open system architecture based on IN and TMN principles.

5. The system will provide a variety of communications services using a range of bearer bit rates.

6. The system will accommodate a variety of mobile terminal types.

7. Users and terminal equipment will have unique identities.

8. The system will allow the connection of users to users of other systems.

9. The system will support handover within operators' networks and roaming between them.

10. The system must not conflict with the needs of national security and licence regulations.

5 Security Threats

5.1 Introduction

This section contains a list of possible threats to the security of third generation mobile telecommunications systems. There are two reasons for constructing such a list of threats:

- It provides a motivation for the security requirements and security features listed in Sections 6 and 7 respectively.

- It will assist in a thorough threat analysis of the UMTS and FPLMTS systems when they are better defined.

We start the discussion of threats in Section 5.2 by reviewing some areas where experience has shown that the security of current second-generation systems, such as GSM and DECT, could be enhanced. Some of these enhancements may be appropriate to third-generation systems.

Some security issues raised by proposed new functionality in third-generation systems are discussed in Section 5.3. For example, there are proposals for service features which do not require a user to be present at the terminal at which he registers (5.3.1). Also, third-generation systems will contain a satellite component (5.3.2).

Finally, the main list of security threats for general third-generation mobile systems is given in Section 5.4. No attempt has been made to evaluate the importance of each of these threats, since third-generation systems have yet to be defined in detail. In order to provide a classification of the threats, they are divided into the following six categories:

- Unauthorised access to services;
- Denial of services;
- Repudiation;
- Unauthorised access to data;
- Threats to integrity;
- Other threats.

Clearly, many other classifications are possible, such as by threatened party, by threatening party, affected network interface, and so on. The relative usefulness of these various classification schemes will become clearer when a threat analysis can be performed on a specific system architecture.

5.2 Threats to Second-Generation Systems

5.2.1 Network Operator Authentication

In some second-generation systems, such as GSM, network operators are not authenticated to subscribers. This means that it is theoretically possible to masquerade as an operator in these systems, by imitating a base station.

For instance, some GSM operators may not have the user data confidentiality feature active (through choice or unavailability). Then, if the imitation base station has attracted a legitimate subscriber's transmissions, the imitator can steal the subscriber's channel. He does this by first relaying the subscriber's registration and authentication information to a genuine network operator's base station, and then using the authenticated channel. Should the user data confidentiality feature be active, then the channel can still be stolen. However it is not clear how this channel could be utilised (except perhaps to accumulate an enormous bill for the subscriber by keeping the channel open).

Operators may be able to switch off the user data confidentiality feature on a subscriber's call. Then an imitator might be able to eavesdrop on a legitimate subscriber's call by switching off the encryption on the link between itself and the subscriber. He could then relay the call to a genuine operator's base station using a personal (legitimate) subscriber identity.

Network operator authentication is a critical issue in systems such as DECT that incorporate `over the air' subscriber control. Here, the omission of network operator authentication may allow an imitator to disable users directly or to alter their billing data. One argument for GSM not supporting network operator authentication is that it does not incorporate any such over the air control. However unforeseen service enhancements may lead to problems in future, so it may be wise to include features such as network operator authentication, although they serve no immediate purpose.

5.2.2 Subscriber Identity Confidentiality

In GSM systems, transmission of the subscriber identity (IMSI) over the air interface is not always carried out confidentially. For example, on initial registration or when the VLR changes, the unprotected IMSI must be transmitted to enable registration. Nevertheless, the limited form of subscriber identity confidentiality provided by GSM is usually enough to prevent tracking of the subscriber's location. However, anyone masquerading as a network operator (by imitating a base station) may request a subscriber to transmit his clear IMSI at any time.

5.2.3 Equipment Checking

If there is no provision for equipment identities (such as GSM IMEIs) to be stored securely in the mobile equipment, then cloning of mobile equipment is possible. This would allow the use of non-type approved equipment and the reuse of stolen equipment by assigning a new terminal identity to it.

5.2.4 The Scope of Standardisation

The scope of standardization for second-generation systems was largely limited to the air interfaces and those functions necessary for internetwork roaming. In particular, many security-related functions are not well defined in the standards, as noted below.

Key Management
In general, recommendations for second-generation systems do not tackle the subjects of subscriber-key generation and distribution.

Specification of Entities
Several entities are defined in GSM whose functions are security related (for example the Authentication Centre (AuC), Administration Centre (AdC), Equipment Identity Register (EIR), and Pre-Personalization Centre (PPC)). The interfaces of these entities with other entities are not specified in adequate detail (or at all) in the GSM recommendations.

Inter-Network Links
The GSM recommendations do not consider the interfaces between different networks.

Data Transmission
Although confidentiality of data sent over the air interface is often specified in second-generation system recommendations, the transmission of data over other links is not usually considered. For example, in the GSM recommendations the confidentiality of speech data sent between the BSS (base-station subsystem) and MSC (mobile switching centre) is not discussed.

5.2.5 Protocol Abuse

It is possible that protocol abuse can lead to security breaches in a system. For example, without network operator authentication, the location updating procedure might be abused in the following manner. We first point out that, although GSM terminology is used, this abuse is not viable in GSM because of the nature of the encryption and data formatting procedures involved.

Suppose an eavesdropper obtains the RAND value used to generate an encryption key, and some data encrypted using this key, transmitted by a subscriber. Then (at any time), by imitating a base station, the eavesdropper can request a location update, and supply the subscriber with the RAND value to reproduce the original encryption key. The imitator feeds the encrypted data to the subscriber under the guise of an encrypted TMSI, and then requests the (unencrypted) TMSI value to be transmitted for a location update.

5.2.6 Evolution of Second-Generation Systems

Second generation mobile standards have continued to evolve after their commercial introduction. For example, the evolution of GSM has involved Phase 2 and Phase 2+ developments to complement the core Phase 1 standards. The work items associated with these evolutionary developments may bring their own security threats. In the case of GSM Phase 2 and Phase 2+, the number of work items is too large to justify a comprehensive security analysis here. Instead, we list and briefly examine *some* of the security threats of two Phase 2+ work items which are currently in the process of being standardized: the General Packet Radio Service (GPRS) and High Speed Circuit Switched Data (HSCSD).

GPRS

GPRS will allow the resources of the GSM Phase 2+ air interface to be packet switched rather than circuit switched [A29, A30, A31, A32]. For certain types of data, this represents a more efficient use of radio resources promoting greater capacity and/or higher quality-of-service.

GPRS facilitates point to multipoint (PTM) in addition to point to point (PTP) services. Obviously, for a given message, the former consume more resources. Great effort must therefore be devoted to ensure that PTM services cannot be invoked fraudulently and it may be necessary to limit the number of recipients of a PTM message as a preventative measure.

For GPRS PTM services, it is possible not only to transfer data packets, but also schedule them to be delivered at a certain time, kill data transfer operations if they have not already taken place and obtain the status of the data transfer operation from the network. Appropriate authentication and integrity measures must be devised to prevent fraudulent activity taking place in connection with these operations.

HSCSD

HSCSD will facilitate higher circuit switched data rates across the GSM Phase 2+ air interface by allocating multiple time slots (rather than just one as at present) on the radio bearers to individual users [A33, A34]. Clearly, this results in individual users being allocated a greater share of the total resources available in a cell. This is very dangerous because not only are HSCSD services likely to be more lucrative and therefore more desirable to fraudsters operating call selling scams (the more resources being used by a user, the more can be charged), but also they are more likely to prevent legitimate subscribers gaining access to the network due to lack of radio resources in a cell. Great effort must therefore be devoted to ensure that HSCSD services cannot be invoked fraudulently and it may be necessary to limit the number of time slots that can be instantaneously allocated to a HSCSD user as a preventative measure.

5.2.7 Lessons to be Learnt

Security features often depend on other security features or functions for their operation (for example user confidentiality requires encryption). This could lead to a compromise in security when a particular feature is disabled. Consideration should be given to separating security functions and reducing interdependencies of security feature provision, especially when the system is liable to have some of its security features suppressed.

Improvements and upgrades usually occur throughout the lifetime of a system. These may require that additional security features be added to maintain the overall integrity of the system. The inclusion of redundant features at the initial stage may therefore be wise.

The restricted scope of recommendations for second-generation systems leaves many aspects of these systems open to abuse. Before developing recommendations, it is important that their scope is made suitably wide.

A common way to compromise the security of a system is through misuse of its security protocols. System designers should be aware of this, and give special regard to protocols involving features that can be disabled.

5.3 Security Issues for Third Generation Systems

5.3.1 Absence of Identity Module

One of the fundamental assumptions for third generation mobile systems is that the user and terminal are logically separate. Furthermore, through their realisation as the user's access device and mobile terminal equipment, the user and terminal may also be physically separable. This separation has given rise to a number of service features andrequirements regarding the presence of the access device in the mobile terminal equipment.

Normally, when a user wishes to utilise the system he must insert his access device into the mobile terminal equipment he intends to use. However, this will not always be the case, and there are potentially three distinct states that may arise in practice:

- the access device is not present (either remotely or locally);
- the access device is not at the registration location, but is present within network (remote);
- the access device is at the registration location (local).

The goal of this subsection is to highlight security issues arising through the first two states, and to encourage further discussion on the subject.

The standardisation of UMTS currently being attempted by ETSI STC SMG5 has led to a number of interesting proposals for features that either do not require, or even preclude, having the user's access device present within the mobile terminal equipment or even the network. We first review these proposals, and summarize the limitations they place upon the system. Following this we attempt to identify areas where security may be compromised. A related problem concerns the verification of the access device's presence, and after a brief discussion on this matter we draw some conclusions and outline a number of areas requiring further investigation.

Proposed UMTS Features

The following paragraphs outline a number of proposals that are currently being discussed by SMG5, and which may have an impact (albeit indirectly) on whether the access device can be present. It must be noted that these proposals are for further study within SMG5. Similar features are also being recommended for FPLMTS.

Support of UPT: It is anticipated that UMTS will support the UPT concept. Whilst this may not impact directly upon whether access devices are present, the additional service features offered by UPT will (see for example remote registration).

Call forwarding: Call forwarding, in its various forms, is likely to be one of the key supplementary services provided in UMTS. It is probable that the party invoking the forwarding will be responsible for charges incurred on the forward leg. Calls are forwarded to a user (more specifically to a user's number) not to a terminal.

Multiple Registration on Terminal: It should be possible for more than one user to be registered on a given terminal at any one time. There are a number of options as to how multiple registration (and subsequent deregistration) could be performed. Perhaps the user inserts his access device, registers, and then removes his access device. The last user to register leaves his access device inserted. To deregister a user may be required to re-insert his access device. When a call arrives, either anyone could take the call, or some form of identifier for the called party is displayed and that user must insert their access device. There could in principle be times when users are registered but no access device is present in the mobile terminal equipment, for example when someone else is required to insert their access device.

If terminal identities cannot be authenticated, they cannot be used as network addresses for the delivery of calls. Hence, the best solution is to insist, as has been argued elsewhere, that at least one UIM (the `representative  UIM) remains permanently in the terminal during the registration.  Other UIMs (`absent UIMs) are registered on the terminal by introducing them temporarily into a second slot on the terminal. Remote registration (see the following item) on the terminal containing the representative UIM may also be possible.

This latter situation described above is identical to call forwarding from the absent UIMs to the representative UIM. The absent UIM can only be absent for incoming calls, and incoming calls are delivered to the representative UIM s location. Outgoing calls will still require the original UIM to be present for authentication purposes.

Once this is accepted, then it becomes clear that, like call forwarding, multiple user registration is a supplementary service. It has all the same security problems as call forwarding (need to authenticate the setup, UIM not directly involved in incoming call, need to restrict use, etc.).

Multiple user registration should not be considered as part of the basic UMTS service. It should be defined as a UMTS supplementary service, and methods of preventing its abuse should be developed along with other similar services.

Remote registration: This will allow users to register on a terminal situated in a different location to themselves. Remote registration to a terminal upon which no user is registered does not seem possible because the terminal cannot be located. This means that it would be necessary for another user to be already registered on the target terminal (which implies that multiple registration on the terminal will take place). If remote registration is limited to incoming calls, then it seems to be merely an instance of call forwarding.

Multiple Registration by a User: It should be possible for a user to be registered on more than one terminal at any given time. The idea behind this is that a user may, for example, wish to be registered in one location for telephony, and somewhere else for fax at the same time.

Inferences

The above proposals show that situations may arise where either the user's access device is not present or where the user's access device is remote. For example:

Access device not present:
- call forwarding on not reachable;
- multiple registration on terminal.

Access device present at remote location:
- call forwarding on busy;
- remote registration;
- multiple registration by user.

Impact on Security

The previous paragraph indicates that the absence or remoteness of a user's access device may be necessary to facilitate certain services. This may lead to abuse of the system. The following paragraphs describe some potential problems.

Other party protection: Users should be located, not terminal equipment. That is to say, all location management activities utilise user identities, not mobile terminal equipment identities. This seems to imply that terminal equipment having no user registered, and therefore no access device inserted, cannot be located. This view is supported by the fact that mobile terminal equipment identities will not be held anywhere in the network. In addition, terminal equipment should not have associated diallable numbers. This is distinct from the case where terminal equipment (such as a company's fax machine) has a permanently registered user associated with it. One reason for not wanting terminal numbering is that it is unclear who would be responsible for paying bills associated with terminals (although perhaps this would not matter if terminals were denied any chargeable activity).

Thus, whether there is no access device present, or it is present at a remote location, there must still be a access device present at the mobile terminal equipment where services are being utilised (for location, routing, and so on). This access device will belong to another user to whom we refer as the representative user.

The representative user is being utilised by other users to provide their location management.

Protection against being utilised as a representative user must be considered.

Incontestable Charging: Incontestable charging is a requirement whereby subscribers, network operators and service providers are correctly charged according to the resources they or their users have used. This means that they cannot deny the use of resources, nor can they be charged for resources they have not used.

Incontestable charging is impossible if no access device is present. The user would have to trust the network operator as to when calls begin and terminate. Alternatively the representative user could sign toll tickets on behalf of the user, in which case the user must trust the representative user. If the access device is present but at a remote location then it may be possible for the user to sign toll tickets, but he must again trust the representative user or network operator as to when calls begin and terminate.

Confidentiality of transmitted data: Confidentiality of sensitive data sent over the air interface, between the user and network, will be provided through encryption based on user's secret keys, and not on terminal-specific keys.

This is impossible if the access device is not present, and would lead to difficulties with key distribution even if the access device was present at a remote location.

Deregistration: A user could easily forget to deregister if his access device is not present at the terminal.

Authentication: Authentication is impossible if the user's access device is not present. For example suppose an incoming call arrives for a user at a terminal that does not have the user's access device inserted, then the call must be accepted without authenticating the receiver. For example, an intruder (who is perhaps a user registered on the same terminal) could arrange for a call to the user (so that the user pays for the roamed leg) which the intruder takes himself.

Verification of access device presence

Given that a access device is required to be present, then its presence must be verifiable in some way. This may be carried out either physically or logically.

Physical presence could, for example, be provided by having a sensor imbedded in the mobile terminal equipment (though this probably won't give any assurance as to the identity of the access device). Logical verification could be through authentication, for instance by a continuous authenticated (signed) data flow between the access device and terminal.

The need for logical verification of a user's SIM to the terminal upon which he is registered, has recently been identified for GSM. This is in addition to the existing requirement for the corresponding physical verification. The proposed logical verification for GSM does not involve a full authentication of the SIM; it merely ensures that a GSM SIM is present, and does not differentiate between SIMs.

Conclusions

We conclude that for any service to be utilised, an access device (not necessarily belonging to the user of the service) must be present (although this assumption may be false under certain unusual circumstances, e.g. emergency calls). Therefore if the user's access device is not locally present, then a representative user must exist, and a trust relationship must exist between him and the user. If the user's access device is remote, then it is possible that a formal trust relationship could be realised through authentication procedures. If the user's access device is not present at all, then this trust must be purely informal. There is scope for either the user or the representative user to be abused. this matter requires further investigation.

Suppose that a feature does not require (or precludes) the user's access device to be locally present. Then limitations should be set, wherever possible, to allow only non-chargeable (to that user) services to be utilised. Where it is not possible or desirable to impose such a limitation, then further specific protective measures should be developed. For example, call forwarding will probably be a core supplementary service offered in UMTS, and one for which the user will be responsible for some of the charges incurred. Therefore, a means of protecting call forwarding features against abuse should be developed.

Remote registration requires further study. If it is limited to enable the user to receive incoming calls (or other services) only, then it appears to be merely call forwarding. If, on the other hand, it allows outgoing services to be utilised, then the user is at the mercy of the representative user. Similarly, procedures for multiple registration by a user and multiple registration on single piece of mobile terminal equipment require further investigation. For instance, do they allow non-chargeable services only? If not, then is the access device required to be inserted at the registration location when attempting to utilise a chargeable service? A fundamental question concerning all of these features is: what is the motivation behind them - who wants them and why?

5.3.2 Satellite component

This subsection examines security issues which are specific to communications involving satellite as opposed to terrestrial access.

Reference Configurations

The UMTS satellite architecture(s) will have an impact on both the UMTS security requirements, and the UMTS security mechanisms. The potential reference configurations identified for UMTS are discussed in Technical Report 3: Security Architecture for Third Generation Systems [F2].

Access Control

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

Denial of service

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

Key Distribution

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

Legal Interception

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

Limitation of Service Domain

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

Impersonation

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

Location Privacy

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

Handover

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

Operation of Mechanisms

All security mechanisms employed in UMTS must operate effectively within the satellite component. Factors that may influence the effectiveness of security mechanisms include:

1. satellite architecture;
2. transmission quality;
3. transmission speed;
4. position location capability.

Other Issues

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

5.4 Threats to Third-Generation Systems

In this section we list a number of possible threats to third-generation mobile telecommunications systems. These threats are classified under the following headings:

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

5.4.1 Unauthorised Access to Services

Unauthorized access to services can take place with or without the assistance of an authorized party. This should be borne in mind when considering each service. Unauthorised access to services can occur in the following ways:

T1 *Masquerading as a user*
An entity impersonating a user might utilise services authorised for that user. The entity may have received assistance from other entities such as a service provider or network operator, or even the user himself.

T2 *Masquerading as a subscriber*
An entity could impersonate a subscriber, either to set up a new subscription, or to modify a subscription belonging to an existing subscriber. A modified subscription could allow a user to access services not authorised by his subscriber.

T3 *Masquerading as a network operator*
An entity could impersonate a network operator (by cloning base stations, satellite receivers, or other network equipment), perhaps with the intention of using a legitimate user's access attempts to gain access to services himself.

T4 *Masquerading as a service provider*
An entity might impersonate a service provider, perhaps with the intention of obtaining a user's identity or authentication data, which could, for example, be used to produce cloned access devices.

T5 *Misuse of privileges*
Entities may abuse their privileges to gain unauthorised access to services. This threat includes misuse of both user and network operator privileges. The subscriber may have to pay the charges incurred by a user who makes unauthorised access to services. An example of this could be when a network operator offers the user services for which the user is not authorised by his subscriber.

T6 *Theft of terminal equipment and access device*
Stolen terminal equipment and access devices could be used to gain unauthorised access to services.

T7 *Cloning of terminal equipment and access device*
Should an entity obtain appropriate user identity and authentication data, this could be loaded into fraudulent terminal equipment and access devices resulting in cloning of the originals. These may subsequently be used to gain unauthorised access to services.

T8 *Non-type-approved equipment*
An entity could use a low-cost terminal or other equipment in place of type-approved terminal equipment to utilise services. The threat here is that type approval is circumvented, with possible consequences including adverse effects on the services available to other users.

5.4.2 Denial of Service

Denial of service occurs when a user is prevented from making use of services to which he is entitled. This can occur in the following ways:

T9 *Denial of access*
Access to a service could be denied due to inadequate access control. This usually involves intervention by another entity. One example would be a user being locked out of his account because of repeated intentional failed authentication attempts by another entity. Denial of access also could be accidental (a user forgetting his PIN), or a side effect of another entity's activities (such as trying to find out the user's PIN).

T10 *Physical intervention*
The transfer of messages could be prevented due to inadequate data transfer mechanisms. This usually involves intervention by another entity. One example would be the jamming of signals sent over a radio interface.

T11 *Protocol intervention*
A protocol failure could be made to occur, through intervention by an entity, causing a service to be terminated. Examples of where problems might occur are handover failure and data origin/delivery authentication failure.

5.4.3 Repudiation

Repudiation occurs when an entity falsely denies participation in some action such as sending or receiving a message. This can occur in the following ways:

T12 *Repudiation of service*
A user could deny having attempted to access a service, or deny that the service was actually provided.

T13 *Repudiation of access to data*
A user could deny the action of accessing data, such as his service profile or billing data.

T14 *Repudiation of charge*
The repudiation of incurred charges could occur, perhaps because of the above threats.

5.4.4 Unauthorised Access to Data

This includes the unauthorised disclosure, interception, eavesdropping, and cryptanalysis of data. This can occur in the following ways:

T15 *Eavesdropping during subscription setup*
There may be eavesdropping on, or interception of, user/subscriber-associated secret information passing between the subscriber and service provider when the subscription is set up.

T16 *Eavesdropping during transmission*
Information could be eavesdropped when transferred between entities over the various interfaces. Examples include an entity using a fake terminal or a terminal with memory, electromagnetic radiation information, tapping the line, or misusing a satellite repeater.

T17 *Disclosure of information whilst accessing terminal equipment with an access device*
User or terminal information could be exposed when the user accesses his terminal equipment with his access device.

T18 *Disclosure of information by a service provider*
User or subscriber information could be exposed by a service provider during auditing, maintenance and backup, as well as during the provision of services.

T19 *Disclosure of information via accounting and billing*
Insecure accounting and billing practices could result in disclosure of information. For example, if an access provider receives an itemized bill based on calls initiated from his network access, then he may also receive the numbers called by registered users. The confidentiality of this data could then be lost.

T20 *Cryptanalysis of data*
User traffic and other encrypted information transmitted over the various interfaces could be intercepted and cryptanalysed.

T21 *Traffic Analysis*
Intruders may observe control data or the lengths, frequencies, sources and destinations of transmitted messages. This may result in the disclosure of confidential information.

5.4.5 Threats to Integrity

This includes unauthorised modification, deletion, reordering or replay (playback) of a valid sequence of communicated messages, as well as the modification or deletion of stored information. The threat may occur in the following ways:

T22 *Manipulation of subscription information*
Subscription data could be modified or deleted by an entity. This includes the possibility that the entity might modify or delete data by mistake. The result could be that a user is denied access to services, the entity can gain unauthorised access to services, or the entity can repudiate access and use of services.

T23 *Manipulation of user information*
User identity, authentication and location information could be modified or replayed on the radio path by an

entity, possibly with the help of another entity such as a service provider, network operator, or even the user himself. The consequence could be that either the service is denied to the user, or the service is taken over.

T24 *Manipulation of user traffic*
User traffic could be modified or replayed by an entity.

T25 *Manipulation of signalling and control information*
Signalling and control information could be modified or replayed by an entity.

5.4.6 Other Threats

T26 *Unwanted incoming calls to the user*
A user may receive unwanted calls. If split charging is used, the subscriber has to pay for these calls.

6 Security Requirements

6.1 Introduction

Security requirements form a natural link between threats to a system and the corresponding features supported by the system to counteract these threats. More precisely, requirements can be derived from threats, and then features may be introduced to address these requirements.

This section provides a set of security requirements on third generation systems. These requirements are engendered by the roles played by the various parties involved in third-generation systems and the relationships between them as described in Sections 2 and 3.

The organization of requirements is with a customer perspective in Section 6.2, and a provider perspective in Section 6.3. This is the same as given for UMTS in [A19].

Section 6.4 reviews the security requirements so far defined for UMTS and FPLMTS respectively.

6.2 Customer Security Requirements

This section identifies security requirements for the benefit of users, subscribers and third parties. We divide the requirements into the following types, and assign a subsection to each:

User Access Device;
Mobile Terminal Equipment;
Access to Telecommunications Services;
Provision of Telecommunications Services;
Access to Service Profiles;
Charging and Billing;
Data Protection;
Third Party Requirements.

6.2.1 User Access Device

The following requirements relate to the user's access device.

R1a The access device should be protected so that it can only be used by the user/subscriber to whom it was issued, or to a party explicitly authorised to use the access device by that user/subscriber.

R1b The privacy and integrity of data stored in the access device should be ensured, in particular user identity and authentication information.

A working assumption is that the access device is used to access telecommunications services. The user is identified with the access device and user identification/authentication is identification/authentication of this device by the service provider/network provider.

6.2.2 Mobile Terminal Equipment

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

R2a The owner of a mobile terminal should be able to secure access to it.

R2b The privacy of any user-related data stored in the mobile terminal should be protected.

6.2.3 Access to Telecommunications Services

The following requirements relate to access to telecommunications services.

R3a Protection should be provided against an intruder impersonating a user and accessing telecommunications services.

R3b A user/subscriber should be able to identify and authenticate the service provider/network provider when he accesses a telecommunications service.

The second requirement is for further study. It may depend upon what data the service provider/network provider can read from or write to the access device or terminal, or whether using telecommunications services supplied by different providers could affect the charges to the subscriber. Consideration needs to be given about whom the user needs to authenticate and under what circumstances.

6.2.4 Provision of Telecommunications Services

The following requirements relate to the provision of telecommunications services.

R4a Unauthorised passive listening/monitoring of user traffic for eavesdropping, in particular on radio paths, should be prevented.

R4b Location privacy for users of telecommunications services should be provided.

R4c An intruder should not be able to identify the user(s) associated with a particular communication.

R4d Intruders should not be able to intercept user traffic, or user-related signalling data, on the radio path for manipulation and retransmission.

R4e An intruder should not be able to take over a telecommunications service already provided to a user.

R4f An intruder should not be able to conduct traffic analysis on the radio path.

Requirement 4f has been put forward by SMG5, but is very unclear. Is the intention to protect against intruders being able to detect whether a particular terminal is being used? If so, this seems to go beyond any commercial requirements for security.

6.2.5 Access to Service Profiles

The following security requirements relate to user, subscriber, and service provider access to service profiles.

R5a Service profile data that may be modified by users, subscribers or service providers should be protected against unauthorised modification.

R5b Privacy and integrity of service profile data should be ensured.

These requirements need to be made more explicit, and the full range of security requirements relating to user, subscriber and service provider access to service profiles needs to be studied. To do this, the content, structure and means of access to these profiles need to be defined. This subject is for further study within the project.

6.2.6 Charging and Billing

The following security requirements relate to charging and billing.

R6a Users and subscribers should be able to limit charges.

R6b Users and subscribers should have the capability to be informed of accumulated charges.

R6c The privacy of billing and charging information should be protected.

R6d Subscribers should have confidence in the integrity of the charging and billing systems.

The topic of charging and billing is for further study. Aspects to be considered include incontestable charging, user/subscriber access to accumulated charges, charges per call, itemised billing, and so on. Consideration will be given to the extent to which this topic is the subject of standardisation.

6.2.7 Data Protection

The following security requirements relate to the rights of customers to expect that data provided by them, or relating to them, that is stored or processed by service providers, network operators or other parties involved in third-generation systems is protected against misuse or misappropriation.

This topic is for further study. It is not clear to what extent this topic needs to be addressed within this report and by standards bodies. Possible requirements are:

R7a The results of user activity monitoring should not be disclosed to unauthorized parties.

R7b Signalling data and management data relating to users that is stored or processed by a service provider or network provider, or sent between service providers or network providers, should be protected with respect to authentication of origin, integrity and confidentiality.

R7c Every attempted interception by means of devices or interfaces which are placed by network operators at the disposal of national law enforcement agencies, according to national law, should be monitored and registered in accordance with national law.

6.2.8 Third Party Requirements

This subsection identifies security requirements related to the need to protect users of other systems and other third parties who may be adversely affected by the use of services. It is motivated by the requirements that arise in UPT such as the need to protect third parties from remote registration. Further study is required of the threats to third parties.

R8a The privacy of third parties should not be affected by the use of equipment or services.

6.3 Provider Security Requirements

This section identifies security requirements for the benefit of service providers and network operators. The requirements are divided into the following types, and a subsection assigned to each:

User Access Device;
Mobile Terminal Equipment;
Access to Telecommunication Services;
Provision of Telecommunications Services;
Service Profiles;
Charging and Accounting;
Protection of Provider Resources;
Protection of Communications Within a Provider Domain;
Protection of Communications Between Provider Domains.

6.3.1 User Access Device

The following requirements relate to the access device.

R9a A service provider should be able to prevent the use of a particular access device. Examples are stolen, lost, defective, cloned or time-expired access devices as well as those belonging to users whose subscriptions have been terminated.

6.3.2 Mobile Terminal Equipment

The following security requirements relate to the use of mobile terminal equipment.

R10a The identity of a mobile terminal should be secured so that it cannot be changed by an unauthorized party.

R10b The use of mobile terminal equipment that is not type approved but is otherwise acceptable for use should be detected and prevented.

R10c The use of faulty mobile terminal equipment should be prevented.

R10d Stolen mobile terminal equipment should be detected and either tracked or its use prevented.

R10e The use of cloned mobile terminal equipment should be detected and prevented.

To provide a management structure to enable registration of type-approved mobiles, registration of manufactured mobiles, and reporting of stolen mobiles, on a national, regional and worldwide basis, it may be necessary to involve roaming administrators in terminal security management. In this case there may be other security requirements, such as the secure management of databases of type-approved mobiles.

6.3.3 User Access to Telecommunications Services

The following security requirements relate to user access to telecommunications services.

R11a A service provider/network provider should be able to identify, authenticate and authorise a user's requests to register for or make use of telecommunications services.

R11b A user should not be able to repudiate the provision of a telecommunications service.

R11c A user should be able to identify and authenticate the network provider/service provider when the user accesses a telecommunications service.

R11d A service provider should be able to limit the services available to a specific user.

Further study of the Requirement 11a is needed to decide whether a user is authenticated to his service provider, the network provider or both, and to decide when authentication is required. To do this it is necessary to have a better understanding of the registration, location updating and call setup principles that are likely to be used in third-generation systems.

Requirement 11c is also for further study. The need for authentication depends upon what data the service provider/network provider can read from or write to the access device or terminal.

Requirement 11d has been suggested by SMG5, but it is not clear that it is a security requirement. Does it mean that a network provider needs to check with the service provider that a user is authorised to use particular services? If so, then it is covered by Requirement 11a.

6.3.4 Provision of Telecommunications Services

The following requirements relate to the provision of telecommunications services.

R12a Service providers and network operators should be protected against intruders intercepting signalling data on the radio path for eavesdropping.

R12b Service providers and network operators should be protected against intruders intercepting signalling data on the radio path for manipulation and retransmission.

R12c It should be very difficult for intruders to restrict the availability of services.

R12d Means should be provided to authenticate the origin of user traffic or signalling data transferred on the radio path.

6.3.5 Service Profiles

The following security requirements relate to service profiles held by network operators and service providers.

R13a Non-repudiation of access by users or subscribers to service profiles should be provided.

This requirement may be too strong and requires further study. Perhaps all that is required is the means to enable service providers to make users and subscribers accountable for the changes they make to their service profiles.

Requirements on privacy and integrity protection of service profiles from the service provider perspective need to be identified. Careful consideration needs to be given to what aspects, if any, of this topic are the subject of standardisation.

6.3.6 Charging and Accounting

The following security requirements relate to charging and accounting.

R14a Charging and accounting data transferred between network providers and service providers should have integrity, privacy and non-repudiation of origin.

R14b Non-repudiation of delivery should be provided for charging and accounting data transferred between network providers and service providers.

R14c Integrity and privacy are required for stored charging and accounting data.

R14d Service providers should be able to limit charges.

The entire subject of charging and accounting is for further study. Much more information is needed about the mechanisms for the transfer of charging and accounting data if specific security features are to be provided. Moreover, careful consideration needs to be given as to the level of standardisation required.

6.3.7 Protection of Provider Resources

The following security requirements relate to the protection of service provider and network provider resources.

R15a Network providers and service providers should be able to protect their data bases against unauthorised access.

R15b Network providers and service providers should be able to prevent intruders restricting the availability of their services.

R15c Network providers and service providers should be able to monitor the use of their resources.

This subject is for further study, in particular the level to which this topic needs to be addressed in a standard.

6.3.8 Protection of Communications within a Provider Domain

This section identifies the requirements for protecting signalling and other data communicated between entities in the same domain, that is, belonging to the same service provider or network provider

R16a An intruder should not be able to impersonate one network entity to another.

R16b Signalling data and management data sent within a service provider domain should be protected with respect to authentication of origin, integrity and confidentiality.

6.3.9 Protection of Communications between Provider Domains

This section identifies the security requirements associated with communications between network providers and service providers.

R17a An intruder should not be able to impersonate one service provider or network provider to another.

R17b The privacy of data sent between provider domains must be ensured.

R17c Unauthorized modification of data sent between provider domains must be prevented.

R17d The origin of data sent between provider domains should not be subsequently denied by the originator.

R17e The delivery of data sent between provider domains should not be subsequently denied by the recipient.

Non-repudiation requirements such as 17d and 17e need to be studied further.

6.4 Contributions to Standardisation

This section reviews the security requirements identified for third generation system that have so far been incorporated in the ongoing standardization processes for UMTS and FPLMTS.

6.4.1 Requirements for UMTS

This section discusses the requirements for security features in UMTS.

The current list of security requirements derived by ETSI/SMG5 for UMTS is given in [A19]. This list is closely based on input from our study and so there are only a few minor differences from the requirements outlined in Subsections 6.2 and 6.3.

As mentioned previously, the classification of requirements is the same as in [A19], with customer and provider perspectives.

An additional requirement for UMTS is that SMG5 identify specific supplementary security services to be supported, namely:

end-to-end user authentication;
end-to-end data integrity;
end-to-end data confidentiality.

6.4.2 Requirements for FPLMTS

A working document towards revising the FPLMTS security principles recommendation M.1078 [B10] was produced by the ITU TG8/1 meeting in October 1994. Despite many changes, largely based on comments made by the LINK 3GS3 project team, there is still a confusion between security-related system requirements, system requirements on security, and security requirements. The requirements themselves are divided into the following categories:

service related;
access related;
radio interface related;
terminal related;
user association related;
network operational;
security management.

All are placed in a section headed `system requirements on security'.

7 Security Features

7.1 Introduction

This section proposes a set of security features aimed at satisfying the requirements identified in Section 6.

There are a number of system requirements that apply directly to security features. Any feature introduced to meet security requirements will also need to meet these system requirements. Subsection 7.2 identifies these system requirements.

Subsection 7.3 describes the security features that exist for the current second-generation systems, particularly those defined for a GSM PLMN. These features can be separated into two distinct areas, namely cryptographic and non-cryptographic.

The crux of Section 7 lies in Subsection 7.4 where we derive a concise set of security features for third-generation mobile systems. The features appearing in Section 7.4 are fairly brief generic descriptions. Generally, they do not state explicitly the information to which the feature applies, who invokes the feature, when the feature is to be invoked, and a number of other essential details. Full descriptions are necessary if the features are to serve any useful purpose. Subsection 7.5 suggests a method for generating full feature descriptions, and includes a number of example descriptions.

7.2 Requirements on Security Features

This subsection identifies a number of system requirements to be imposed upon security features.

1. Security features should be user-friendly and easy to use. In particular, any security keys and access devices distributed to the user should be easy to manage and update.

2. Security features should be transparent to users as far as possible.

3. Security features should require as little user interaction as possible.

4. Security features should not significantly increase call setup times.

5. The security features should work with the various radio environments and should not be constrained by any one physical layer or access method.

6. The security features should have mechanisms for version management, and should be easy to update during the lifetime of the system.

7. It should be possible for a limited service to be provided in the event of failure of particular security features. For instance, in case of encryption failure, identified emergency transmissions should be permitted on the clear data channel.

8. Security features should have the least possible impact on the traffic capacity of the air interface.

9. The security to be provided should be adequately standardised to provide secure international interoperability and roaming. However, within the security mechanisms, the maximum independence between the parties involved in the operation should be allowed, as well as the maximum freedom for all parties to make their own security policies and mechanisms.

7.3 Features for Second Generation Systems

This section reviews the security features defined for the GSM system.

7.3.1 Cryptographic Security

Cryptographic security features include subscriber authentication, subscriber identity confidentiality, and the confidentiality of user data and signalling information.

Subscriber Identity Authentication
In GSM each subscriber is identified by an IMSI (International Mobile Subscriber Identity) and a secret personal subscriber key Ki. Ki is stored securely in the mobile's SIM and by the network.

To access the network, a subscriber must first be authenticated. To achieve this, the subscriber must display knowledge of his Ki to the network. This is accomplished in the following manner. First, the network issues a randomly generated number RAND over the air interface to the mobile. The mobile then inputs RAND and Ki to algorithm A3. The output from A3 is a number SRES. This value is sent back over the air interface, to be authenticated by the network.

Authentication is required upon registration, on call set up attempts, and prior to utilising certain supplementary services.

An additional feature proposed in GSM recommendation 02.03 [A1] is that, in the event of authentication failure, emergency calls may still be made from the mobile. This feature can be paralysed by an authorised party such as the network operator.

Confidentiality of User Data and Signalling Information
All digitised speech data and most signalling data is encrypted when sent over the air interface. This does not however constitute end-to-end encryption of the data.

Encryption is achieved with the ciphering algorithm A5. The key Kc used for the encryption is generated by both the mobile and the network. Kc is the output obtained from algorithm A8, by inputting the subscriber key Ki and the most recently generated RAND value.

Confidentiality of Subscriber Identity
The network must know the location of subscribers so that it can route the calls. This is achieved by each mobile regularly and automatically performing a location update and informing the network of its identity.

When a subscriber performs this location update it does not send its IMSI (International Mobile Subscriber Identity) over the air, but instead sends a derived value, a TMSI (Temporary Mobile Subscriber Identity), allocated to it by the network. If for any reason, the subscriber does not possess a valid TMSI, then the IMSI is sent over the air interface to perform the location update.

To perform the update, the subscriber sends its current TMSI (or IMSI if necessary), from which the network can ascertain its identity and register it in the locality. Following this, the network can authenticate the subscriber and allocate a new TMSI, which it sends, encrypted, over the air interface. This new TMSI will be used for the mobile's next location update.

7.3.2 Non-Cryptographic Security

Non-cryptographic security consists of a number of access control features. These may be further split into two types: those controlled by the subscriber (namely SIM-based features), and those controlled by the network operator (or some other authorised party).

Subscriber Controlled Features
Most subscriber information held within a mobile is stored securely in a removable SIM (Subscriber Identity Module). For example the subscriber key Ki and IMSI are stored in the SIM. Furthermore, the algorithms A3 and A8 are

implemented within the SIM.

The SIM is equipped with its own internal security. This security relies on two numbers: the PIN (Personal Identification Number) and the PUK (PIN Unblocking Key). Both are known only to the subscriber (and possibly the network operator). When the SIM is inserted into the mobile, the PIN must be correctly entered before the unit will function. Should the PIN be incorrectly entered three consecutive times then the SIM will automatically block itself, and allow no further attempts at PIN entry until the correct PUK is entered. Should the PUK be incorrectly entered ten consecutive times, then the SIM becomes permanently blocked. The `incorrect entry' count for PINs and PUKs is not affected by removal of the SIM from the mobile, or by switching the mobile off. The count is reset when the correct number is entered.

The PIN can be changed at any time using knowledge of the existing PIN or PUK, but the PUK cannot be changed.

The PIN feature can be disabled by the subscriber, using knowledge of the existing PIN or PUK. This disabling function can be paralysed by an authorised party such as the network operator.

Emergency calls may be made without a SIM present in the mobile, although an authorised party such as the network operator can disable this feature.

When the mobile is switched off, or the SIM removed, all subscriber-related information that has been transferred from the SIM to the unit is deleted. This action also terminates any call that is in progress.

Operator-Controlled Features
Upon registration, each subscriber is assigned to a particular `user class' in the range 0 to 9. In addition, some users may be members of one or more of five special classes 11 to 15 (these classes correspond to specific high priority users, such as the emergency services). The classes to which a subscriber belongs are programmed into the SIM at manufacture, and cannot be changed thereafter. Access to the network is determined by membership of the appropriate class. The operator has the ability to bar any specified class from a particular part of the network at any time. However, it is not intended for this form of access control to be used under normal operating conditions.

Each piece of mobile equipment has a unique IMEI (International Mobile Equipment Identity). When the unit is used, this number is sent over the air interface and checked by the network operator, to determine whether the unit is registered as stolen or otherwise outlawed. This procedure is described in detail in [A3].

The security features described in this section are utilised at the discretion of the operator for subscribers on the home network but, for roaming subscribers, the features are mandatory unless otherwise agreed by all affected operators.

7.4 Security Features for Third Generation Systems

7.4.1 Introduction

Many security features have been identified for third generation mobile telecommunications systems (3GS). Current attempts at describing and classifying these features are inadequate in a number of ways. For example, some feature descriptions are too vague, many features are repetitious, and the proposed classifications are somewhat arbitrary and of little practical value.

Section 7.4 is intended to contribute to a discussion on deriving a coherent and useful classification of security features. Firstly three candidate classifications of security features, in connection with different security properties, roles and information types respectively, are considered in Subsection 7.4.2. The discussion of these three candidates results in a classification of security features which is based on security properties, namely confidentiality, integrity, authentication, non-repudiation, access control, security of management, management of security and supplementary. Secondly a list of *security elements,* which are referred to as features by standards bodies such as ETSI and ITU, is compiled in Subsection 7.4.3. This list includes all elements currently proposed for UMTS, FPLMTS and GSM systems. In order to obtain a set of security features that is fairly small but encompasses all elements previously identified, a combination of the elements is made in Subsection 7.4.4. In this subsection, we also identify a set of features, and Subsection 7.4.5

provides the description for each feature of this set.

7.4.2 Classification of Security Features

In this section we consider several possible classifications for security features in 3GS and decide on one. The following three methods are candidates:

1. According to different security properties. Each of the security features can be assigned to one of the following categories:

    - confidentiality;
    - integrity ;
    - authentication;
    - non-repudiation;
    - access control;
    - security of management;
    - management of security.

2. Based on the role which benefits. The classification of security features is as follows:

    - user-related security features;
    - subscriber-related security features;
    - network operator-related security features;
    - service provider-related security features.

3. Depending on the information types identified in Section 4.4.2. Security features can be divided in two ways:

    - transmitted data-related security features;
    - stored data-related security features;

    or

    - signalling data-related security features;
    - control data-related security features;
    - user traffic-related security features.

Every security element listed in Subsection 7.4.3 can be associated with at least one security property, one role and one information type.

Attempts have been made to use the second method of classification. However, it became apparent that a major disadvantage of the method is its inherent redundancy because some of the security features benefit more than one role and so are included in more than one category.

A classification combining the first and second methods has been identified for study in UMTS. It has two small disadvantages which are: some of the features are difficult to assign to a single category, such as *Signalling Data Origin Authentication* and *Non-repudiation of Access to Stored Data*, and a portion of signalling data is also stored data.

Based upon the discussion above, we decided to classify the security features by using the first method and adding supplementary features. The supplementary part is added because these features (such as *support for end-to-end security service*) are difficult to assign to a single security property. So the classification of security features is as follows:

- confidentiality;
- integrity;
- authentication;
- non-repudiation;
- access control;
- security of management;

- management of security;
- supplementary.

7.4.3 A List of Security Elements

This section contains a list of security elements, which are referred to as features by standards documents such as SMG 05-0901 [A19], ITU Recommendation M.1078 [B13] and GSM 02.09 [A2]. The categories of the elements are according to the classification at the above section.

In this list, parts of the meaning of some of the elements identified in the different documents are redundant. We keep all of them here in order to make the list as complete as possible.

Confidentiality

User traffic confidentiality (UMTS, FPLMTS, GSM)
This element protects against unauthorised eavesdropping on user traffic.

User identity confidentiality (FPLMTS, GSM)
An element by which the identity of a user is protected against disclosure over a radio interface.

User location confidentiality (FPLMTS)
An element by which the physical location of a user is protected against disclosure over a radio interface.

Signalling data confidentiality (UMTS, FPLMTS, GSM)
This element ensures that the signalling data is not made available or disclosed to unauthorised parties.

Confidentiality of stored data (UMTS)
This element ensures that stored data is not made available or disclosed to unauthorised parties.

Protected DTMF (FPLMTS)
An element by which DTMF is protected against eavesdropping over the radio interface.

Secure distribution of user identity and its associated security information (FPLMTS)
An element by which the user identity and its associated security information can be securely distributed to the UIM by the service provider at the time of registration of the user. This feature only applies when the UIM is used for the user association with the mobile terminals.

Secure distribution of mobile terminal identity and its associated security information (FPLMTS)
An element by which the mobile terminal identity and its associated security information can be securely distributed to the mobile terminal, if they are assigned by the terminal manager, or to the terminal manager, if they are assigned by the terminal manufacturers, at the time of registration of the mobile terminal.

Integrity

User traffic integrity (UMTS)
This element protects against manipulation (modification, insertion and/or replay) by unauthorised parties of user data on the radio path or in the fixed network.

User location integrity (FPLMTS)
An element by which the service provider and/or the network operator can have some assurance that the user location related information cannot be modified by the intruders.

Terminal location integrity (FPLMTS)
An element by which the service provider and/or the network operator can have some assurance that the mobile terminal location related information cannot be modified by the intruders. It may effectively be implemented by the user location

integrity.

Integrity of stored data (UMTS)
This element offers protection for stored data against unauthorised writing and modifying.

Signalling data integrity (UMTS, FPLMTS)
This element provides protection against manipulation (modification, insertion or replay) by unauthorised parties of signalling data.

Authentication

Authentication of service provider to user (UMTS, FPLMTS)
This element provides corroboration of the identity of a service provider to a user.

Authentication of user to service provider (UMTS)
This element provides corroboration of the claimed identity of a user to a service provider.

User identity authentication (FPLMTS, GSM)
An element by which the identity of a user is verified to be the one claimed.

Authentication of terminal to terminal manager (UMTS, GSM, FPLMTS)
This element provides corroboration of the identity of a terminal to a terminal manager.

Authentication of providers (UMTS)
This element provides corroboration of the identity of one network operator or service provider to another.

Authentication of network operator to user (UMTS)
This element provides corroboration of the identity of a network operator to a user.

Authentication of user to network operator (UMTS)
This element provides corroboration of the claimed identity of a user to a network operator.

Re-authentication of users (FPLMTS)
An element by which the identity of a user is re-verified to be the one claimed. This feature may be invoked repeatedly or at any appropriate instant.

Re-authentication of terminals (FPLMTS)
An element by which the identity of a mobile terminal is re-verified to be the one claimed. This feature may be invoked repeatedly or at any appropriate instant.

User traffic origin authentication (UMTS)
This element provides verification that the user traffic originates from the claimed entity.

Signalling and control data origin authentication (UMTS)
This element provides verification that signalling or control data originates from the claimed entity.

Non-repudiation

Non-repudiation of origin of signalling and control data (UMTS)
This element provides proof to a third party that a message was sent by a certain entity.

Non-repudiation of delivery of signalling and control data (UMTS)
This element provides proof to a third party that a message was received by a certain entity.

Non-repudiation of access to stored data (UMTS)
This element provides protection against an entity denying having attempted to access stored data.

Access Control

Access control to UIM (UMTS, GSM, FPLMTS)
This element ensures that a UIM can only be used by an authorised party.

Access control to terminal equipment (UMTS)
This element ensures that terminal equipment can only be utilised by authorised parties.

Access control to service profile (UMTS, FPLMTS)
This element ensures that only authorised parties can access a service profile.

Access control to subscription data (FPLMTS)
An element by which there are restrictions in the access to the personal data of a user or subscriber stored in the network.

Access Control to telecommunication services (UMTS)
This element ensures that only authorised parties can access a telecommunication service.

Subscriber access control to service profile (FPLMTS)
An element by which the subscriber has direct and limited access to the personal service profile of his associated users, by means of which he may be able to restrict access to services.

User action authorization (FPLMTS)
An element by which the various actions allowed for a mobile terminal are exposed to various degrees of restriction. It requires a mobile terminal to be authorised for its actions.

Denial of user's access to the service (FPLMTS)
An element by which the service provider denies access to service by a particular user.

Denial of mobile terminal access to the service (FPLMTS)
An element by which the service provider/network operator may deny a particular mobile terminal access to service.

Access control of user groups by network operator (GSM)
This element ensures that only authorised members of appropriate classes can access to a network.

Security of Management

User event reports (FPLMTS)
An element by which the user will receive warning announcements or indications at critical moments in the operation of services.

Backup of subscription data (FPLMTS)
An element by which the service provider can restore data relating to users or subscribers upon failure.

Event logging (FPLMTS)
An element by which the service provider can log activities relating to a user or subscriber.

Blacklisting (FPLMTS)
An element by which the service provider can refuse access to services requested by a particular user.

Security audit trail (FPLMTS)
An element by which an independent review and examination of system records and activities can be examined for security policy adherence and security violations.

Management of subscriber related credential data (FPLMTS)
An element by which a service provider protects, retains and traces a subscriber.

Management of Security

Security key management (FPLMTS)
An element by which a service provider and or network operator can manage keys used for the establishment of a private control and communication channel between the network and mobile terminal.

Cryptographic information management (FPLMTS)
An element of management which manages the secret information associated with cryptographic security mechanisms. It is concerned with the generation, distribution, storage, updating and deletion of cryptographic information. The integrity of this information must be assured.

Supplementary

Support for end-to-end security services (UMTS)
This element ensures that the service provider/network operator can provide end-to-end security services to particular fixed or mobile users, subject to the availability of additional end user equipment.

7.4.4 Identification of Security Features

Combination of Security Elements

Before identifying a concise set of security features, we try to combine the elements listed in Subsection 7.4.3. The combination compresses the list and encompasses all of the elements.

We discuss which roles and information should be protected in relation to each of the security feature classes.

Confidentiality
Some transmitted and stored data in 3GS environments should be protected against disclosure to unauthorised parties. The data considered here includes signalling data, control data and user traffic, in particular, user identity, user location, terminal location, service profile, charging and billing data, and some management information. The transmitting interfaces considered here include deliveries from a service provider to a user, a terminal manager to a user, between a user and a network operator, one network operator and another, a network operator and a service provider, and one service provider and another. The storage areas include a user access device or, in UMTS terminology, a user identity module (UIM), a terminal, a service provider's databases and a network operator's databases.

Integrity
As for confidentiality, transmitted and stored data in 3GS environments should be protected in order to meet the needs of integrity. The data considered here includes signalling data, control data and user traffic, in particular, user location, terminal location, charging and billing data, and some management information. The transmitting interfaces considered here include deliveries from a service provider to a user, a terminal manager to a user, between a user and a network operator, one network operator and another, a network operator and a service provider, and one service provider and another. The storage areas include a UIM, a terminal, a service provider's databases and a network operator's databases.

Authentication
Authentication includes both entity authentication and message authentication. Entity authentication involves some roles in 3GS, particularly authentication among users, service providers and network operators, authentication among terminals, terminal managers and network operators, and authentication between service providers/network operators. Message authentication as considered here is message origin authentication, in particular, signalling or control data origin authentication and user traffic origin authentication.

Non-repudiation
Non-repudiation includes non-repudiation of data origin and delivery, and non-repudiation of access. The data encompasses signalling data, control data and user traffic. The access encompasses access to stored data and access to services.

There may be some argument as to whether these features should be covered under a different heading, such as *authentication* or *access control*.

Access Control
Access control includes access to a facility (e.g., a UIM or terminal equipment), access to a service, and access to stored data.

Security of Management
Security of management is service providers and/or network operators to manage events relating to users and subscribers, including event reporting, logging, recording and recovering securely.

Management of Security
Management of security includes key management and cryptographic information management.

A Set of Security Features

Based on the combination of the elements, this subsection identifies a set of security features. The features are divided according to the classification of security features defined in Section 2.

Confidentiality

The following two security features are included in this category:

1. Confidentiality of signalling and control data

This feature ensures that the signalling and control data are not made available or disclosed to unauthorised parties.

2. Confidentiality of user traffic

This feature protects against unauthorised eavesdropping on user traffic.

Integrity

The following two security features are included in this category:

3. Integrity of signalling and control data

This feature provides protection against manipulation (modification, insertion or replay) by unauthorised parties of signalling data or control data.

4. Integrity of user traffic

This feature protects against manipulation (modification, insertion and/or replay) by unauthorised parties of user data on the radio path or in the fixed network.

Authentication

The following three security features are included in this category:

5. Service related authentication (or *Authentication among users, service providers and network operators*.)

This feature provides corroboration of the identities of a user, corresponding service provider and network operator underlying the provision of service to the user.

The name *service related authentication* is preferred because it covers authentication relating to the terminal, which will be for further study.

6. Authentication between network operators/service providers (or *Management related authentication*)

This feature provides corroboration of the identity of one service provider or network operator to another.

The name *authentication between network operators/service providers* seems more natural, but it needs to be distinguished from feature number 5.

7. Message origin authentication

This feature provides verification that transmitted signalling or control data and user traffic originates from the claimed entity.

Non-repudiation

The following three security features are included in this category:

8. Non-repudiation of origin and delivery of transmitted data

This feature provides proof to a third party that a message was sent or received by a certain entity.

9. Non-repudiation of access to stored data

This feature provides protection against an entity denying having attempted to access stored data.

10. Non-repudiation of access to a service

This feature provides protection against an entity denying having attempted to access a service.

Access Control

The following three security features are included in this category:

11. Access control to a facility

This feature ensures that a UIM or terminal equipment can only be used by an authorised party.

12. Access control to a service

This feature ensures that only authorised parties can access a service.

The question of how this feature will be supported by *service related authentication* is for further study.

13. Access control to stored data

This feature ensures that only authorised parties can access stored data.

Security of Management

The following three security features are included in this category:

14. User event reports

This feature ensures that a user will receive warning announcements or indications at critical moments in the operation of services.

15. Event logging and recording

This feature ensures that a service provider can log and record activities relating to a user or subscriber.

16. Event recovery

This features ensures that a service provider can restore data relating to a user or subscriber upon failure, trace a particular user and refuse access to services requested by a particular user.

Management of Security

The following two security features are included in this category:

17. Key management

This feature ensures that a service provider and or network operator can manage keys used for the establishment of a private control and communication channel between the network operator and user.

18. Cryptographic information management

This feature ensure that a service provider and or network operator can manage the generation, distribution, storage, updating and deletion of cryptographic information to assure the integrity of this information.

Supplementary

The following security feature is included in this category:

19. Support for end-to-end security service

This feature ensures that the service provider/network operator can provide end-to-end security services to particular fixed or mobile users, subject to the availability of additional end user equipment.

7.4.5 Description of Security Features

This section provides a description of each feature identified in Subsection 7.4.4, using a method which ensures that descriptions are of a uniform nature, concise and informative. A feature may be expanded into a number of instances, corresponding to the different interfaces or different information types involved. One or two such individual instances of a feature are given in the subsections below. Each description of an instance of a feature contains the following fields:

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

These fields contain the following information:

entity or interface involved
If the feature concerns stored data, this field identifies the entity where the data is stored. Similarly, if the feature concerns any action to be performed by an individual entity, then this field identifies the pertinent entity. If the feature concerns transmitted data, then this field identifies the particular interface over which the data is transmitted.

information types
The information types used within this field include user traffic, charging, billing, location, dialling, routing, network resource management, identity, security management, service profile and access control management. The details of every information type can be found in Section 4.4.2.

requirements addressed

Each feature will satisfy, or contribute towards satisfying, one or more of the requirements set out in Sections 6.2 and 6.3. This field lists these requirements.

when utilised
This field specifies the occasions when the feature will be used.

invoking entity
A specific entity will be responsible for invoking a feature. This entity is listed here, and will usually be one of those entities identified under `entity or interface involved'.

notified entities
In addition to the entity or entities directly involved in a feature, there may be a number of other entities which are notified when the feature is invoked.

extent of standardisation
This field identifies to what extent the feature should be standardised.

Confidentiality of Signalling and Control Data

Description: This feature ensures that the signalling and control data are not made available or disclosed to unauthorised parties.

Instance one:

interface involved
user - network operator.
information types

location, dialling, identity, authentication, network resource management, access control management, service profile.

requirements addressed

location privacy of users, protection of users' identities, protection against interception of signalling and control data, privacy of service profile data, privacy of signalling and control data.

when utilised

registration, location updating, call setup, handover, service profile modification, speech-data phase, call release, deregistration.

invoking entity

user or network operator.

notified entities

user, network operator and service provider.

extent of standardisation

mechanism completely specified.

Instance two:

interface involved

service provider - network operator.

information types

identity, location, charging, service profile, authentication.

requirements addressed

privacy of charging data, location privacy of users, protection of users' identities, privacy of service profile data, privacy of signalling and control data.

when utilised

registration, location updating, handover, service profile modification, deregistration.

invoking entity

service provider or network operator.

notified entities

service provider and network operator.

extent of standardisation

mechanism completely specified.

Confidentiality of User Traffic

Description: This feature protects against unauthorised eavesdropping on user traffic.

interfaces involved

user - network operator, one network operator - another.

information type

user traffic.

requirements addressed

privacy of user traffic.

when utilised

speech-data phase.

invoking entity

user or network operator.

notified entities

user, network operator.

extent of standardisation

mechanism completely specified.

Integrity of Signalling and Control Data

Description: This feature provides protection against manipulation (modification, insertion or replay) by unauthorised parties of signalling data or control data.

Instance one:

interface involved
user - network operator.
information types
location, dialling, identity, authentication, network resource management, access control management, service profile.
requirements addressed
protection of users' identities, protection against unauthorised modification of service profile data, protection against unauthorised modification of signalling and control data.
when utilised
registration, location updating, call setup, handover, service profile modification, speech-data phase, call release, deregistration.
invoking entity
user or network operator.
notified entities
user, network operator and service provider.
extent of standardisation
mechanism completely specified.

Instance two:

interface involved
service provider - network operator.
information types
identity, location, charging, service profile, authentication.
requirements addressed
integrity of charging data, protection of users' identities, protection against unauthorised modification of service profile data, protection against unauthorised modification of signalling and control data.
when utilised
registration, location updating, handover, service profile modification, deregistration.
invoking entity
service provider or network operator.
notified entities
service provider and network operator.
extent of standardisation
mechanism completely specified.

Integrity of User Traffic

Description: This feature protects against manipulation (modification, insertion and/or replay) by unauthorised parties of user data on the radio path or in the fixed network.

interfaces involved
user - network operator, one network operator - another.
information types
user traffic.
requirements addressed
protection against interception and unauthorised modification of user traffic.
when utilised
speech-data phase.
invoking entity
user or network operator.
notified entities
user, network operator.

extent of standardisation
mechanism completely specified.

Service Related Authentication

Description: This feature provides corroboration of the identities of a user, corresponding service provider and network operator underlying the provision of service to the user.

interfaces involved
user - network operator, network operator - service provider.
information types
authentication, identity, location.
requirements addressed
protection against an intruder impersonating a user, provision of identification and authentication of users, network operators and service providers.
when utilised
registration, location updating, call setup, call release, deregistration.
invoking entity
user or network operator.
notified entities
user, network operator, service provider.
extent of standardisation
mechanism completely specified.

Authentication between Network Operators/Service Providers

Description: This feature provides corroboration of the identity of one service provider or network operator to another.

interfaces involved
network operator - service provider, one network operator - another, one service provider - another.
information types
identity, authentication.
requirements addressed
protection against impersonation of service providers/network operators.
when utilised
service profile modification, network management process.
invoking entity
network operator or service provider.
notified entities
network operator, service provider.
extent of standardisation
mechanism completely specified.

Message Origin Authentication

Description: This feature provides verification that transmitted signalling or control data and user traffic originates from the claimed entity.

Instance one:

interfaces involved
user - network operator, one network operator - another, network operator - service provider.
information types
charging, billing, location, dialling, identity, authentication, network resource management, access control management, service profile.
requirements addressed

protection signalling and control data with respect to origin authentication.
when utilised
registration, location updating, call setup, handover, service profile modification, speech-data phase, call release, deregistration.
invoking entity
user, network operator or service provider.
notified entities
user, network operator, service provider.
extent of standardisation
mechanism completely specified.

Instance two:

interfaces involved
user - network operator, one network operator - another.
information types
user traffic.
requirements addressed
protection user traffic with respect to origin authentication.
when utilised
call setup, speech-data phase, call release.
invoking entity
user or network operator.
notified entities
user, network operator.
extent of standardisation
mechanism completely specified.

Non-repudiation of Origin and Delivery of Transmitted Data

Description: This feature provides proof to a third party that a message was sent or received by a certain entity.

Instance one:

interfaces involved
user - network operator, network operator - service provider.
information types
charging, billing, location, dialling, identity, authentication, routing, network resource management, access control management, service profile.
requirements addressed
provision of non-repudiation of origin and delivery of signalling and control data.
when utilised
registration, location updating, handover, call setup, speech-data phase, call release, service profile modification, deregistration.
invoking entity
user, network operator or service provider.
notified entities
user, network operator, service provider.
extent of standardisation
mechanism completely specified.

Instance two:

interfaces involved
user - network operator, one network operator - another.
information types

user traffic.

requirements addressed

provision of non-repudiation of origin and delivery of user traffic.

when utilised

call setup, speech-data phase, call release.

invoking entity

user or network operator.

notified entities

user, network operator.

extent of standardisation

mechanism completely specified.

Non-repudiation of Access to Stored Data

Description: This feature provides protection against an entity denying having attempted to access stored data.

entities involved

user, network operator, service provider.

information types

charging, billing, location, identity, authentication, network resource management, access control management, service profile.

requirements addressed

provision of non-repudiation of access to service profile and other stored data.

when utilised

service profile modification, network management process.

invoking entity

user, network operator or service provider.

notified entities

user, network operator, service provider.

extent of standardisation

mechanism completely specified.

Non-repudiation of Access to a Service

Description: This feature provides protection against an entity denying having attempted to access a service.

entities involved

user, network operator, service provider.

information types

charging, billing, location, identity, authentication, network resource management, access control management, service profile.

requirements addressed

provision of non-repudiation of access to a service.

when utilised

registration, call setup, call release, deregistration, service profile modification.

invoking entity

network operator or service provider.

notified entities

user, network operator, service provider.

extent of standardisation

mechanism completely specified.

Access Control to a Facility

Description: This feature ensures that a UIM or terminal equipment can only be used by an authorised party.

Instance one:

interface involved
user - UIM.
information types
identity, authentication, service profile.
requirements addressed
prevention of the use of a particular UIM, prevention of using a UIM by unauthorised parties.
when utilised
a user access to a UIM, a user access to a service.
invoking entity
user.
notified entity
UIM.
extent of standardisation
mechanism completely specified.

Instance two:

interface involved
user - terminal equipment.
information types
identity, authentication.
requirements addressed
prevention of the use of terminal equipment, prevention of using terminal equipment by unauthorised parties.
when utilised
a user access to terminal equipment, a user access to a service.
invoking entity
user.
notified entity
terminal equipment.
extent of standardisation
mechanism completely specified.

Access Control to a Service

Description: This feature ensures that only authorised parties can access a service.

interfaces involved
user - network operator, network operator - service provider.
information types
identity, authentication, network resource management, access control management, service profile.
requirements addressed
prevention of access to a service by unauthorised parties.
when utilised
a user access to a service.
invoking entity
network operator or service provider.
notified entities
user, network operator, service provider.
extent of standardisation
mechanism completely specified.

Access Control to Stored Data

Description: This feature ensures that only authorised parties can access stored data.

entities involved
user, network operator, service provider.
information types
charging, billing, location, identity, authentication, network resource management, access control management, service profile.
requirements addressed
prevention of access to stored data by unauthorised parties.
when utilised
stored data modification.
invoking entities
user, network operator or service provider.
notified entities
user, network operator, service provider.
extent of standardisation
mechanism completely specified.

User event reports

Description: This feature ensures that a user will receive warning announcements or indications at critical moments in the operation of services.

interfaces involved
user - network operator.
information types
warning announcements or indications. (Note: this information type is not covered in Section 4.4.2.)
requirements addressed
secure provision of telecommunications services to the user.
when utilised
critical moments in the operation of services.
invoking entity
user, network operator or service provider.
notified entities
user, or user and service provider.
extent of standardisation
mechanism completely specified.

Event logging and recording

Description: This feature ensures that a service provider can log and record activities relating to a user or subscriber.

entities involved
service provider, user and subscriber.
information types
charging, billing, service profile and access control management.
requirements addressed
protection against unauthorised modification of service profile, charging and billing information.
when utilised
system management.
invoking entity
service provider.
notified entities
user, subscriber and/or service provider.
extent of standardisation
mechanism completely specified.

Event recovery

Description: This features ensures that a service provider can restore data relating to a user or subscriber upon failure, trace a particular user and refuse access to services requested by a particular user.

interfaces involved
service provider, user and subscriber.
information types
charging, billing, dialling, identity, service profile and access control management.
requirements addressed
protection against unauthorised modification of service profile, provision of the integrity of the charging and billing systems.
when utilised
system management, user access to a service.
invoking entity
service provider.
notified entities
user and subscriber.
extent of standardisation
mechanism completely specified.

Key management

Description: This feature ensures that a service provider and or network operator can manage keys used for the establishment of a private control and communication channel between the network operator and user.

entities involved
service provider, network operator and user.
information types
security management.
requirements addressed
provision of secure communication channel between the network operator and user.
when utilised
system management, to provide telecommunications services to user.
invoking entity
service provider or network operator.
notified entities
user, network operator and service provider.
extent of standardisation
mechanism completely specified.

Cryptographic information management

Description: This feature ensure that a service provider and or network operator can manage the generation, distribution, storage, updating and deletion of cryptographic information to assure the integrity of this information.

entities involved
user, network operator and service provider.
information types
security management and identity.
requirements addressed
provision of secure communication channel between the network operator and user.
when utilised
system management, to provide telecommunications services to user.
invoking entity
service provider or network operator.

notified entities
user, network operator and/or service provider.
extent of standardisation
mechanism completely specified.

Support for End-to-end Security Service

Description: This feature ensures that the service provider/network operator can provide end-to-end security services to particular fixed or mobile users, subject to the availability of additional end user equipment.

interfaces involved
user - network operator, one network operator - another, network operator - service provider.
information types
identity, authentication, user traffic, service profile.
requirements addressed
provision of end-to-end security service.
when utilised
end-to-end secret communications.
invoking entity
user.
notified entities
user, network operator, service provider.
extent of standardisation
mechanism completely specified.

7.4.6 Standardization Guidelines for Security Features

One important question is to what extent the security features and the mechanisms that implement them need to be standardized. To assist in answering this question for each feature, the following set of guidelines are suggested. However, the following points should be noted.

1. The extent of standardization supported is largely a function of company or organization policy.
2. There are differences between *de facto* or *a posteriori* standards such as those prevalent in the computer industry (Unix, C, DOS, Internet) and *a priori* standardization, such as that undertaken by ETSI.
3. ETSI's policy towards standardization is currently under review by the High-Level Task Force.
4. Regarding ETSI standards, NA STAG advise on the extent of security standardization.

The first question to ask is: why is it necessary to standardize security features?
Possible answers are:

- to allow inter-operator roaming;
- to encourage manufacturers to build equipment meeting the standards;
- to create open interfaces, allowing a multi-vendor environment;
- to allow new services to be introduced efficiently and securely;
- to ensure that security features meet any regulatory requirements;

The basic principles seem to be as follows:

1. *Unnecessary standardization should be discouraged.* As an example, the GSM suggested authentication algorithm is not compulsory, and the system is designed so that operators can use their own algorithms. Another example might be where commercial products are available, and the choice of product has no impact on anyone else. For instance, the physical security of switches is not a subject for standardization.
2. *Standardization can be an efficient form of specification.* The experience of GSM is that some security features were defined in detail at the customer specification phase. Different operators with slightly different requirements, and different manufacturer solutions, led to a considerable expenditure of time and effort that could have been avoided if more detailed standards were in place.

3. *Sufficient standardization should be in place to permit competition amongst equipment manufacturers and vendors and amongst service providers and network operators*. This means that interfaces between physical and logical network entities should be as open as possible.
4. *Sufficient standardization should be in place to allow international roaming and availability of services.* Sufficient standardization of the authentication process is required to allow a roamed user to authenticate himself to his service provider via any network operator.
5. *Standards should not discourage the development of improved security techniques.* One example might be fraud management. Here, there is a common interest among providers and operators to reduce fraud. Standards might be put in place to define what and how data on roaming users' activity is transferred between providers and operators, but the techniques used to process this information should be outside the scope of standardization.
6. *Standardization can be used to encourage compliance with regulatory requirements.* For instance, the use of non-standard end-to-end encryption techniques can make legal interception difficult or impossible. The existence of an acceptable standard for end-to-end encryption might discourage legitimate users from seeking other solutions.
7. *Security features will need to deal with unexpected attacks.* So security standards need to err on the side of caution, and need to flexible enough to allow a quick response to new forms of attack or fraud.

8 Verification of the Security Architecture

8.1 Introduction

In this section, we aim to verify the security architecture by comparing security threats and features against security requirements.

8.2 Security Threats Against Security Requirements

Potential security requirements described in Subsections 6.2 and 6.3 were derived from threats to the systems described in Subsection 5.4. This section tabulates threats against requirements for the purpose of checking whether they match each other.

Table 8.1: Security threats against security requirements

threats requirements	1	2, 22	3,4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20, 21	23	24	25	26
1a, 9a					Y	Y	Y																
1b, 2a, 2b																Y							
3a	Y																						
4a, 12a															Y								
4d															Y					Y	Y	Y	
4e, 12c								Y															
4f																			Y				
5a		Y																					
5b														Y	Y								
6c																		Y					
7b, 12b																						Y	
10b							Y																
10d					Y																		
10e						Y																	
11a				Y																			
11b											Y												
13a, 14b												Y											
14a, 14c																		Y					
15a																	Y						
16a, 17a			Y																				
17b															Y				Y				
17c																					Y	Y	
17d												Y	Y										
17e											Y												
3b, 4b, 4c, 6a, 6b																							
6d,7a, 7c, 8a, 10a																							
10c, 11c, 11d																							
14d, 15b, 15c, 16b																							

Legend:	space	The threat and requirement are considered not to be appropriate to each other.
	Y	The threat and requirement are considered to appropriate to each other.

From Table 8.1, the following results can been seen:

1. Three threats (T10 *physical intervention*, T11 *protocol intervention* and T26 *unwanted incoming calls to the user)*, are not appropriate to any requirement.

2. The seventeen requirements in the bottom of the table do not correspond to any currently identified threat.

8.3 Security Features against Security Requirements

In this section, we tabulate security features against security requirements for the purpose of checking whether they match each other. The features are referenced by numbers defined in section 7.4.4.

Table 8.2: Security features against security requirements

features requirements	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1a, 9a, 10b, 10c,10d, 10e					Y						Y								
1b									Y		Y		Y						
2a											Y								
2b, 10a											Y		Y						
3a, 11a					Y							Y							
3b, 11c					Y														
4a,4f		Y																	
4b, 12a	Y																		
4c	Y	Y																	
4d			Y	Y															
4e												Y							
5a, 6d, 14c, 15a, 15c									Y				Y						
5b													Y						
6a, 6b														Y					
6c	Y					Y							Y					Y	
7a	Y								Y				Y						
7b, 14a, 16b	Y		Y				Y												
7c															Y				
8a											Y	Y							
11b										Y									
11d					Y							Y				Y			
12b			Y																
12c, 15b	Y		Y	Y	Y	Y	Y						Y		Y	Y			
12d							Y												
13a									Y										
14b								Y											
14d															Y	Y			
16a					Y	Y													
17a						Y												Y	
17b	Y	Y																Y	
17c			Y	Y														Y	
17d								Y										Y	
17e																		Y	

Legend:	space	The feature does not support meeting the requirement
	Y	The feature assists in meeting the requirement

From Table 8.2, the following results can been seen:

1. Each requirement is supported by at least one feature. This does not mean, of course, that the features are adequate to meet the requirement.

2. The features, **Key management** and **Support for end-to-end security service**, are not appropriate to any requirement.

9 Bibliography

9.1 ETSI

[A1] ETSI ETS 300 502:1994 (GSM 02.03 version 4.3.1). *European digital cellular telecommunications system (Phase 2); Teleservices supported by a GSM Public Land Mobile Network (PLMN)*. September 1994.

[A2] ETSI ETS 300 506:1994 (GSM 02.09 version 4.2.4). *European digital cellular telecommunications system (Phase 2); Security aspects*. September 1994.

[A3] ETSI ETS 300 508:1994 (GSM 02.16 version 4.3.4) *European digital cellular telecommunications system (Phase 2); International Mobile station Equipment Identities (IMEI)*. September 1994.

[A4] ETSI ETS 300 534:1994 (GSM 03.20 version 4.3.1). *European digital cellular telecommunication system (Phase 2); Security related network functions*. September 1994.

[A5] ETSI DTR/NA-43308, *Baseline document on the integration of IN and TMN*. Version 3, September 1992.

[A6] ETSI ETR 083, *General UPT security architecture.*

[A7] ETSI Final Draft TCRTR 015 (DTR/SMG-050001). *Work programme for the standardization of the UMTS*. June 1994.

[A8] ETSI SMG-TR 001 (DTR/SMG-050002) *Coordination Guideline for SMG on UMTS with respect to ITU and European research programmes*. August 1993.

[A9] ETSI ETR/SMG-50101. *UMTS Objectives and Framework.* Version 2.0.0, September 1994.

[A10] ETSI ETR/SMG-50102. *Vocabulary for the UMTS.* Version 2.0.0, September 1994.

[A11] ETSI ETR/SMG-50201. *Framework for services to be supported by the UMTS.* Version 2.0.0, September 1994.

[A12] ETSI Draft ETR/SMG-50301. *Framework of network requirements, interworking and integration for the UMTS.* Version 1.0.0, January 1995.

[A13] ETSI ETR/SMG-50401. *Overall requirements on the radio interface(s) of the UMTS*. Version 2.0.0, December 1994.

[A14] ETSI Draft ETR/SMG-50402. *Selection procedures for the choice of radio transmission technologies of the UMTS.* Version 0.8.0, August 1994.

[A15] ETSI Draft ETR/SMG-50403, *Choice of radio access principles for the interfaces of the UMTS*. Version 0.0.2, September 1992.

[A16] ETSI ETR/SMG-50501, *UMTS: Objectives and framework for the TMN*. Version 2.0.0, December 1994.

[A17] ETSI ETR/SMG-50601. *Quality Requirements for Speech and Associated Channel Coding for the UMTS*. Version 2.0.0, December 1994.

[A18] ETSI Draft ETR/SMG-50801, *Principles for handling of (digital) data services in the UMTS*. Version 0.2.1, September 1994.

[A19] ETSI ETR/SMG-50901, *Security principles for the UMTS*, Version 2.2.0, June 1995.

[A20] ETSI Draft ETR/SMG-50902, *Security studies for the UMTS*. Version 1.0.0. December 1993.

[A21] ETSI ETR/SMG-51201, *Framework for satellite integration within the UMTS*. Version 2.0.0, December 1994.

[A22] ETSI Draft ETR/SMG-50103. *UMTS System Requirements.* Version 2.0.0, December 1994.

[A23] ETSI Working Document towards ETR 50403. *Choice of Radio Transmission Technologies of the UMTS.* Version 0.0.4, September 1994.

[A24] ETSI Draft ETR/SMG-50602. *UMTS Quality Requirements and Selection Procedure for the Support of Voice-Band Data Coding Principles*. Version 0.0.1, June 1994.

[A25] ETSI ETR/SMG-51202, *Technical Characteristics, Capabilities and Limitations of Mobile Satellite Systems Applicable to the UMTS.* Version 2.0.2, December 1994.

[A26] ETSI Draft ETS 510201 Part 9. *UMTS Service Requirements for Numbering, Addressing and Identification.* Version 0.2.0, September 1994.

[A27] ETSI Draft ETS 510201 Part 11. *Human Factors Service Principles and Their Application to UMTS.* Version 0.0.1, September 1994.

[A28] ETSI Draft prETS 50501. *UMTS Overall TMN Network.* Version 0.0.2, June 1994.

[A29] ETSI GSM 01.60 version 1.1.0, *European digital cellular telecommunications system; (Phase 2+); Requirements Specification of General Packet Radio Service (GPRS)*, November 1994.

[A30] ETSI GSM 02.60 version 0.4.0, *European digital cellular telecommunications system; (Phase 2+); General Packet Radio Service (GPRS); Service Description; Stage 1*, February 1995

[A31] ETSI GSM 03.60 version 0.11.0, *European digital cellular telecommunications system; (Phase 2+); General Packet Radio Service (GPRS);Service Description; Stage 2*, October 1995.

[A32] ETSI GSM 04.60 version 0.4.0, *European digital cellular telecommunications system; Overall description of the General Packet Radio Service (GPRS) radio interface (Um)*, November 1995.

[A33] ETSI GSM 01.34 version 0.3.0, *European digital cellular telecommunications system; (Phase 2); Requirements of High Speed Circuit Switched Data (HSCSD)*, October 1995.

[A34] ETSI GSM 02.34 version 0.0.0, *European digital cellular telecommunications system; (Phase 2); High Speed Circuit Switched Data (HSCSD) - Stage 1*, October 1995.

9.2 ITU (former CCIR/CCITT)

[B1] ITU-R Recommendation M.687-1. *Future Public Land Mobile Telecommunications Systems (FPLMTS)*, September 1992.

[B2] ITU-R Recommendation M.816. *Framework for Services Supported on Future Public Land Mobile Telecommunications Systems (FPLMTS)*, September 1992.

[B3] ITU-R Recommendation M.817. *Future Public Land Mobile Telecommunications Systems (FPLMTS) Network Architectures*, September 1992.

[B4] ITU-R Recommendation M.818. *Satellite Operations within Future Public Land Mobile Telecommunications Systems (FPLMTS)*, September 1992.

[B5] ITU-R Recommendation M.819. *Future Public Land Mobile Telecommunications Systems (FPLMTS) for Developing Countries*, September 1992.

[B6] ITU-R Recommendation M.1034. *Requirements for the Radio Interface(s) for Future Public Land Mobile Telecommunications Systems.*

[B7] ITU-R Recommendation M.1035. *Framework for the Radio Interface(s) and Radio Subsystem Functionality for Future Public Land Mobile Telecommunications Systems.*

[B8] ITU-R Recommendation M.1036. *Spectrum Considerations for Implementation of Future Public Land Mobile Telecommunications Systems (FPLMTS) in the Bands 1885-2025 MHz and 2110-2200 MHz.*

[B9] ITU-R. *Revised Draft New Recommendation on Framework of FPLMTS Management (FPLMTS.NMGM)*, 8-1/TEMP/62 (Rev. 1)-E, October 1994.

[B10] ITU-R Recommendation M.1079. *Speech and Voiceband Data Performance Requirements for FPLMTS.*

[B11] ITU-R. *Provisional Draft New Recommendation on Procedure for Selection of Radio Transmission Technologies for FPLMTS (FPLMTS.RSEL)*, 8-1/TEMP/158-E, October 1993

[B12] ITU RS. *Working Document Towards a Series of New Recommendations: Detailed Specifications of Radio Interfaces of FPLMTS (FPLMTS.RSPC)*, 8-1/TEMP/88-E, October 1994.

[B13] ITU RS. *Working Document Towards Revision of Recommendation M.1078: Security Principles for FPLMTS*, 8-1/TEMP/98-E, October 1994.

[B14] ITU RS. *Working Document Towards a Draft New Recommendation: Framework for the Satellite Component of FPLMTS (FPLMTS.SFMK)*, 8-1/TEMP/101-E, October 1994.

[B15] ITU RS. *Vocabulary of Terms for FPLMTS (FPLMTS.TMLG).* 8-1/TEMP/95, October 1994.

[B16] ITU CCITT Series E Recommendations (E.401-E.880). *International telephone network management and checking of service quality.*

[B17] ITU CCITT Series F Recommendations (F.160-F.730). *Telematic, data transmission and teleconference services: Operations and quality of service.*

[B18] ITU CCITT. Series I of Recommendations (I.110-I.257). *Integrated services digital network (ISDN).*

[B19] ITU TS. Recommendation F.115. *Operational and Service Provisions for FPLMTS*, Version 6, 1994

[B20] ITU CCITT Recommendation Q.1202, *Intelligent network service plane architecture*.

[B21] ITU CCITT Recommendation Q.1203, *Intelligent network global functional plane architecture.*

[B22] ITU CCITT Recommendation Q.1204, *Intelligent network distributed functional plane architecture.*

[B23] ITU CCITT Recommendation Q.1211, *Introduction to intelligent network capability set 1*.

[B24] ITU CCITT Recommendation Q.1213, *Global functions for intelligent network capability set 1.*

[B25] ITU CCITT Recommendation Q.1214, *Distributed functional plane for intelligent network capability set 1.*

[B26] ITU CCITT Recommendation Q.1218, *Interface recommendations for intelligent network capability set 1.*

[B27] ITU CCITT Recommendation Q.1290, *Glossary of terms used in intelligent networks.*

[B28] ITU CCITT Recommendation X.411-1988, *Message Handling Systems: Message Transfer System: Abstract Service Definition and Procedures*, 1988.

[B29] ITU CCITT Recommendation X.509-1988, *The Directory: Authentication framework,* 1988.

[B30] ITU RS. *Working Document Towards New Recommendation: Security Mechanisms and Operating Procedures for FPLMTS (FPLMTS.SECMOP).* 8-1/TEMP/79-E. October 1994.

[B31] ITU RS. *Working Document Towards Draft Recommendation on radio-related functions for FPLMTS (FPLMTS.RRF).* 8-1/TEMP/68-E. October 1994.

[B32] ITU RS. *Key Choices of Technologies for the Radio Interfaces of FPLMTS (FPLMTS.RKEY).*

9.3 ANSI

[C1] ANSI Standard X3.92-1981. *Data Encryption Algorithm*.

[C2] ANSI Standard X3.106-1983. *Date Encryption Algorithm: Modes of Operation*.

[C3] ANSI Standard X9.9-1986. *Financial institution message authentication (wholesale)*.

[C4] ANSI Standard X9.17-1985. *Financial institution key management (wholesale).*

[C5] ANSI Standard X9.19. *Financial institution retail message authentication.*

[C6] ANSI Standard X9.24. *Financial services: Retail key management*.

[C7] ANSI Standard X.9.30. *Public-key cryptography using irreversible algorithms for the financial services industry: Part 3: Certificate management for DSA.* N10.93, March 1993.

9.4 ISO

[D1] ISO 7498-2. *Information processing systems - Open Systems Interconnection - Basic reference Model - Part 2: Security Architecture*. 1989.

[D2] ISO 8730. *Banking - Requirements for message authentication*. 1986.

[D3] ISO 8731-1. *Banking - Approved algorithms for message authentication - Part 1: DEA*. 1987.

[D4] ISO 8731-2. *Banking - Approved algorithms for message authentication - Part 2: Message authenticator algorithm*. Second edition, 1992.

[D5] ISO 8732. *Banking - Key management (wholesale)*. 1988.

[D6] ISO/IEC 9796. *Information technology - Security techniques - Digital signature scheme giving message recovery*. 1991.

[D7] ISO/IEC 9797. *Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.* Second edition, 1994.

[D8] ISO/IEC 9798-1. *Information technology - Security techniques - Entity authentication mechanisms - Part 1: General model*. 1991.

[D9] ISO/IEC 9798-2. *Information technology - Security techniques - Entity authentication - Part 2: Mechanisms* *using symmetric encipherment algorithms*. 1994.

[D10] ISO/IEC 9798-3. *Information technology - Security techniques - Entity authentication mechanisms - Part 3: Entity authentication using a public key algorithm*. 1993.

[D11] ISO/IEC 9798-4. *Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function*. 1995.

[D12] ISO/IEC 9979. *Data cryptographic techniques - Procedures for the registration of cryptographic algorithms*. 1991.

[D13] ISO/IEC 10116. *Information technology - Modes of operation for an n-bit block cipher algorithm*. 1991.

[D14] ISO/IEC 10118-1. *Information technology - Security techniques - Hash-functions - Part 1: General*. 1994.

[D15] ISO/IEC 10118-2. *Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher algorithm*. 1994.

9.5 NIST/NBS

[E1] National Bureau of Standards, Federal Information Processing Standards Publication 46. *Data Encryption Standard (DES)*. 1980.

[E2] National Bureau of Standards, Federal Information Processing Standards Publication 81. *DES modes of operation*. 1980.

[E3] National Institute of Standards and Technology, Federal Information Processing Standards Publication 180. *Secure Hash Standard*. 1993.

[E4] National Institute of Standards and Technology, Federal Information Processing Standards Publication 186. *Digital Signature Standard*. 1994.

9.6 LINK 3GS3

[F1] DTI/EPSRC LINK PCP 3GS3. *Security Mechanisms for Third-Generation Systems.* Technical Report 2, Version 3, 14 February 1996.

[F2] DTI/EPSRC LINK PCP 3GS3. *Security Architecture for Third-Generation Systems.* Technical Report 3, Version 3, 14 February 1996.

10 Abbreviations

ACCF	Access and Call Control Function
AdC	Administration Centre
ANSI	American National Standards Institute
AuC	Authentication Centre
BC	Bearer Control
BSS	Base Station Subsystem
CCF	Call Control Function
DECT	Digital European Cordless Telephone
DTMF	Dual Tone Multi Frequency
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
FE	Functional Entity
FPLMTS	Future Public Land Mobile Telecommunications System
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSCSD	High Speed Circuit Switched Data
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IN	Intelligent Networks
ISDN	Integrated Services Digital Network
ISO	International Standards Organisation
ITU	International Telecommunications Union
LE	Local Exchange
MCCF	Mobile Call Control Function
MCF	Mobile Control Function
MRRC	Mobile Radio Release Control
MRTR	Mobile Radio Transmission and Reception
MSF	Mobile Storage Function
NIST	National Institute of Standards and Technology (US)
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PMR	Private Mobile Radio
PPC	Pre-Personalisation Centre
PSTN	Public Switched Telephone Network
PUK	PIN Unblocking Key
RBC	Radio Bearer Control
RFTR	Radio Frequency Transmission and Reception
RRC	Radio Resource Control
SCEF	Service Creation Environment Function
SCF	Service Control Function
SCP	Service Control Point
SDF	Service Data Function
SDP	Service Data Point
SIM	Subscriber Identity Module
SMAF	Service Management Access Function
SMF	Service Management Function
SMG	Special Mobile Group
STC	Sub Technical Committee
TC	Technical Committee
TMN	Telecommunications Management Network
TMSI	Temporary Mobile Subscribers Identity
UIM	UMTS Identity Module
UMTS	Universal Mobile Telecommunications System

UPT	Universal Personal Telecommunications
VLR	Visitor Location Register

Appendix A: Description of functional entities

This appendix contains descriptions of the basic IN functional entities.

Functions related to service management

These functions support service creation, service provision, customer control capabilities, and support for the administration, coordination and control of a data base.
SMF - Service Management Function: This function involves service management control, service provision control and service deployment control.
SMAF - Service Management Access Function: This function provides an interface (e.g. screen presentation) to the SMF.
SCEF - Service Creation Environment Function: This function allows a service to be defined, developed, tested and input to the SMF. The output of this function involves service logic and service data templates.

Functions related to service control

These functions provide the control of the supported services and capabilities. Together they form what could be regarded as the "intelligent" part of a network. Specifically, the mobile environment and mobility services are supported by these functions.
SDF(M) - Service Data Function (Mobile): This function handles storage and access to service related data and network data and provides consistency checks on data. It hides from the SCF the real data implementation and provides a logical data view to SCF. The suffix (M) is included to indicate that this is a mobile related functionality which may differ from the SDF associated with fixed network developments.
In general the SDF(M) includes functionalities to:
- store service and mobility related data, e.g.:
- location information;
- service profile;
- security related parameters;
- check data consistency;
- initiate data up-dating (e.g. security parameter download).

As indicated, the SDF(M) will contain more functionalities than pure data storage. It must also contain functions for some data management, e.g. to request for more data from another SDF, and SCF or an SMF in case it is running out of data (e.g. security parameter sets) or to update dependent SDFs in case some basic data is changed (e.g. to update a visited SDF(M) in case the service profile is changed in the (home) service providers SDF(M).
Note: In a mobile network consisting of several UMTS, it may be necessary to differentiate between (home) the service providers and visited SDF(M)s. However, in a functional model no such distinction is made.

SCF(M) - Service Control Function (Mobile): This function contains the overall service logic, mobility control logic and handles service related processing activity. It supports all mobile specific functions and provides overall service control. Service logic is invoked by service requests from other functionalities to support location management, security management and user service control as defined.

The suffix (M) is included to indicate that this is a mobile related functionality which may differ from the SCF associated with fixed network developments.

In general the SCF(M) includes the following functionalities:
- paging control (e.g. initiate paging, process paging response);
- service feature analysis (e.g. compatibility checking);
- provide routing information;
- perform location management;
- perform identity management;
- subscriber verification;
- subscriber authentication;

- authentication processing;
- confidentiality control (e.g. ciphering management).

The SCF is involved in certain cases of handover, for example: inter ACCF.
Note: The need to define a paging control functional entity separate from SCF(M), specifically in a scenario with paging via a separate radio access system, is for further study.

MSF - Mobile Storage Function: This is a pure data storage function at the mobile side of the radio interface. In addition to subscription or service related parameters it stores:
- location information, and,
- identity and security related parameters.

MCF - Mobile Control Function: This function contains the service logic and service related processing required at the mobile side of the radio interface. It supports all mobile specific functions (e.g. location management, mobility management, identity management) and provides local service control.
In general the MCF includes the following functionalities:
- network information monitoring and analysis;
- location up-date initiation;
- authentication processing;
- confidentiality control (e.g. ciphering management);
- paging recognition and response.

Functions related to access, call and bearer control

This group of functions encompasses all handling of the physical communication resources. This includes both the radio resources used between the mobile stations and the network, and the fixed network resources used for mobile related transactions.

In the model, the call control logic is separated from the physical bearer control itself. At the fixed network side, this is not significant, i.e. CCF and BC functionalities could well be combined. However, at the radio side there has to be a physical distribution of at least the radio emission and reception functionalities due to the necessary physical distribution of cells. Therefore, the model has been fitted to support such a physical distribution of functionalities.
ACCF - Access and Call Control Function: The basic task of the ACCF is to establish (based on instructions from SCF(M)) a call to the distant end of a network and to associate radio and network node resources to the call.
In general the ACCF includes the following functionalities:
- analyse and process mobile service requests;
- establish, manage and release a call;
- call control adaptation between UMTS and PSTN/ISDN;
- maintain network call states;
- invoke service logic (e.g. request for routing information);
- provide special resources;
- request for allocation of radio resources;
- request for allocation of network resources;
- inter-RRC hand-over execution (inter-and intra-ACCF);
- provide information relevant to charging;
- ciphering and deciphering execution, for encryption across shared access network.

BC - Bearer Control: This function controls the bearer connection elements in order to provide the bearer service requested by the ACCF. In general it includes the following functionalities:
- select and create/delete bearer resources;
- connect, maintain and disconnect bearer connections;
- perform routing for network side bearer connections;
- provide information relevant for charging.

RRC - Radio Resource Control: This function handles the overall control of the radio resources and radio connections within a given area (typically many cells).
In general the RRC includes the following functionalities:
- radio channel management (including access control);
- radio channel supervision (including assessment of radio channel measurement results from RFTR);
- radio channel power control;

- analysis of mobile radio environment reports;
- hand -over initiation due to changes in radio environment (inter-and intra-RRC);
- intra-RRC hand-over execution;
- system information broadcast management (radio access information and network information);
- paging execution.

Note: It may be appropriate to define a paging execution functional entity separate from RRC, specifically in a scenario with paging via a separate radio access system.

RBC - Radio Bearer Control: This function is closely related to the RRC. It connects, maintains and disconnects radio bearer connections and interconnects them with the fixed network bearer resources.

RFTR - Radio Frequency Transmission and Reception: Typically, this function will manage the radio resources available within a single cell. It includes the following functionalities:

- RF generation, emission and reception including:
- source (e.g. speech) coding and decoding;
- error protection coding and decoding;
- ciphering and deciphering;
- baseband channel multiplexing and demultiplexing;
- modulation and demodulation;
- RF carrier multiplexing and demultiplexing;
- RF amplification;
- initial (random) access detection;
- radio and network channel interworking;
- radio channel measuring and reporting;
- power control execution.

MCCF Mobile Call Control Function: This function will handle the mobile side of access control and call control and is responsible for initiating functional requests based on requests from the user or other functional entities. In general the MCCF includes the following functionalities:

- maintain mobile side call states;
- formulate service requests;
- call control adaptation between UMTS and PSTN/ISDN.

MRRC - Mobile Radio Resource Control: This function handles the mobile side of the radio connection. In general it includes the following functionalities:

- radio channel supervision;
- local radio environment reporting (if mobile assisted or mobile controlled handover);
- handover initiation (if mobile controlled handover);
- radio access information monitoring and analysis.

MRTR - Mobile Radio Transmission and Reception: This function handles the radio transmission and reception on the mobile side. It includes the following functionalities:

- RF generation, emission and reception including:
- source (e.g. speech) coding and decoding;
- error protection coding and decoding;
- ciphering and deciphering;
- baseband channel multiplexing and demultiplexing;
- modulation and demodulation;
- RF carrier multiplexing and demultiplexing;
- RF amplification;
- radio channel measurements;
- power level adjustment.

Appendix B: Services

This appendix comprises a list of services to be supported by UMTS. This list is taken directly from [A11]. It is not claimed to be exhaustive.

Bearer Services Provided by Fixed Networks

Preliminary ISDN Bearer Services

Services in this subsection either exist as standards or are currently in the process of being standardised ([B16], [B17] and [B18]).

- Circuit Mode
    - unrestricted; 64, 2x64, 384, 1536, and 1920 kbps
    - suitable for speech information transfer
    - suitable for 3.1, 7, and 15kHz audio information transfer
    - alternate speech/unrestricted digital information
- Packet Mode
    - virtual call and permanent virtual call
    - ISDN connectionless
    - user signalling

B-ISDN Bearer Services

Services in this subsection are intended as standards ([B2]),

For further study.

Teleservices

Teleservices based on CCITT E, F, and I series, and existing in fixed networks

Services in this subsection either exist as standards or are currently in the process of being standardised (see CCITT series [B16], [B17] and [B18]).

- Telephone
    - speech
    - in-band facsimile
    - in-band modem
- teleconference
- high quality audio/speech
- message handling service
- teletex
- telefax
- videotex
- videotelephony
- videoconferencing

Teleservices for FPLMTS

Services in this subsection are intended as standards ([B2]).

- programme sound
- programme video
- paging
- audio-visual
- Short Messaging
    - user originated
    - user terminated

    - store and forward
        - voice mail
        - facsimile
        - electronic mail
- video surveillance/monitoring
- Broadcast services
    - message broadcast
    - multicast
    - SMS cell broadcast
    - emergency announcement
    - public announcement
    - dat broadcast/multicast

UMTS Specific Teleservices

Services listed in this subsection are intended as European standards (see [A11]).

- emergency call
- emergency broadcast
- high quality audio
- voice messaging
- voice mail
- Drive
    - localisation
    - congestion avoidance
    - navigation
- video monitoring
- Data Transfer
    - unrestricted
    - restricted
- multimedia/integrated voice and data

UMTS Applications

Services listed in this subsection are not intended to be standardised.

- database access
- Directory Services
    - telephone directory
    - classified directory
- Electronic Newspaper
    - news agency
    - news distribution
    - special needs news media
- Teleaction Services
    - remote control
    - remote terminal applications
- teleshopping

Appendix C: Document History

Release Dates

The first version of this document was released to the LINK PCP Committee on 4 February 1994, with a second version being released on 1 May 1995. This final version has a release date of 14 February 1996.

Document History

Date	**Version**	**Changes**
1 November 1993	v1 Draft 1	Initial Draft
23 December 1993	v1 Draft 2	Major Revisions made independently by all partners.
18 January 1994	v1 Draft 3	Further major restructuring and revision by responsible partner (Vodafone).
28 January 1994	v1 Draft 4	Contains minor structural and typographic changes throughout.
4 February 1994	v1 Final	Contains minor typographic changes.
21 November 1994	v2 Draft 1	Additional material included.
23 December 1994	v2 Draft 2	Aligned text on security features, threats and requirements with corresponding tables.
23 January 1995	v2 Draft 3	Contains minor structural and typographic changes throughout.
1 May 1995	v2 Final	Contains minor changes to the executive summary.
19 December 1995	v3 Draft 1	Additional material included, existing material updated.
8 January 1996	v3 Draft 2	Contains minor typographic changes throughout.
14 February 1996	v3 Final	Contains minor typographic changes throughout.