LINK Personal Communications Programme

# Third Generation Mobile Telecommunications Systems Security Studies

## Technical Report 3:

# Security Architectures 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 3:
Security Architectures for Third Generation Systems
Final Version

**Responsible Partner:**

GPT Ltd.

**Contributors:**

Ms. Marion Borman (GPT)
Dr. Liqun Chen (RHUL)
Mr. Peter Creteau (GPT)
Dr. Raymond Forbes (GPT)
Dr. Nigel Jefferies (Vodafone)
Prof. Michael Walker (Vodafone)
Dr. Jason Brown (Vodafone)
Dr. Dale Youngs (Vodafone)
Ms Stephanie Manning (Vodafone)

**Approved for Distribution:**

.......................................................... Dr. Raymond Forbes
(Partner Manager)

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

**0. EXECUTIVE SUMMARY .......... 5**

1. **INTRODUCTION .......... 6**

2. **SECURITY CONTEXT : ENVIRONMENTS .......... 7**

2.1 INTRODUCTION .......... 7
2.2 OPERATING ENVIRONMENTS .......... 7
  *2.2.1 Terminal .......... 9*
  *2.2.2 Access Network .......... 9*
  *2.2.3 Core Network .......... 9*
  *2.2.4 Satellite Access .......... 10*

**3. ARCHITECTURE ..........** Error! Bookmark not defined.

3.1 INTRODUCTION .......... 11
3.2 OBJECTIVES OF INTELLIGENT NETWORKS (IN) .......... 11
3.3 DEFINITION OF IN .......... 11
  *3.3.1 Standards - Proposed Security Requirements for IN .......... 12*
  *3.3.2 IN framework for the functional model .......... 12*
3.4 FUNCTIONAL ARCHITECTURE .......... 13
  *3.4.1 Description of additional Functional Entities .......... 14*
  *3.4.2 Functional entities with security related capability .......... 15*
3.5 PHYSICAL ARCHITECTURE .......... 17

4. **MANAGEMENT AND SECURITY .......... 19**

4.1 OBJECTIVES OF TMN .......... 19
  *4.1.1 Definition .......... 19*
  *4.1.2 Functions associated with TMN .......... 19*
  *4.1.3. TMN Functional Architecture .......... 20*
  *4.1.4. TMN Function Blocks .......... 20*
4.2 SERVICE MANAGEMENT - AN IN VIEW .......... 21
  *4.2.1 Definition .......... 21*
  *4.2.2 Functional Entities for Service Management - IN view .......... 22*
4.3 USAGE OF RELATIONSHIP REFERENCE POINTS .......... 24
  *4.3.1 SMAF Relationships .......... 24*
  *4.3.2 SMF Relationships .......... 26*
4.4 INTEGRATION OF SECURITY SERVICE MANAGEMENT WITHIN TMN .......... 27
  *4.4.1 Categories of Security Management .......... 27*
  *4.4.2 Mapping of Security Management to TMN .......... 28*
  *4.4.3 Common Security Data to be Managed .......... 28*
4.5 THREATS TO SERVICE MANAGEMENT RELATIONSHIPS .......... 29
  *4.5.1 Misuse .......... 29*
  *4.5.2 Threats to SMAF .......... 29*
  *4.5.3 Threats to SMF .......... 30*
4.6 SECURITY FEATURES FOR SERVICE MANAGEMENT .......... 30
  *4.6.1 Proposed Access Control for Service Management. .......... 31*
4.7 MANAGEMENT FUNCTIONS FOR SECURITY FEATURES .......... 33
  *4.7.1 System Security Management Activities .......... 33*
  *4.7.2 Security Service Management .......... 34*
4.8 MANAGEMENT OF SECURITY MECHANISMS: A 3GS3 VIEW .......... 34
  *4.8.1 Introduction .......... 34*
  *4.8.2 Service-related Authentication and Key Distribution .......... 35*
  *4.8.3 Identity and Location Privacy .......... 36*
4.9 CONCLUSION .......... 37

5. **CHARGING AND ACCOUNTING SECURITY NEEDS .......... 38**

5.1 CATEGORIES OF CHARGING .......... 38

5.2 CHARGING IN A MANAGEMENT DOMAIN ........ 38
5.3 INTER-OPERATOR TMN CHARGING RELATIONSHIPS FOR UMTS ........ 38
*5.4.1 Off-Line ........ 44*
*5.4.2 On-Line ........ 45*
5.5 ISSUES ........ 45
5.6 CHARGING SCENARIOS OF 3GS3 OFF-LINE CASES ........ 45
*5.6.1 Outgoing Calls ........ 45*
*5.6.2 Incoming Calls ........ 47*
*5.6.3 Registration/De-registration for UPT user ........ 47*
*5.6.4 Location Registration ........ 48*
*5.6.5 Record Content ........ 50*
5.7 OWNERSHIP ........ 51

6. **INFORMATION FLOWS ........ 54**

6.1 SUPPORT OF AUTHENTICATION PROCEDURES ........ 54
*6.1.1 Assumptions ........ 54*
*6.1.2 Access Network Signalling ........ 54*
*6.1.3 Functional Structure in core network ........ 54*
*6.1.4 Mutual Authentication Information flows ........ 56*
6.2 SUPPORT FOR UIM DATA AND UIM MANAGEMENT ........ 61
*6.2.1 Assumptions ........ 61*
*6.2.2 UIM and Mobile Station Interaction ........ 62*
*6.2.3 UIM/Terminal Interface Issues ........ 63*
*6.2.4 Summary ........ 63*
6.3 SUPPORT FOR IDENTITY PASSING ........ 64
*6.3.1 Scenarios for transmitting line identities ........ 64*
6.4 SUPPORT FOR LEGAL INTERCEPTION REQUIREMENTS ........ 65
*6.4.1 Introduction ........ 65*
*6.4.2 Problems and Effects on the Network ........ 65*
*6.4.3 Conclusion ........ 66*

7. **FRAUD INDICATORS ........ 68**

7.1 INTRODUCTION ........ 68
7.2 IDENTIFICATION OF POTENTIAL FRAUD INDICATORS ........ 68
7.3 CLASSIFICATION OF INDICATORS BY TYPE ........ 68
*7.3.1 Usage Indicators ........ 68*
*7.3.2 Mobility Indicators ........ 70*
*7.3.3 Deductive Indicators ........ 73*
7.4 CLASSIFICATION OF INDICATORS BY USE ........ 73
7.5 SUMMARY OF USEFUL INDICATORS ........ 75
7.6 MEASUREMENT OF INDICATORS ........ 76
7.7 FRAUD DETECTION IN GSM AND UMTS/FPLMTS ........ 77
*7.7.1 GSM Fraud Detection ........ 77*
*7.7.2 UMTS/FPLMTS Fraud Detection ........ 77*

8. **REFERENCES AND BIBLIOGRAPHY ........ 79**

**9. ABBREVIATIONS ........ 80**

**10. APPENDIX ........ 82**

**APPENDIX A SECURITY REQUIREMENTS OF CO-OPERATING IN ENTITIES INSIDE A MANAGED DOMAIN**

**APPENDIX B REFERENCE POINTS BETWEEN THE MANAGEMENT FUNCTION BLOCKS**

**APPENDIX C DOCUMENT HISTORY**

# 0. Executive Summary

This report is the third deliverable from the DTI/EPSRC LINK Personal Communications Programme project *'Security Studies for Third Generation Mobile Telecommunications Systems'*. 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 highlight some areas where the security features, mechanisms and infrastructure elements need to be standardised.

During the first year of the project (February 1993-January 1994) the work of the project was dominated by major contributions to, and the continuing influence of, standardisation activity within ETSI SMG5 (UMTS) and ITU TG 8/1 (FPLMTS). This work culminated in the production of the Technical Report 1 [1], the first project deliverable, dealing with the first of the above projective objectives.

During 1994 the project moved on to a more intensive study of the second of the project objectives, namely a consideration of security mechanisms to support various of the security features required in third generation mobile telecommunications systems. This work culminated in the production of the of Technical Report 2 [2], dealing with the second of the above objectives.

Also, during 1994 the project began its studies towards the specification of the third of the project objectives. Specifically, a consideration of security architecture to support various of the security mechanisms and management requirements required in third generation mobile telecommunications systems. This report describes the results of this work, considers in detail how security architecture can be used to provide for some of the more problematic of the security mechanisms and management requirements required for third generation systems.

In 1995 the actual uses of security mechanisms were considered and the legal and technical implications covered in some detail. These uses included the detection of the fraudulent use of mobile phones and also the necessity of catering for legal interception when considering mobile security mechanisms.

The report begins, in Section 2, with a brief summary of the security context and environments that require consideration in a likely physical architecture from the features identified in Technical Report 1, for third generation systems. Section 3 gives a general introduction to security architecture, and is intended to provide a general motivation for the specific elements of the architectural approach considered in detail in subsequent sections of this report. Section 4, contains the results of the studies on management and security. In Section 5, the problem of providing security necessary to provide for the requirements of charging and accounting is considered, outlining means for providing this security. Section 6 outlines the information flows required to provide a number of security features. Finally Section 7 provides a general indication of fraud requirements which need to be considered.

The report is a detailed description of the results obtained by the project, and indicates possible areas of future work.

# 1. Introduction

The main purpose of this document is to consider the likely security architecture appropriate for providing certain security features and mechanisms, including management features, to be supported by third-generation mobile telecommunications systems (3GS). The features considered are those whose provision appears likely to be most difficult or most relevant for architectural integrity. This includes those security aspects either catered for by architectural aspects in use in first and second generation mobile telecommunications systems which may no longer be appropriate, or which are not provided for in existing systems.

The main security aspects for which architectural aspects are examined in detail are as follows.

- Environments and resultant aspects which result in security implications, including the user, network and service provision environments.
- Architectural entities and the relationships between these elements, including the identification of interfaces and the resolution of the security threats imposed by these interfaces.
- Aspects resulting from management activities using identified interfaces, including management of security mechanisms.
- Aspects resulting from the collation of charging records and the passing of accounting information.
- Requirements on mechanisms in the form of information flows.
- Basic indications of the areas where fraud must be detected to enable it to be monitored.

Before proceeding, the structure of this document is now described in more detail, outlining the contents and status of each section in turn.

To put the work described in this report into context, Section 2 reviews briefly the environments and security context likely to be required for 3GS. A complementary description of the security context likely to be appropriate for 3GS can be found in 3GS3 Technical Report 1 [1].

In Section 3 we make some general observations about system architecture for 3GS, including criteria seen from a security perspective, also giving reasons why certain aspects are considered relevant for further study.

In Section 4 we consider security and management aspects in some detail, including both the security of management and the management of security.

Charging and accounting specific issues are the main concern of Section 5.

Section 6 considers the requirements on protocols for a number of procedures described in terms of information flows.

Section 7 considers some basic indicators of fraud detection and outlines mechanisms to monitor and circumvent fraud.

A brief bibliography is given in Section 8 followed by a table of abbreviations in Section 9.

# 2. Security Context : Environments

## 2.1 *Introduction*

In considering a security architecture for third generation systems, the operating environments must be considered since they have a direct bearing on the security of the system. Third generation systems like UMTS, as defined by ETSI, and FPLMTS, as defined by the ITU, encompasses several different environments and these are indicated in the following text.

## 2.2 *Operating Environments*

The support of the UMTS service environment results in a set of considerations and service features. This includes interworking with the services of existing networks and support of personal mobility.

The extension of fixed network services and the provision of additional services by means of a radio link requires special attention to be paid to the following:

1. For access to the fixed networks: UMTS may be either an adjunct to or an integral part of the PSTN/ISDN. Services offered in the PSTN/ISDN should, as far as possible, be offered to UMTS users.

2. For International Operation: UMTS should allow international operation and automatic roaming of mobile users and stations to the extent practical or permitted.

3. For Maritime and Aeronautical: UMTS should allow operation in the maritime and aeronautical environment to the extent permitted by national and international regulatory authorities.

4. For Satellite Systems: UMTS should allow operation either directly or indirectly via satellite.

5. Served Environments: UMTS should allow access in a wide variety of different environments including; sparse areas (deserts and oceans), rural areas (including coastal and off-shore), hilly terrain, suburban areas, urban areas, dense areas (railway concourses, shopping centres, office complexes, etc.), high-speed corridors (motorways and railway lines), indoor and outdoor environments.

Elaborated into some detail, the operating environments for UMTS include:

A. Residential
B. Indoor office
C. Vehicle with Mobile Base Station
D. Mobile Vehicle
E. Pedestrian
F. Rural and Remote

6. UMTS should provide service to stationary and mobile users whether pedestrians or travelling in cars, lorries, buses, trains, ferries ships or aircraft. Allowing a variety of speeds from stationary users to users on high speed trains, currently up to 300km/h
A composite of the operating environments are illustrated in figure (1).

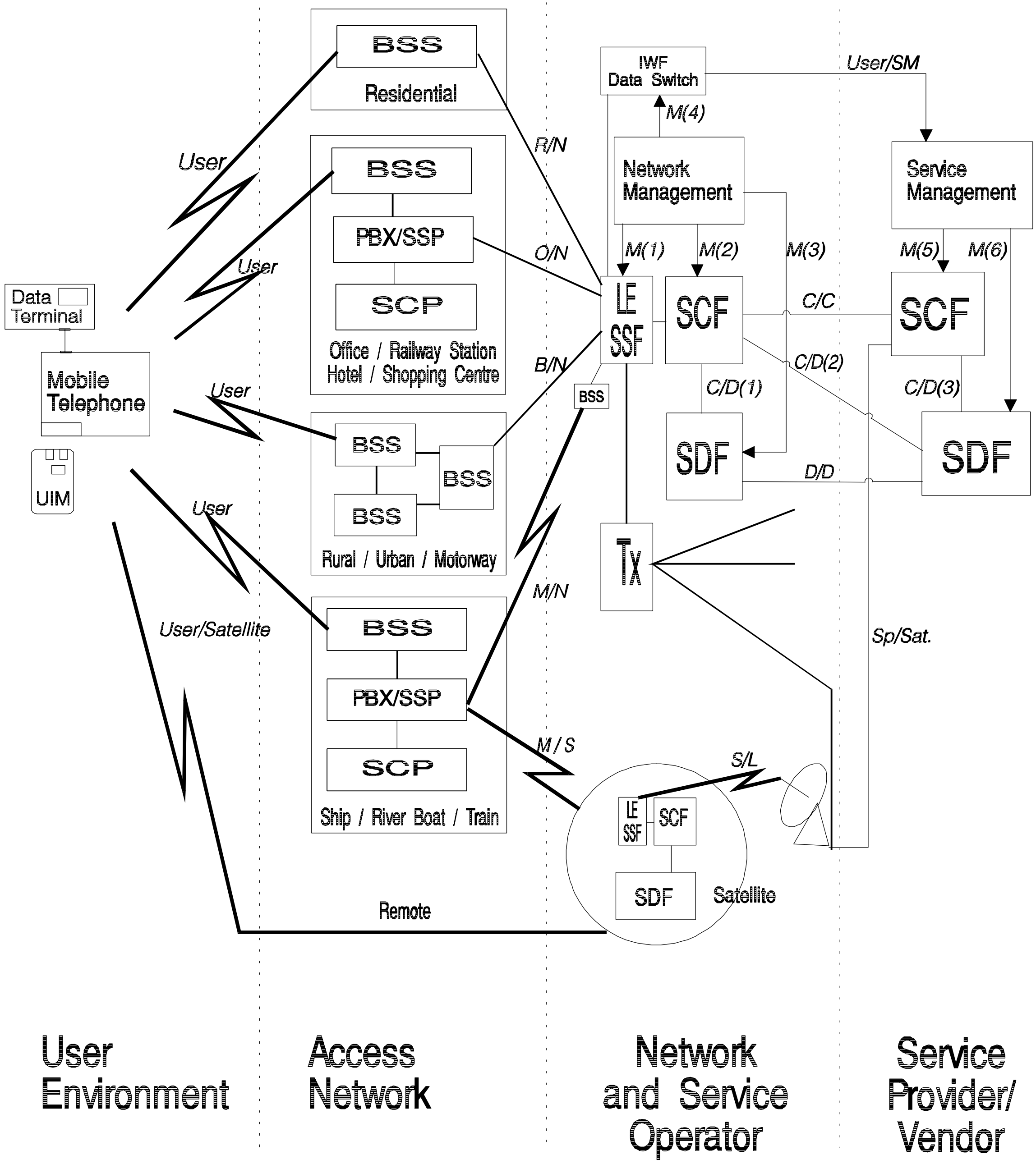


**Figure 1: Operating Environments**

Each environment of figure 1 may be considered for convenience to have a structure consisting of the following:

- Terminal
- Access Network
- Core Network
- Satellite Access.

This enables implementations of UMTS in a particular environment to be modelled. Figure 2 represents such a model.

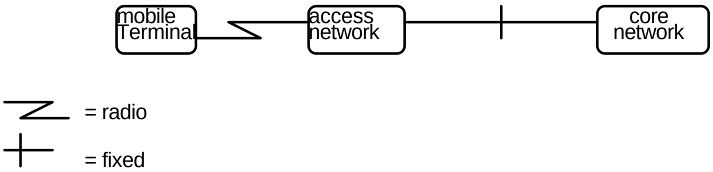


**Figure 2: Structure of a Mobile Network**

### 2.2.1 Terminal

Terminals provide the mobility of access to users. They could be attached by radio or fixed line to mobile networks, or by radio to private and public networks, or by satellite. These terminals and their functional groupings depend on the environment, for example, fixed terminal connected to a mobile termination unit (MTU) providing transceiving capability to the access network. Other cases could be a switching capability (PBX) at the terminal side of the radio path. All of these interconnections carry information that needs to be secure from eavesdroppers and misuse.

### 2.2.2 Access Network

The access network can be either a public or private network. Different mobile adaptation units to cater for the interface structures might be required. Such environments could have mobility and switching functions included in the domestic and business environment. An example is shown in figure 3.

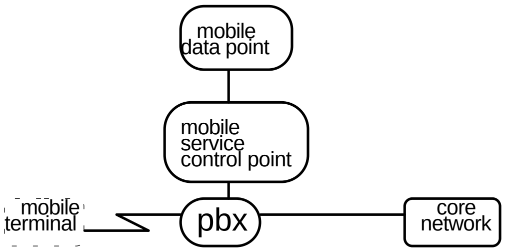


**Figure 3: Private and Business Environment**

There are other configurations, for example, in the private environment they may only have a mobile control point in which the service data is held and in the business environment a PBX may exist. In both cases the user data and mobility functions being held in the core network. Such configurations require user privacy and confidentiality of information for ‘home’ or visiting users.

### 2.2.3 Core Network

The core network is usually in the public environment. The network can be a public switched telephone network (PSTN) or an integrated service digital network (ISDN), whose functionality must enable mobile users to exist within them or traverse such networks to adjacent ones. To achieve this capability with minimum change, the network uses the intelligent network concepts and functionality, see Section 3 for a functional description. The access capabilities of the network can vary from simple to complex, for example, basic mobility functions (i.e. control functions and functions related to the radio transmission/reception) can be handled by a base station for low traffic situations but additional mobility functions such as user authentication, location management, handover etc., are handled by the core network.

### 2.2.4 Satellite Access

The satellite architecture will have a strong impact on security. To some extent it determines what is necessary and what is possible as far as security is concerned.

Three configurations are defined by the capabilities of the constituent satellites:

- **Dumb Repeater Configuration**

  In this configuration, each satellite acts as a simple relay or repeater. The only functions performed are amplification and frequency shifting. No routing is performed by the satellite and in general inter-satellite traffic is not possible.

- **Processing Configuration**

  This is an intermediate case in which the each satellite performs some on-board processing which is more complicated than in the ‘dumb repeater’ configuration. For example, this processing may involve a full demodulation and decoding of the received signal, baseband processing followed finally by coding and modulation before re transmission. Again, no routing is performed by the satellite and in general inter-satellite traffic is not possible.

- **Switching Configuration**

  In this configuration, each satellite can make an intelligent decision as to where to (selectively) route a particular transmission. The satellite by definition has to be capable of full demodulation, decoding and interpretation of at least part of individual transmissions in order to perform the routing function. The principal application of this routing is to facilitate inter-satellite traffic.

# 3. Architecture

## 3.1 *Introduction*

The security architecture of a third generation mobile system relates to the way in which the component parts interrelate. The architecture refers to the logical structure of a system, rather than the specification details of the individual components used to construct the system. The logical structure for third generation mobile systems identifies the behaviour and relationships of the different functional entities in the different operating environments that go to make up the concept of UMTS or FPLMTS.

The security architecture thus describes where the features and mechanisms of authentication, access control, integrity etc., are logically located with respect to the functional entities in the model. These functional entities are mapped into necessary or likely physical entities such as a satellite, a private network, a base station controller, an ‘home’ database, call originating switch/node, or a visited switch/node. It is through these mappings of the functional into real “physical” environments that the real security threats occur and illustrate where the possible placement of security functions would be required.

This basic precept will be used starting with the functional model for third generation mobile systems and the security features as stated in the 3GS3 Technical Report 1[1], will be allocated according to the security requirements. This allocation will be limited to the IN structured core network types.

A brief introduction to the underlying Intelligent Network telecommunication principles are first given. For a more detailed introduction see [3], [4].

## 3.2 *Objectives of Intelligent Networks (IN)*

The objectives of IN are to provide additional capabilities to services and networks to make the provisioning of services implementation independent in a multi-vendor environment.

Service implementation independence allows Service Providers to define their own services independent of service specific developments by equipment vendors. This, in theory, allows services to be deployed quickly.

Network implementation independence allows Network Operators to allocate functionality and resources within their networks and to manage their networks independently of network vendors equipment.

These objectives apply to the needs of third generation mobile systems and the allocation of security services to such networks.

## 3.3 *Definition of IN*

In IN the operation and provisioning of services is characterised by :

- Modularisation and reusability of network functions
- integrated service creation and implementation
- flexible allocation of network functions to physical entities
- standardised communication between network features via service independent interfaces
- subscriber and user control of some of their service specific attributes
- service provider and network operator control of services and their network attributes
- standardised management of service logic.

IN, thus has the capabilities to allow implementation of mobility services for intra and inter networking and this includes the signalling and connection control aspects required for personal and terminal mobility.

### 3.3.1 **Standards - Proposed Security Requirements for IN**

ETSI have produced a set of security requirements for IN [5]. Their results are summarised in appendix A.

### 3.3.2 **IN framework for the functional model**

The framework arises out of the requirements to provide network capabilities for all users (service requirements), network operator needs (network requirements) and the evolution of IN through its various phases of development. The framework is called the IN Conceptual Model (INCM). It consists of 4 planes where each plane represents different abstract views of the capabilities of IN. These views address service aspects, the global functionality, distributed functionality and physical aspects of IN.

#### 3.3.2.1 ***Service plane***

The service plane expresses a service oriented view with no regard to implementation of the service in a network or across networks. All that is perceived by a user is the network service-related behaviour.

#### 3.3.2.2 ***Global functional plane***

The global functional plane models an IN-structured network as a single entity.

#### 3.3.2.3 ***Distributed functional plane***

The distributed functional plane models a distributed view of an IN-structured network. It contains functional entities which perform functional entity actions. These actions sometimes result in an information flow between entities. For more detailed information see [6].

#### 3.3.2.4 ***The Radio Resource Control Plane (RRCP)***

In order to accommodate the radio aspects of mobility a subplane, the Radio Resource Control Plane, has been introduced to the distributed functional plane allowing relationships to be created between the radio aspects and the main functional entities in the distributed functional plane [7].

The functions in the RRCP are in charge of control of the radio resources. This plane contains functional entities, (e.g. MRRC, MRTR, RFTR, RRC - these are defined in Appendix A of [1]) which are part of the radio access subsystem, two on each side of the radio interface i.e. mobile side and network side.

#### 3.3.2.5 ***Physical plane***

The Physical plane models the physical aspects of IN-structured networks. It contains the mappings of the functional entities from the distributed functional plane into realisable different physical entities, interfaces, and communication protocols that may exist in real IN-structured networks. For further details see [8].

The functional architectures from the distributed functional plane and the physical plane for third generation systems will now be considered.

## 3.4 *Functional Architecture*

In Technical Report 1 [1], section 4, a generic functional model and an IN access model are shown for the third generation mobile telecommunications systems. These models are still unstable, as far as the entities of the radio access parts of the model are concerned. These functional entities are described in [1] and will not be expanded on here.

Figure 4 shows the current version from the ITU -T FPLMTS standards [37], for IN based call and service control.

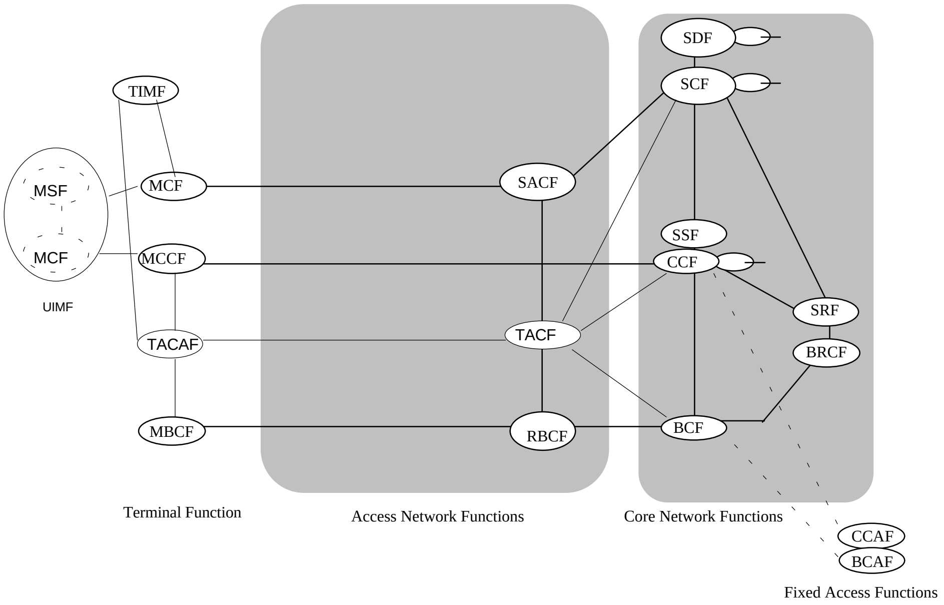


**Figure 4: IN/mobile functional model**

In the model a distinction has 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 for call and service control. The radio resource management entities are shown separately in figure 5.

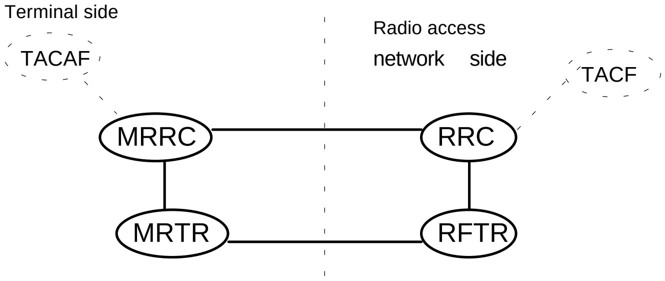


**Figure 5: Radio Resource Management and Control Entities**

The Service Management functions of SMF, SMAF, and SCEF, which are applicable to UMTS for the management of the mobile services as shown in figure 6 and will be considered in section 4 from a security point of view.

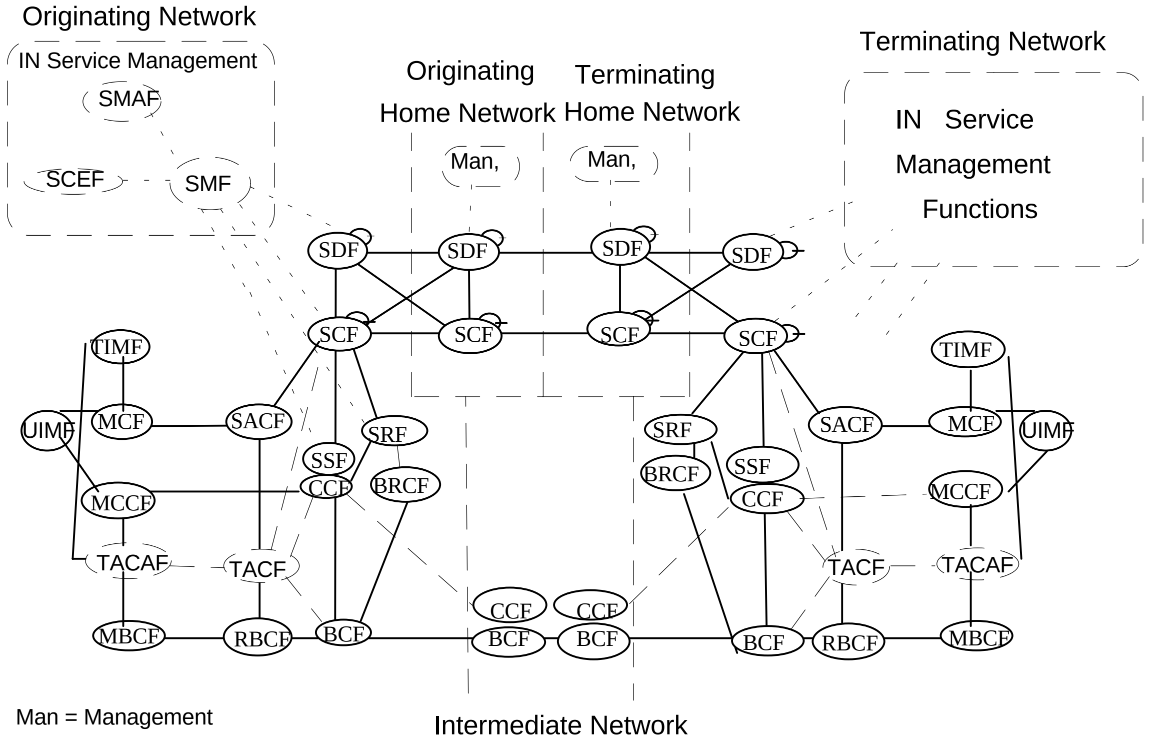


**Figure 6: A possible end-to-end service and control functional model**

### 3.4.1 Description of additional Functional Entities

Additional functional entities (FEs) to those shown in Technical Report 1 [1] have been added to the generic architecture. Such FEs as identified by ITU-T (FPLMTS model ) are as follows :

- Terminal Access Control Function (TACF) - provides the overall control of the access and connection between the mobile terminal and the network. It includes functionality to:
  - establish, maintain, modify and release the radio bearer connections between the terminal and network
  - trigger access to IN functionality
  - initiate paging execution, paging responses, detection and handling
  - interact with RRC regarding the assignment of radio resources
  - handover decision, execution and completion.

- Terminal Access Control Agent Function (TACAF) - This FE provides access for the mobile terminal. Its functionality includes:
  - interaction with the MBCF regarding the assignment of user bearers
  - interact with MRRC regarding the assignment of radio resources
  - paging detection, paging response interaction
  - relaying indications from the TACF to the rest of the terminal.

- Service Access Control Function (SACF) - This FE provides non-call and non-bearer associated control and processing, for example in relation to mobility management. It includes functionality to:

- establish, maintain, release instances of non-call associated messages requested by other functional entities e.g. in terminal location registration, or user requests to interrogate their profiles.
- manages the relationship between the MCF and the network for non-call/non-bearer associated interactions
- it also provides trigger mechanisms to access the IN functionality.

- Mobile Bearer Control Function (MBCF). - This FE is an agent function that controls the interconnection and adaptation of the radio bearers to the rest of the mobile terminal. In UMTS it also initiates the encryption procedures.

- Radio Bearer Control Function (RBCF) or (BCFr) - This FE controls the interconnection and adaptation of radio bearers to the corresponding fixed line bearers.

### 3.4.2 **Functional entities with security related capability**

The new functionality of interest to this study are the entities identifying security functions as part of their capabilities; such entities are listed here for convenience.

From the requirements and the current descriptions of the functional entities the appropriate FEs are grouped into:

#### 3.4.2.1 ***Functions related to the mobile terminal***

- Mobile Radio Transmission and Reception (MRTR): this entity has the security functionality of ciphering and deciphering for radio channels on the mobile side.

  The bearer control capability at the radio access is distributed between the functional entities of MBCF and RBCF where, MBCF is on the mobile side, and RBCF is in the fixed part of the radio access sub-network.

- The Mobile Bearer Control Function (MBCF): initiates encryption coding in UMTS, but is not identified as a function in FPLMTS

- The Mobile Control Function (MCF): contains the service logic and service related procedures on the mobile side for interacting with the terminal functional entities and SCAF to establish, maintain and release an instance of non-call/ non-bearer associated services e.g. registration, terminal location.
  Currently in FPLMTS, no security aspects are identified for MCF. However, in UMTS the functionality of CF include terminal authentication and ciphering management, see [37, 38].

- Terminal Identification Management Function (TIMF): as indicated in figure 4, provides the means to identify the mobile terminal to the network and /or the service provider. It stores the terminal identification information, security parameters e.g. keys, and provides functions for terminal authentication processing and responses, also generation of the ciphering key.

  Note: It should be noted this functionality differs from the ETSI proposals, in that Terminal authentication may not be required. In addition, the terminology and description of TIMF is still unstable in ITU at this time.

#### 3.4.2.2 ***Functions associated with the user of mobile terminal***

- The User Identification Management Function (UIMF), shown in figure 4, provides the means to identify the user to the network and service provider. It has as part of its functionality an MCF, which at subscription time acquires authenticating procedures, and associated data items e.g. private keys, PIN. They are stored in the mobile storage function (MSF) of the UIMF. The UIMF performs the user authentication processing and response to the network, including the generation of the ciphering key. See also the note associated with TIMF.

#### 3.4.2.3 *Functions related to the radio - access network*

- Radio Frequency Transmission and Reception (RFTR): This entity will manage the radio resources available in a single cell and has the security function of ciphering and deciphering including the handling of the radio transmission and reception of control and user information across the radio interface.

- The Radio Bearer Control Function (RBCF) or (BCFr): Initiates the encryption encoding, in UMTS functionality, but not identified in FPLMTS.

#### 3.4.2.4 *Functions related to the core network*

The basic IN functions of SDF, SCF are already described in TR 1, Appendix A [1]. They have already been allocated a suffix (M) to indicate that they have mobile related functionality which may differ from the SCF or SDF associated with fixed networks developments.

- In general the Service Control Function SCF (M) contains the overall service and mobility control logic and handles service related processing activities including, the security features of user verification, service related authentication and authentication processing, including confidentiality control (e.g. ciphering management).

- The Service Data Function SDF(M) stores service and mobile related data associated with security aspects of service profile, security related parameters (e.g. user private keys). The SDF(M) is also involved in checking data consistency, initiating security data updating, for example the management security parameter download.

#### 3.4.2.5 *Functions related to Service Management*

The security requirements of the service management FEs (SMF, SMAF, and SCEF) have not been identified and are for further study by the standards bodies. Section 4 highlights the need and suggests some possible security features.

#### 3.4.2.6 *Allocation of security features to functional model*

Following the analysis work of threats versus requirements and requirements versus security features as reported in the 3GS3 Technical Report 1 [1], and the functional entity descriptions as defined in [9] and [10], the security features of 3GS3 are allocated to the appropriate functions of the model, e.g. SCF, SDF. By this methodology the first steps towards a security architecture are considered.

From figure 4, the core part of the fixed network (the IN parts), will be considered first.

The core network functional entities of SDF, SCF, SRF, and SSF/CCF constitute the basic IN functionality, whose descriptions and relationships are defined in ETSI and ITU-T [3] and [4] respectively and TR1 [1]. The standards proposed security features applied to the relationships can be found in appendix A.

### 3.5 *Physical Architecture*

The mapping of the Functional Model to a Physical Model can be done in a variety of ways. The following diagrams give one illustration of how this can be achieved **-** the solid lined enclosures represent the physical entities and the dotted lines the associated functional entities.

The interfaces for functional authentication are shown as described in TR2 [2]. The physical interface illustrates how the functional interface may exist in reality. Where two or more functional entities exist within one physical entity the authentication may still be done as per the functional interface but the security will not need to be as tight. Where there is distance between the physical entities and thus more likely to be a loss of control of the interfaces, security will still be a major issue.

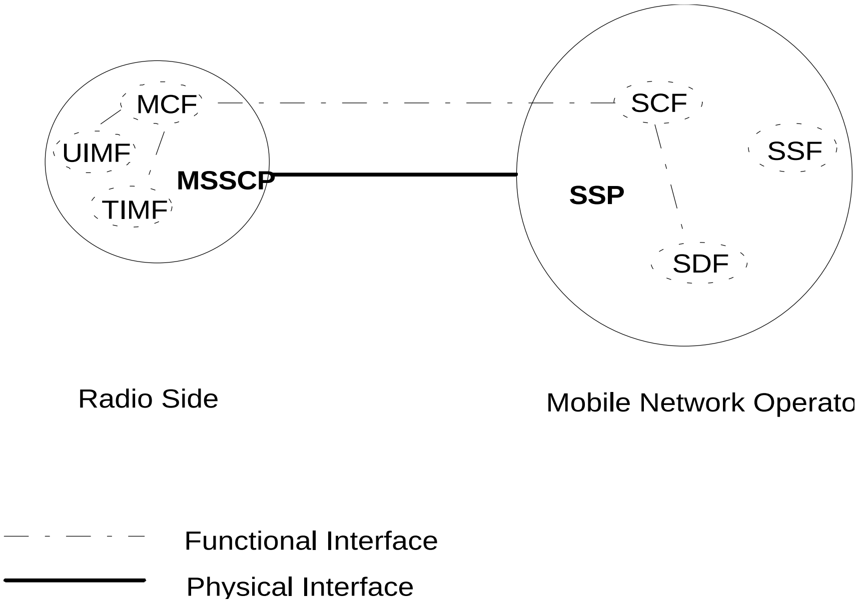


**Fig 7: Access Network - Authentication Option F1 of TR 2.**

The above diagram shows authentication of the user to the access network, including terminal authentication. The functional entity for the terminal (TACAF) could be included in the terminal itself and the TACF in the SSCP.

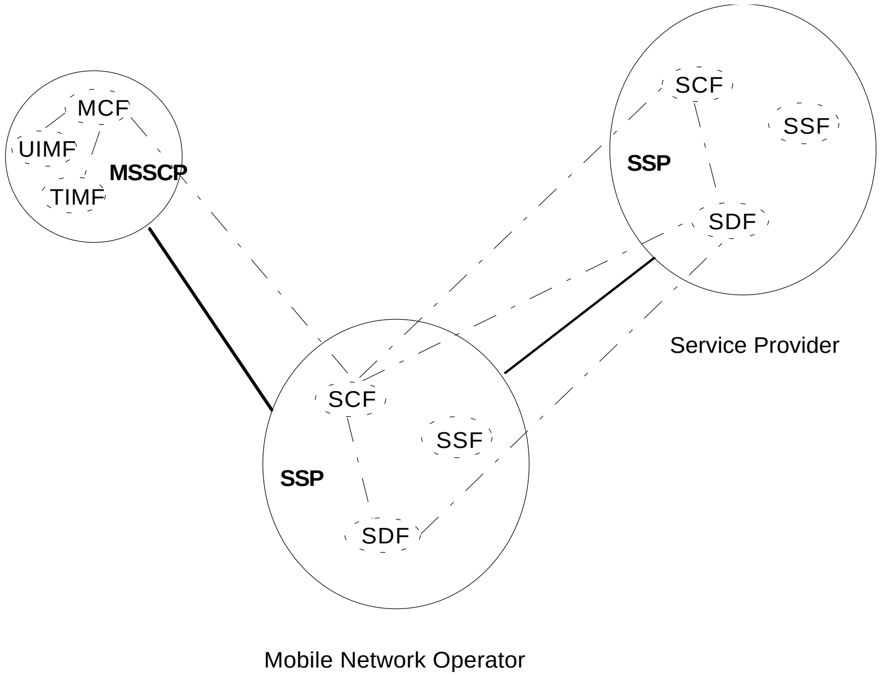


**Fig 8: Access/Core Network - Authentication Option F3 of TR 2.**

Figure 8 could show the authentication mechanism that takes place between the user and the access network, the user and the core network or the access network and the core network. As has been said before the implementation of this is variable.

Figure 9 shows one possible physical implementation of a third generation mobile network.

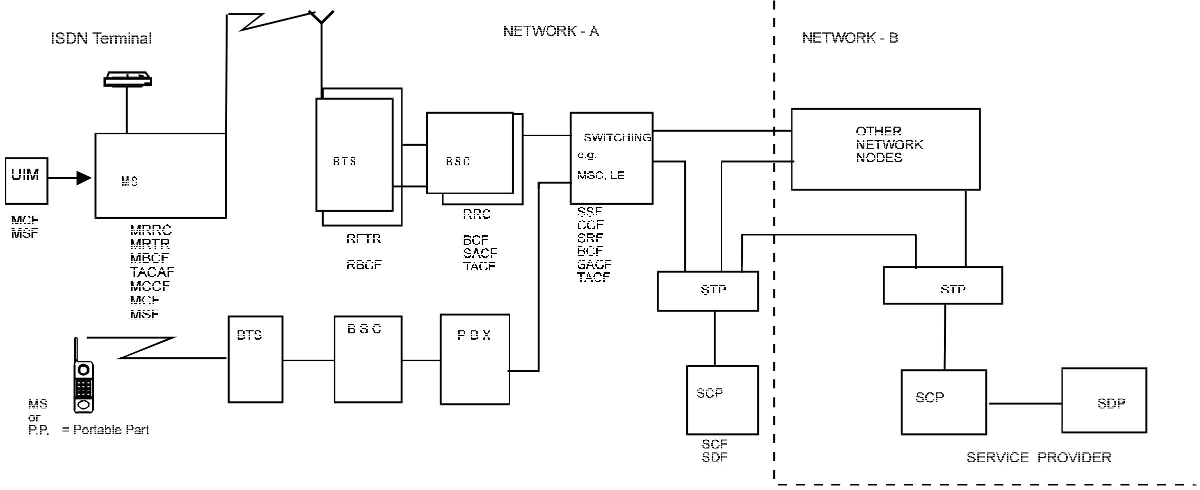


**Fig 9: Example of a Physical Network Implementation**

Other functional entity allocations to physical entities creating different nodal types, can be found in the ITU - T Draft Q.FNA new Recommendation for FPLMTS [37 ] including different physical network structures.

# 4. Management And Security

In this section the security needs of service management are considered, based on the concepts of TMN, since this is the requirement for the third generation mobile systems. The possible security features identified for IN in the SMAF, SMF and SCEF are aligned with those in the 3GS3 Technical Report 1 [1] and allocated to the ISO/TMN security functions.

Standardisation activities in [13] and [15] decomposes the IN service management and attempts to map the decomposed parts into TMN but excludes security features. Before proceeding with the identification of the security needs of IN service management a brief introduction to TMN and IN Service Management are outlined in the following subsections.

## 4.1 *Objectives of TMN*

The objective of TMN, is to support management activities associated with telecommunication networks, by providing a framework specification enabling the management of diverse equipment (both hardware and software), using generic information models and standardised interfaces.

### 4.1.1 Definition

Management, in the context of TMN refers to a set of capabilities to allow for the exchange and processing of management information (i.e. accounting, fault, security, etc.) so as to assist the administering body (Service Provider or Network Operator for example) in conducting their business efficiently - see [16].

It provides management functions for telecommunication networks and services, and offers communication to and from telecomms equipment irrespective of manufacturer, including the provision of access to the administrating body’s customers.

TMN provides an organised architecture to achieve the interconnection between various types of Operating Systems (OSs), in addition to providing standardised interfaces including protocols and messages for the exchange of management information. The managed equipment is referred to as a Network Element (NE).

The general relationships between the OSs and the NEs can be found in [16].

### 4.1.2 Functions associated with TMN

TMN is intended to support a variety of management functional areas. Such areas could be :

- planning
- installation
- operation
- administration
- maintenance and provisioning

They apply to telecommunication networks and services which support an administrations business needs. The functionality of applications to support the management areas is categorised under five broad headings - see [20]. These areas are:

- Fault management
- Configuration management
- Accounting management

- Performance management
- Security management

for convenience some times referred to as FCAPS.

A possible logical representation of the management areas mapped to a TMN enterprise abstraction of business, service, network and element is shown in figure 10, called for convenience an "Organisational Model".

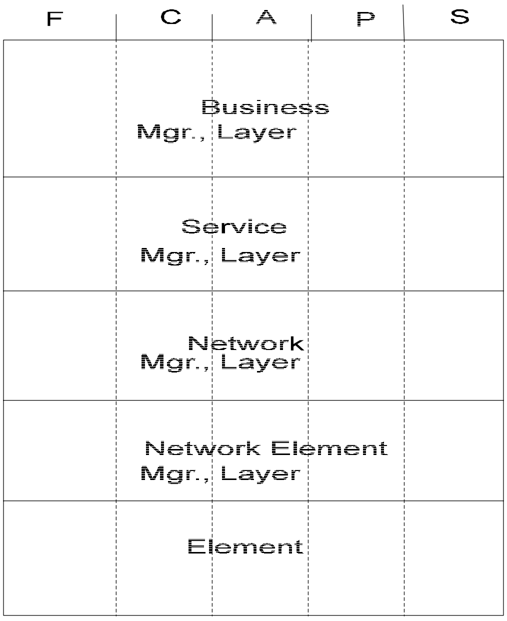


**Figure 10: A Possible Logical TMN Management Layered Model (Organisational Model).**

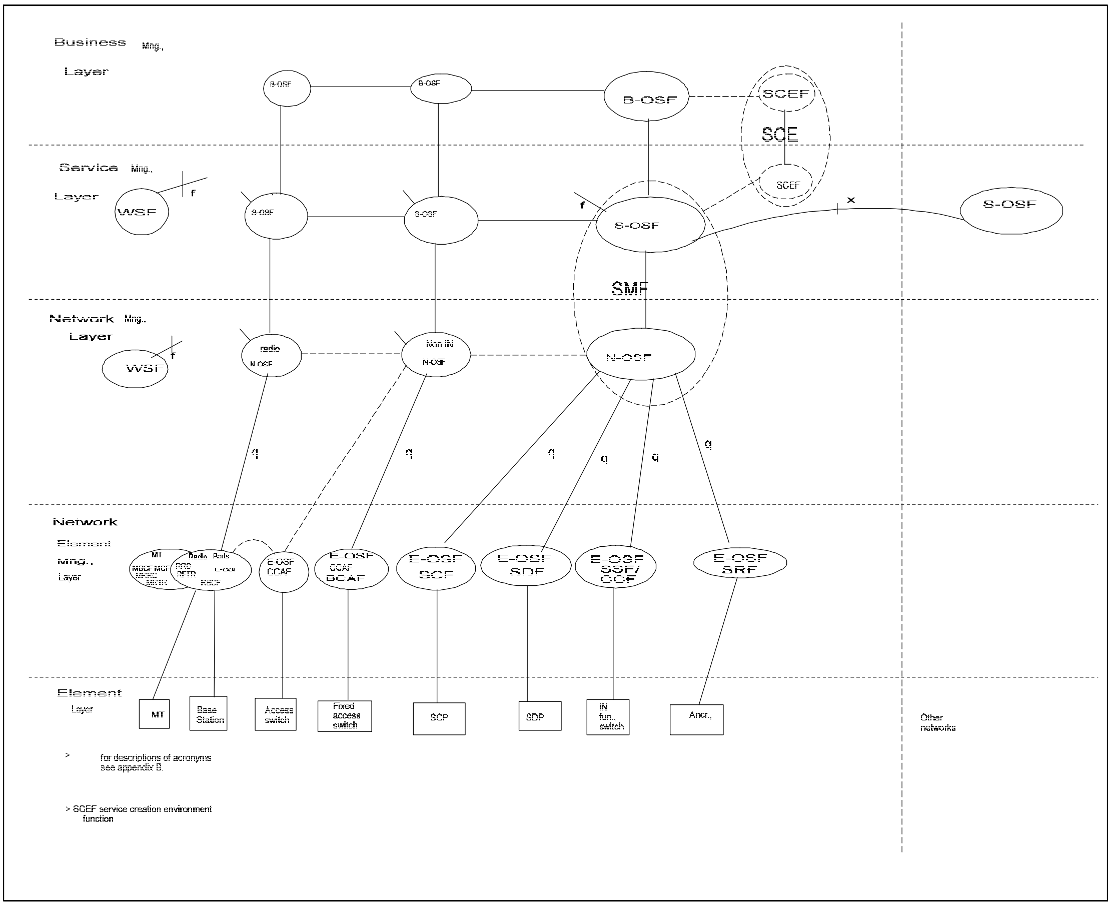
### 4.1.3. TMN Functional Architecture

The TMN functional architecture is based on a number of 'functional blocks' with associated reference points between them. Descriptions of the functional blocks can be found in [16]. They are repeated here for convenience and illustrated in Appendix B. Only those of immediate interest are listed in the text.

### 4.1.4. TMN Function Blocks

- Operating System Function (OSF) block
- Workstation Function (WSF) block
- Network Element Function (NEF) block
- Mediation Function (MF) block
- Q adaptor Function (QAF) block

There are many types of OSF, which are dependant on the structure of the TMN. A possible categorisation of OSFs can be based on abstraction and layered according to business, service, network etc. An example for the mobile third generation system is shown in figure 11. It represents the total enterprise including the business co-ordination and shows inter domain linking via the TMN X interface at the service management layer.



> for descriptions of acronyms see appendix B.

> SCEF service creation environment function

**Fig 11: Possible UMTS/FPLMTS Management Mapping of Functional Groups**

The Service Management layer OSF (S-OSF) is concerned with the service aspects of one or more networks performing a "customer" interfacing role.

The Network Management layer OSF (N-OSF) handles the realisation of network-based TMN application functions by communicating with the NEFs. It co-ordinates activity across the network and supports 'networking' demands of S-OSF (see [5]) which links IN management into TMN.

## 4.2 Service Management - an IN View

### 4.2.1 Definition

'Service management (in IN terms) is an activity of network operators and other stake-holders in telecommunication services, to support the proper operation of a created service and the administration of information relating to users and/or the network views of such information' [3]. A representation of the requirements for service management is illustrated in Figure 12.

Note: Only security aspects of network management capabilities will be considered other aspects are not within the scope of this report.

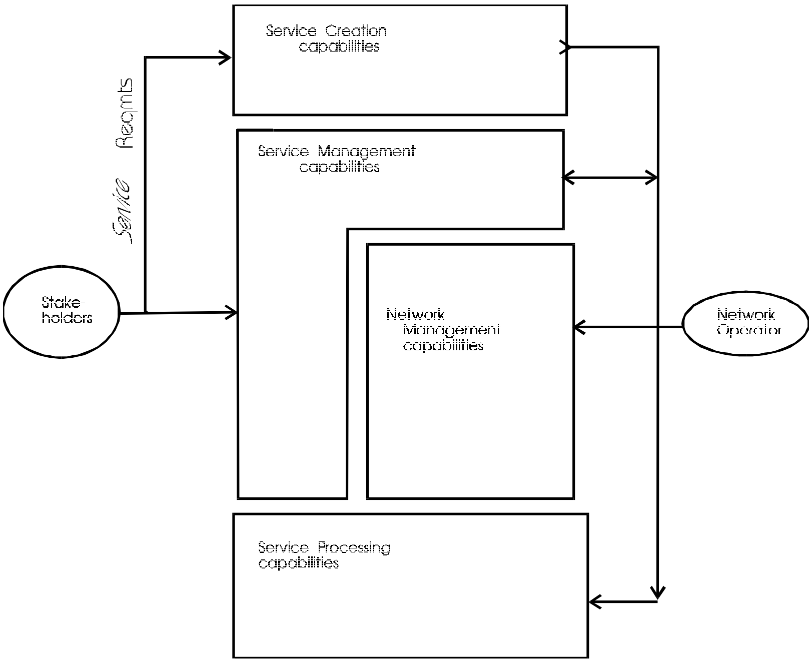

Service Creation capabilities
Service Reqmts
Service Management capabilities
Stake-holders
Network Management capabilities
Network Operator
Service Processing capabilities

Fig 12: Service Management Requirements

In figure 12, the Stake-holders are service providers, service brokers, and subscribers. There stated needs are telecommunications service requirements, which are feed to the service creation capabilities to realise those needs for the telecommunications environment.

Services and subscriptions created to become operational or be made non operational must be loaded or unloaded via service management capabilities to service processing capabilities where users and subscribers may gain access to utilise the services.

These services and service subscriptions must be managed for network efficiency by the network operator who has access via network management or directly through service management. In addition Service providers and subscribers have controlled access to perform their own level of management.

It is through service management that service data, user data, and provider data is managed and is a candidate for misuse from a security point of view.

### *4.2.2 Functional Entities for Service Management - IN view*

An IN view of the overall Service Management area includes the functional entities SMAF (Service Management Access Function), SMF (Service Management Function) and SCEF (Service Creation Environment Function) constitute the IN service management capability as shown in the functional model of figure 6.

They provide a commercial offering to network operators, service providers, subscribers and users to satisfy their requirements to create, customise, control and monitor their particular telecommunication service(s).

#### *4.2.2.1 Service Creation Environment Function (SCEF)*

The Service Creation capabilities encompassed in SCEF are composed of two aspects, ‘SCE-Upper’ and ‘SCE-Lower’. The former contains the service specification, service development and service verification processes and would normally exist in stake-holders domains. It is the functionality used in capturing the abstract service ideas and developing the potential telecommunication service with its associated management, using and possibly creating, new service independent building blocks (SIBs). The output of this function would include service scripts, service management logic, data templates, service trigger information and test specification data. The likely users of it would be the ‘building block creator’ and ‘service creator’. The ‘SCE-Upper’ when mapped into the physical plane of IN creates a physical entity called the Service Creation Environment Point (SCEP). This entity interacts directly with the Service Management Point (SMP) - see [8].

The latter exists as a sub-function within the Services Provisioning function of the SMF. It is in the service provisioning function that stake-holders select and compose their individual services.

The SCE-Lower performs the translation from the service script source that the SCE-Upper created to service-script-object, which will be used by equipment manufacturer dependent programs in the SCP, SDP, SMP etc.

#### *4.2.2.2 Service Management Function (SMF)*

This function of service management allows the provision and deployment of IN provided services and supports the ongoing operations of modification, monitoring and co-ordination of different SCFs and SDFs. In addition it manages, updates and/or administers service related information in SSF/CCF and SRF. It maps into the IN physical entity of Service Management Point (SMP) - see [8]. The main areas of functionality of SMF are described below.

Service Provisioning:

It performs the tasks of translation of source service scripts to object scripts, assembly and organisation of the service and service features for a user. It does this by the introduction of user specific selected routines and other information appropriate to the management of the particular subscription.

Service Customisation:

This function provides the ability to alter the parameters that control the operation of a service. These service parameters are defined as part of a service design operation in the SCE-Upper creation process. The parameter changes do not fundamentally change the functional capability of the service but merely alter the behaviour within the total set of possible behaviours defined by the service created.

Service Testing:

An extension of the service verification function in SCE-Upper. It assembles the test suite, verifies and checks the logical operation of the service and checks for possible feature interaction between the created service and already existing deployed services.

Service Control:

This function is performed to ensure reliable and proper operation of a service. For example it enables users of the service provider or service vendor to activate/deactivate the subscription service. It enables the various users of the SMF to manage their subscription via a service profile specifying for example, termination destinations, announcements to be played, distribution of calls etc.

Service Monitoring:

This involves collecting, logging and reporting statistics on a service(s) to determine the quality of service to users and adjusting the operation to suit prevailing conditions. Information on performance, congestion, and faults are all handled by the service monitoring function.

Service Deployment:

This is the process of introducing the tested service logic programs and service generic data into the IN structured network in a user independent manner.

Accounting:

This task covers the collecting of service dependent data and performing service independent billing operations, for example, collecting accounting information, generating and modifying data. There are many billing scenarios and these are outstanding issues with the standard bodies.

#### *4.2.2.3 Service Management Access Function (SMAF)*

The IN functional architecture provides an access function for service management. It is the interface between service managers and the Service Management Function (SMF). It allows service managers and some service users to manage their services [6], [11]. The SMAF has a number functions - see [14], which are described below.

Human Interface Functions:

It enables users to gain access to the service management function, and performs the same functions as the workstation function (WSF) functionality of TMN- [15], [16].

Note: ETSI do not intend to give a detail description of this human interface. Therefore it has been referred to TMN because, in the long term, the standard bodies intend to amalgamate the functionality.

Management Support Functions:

The Management support function contains several sub-functions, for instance:

(a) Human Interface Management - this deals with display manipulation i.e. graphics, menus, textual representation, User profile (definition of actions and schedules), ‘Help functions’, etc.

Relating this function to TMN, see Note above, it could have functions of Identification and Authentication of users which would map to the TMN OSF functional block. See section 4.1.3 , 4.1.4 for OSF and [16 ].

(b) System Management - this contains data back-up and user definition with an authorisation function. It refers to the definition of user access rights, see Figure 10, and data needed to identify and authorise the user.

(c) Service Management control Support - this refers to the functionality needed to exchange information with the IN SMF. This communication function appears to map to the TMN S-OSF - [15].

The above functionality of the SMAF implies it is the point of access through which subscriptions are set-up and user profiles are managed. It therefore requires, as part of its functionality, security control. Such functionality is not identified by ITU IN CS-1 standards, but implied in ETSI earlier documents [15].

## 4.3 *Usage of Relationship Reference Points*

### 4.3.1 **SMAF Relationships**

The users of the SMAF are illustrated in Figure 13. The relationships exist to allow users to exercise control of their service(s) and get feedback on the use of those services including reports from the Service Management system. The users, Service Provider, and Other Networks are given access to enable:

- Other network management systems (reference point d), to pass Service Provider and Service Subscriber charges to and from their home networks so the appropriate billing may be expedited. Such a relationship maps to the 'X' (inter domain) interface of TMN (see TMN subsection 4.5 and appendix B).

- Service Provider and End Users (reference points b, c and e), to perform customisation actions, for example, to change their announcements or interrogate their profiles. Alternative management of End User access is possible via the standard call path, but the actual point of entry is dependent on the network implementation. (It may not be wise to give End Users direct access to the management system, because of the high probability of 'hacking').

- Network operators and/or Service Providers reference points (b and e), to allocate/de-allocate subscriptions to Service Subscribers and End Users, and to monitor usage of services, security violations and the general health of the IN network elements. Subscriptions would have agreement data about access to the service profiles, charging, with possible limits on remote registration where appropriate. There is also the possibility of service instance parameters which are changeable by customisation and restrictions on remote access.

Economics and the location of users, local or remote, have an important part to play in establishing the type of interface and the protocols that would be needed to carry the sensitive information.

In the case of remote users the type of data to be passed over the interface would suggest the need for a "security communication function" [17] to counteract likely threats. These remote user interfaces are likely to be 'Open' i.e. published and non-proprietary, particularly between network SMAFs. The SMAF must therefore contain the appropriate security features.

Local users on the other hand, where the interfaces and connections are within the same building, would not require the same level of security communication function. The probability of intruders is much lower.

In both cases however, because of the diverse and commercially competing organisations of Service Providers and Service Subscribers that might share the same computing environment, assured privacy and non-disclosure of information to competitors would be required. In addition, because of 'Open' inter and possibly intra network communication, the SMAF and SMF must also contain 'system security functions' [17] to provide the privacy and confidentiality needed to prevent misuse. One such proposal is illustrated in sub-section 4.6.1.

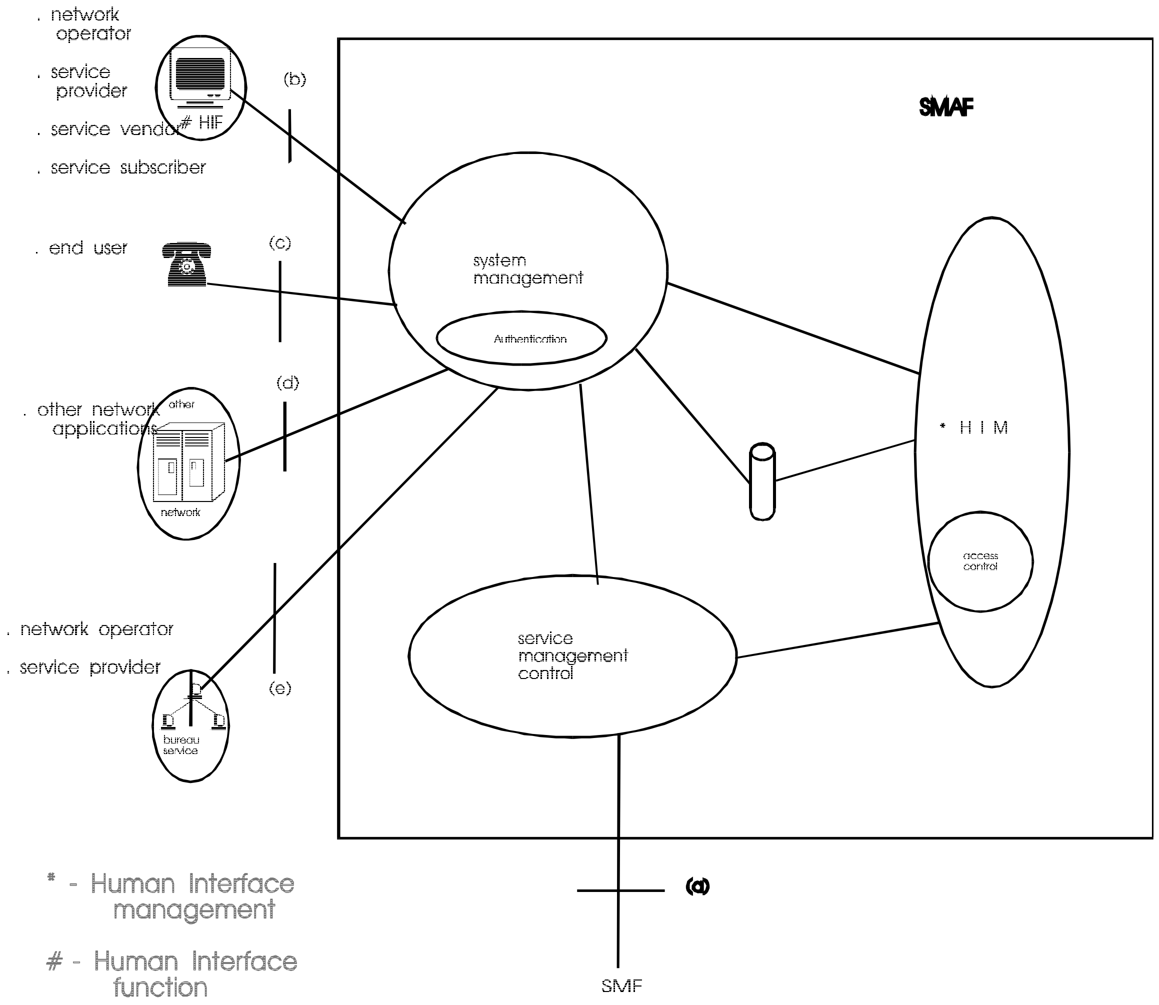


**Fig 13: Access to/from Service Management Access Function**

### 4.3.2 SMF Relationships

Access to the SMF is illustrated in Figure 14 and is via the indicated reference points (a, b, d, r, s and t). Reference points a, b, d, r and t are not directly connected to stake-holders (human-beings), but interconnect via ‘Open’ interfaces to other IN network entities which could be local or remote. Direct user access is via reference point (s) - the Creator’s access, which could also be a local or remote connection. It is not decided whether this will be ‘Open’.

Commands and information for customisation, setting-up, activation, de-activation, interrogation of a subscription, monitoring and alarms are passed between the SMAF and SMF across reference point (a). Reference point (b) carries the arming trigger detection point data and the ‘trigger table’ ancillary information that is needed for the proper operation of any IN service triggered from that network element. This information is supplied during the deployment phase of an IN service from SMF, performed by the Network Operator (Service Manager) via the SMAF functionality. Requests to interrogate, activate or deactivate the trigger point information is also transported through reference point (b).

The reference point (d) information flow is complex and in some cases it incorporates reference point (r) information but this is dependent on the particular network structuring. It is intended to be an

'Open' interface whose type is still an issue. Service subscribers, and End Users will not be given access to such an interface, it will remain in the domain of the Network Operator.

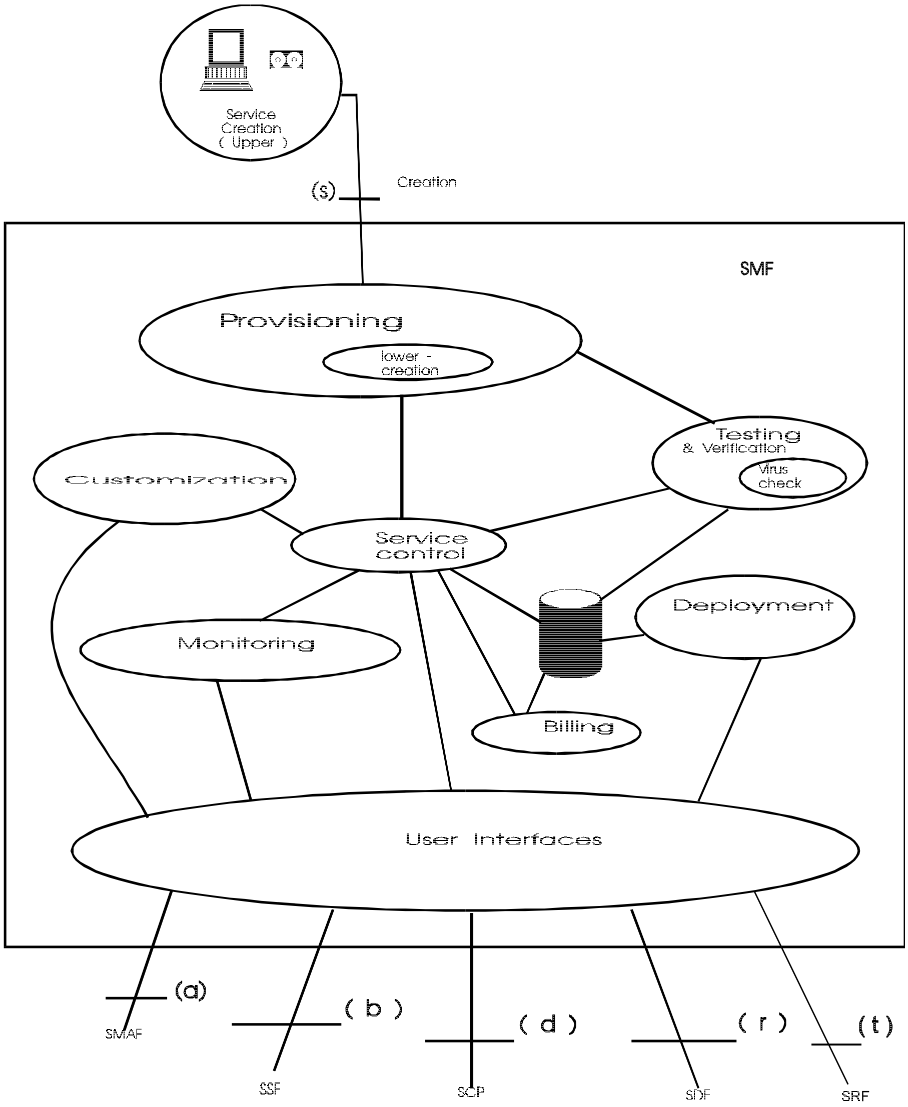


**Fig 14: Access to/from Service Management Function**

## 4.4 *Integration of Security Service Management within TMN*

In TMN the functions necessary to perform the tasks of 'system management' are defined [33] and [20].

The function that is of concern here is the Security Management and the categories of security management. It is into these categories that the SMAF, SMF and SCEF security features will be mapped to achieve integration for the security of service management.

### 4.4.1 Categories of Security Management

In accordance with [21] the management of the classified features in [1] are managed by the functions within Security Management of TMN. Security Management (SM) is itself categorised into:

- System Security Management
- Security Service Management
- Security Mechanism Management

The activities of the categorised functions are quite clearly specified in [21] and would apply to the security management of UMTS and FPLMTS.

### 4.4.2 **Mapping of Security Management to TMN**

The mapping of security management categories on to the organisational management layers of TMN is shown in Table 1.

| | | |
|---|---|---|
| **Business Management Layer** | **System Security Management, (common S. Policy)** | |
| **Service Management Layer** | **System Security Management (common to Services)** | **Security Service Management** |
| **Network Management Layer** | | |
| **Network Element Management Layer** | **System Security Management (common to mechanisms)** | **Security Mechanism Management** |

**Table 1. Possible mapping of SM to TMN layers.**

The mapping results in splitting System Security Management into three components:

- Security management common to the creation of security policies incorporating agreements at the Business management layer.
- Management common to security services and features at the Service management layer.
- Security management common to the mechanisms at the Network element management layer.

### 4.4.3 **Common Security Data to be Managed**

The security classes identified in 3GS TR1 [1] of :
- Confidentiality
- Integrity
- Authentication
- Access control
- Non-repudiation
- Supplementary

are managed by Security Service Management. The data items to be managed for each category are now listed below :

Confidentiality

- feature of identity involved (SCP, Base station, etc.)
- confidentiality feature parameters (e.g. events that should cause security alarms defined by security policy)
- signature and token data handling, storage and validation
- user security data

Integrity

- feature user identity
- integrity feature parameters
- user security data

Authentication

- identity information (e.g. IMTN, IMUN)
- authentication verification parameters (e.g. events that should be logged in a security audit trail file)
- user authentication information (e.g. Service related algorithms ID, certificates, key data etc.).

Access Control

- access Control Decision Information
- target identities
- initiator identities
- access control parameters
- access control information

Non-repudiation

- possible management data items
- trusted authority certificate
- indicator certified identity
- recipient identity

Supplementary

This category is outside the scope of the study.

## 4.5 *Threats to Service Management Relationships*

The threats to the service management relationships are considered in this subsection. It looks at misuse of the system and other threats to the SMAF and SMF relationships as they apply within a TMN environment.

### 4.5.1 **Misuse**

Misuse may be classified as:
- Unintentional
- Intentional

Unintentional misuse of the service management functionality by users of the SMAF may be caused by system malfunction, for instance, operational errors, input data errors, program errors and system resource errors which are accidental. Other misuse by users may be caused by administrative failure to implement an adequate security policy. These risks may be considered less onerous from an access security point of view.

Intentional misuse, however, particularly from the threats of ‘hacking’ i.e. masquerading, repudiation, service privacy violation, viruses and denial-of-service at the SMAF is more serious. The threats have a significant effect on reference points (b) and (e) of Figure 13 because subscriptions of Service Subscribers, End Users and even Network Operators service network data (including authentication data) can be interfered with by an intruder.

### 4.5.2 **Threats to SMAF**

The identification and analysis of other threats to users of the IN SMAF is based on the UPT security architecture study [18]. The document views security from the call path side of a network but there are a number of threats that are general and applicable to service management in an IN structure.

A selection of appropriate threats relating to the environment in which the management functions are performed were considered. These are already identified in Section 3 and 4 of Reference [18]. For each pair of roles (network operator, service provider, subscriber and user) involved and each feature, the threats posed by such an intruder are considered..

#### 4.5.2.1 *Additional Threats*

Two major threats which do not appear to be included in the UPT analysis and which could exist in IN are ‘Hacking’ and the introduction of ‘Viruses’ into services and service features.

Hacking:

Hacking is a highly publicised threat to ‘Open Systems’ and to open management systems. Those that are frequently used by Service Providers, Network Operators and Service Subscribers with dial-up connections have a significantly increased risk. Hackers may be of two types, those who simply wish to beat the system and gain access, and those whose intentions are more sinister. ‘Hacking’ could be classed as masquerading as a service managers, a Network Operator, a Service Provider or a Service Subscriber in the management system. The counter-measures of Authentication and Access Control should be incorporated into the functionality of the SMAF.

Viruses:

Viruses in an IN telecommunications system would be a significant threat. The deliberate or accidental introduction of such software by an intruder, as part of a service feature or service created by a service provider or service subscriber and subsequently distributed could cause a network collapse.

The counter-measure to such a threat must be part of the functionality of the service management architecture and must not be accessible to end users. This counter-measure must be added to the service/feature test functionality of service management before deployment.

### 4.5.3 **Threats to SMF**

Intruders into the SMF must first negotiate the SMAF user security checks or enter on reference points a, b, d and r of figure 14. Malicious actions at these points could alter the detection point information, the service network status, or the stake-holders service profile, authorisation codes and identities, charging parameters and other sensitive information. Data integrity and privacy from such intruders are needed.

The introduction of virus service logic into the SMF or the SCP (Service Control Point) would be possible by means of ‘tapping’ into a remote SCE reference point (s), and modifying the appropriate service feature. Entry into (d and r) by intercepting messages, creating virus service logic and reintroduced on the ‘Open’ interface is possible, with devastating results to the network.

## 4.6 ***Security Features for Service Management***

The security features to be supported by third generation systems can be found in Technical Report 1 [1]. The specific features for Service Management to counter the threats are as follows:

- Identification of the user (e.g. Service Provider, Subscriber, etc.)
- Authentication of User (Service-related authentication)
- Non-repudiation of origin and delivery of transmitted data
- Access control of user (i.e. access control to stored data)

- Confidentiality of stored data (although this may be part of the access control feature)
- Security of management (i.e. event logging and recording)
- Virus check feature (service-access control)

**Note:** Virus check is an additional feature not found in TR 1 [1].

A possible allocation of the security features is shown in Figure 15 with an example of a likely architecture for user access control described in the text below. Additional examples of an architecture using some of these features could be found in ([19], Section 3.2).

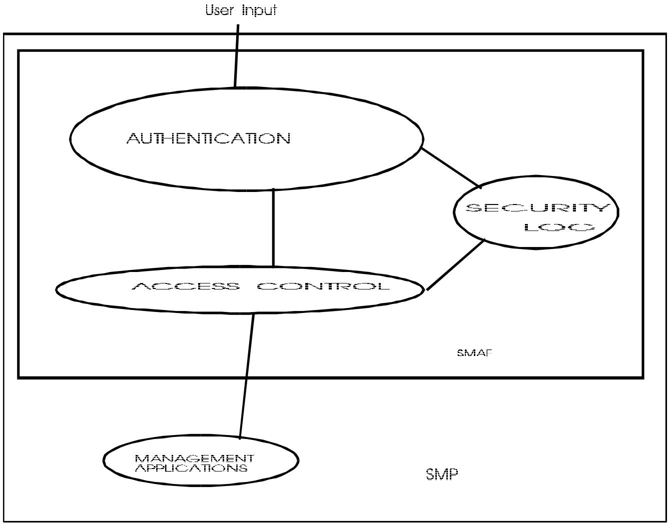


**Fig 15: SMAF Security Features**

### 4.6.1 Proposed Access Control for Service Management.

IN Phase 1, (CS-1) recommendations do not identify the need for security in the Service Management functionality.

Figure 15 represents a proposal to allocate security features to the service management functionality.

a) Authentication

The authentication facility indicated in the diagram can be sub-divided into two functions:

- The User-agent
- The authenticator

User-agent function

The User-agent function when invoked requests logon from the user and is the intermediary between the user and other security facilities. It is the only function in a distributed system that is aware of all user transactions while accessing applications in the management system, thus transaction information can be supplied to a security log. The user involved could be another application.

Authenticator

The authenticator accepts and checks a user’s authentication information e.g. password. For the SMAF it is not recommended that simple passwords are used, ‘stronger’ authentication is proposed e.g. passcard with encrypted data. The user identity i.e. security identity, and authenticated information is passed to access control if successful. Successful or unsuccessful authentication attempts are sent to the security log.

b) Access Control

Once the user has been identified and authenticated within Service Management ‘Organisational access control’ is applied. The following text suggests a structuring based on Class theory to enable flexible access control to be applied.

Many potential organisations using the Service Management function will have different organisational structures with differing levels of staff, and staff with great diversifying roles.

The SMF shall provide a view from which an SMP owner can define the organisational structure which shall use the SMP. The main objective of the SMF is to provide a flexible approach for doing this while providing security for the users.

The organisational structure consists of classes of user. The class defines the access to views and functions, plus services for all users in the class. Each class will have one or more users. One user in the class will be the class owner, who will be able to further restrict the individual users within the class.

It shall be possible over time to add new views, functions, services and individuals to existing classes.

The users identity within the class, the views and functions, the services they have access to, plus service data defined by the users within the class will be private to the class. It shall be possible to define access rights to this information for other classes.

The data entered by each individual user shall be private, the class owner shall be able to access the individual user’s data.

A class of user can be defined that identifies a different organisation to the SMP owner. This allows different competing organisations to have access to the same platform.

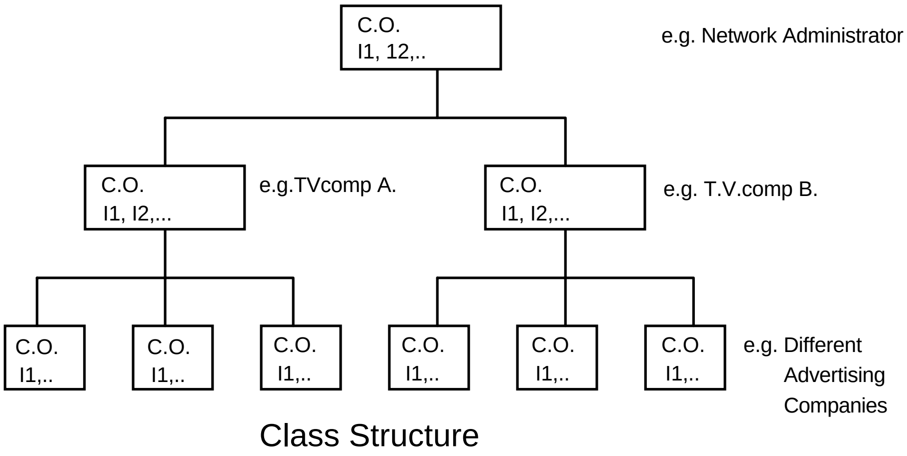
In doing this there are many security implications: the identity of an organisation, its customers and services must be kept private in order to ensure that one organisation's customers can not be poached by another.

A user if authorised may create a new subordinate class of users with less than or equivalent functionality. When creating such a user class, the maximum number of users in the class shall be defined. The user creating the new class shall become its class owner. The class will inherit the access to the views, functions, plus services of its creator.

This approach does not presuppose how the customer intends to use the SMP platform and allows him to reflect his own organisation onto the SMP. In the situation where different organisations use the platform, the users and data can be defined as private.

The following is an example of a possible organisational structure, and illustrated in figure 16. A Network Provider who owns the SMP platform, sells on the use of the platform to two competing television companies. The television companies in turn sell on the use of the platform and IN services to companies advertising on their television channel.

Here it can be seen that the identity of the television companies clients must be secure, in order to prevent other competing companies from poaching clients. Also data owned by one Advertising company must be secure from the other, in order to prevent information concerning a product, being obtained by a competing advertising companies.



C.O.: Class Owner (Each Class Owner can further restrict individuals)
I1: Different individuals.

**Figure 16: Organisational structure.**

In this example there can be several classes of user with access to different views and functions, plus services. Each TV company is a subordinate class of the Network Provider. Each advertising company is a subordinate class of the Television Company it advertises on.

Each Class may have many users; the class owner can further restrict the individual users within the class in order to further define the role of an individual.

## 4.7 *Management Functions for Security Features*

The security features identified for 3GS in TR1 [1] are categorised in the following classes:

- Confidentiality
- Integrity
- Authentication
- Access control
- Non-repudiation
- Supplementary

and are managed by Security Service Management. For each category the data to be managed and the appropriate management function can be identified.

Because of the close relationship between System Security management activities and Security service management it will be included in the function list.

### 4.7.1 System Security Management Activities

- security policy management
- interaction with other FPLMTS & UMTS management functions
- interaction with security service management
- security audit management
- event handling management
- security recovery management

### 4.7.2 Security Service Management

The management functions for Confidentiality and Integrity:

- the manipulation of security data (e.g. updates, installation, deletion) etc. of keys supported by other management functions e.g. key management and version management
- security audit trail functions (provides for the collection of security related events to allow a security audit to be performed)
- security alarm reporting function (event reporting to detect security attacks and malfunctions)
- security recovery function (to establish the required security state of UMTS or FPLMTS after a breach has occurred. Its behaviour is dependent on Security Policy rules i.e. disable access, reroute, play announcements etc.).

Management functions for Authentication

- manipulation of administrative imposed security information (e.g. install, change, distribute etc. security policy information)
- the security functions of audit trail, alarm reporting and recovery are also used.

Management functions for Non-repudiation

- the security function of audit trail plus the management facility of authentication
- security alarm reporting function
- algorithmic functions for the generation of electronic signatures or tokens.

Management functions for Access Control

- manipulation of access control information
- security audit trail function
- security alarm reporting function
- security recovery function
- attempted retry limitation function

Management functions for Supplementary

- security alarm reporting function (supported by event handling function when end-to-end facilities are available)
- manipulation of authentication information

## 4.8 *Management of Security Mechanisms: a 3GS3 View*

The features identified above represent a possible management security view as seen from the management entities in the management system. A study of potential security mechanisms as seen from the ‘Operations and Maintenance’ (O&M) side of the stake-holders (i.e. users service providers, and network operators) are now considered.

### 4.8.1 Introduction

A study of potential security mechanisms appropriate for providing certain security features to be supported by third generation mobile telecommunications systems (3GS) can be found in 3GS3 Technical Report 2 [2]. The main purpose of this section is to give a discussion of management of security mechanisms providing the following security features.

- Service-related authentication and key distribution
- Identity and location privacy

For the purpose of this report, the management of security mechanisms is divided into information management and key management. The information storage and the key management requirements will be listed. The following sub-sections are an initial investigation into the two requirement examples.

### 4.8.2 Service-related Authentication and Key Distribution

#### 4.8.2.1 *Information Storage Requirements*

The following two information types identified in subsection 4.4.2 of 3GS3 Technical Report 1 [1] are considered in service-related authentication and key distribution:

1. **Identity.** All users, service providers and network operators involved in service-related authentication have identities. The entity of interest here is the user. User identity is generated by the appropriate service provider and is held by both the service provider and the user. During service-related authentication processing, the user identity is transmitted between the user and the service provider via a relevant network operator.

2. **Authentication message.** Authentication messages are generated by users, service providers or network operators and transmitted among them during the authentication processing.

The storage requirements for the above information are as follows:

1. The privacy and integrity of user identities stored in the user access device and corresponding service provider's databases should be protected. The security mechanisms appropriate to this requirement should cover access control to a user access device, access control to a service provider's databases, non-repudiation of access to a user access device and non-repudiation of access to service provider's databases.

2. Authentication messages stored in the user access device, corresponding service provider's databases and network operator's databases should be protected from being made available or disclosed to unauthorised entities or processes. The security mechanism appropriate to this requirement should cover access control to a user access device, access control to a service provider's databases, access control to a network operator's databases, non-repudiation of access to a user access device, non-repudiation of access to a service provider's databases, and non-repudiation of access to a network operator's databases.

#### 4.8.2.2 *Key Management Requirements*

The following three keys (described in Section 4 of [2]) are involved in service-related authentication and key distribution and depending on using symmetric encryption techniques, a public key algorithm or a cryptographic check function:

1. shared authentication key
2. public key for authentication, and
3. shared session key.

The requirements for the key management are as follows:

1. If using symmetric encryption techniques, a user and corresponding service provider share an authentication key, which is generated by an authorised entity and held by the user and service provider. A service provider and network operator share an authentication key, which is generated by an authorised entity and held by the service provider and network operator. During the authentication and key distribution processing, a session key is distribution to the user and network operator. The generation, distribution, storage, updating and deletion of all shared keys should be protected from unauthorised entities or processes.

2. If using a public key algorithm, each entity, including a user, service provider and network operator, has a public key and private key. The public key is known to all relevant entities and the private key is only known to himself. During the authentication and key distribution processing, a session key which could be a shared key is distributed to the user and network operator. The generation, distribution, storage, updating and deletion of all keys should be protected from unauthorised entities or processes.

3. If using a cryptographic check function, a user and corresponding service provider share an authentication key, which is generated by an authorised entity and held by the user and service provider, and a cryptographic check function. A service provider and network operator share an authentication key, which is generated by an authorised entity and held by the service provider and network operator, and a cryptographic check function. During the authentication and key distribution processing, a session key is distributed to the user and network operator. The generation, distribution, storage, updating and deletion of all shared keys should be protected from unauthorised entities or processes.

### 4.8.3 **Identity and Location Privacy**

#### 4.8.3.1 ***Information Storage Requirements***

The following two information types (identified in subsection 4.4.2 of [1]) are considered in identity and location privacy:

1. **Identity.** All entities have identities. The entities of interest here are users or terminals. By the registration and location update mechanisms the user or terminal sends its identity (real identity or temporary identity) to its service provider or terminal manager via a relevant network operator.

2. **Location.** The location information concerns a user and/or terminal. Such information is generated by a network operator and passed to the user's service provider (and/or the terminal's terminal manager). The storage requirements for the above information are as follows:

1. The privacy and integrity of user identity stored in the user access device and corresponding service provider's databases should be protected. The security mechanisms appropriate to this requirement should cover access control to a user access device, access control to a service provider's databases, non-repudiation of access to a user access device and non-repudiation of access to a service provider's database.

2. The privacy and integrity of terminal identity stored in the terminal equipment and appropriate terminal manager's databases should be protected. The security mechanisms appropriate to this requirement should cover access control to a terminal, access control to a terminal manager's databases, non-repudiation of access to a terminal and non-repudiation of access to a terminal manager's databases.

3. The location information stored in the user access device, terminal, service provider's databases, terminal manager's databases and network operator's databases should be protected from being made available or disclosed to unauthorised entities or processes. The security mechanisms appropriate to this requirement should cover access control to a user access device, access control to a terminal, access control to a service provider's databases, access control to a terminal manager's databases, access control to a network operator's databases, non-repudiation of access to a user access device, non-repudiation of access to a terminal, non-repudiation of access to a service provider's databases, non-repudiation of access to a terminal manager's databases, and non-repudiation of access to a network operator's databases.

#### 4.8.3.2 *Key Management Requirements*

Based on asymmetric techniques, the user public key and the certificate of the public key may include some information about the user's identity. If so there is a requirement to avoid the transmission of the user public key and its certificate across the air interface.

If it is required that network operators need never know users real identity, temporary keys of the user, including a temporary shared key with respect to the user and a temporary public key of the user should be used.

### *4.9* **Conclusion**

A very preliminary allocation of the 3GS3 categorised features in TR 1 [1] to the security service management functions has been achieved.

It is not clear whether the UMTS/FPLMTS security functions in SMAF and SMF are the same as those for TMN, although mapping was attempted by ETSI in [35]

The following issues need to be investigated

- Identification of the SMF security functions and how they map fully into the TMN functionality
- Interaction of security domains including inter network
- Identification of the managed objects in the security management domain.

It is not clear whether the radio and mobile entities will have their security services/feature aspects managed by an SMF.

# 5. Charging and Accounting Security Needs

The security considered in this section is that associated with charging and accounting between different network types and providers in a TMN environment for UMTS and FPLMTS. Charging is categorised, management processes associated with charging stated, and the relationships in the management domains identified. In addition charging scenarios for Off-line cases are considered .

## 5.1 *Categories of charging*

Charging as a process may be categorised into two types, Off-line and On-line.

Off-line implies non real time analysis of accountable events, tariffed, costed, formatted and supplied to the billing process [22]. Such activities are normally performed in the management domain of network operators.

On-line charging implies near real time where duration and cost of a call or intended call, must be calculated and supplied to the requesting application or user. This charging category is considered in this contribution from the viewpoint of handover between different networks.

## 5.2 *Charging in a management domain*

As suggested in [22], charging is a sub-sub-process of the ISO/TMN (FCAPS) system management containing the account metering process. The account process consist of three sub-processes:

1) Usage metering - responsible for:
   - Creation of usage records i.e. from accountable events in a system. e.g. location updates, call attempts, registrations in UMTS etc.
   - Logging of the activities in the account process.

2) Charging - responsible for:
   - Collecting usage records
   - Combining the usage records into a single subscriber “service/call usage record” and formatting it into a “mediated charge record” (service transaction record ).
   - Tariffing i.e. the analysis and costing, which is added to the charge record.
   - Logging of the charge record.

3) Billing - responsible for:
   - Collecting of the charge records
   - Selecting, on a per user/subscriber basis over a particular time-period the charges and charge records
   - Producing bills from the selected information to the format of providers and subscribers.

## 5.3 *Inter-operator TMN charging relationships for UMTS*

With reference to the charging service descriptions in [23], figures 17a to 17d, represent a possible TMN layered domain structure for the different network types. The off-line charging and accounting management relationships between the types are shown,for calls made from CPN/PTN networks. The figures show different scenarios to be expected.

Figure 17a. shows the scenario for a UMTS user who has made a call terminating in the PSTN.

- The public UMTS network generates the charge record (CR) for the call and any additional services that might be used. No CPN/PTN resource usage charges are accounted for (this is an agreement between the CPN/PTN and the public network operator).

- The CR is passed up the PSTN TMN layered structure to the service management domain, where the call is logged, the appropriate service provider is selected, the relationship is activated, and the CR passed for the provider to perform the billing function for the specific subscriber.

- The cost for use of the PSTN is passed from the service to the business management domain of the provider, from which the public operator is reimbursed for the use of the network. This may be the case for residential access networks.

Figure 17b highlights the situation where the CPN/PTN has limited accounting functionality e.g. call logging and pulse metering.

- The public network operator generates the usage records for the user call, service used, and access network resource and these will be included in its accounting charge record to the provider. The procedure is not dissimilar to what happens in scenario 1, except the provider pays the network operator for accounting the resources used and the network operator rebates the CPN/PTN.

Figures 17c and 17d, represent the scenarios where the CPN/PTN has more complex charging and accounting facilities.

In 17c, the CPN/PTN raises the charge record (CR) for the subscriber related to the mobile user for itself and the public network, with the public network supplying a possible resource used record.

The records are passed up the TMN management layered structure as illustrated. This scenario may be the case for mobile users in the private network using services involving the public network (PSTN), as well as the CPN offering pay-phone and/or credit-card type services.

17d illustrates the case when both public and private raise independent charge records for the call/service used by the mobile user. They thus have independent management relationships with the provider. The accounting is done by the provider, revenue retrieved by both administrations from the provider.

**Note**: Calls which lie solely within the CPN/PTN are not considered in this report.

Transit operators usage metering charges might be passed to the preceding operator via the TMN X interface. This is to be clarified.

The interfaces used Qx, Q3, and X of TMN over which the relationships are established, carry similar information for the different scenarios; such interfaces from a security view point must be confidential and have a high degree of integrity. Mutual authentication and non-repudiation by the participating administrations would be necessary [28].

It is possible that common mechanisms could be used between the different management administrations.

**Figs 17a-17d show the relationships of Off-line Charging cases between TMN Management Functions**

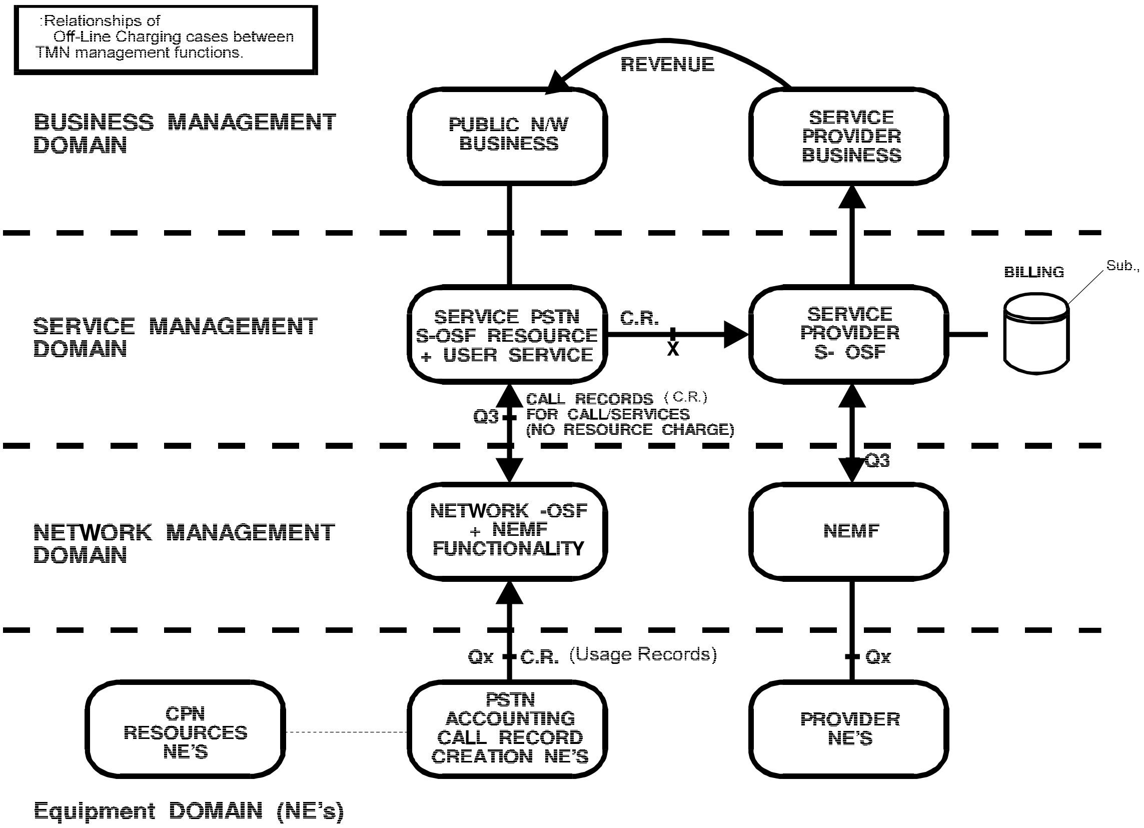

:Relationships of Off-Line Charging cases between TMN management functions.
REVENUE
BUSINESS MANAGEMENT DOMAIN
PUBLIC N/W BUSINESS
SERVICE PROVIDER BUSINESS
BILLING
Sub.,
SERVICE MANAGEMENT DOMAIN
SERVICE PSTN S-OSF RESOURCE + USER SERVICE
C.R.
X
SERVICE PROVIDER S- OSF
Q3
CALL RECORDS ( C.R. ) FOR CALL/SERVICES (NO RESOURCE CHARGE)
Q3
NETWORK MANAGEMENT DOMAIN
NETWORK -OSF + NEMF FUNCTIONALITY
NEMF
Qx
C.R. (Usage Records)
Qx
CPN RESOURCES NE'S
PSTN ACCOUNTING CALL RECORD CREATION NE'S
PROVIDER NE'S
Equipment DOMAIN (NE's)

Fig 17a

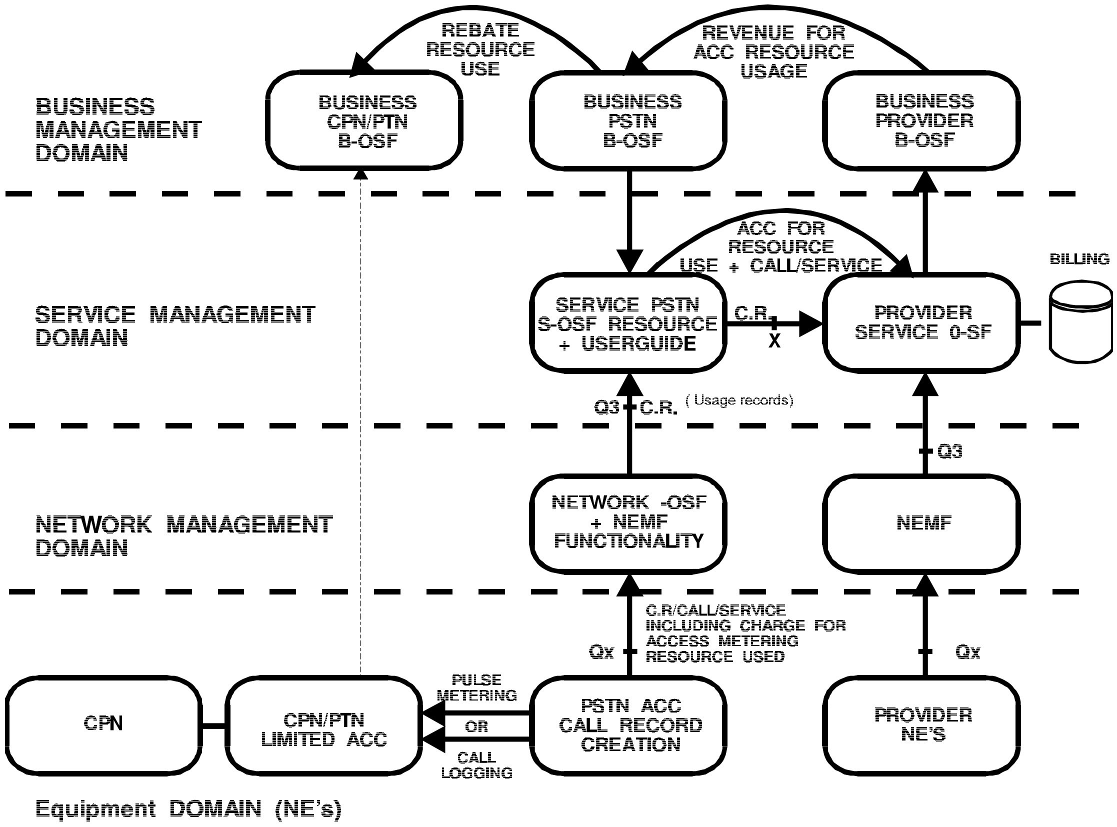

REBATE RESOURCE USE
REVENUE FOR ACC RESOURCE USAGE
BUSINESS MANAGEMENT DOMAIN
BUSINESS CPN/PTN B-OSF
BUSINESS PSTN B-OSF
BUSINESS PROVIDER B-OSF
ACC FOR RESOURCE USE + CALL/SERVICE
BILLING
SERVICE MANAGEMENT DOMAIN
SERVICE PSTN S-OSF RESOURCE + USERGUIDE
C.R.
X
PROVIDER SERVICE 0-SF
Q3
C.R. ( Usage records)
Q3
NETWORK MANAGEMENT DOMAIN
NETWORK -OSF + NEMF FUNCTIONALITY
NEMF
C.R/CALL/SERVICE INCLUDING CHARGE FOR ACCESS METERING RESOURCE USED
Qx
Qx
PULSE METERING
OR
CALL LOGGING
CPN
CPN/PTN LIMITED ACC
PSTN ACC CALL RECORD CREATION
PROVIDER NE'S
Equipment DOMAIN (NE's)

Fig 17b

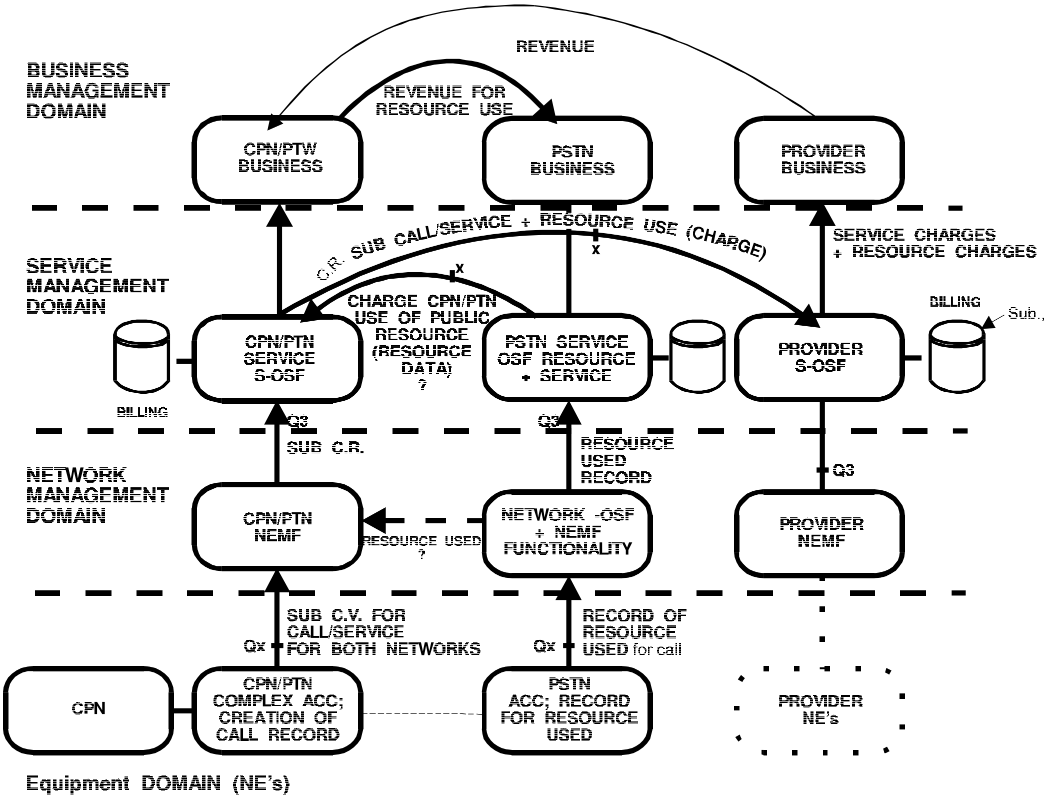

REVENUE
BUSINESS MANAGEMENT DOMAIN
REVENUE FOR RESOURCE USE
CPN/PTW BUSINESS
PSTN BUSINESS
PROVIDER BUSINESS
C.R. SUB CALL/SERVICE + RESOURCE USE (CHARGE)
x
SERVICE CHARGES + RESOURCE CHARGES
SERVICE MANAGEMENT DOMAIN
CHARGE CPN/PTN USE OF PUBLIC RESOURCE (RESOURCE DATA) ?
BILLING
Sub.,
CPN/PTN SERVICE S-OSF
PSTN SERVICE OSF RESOURCE + SERVICE
PROVIDER S-OSF
BILLING
Q3
SUB C.R.
Q3
RESOURCE USED RECORD
Q3
NETWORK MANAGEMENT DOMAIN
CPN/PTN NEMF
RESOURCE USED ?
NETWORK -OSF + NEMF FUNCTIONALITY
PROVIDER NEMF
SUB C.V. FOR CALL/SERVICE FOR BOTH NETWORKS
Qx
RECORD OF RESOURCE USED for call
Qx
CPN
CPN/PTN COMPLEX ACC; CREATION OF CALL RECORD
PSTN ACC; RECORD FOR RESOURCE USED
PROVIDER NE's
Equipment DOMAIN (NE's)

Fig 17c

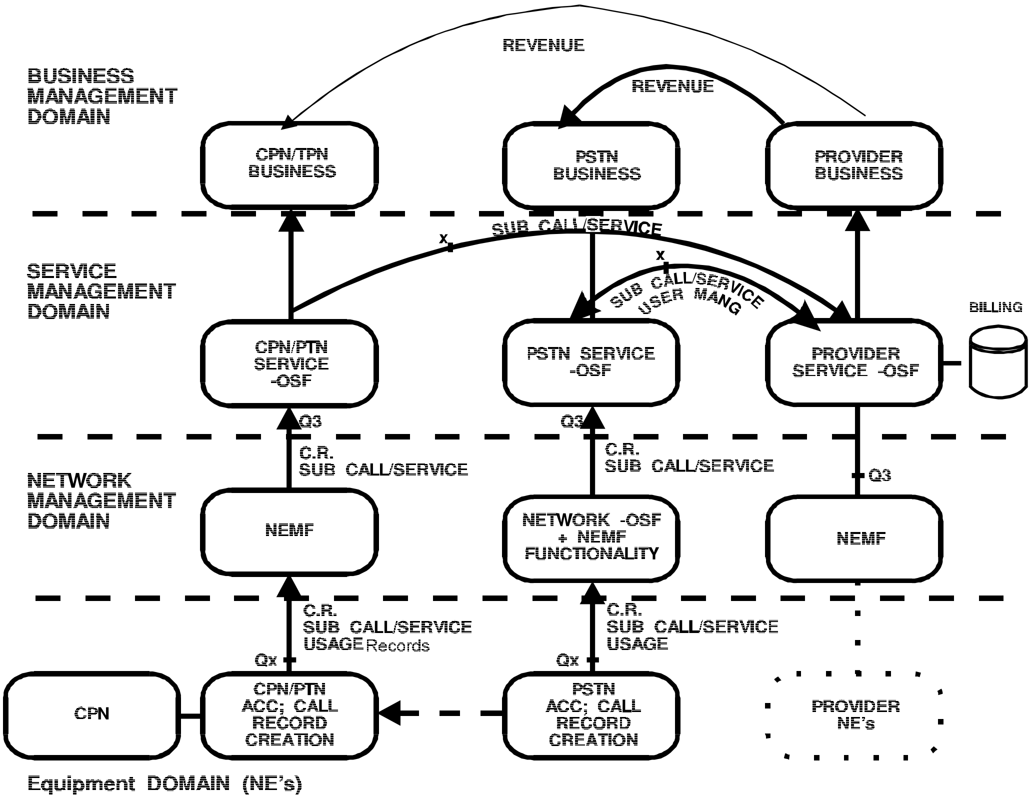

REVENUE
REVENUE
BUSINESS MANAGEMENT DOMAIN
CPN/TPN BUSINESS
PSTN BUSINESS
PROVIDER BUSINESS
SUB CALL/SERVICE
x
x
SUB CALL/SERVICE USER MANG
SERVICE MANAGEMENT DOMAIN
BILLING
CPN/PTN SERVICE -OSF
PSTN SERVICE -OSF
PROVIDER SERVICE -OSF
Q3
Q3
C.R. SUB CALL/SERVICE
C.R. SUB CALL/SERVICE
Q3
NETWORK MANAGEMENT DOMAIN
NEMF
NETWORK -OSF + NEMF FUNCTIONALITY
NEMF
C.R. SUB CALL/SERVICE USAGE Records
C.R. SUB CALL/SERVICE USAGE
Qx
Qx
CPN
CPN/PTN ACC; CALL RECORD CREATION
PSTN ACC; CALL RECORD CREATION
PROVIDER NE's
Equipment DOMAIN (NE's)

Fig 17d

### 5.3.1 Inter-Operator Accounting

#### 5.3.1.1 *Off - Line*

An additional accounting sub-process to cater for inter-operator charging is introduced. A possible allocation of these functions and their relationships with security functions in the TMN architecture is illustrated in figure 18. See also [22].

The Inter-operator accounting will exchange usage metering information based on the actual route the call has taken. It may also include the signalling traffic call management procedures e.g. interrogation, location updates etc.

In Figure 18 and 19, the Network Element Function (NEF) is part of a functional entity (FE), such an FE might generate accounting information and would contain the usage metering and on-line charging functions. In [34], it is declared that no decision has been made on which FE will be responsible for generating (part of) the accounting information. It is meant to apply to any FE that generates accounting information, e.g. CCF, SCF etc.

#### 5.3.1.2 *On-Line*

On-Line charging in the context of inter-operator charging, concerns the passing of real time charging associated with the selected service information accrued by a user while traversing network boundaries.

Charge activating supplementary services such as AD&C, Credit Limit, etc., by a user, used in a mobile environment can be problematic as identified in [26], particularly between network operators and service providers at handover time. The passing of such personalised services and notification of costs is an issue that needs clarifying.

Other forms of on-line real-time charging such as Coin boxes/Payphones and through pulsed analogue junctions to a subscriber provided meters, are not considered here. The accumulation of cost and collection of revenue is relatively straight forward and would follow an off-line procedure.

A possible allocation of on-line charging functions are shown in figure 18 and 19. Figure 19 represents on-line charging for supplementary services. The SCFs contain charging service logic programs (SLPs) that activate the on-line charging functions and collects the appropriate accountable events which are supplied to the on-line main function. At handover it stops the on-line charging function requesting further information and then performs further operations by the SLPs.

Consider a user (A), crossing the network boundary and requiring handover of “live” charging information so that the new network can continue with the charging required by the supplementary service. Two possible routes for information transfer to the other network is illustrated during the Handover process [27]:

1a. The charging info., is passed from the on-line function to SCF1 then stored in SDF1.
1b. SCF2 then requests the information from SDF1 and passes it to its own on-line charging function, where charging will be resumed using its own tariffing data, at the appropriate time.

OR

2. The SCF1 gets the information from the on-line charging, and temporarily holds it until SCF2 requests it. SCF2 supplies the information to its own on-line charging mechanism. Charging will recommence at the appropriate time.

This very abbreviated explanation of the operation is to highlight that users, service provider/network operator charging information, require a secure transfer mechanism to ensure confidentiality and integrity including access control for inter-operator communications.

The smooth crossing into adjacent management domains requires the real-time handover of user state, current session activity data (service & call) and authentication/authorisation information.

In [27], Integrity and confidentiality are considered to be optional. Possible mechanisms are identified in section 5 to provide the necessary protection at the level specified by the service providers/ network operators security policies.

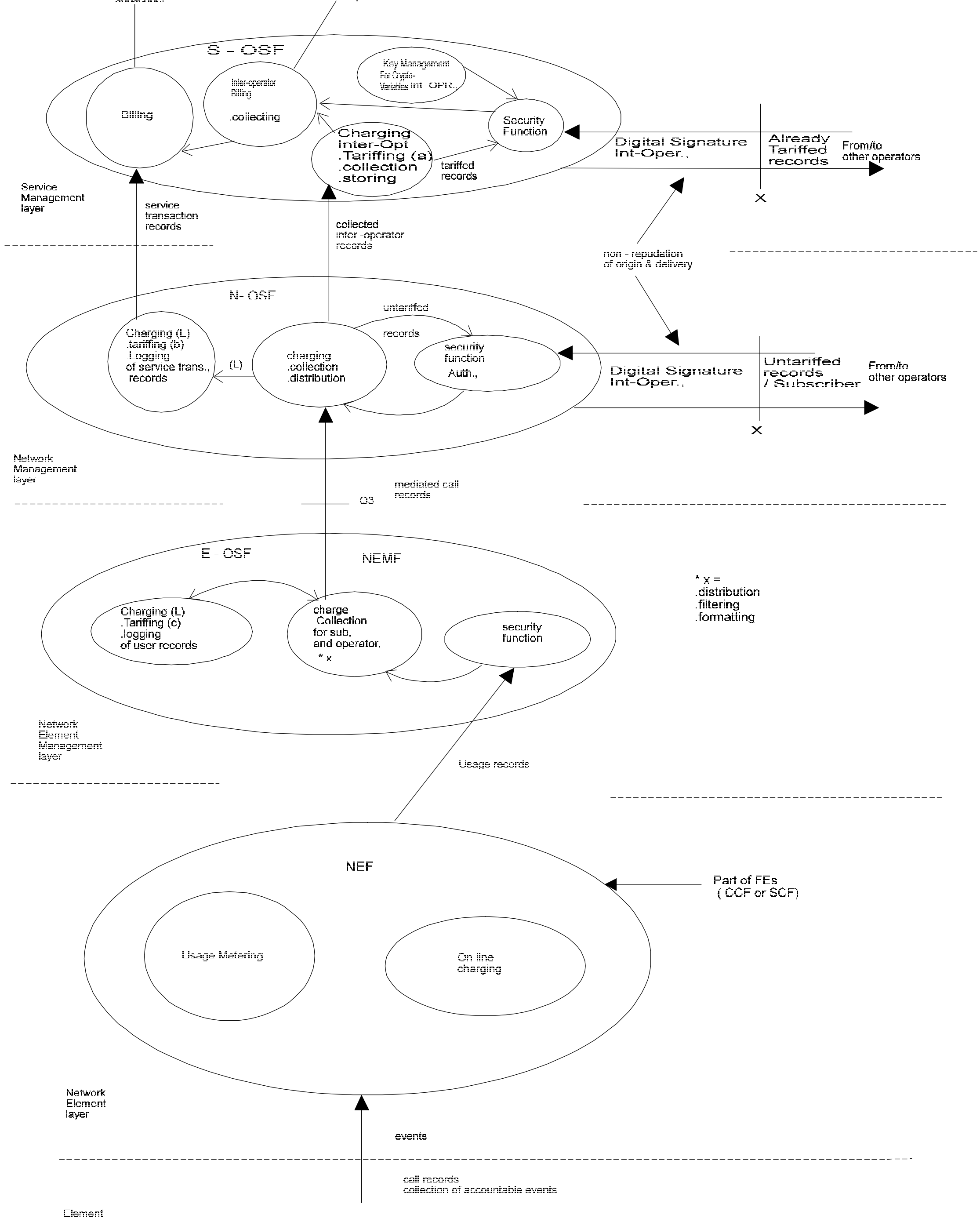

subscriber
other operators
S - OSF
Billing
Inter-operator Billing
.collecting
Key Management For Crypto-Variables Int- OPR.,
Security Function
Charging Inter-Opt .Tariffing (a) .collection .storing
tariffed records
Digital Signature Int-Oper.,
Already Tariffed records
From/to other operators
×
Service Management layer
service transaction records
collected inter -operator records
non - repudation of origin & delivery
N- OSF
untariffed
records
Charging (L) .tariffing (b) .Logging of service trans., records
(L)
charging .collection .distribution
security function Auth.,
Digital Signature Int-Oper.,
Untariffed records / Subscriber
From/to other operators
×
Network Management layer
Q3
mediated call records
E - OSF
NEMF
Charging (L) .Tariffing (c) .logging of user records
charge .Collection for sub. and operator. * x
security function
* x = .distribution .filtering .formatting
Network Element Management layer
Usage records
NEF
Part of FEs ( CCF or SCF)
Usage Metering
On line charging
Network Element layer
events
call records collection of accountable events
Element

**Figure 18: A possible allocation of security and accounting functionality in a TMN architecture**

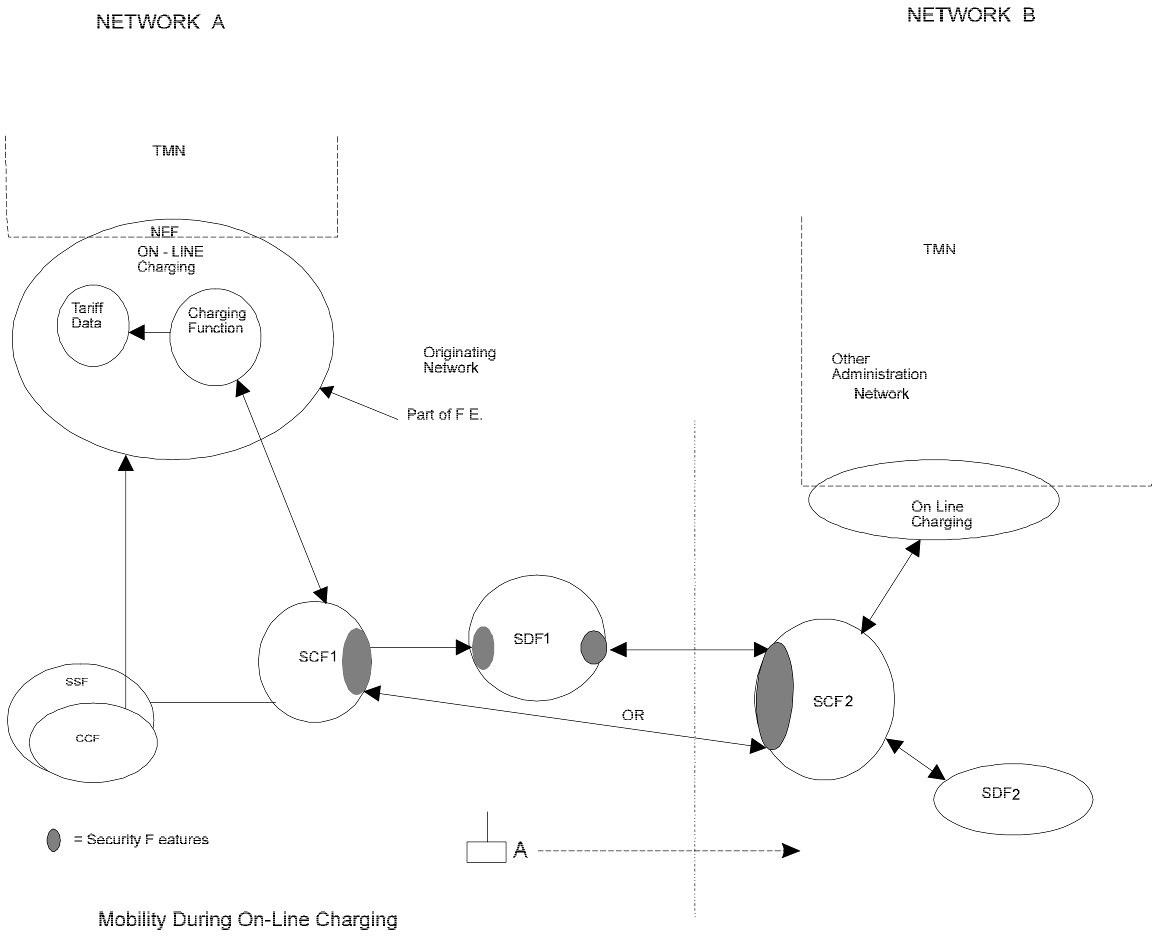


Figure 19: Mobility during On-Line Charging

## *5.4* Security features for charging, between Operators and Service Providers

### 5.4.1 **Off-Line**

The security function indicated in figure 18, uses the security features identified in TR 1 [1] of Confidentiality 1, Integrity 3, Authentication 6, and Non-repudiation 8.

A possible mechanism set from ISO 7498 - 2 security architecture [21], is selected and shown in table 2.

| **Mechanisms** | | |
|---|---|---|
| **For Authentication 6.** | **For Integrity 3.**<br>**For Confidentiality 1.** | **For Non - Repudiation 8.** |
| Password<br>Encipherment<br>Cryptographic | Handshake with protected parameters.<br>Time stamping with trusted clock. | Digital Signature and / or<br>Notarisation |
| | | |

**Table 2. Example mechanisms for management communication feature set.**

A combination of these mechanisms organised in a hierarchical structure could provide the management communication security needs as required in [23] and [24]. The structure of such a hierarchy is for further study.

### 5.4.2 On-Line

The security functional areas highlighted in figure 19, use the security features identified in [25] of:

- Confidentiality 1. Instance two;
- Integrity 3. Instance two;
- Non-repudiation 8. Instance one;
- Authentication 7. Instance one.

Mutual authentication is needed between the inter working entities of SCF - SDF, and SCF - SCF performed during the Decision Phase of handover [27].

**Note:** TMN does not take part in the on-line charging transfer but only in the setting up of the tariff data for a particular administrative network. This charging information is classed as Call Data. The security mechanisms are for further study.

## 5.5 *Issues*

In the SMF it is not known if charging will be performed as part of its overall functionality, or whether the SMF will only perform the account metering functionality of Usage metering.

## 5.6 *Charging Scenarios of 3GS3 Off-line Cases*

In this subsection UPT charging has been used as an example to illustrate the flow of charging information in the network and the appropriate roles that are involved in the management area.

### 5.6.1 Outgoing Calls

The charging and accounting information flow for a mobile user making a call in the UMTS environment is depicted by Figure 18. It illustrates that the charge and resource usage information generated by the used networks, where appropriate, are supplied to the user's Service Provider for billing of the subscriber and accounting of network usage to the concerned network operators.

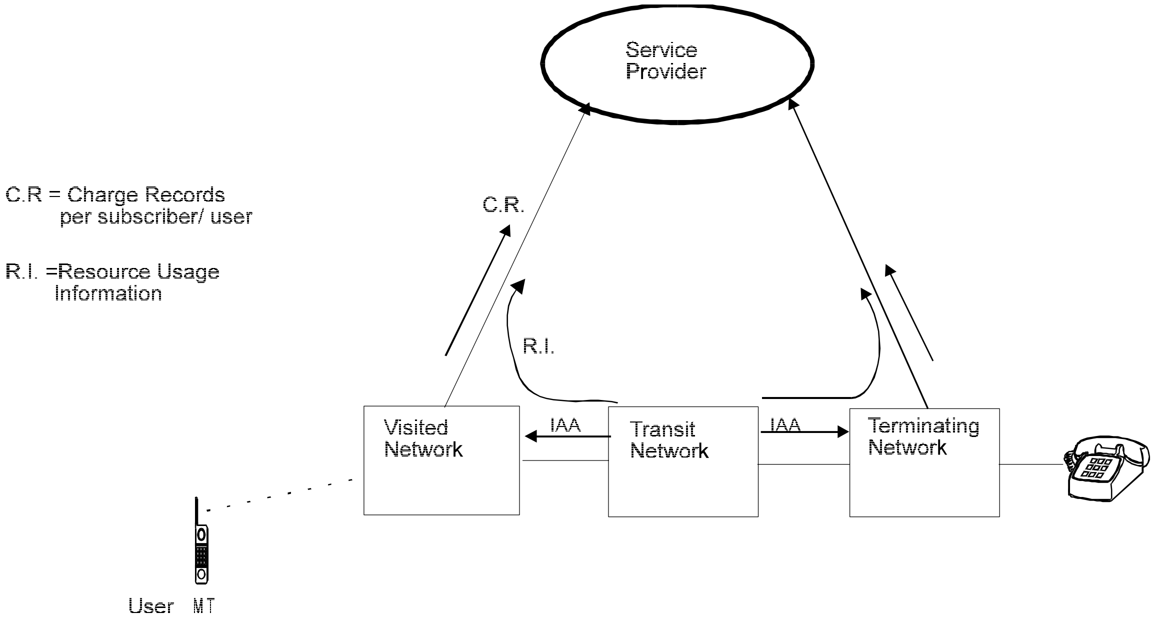


**Fig 20: Charging and Accounting Information Flow**

The Charge Record supplies information from the user’s subscription and actions. The Resource Usage Information provides the network resource information used in establishing the communication.

Each network illustrated in figure 18 represents a different administrative domain in which management functionality, switching, and service control nodes exist.

When a call is made, administration specified chargeable events are collected and a call record is created. This may be done by one or more node types in the domain, for example SSP, SCP or Adjunct. The call records are passed to the charging management functionality from which a Charge Record for the user/subscriber usage is generated and passed to the relevant Service Provider.

The Charge Records created by the charging management functionality contain for example, date, time of call, duration of call, service, service features used and resources used by the call.

Resource Usage information, for example, route used, circuit used, Call ID, Node ID, and any other resources that have been used in the call, are placed in the appropriate Call record and sent to the management functionality of that network's domain. These records are logged.

The charging management functionality in addition to generating Charge Records, generates Inter-administration Accounting records (IAA) from the composite Call record information. It is ‘screened’ and then dispatched or fetched.

The screening exists to provide a network operator with some degree of privacy from other communication network operators concerning his network.

The IAAs are generally bulk supplied on a monthly basis, or more frequently by agreement between network operators (NO), and/or Service Providers (SP). Figure 21 is an expanded version of outgoing calls illustrating the off-line charging information flow between networks.

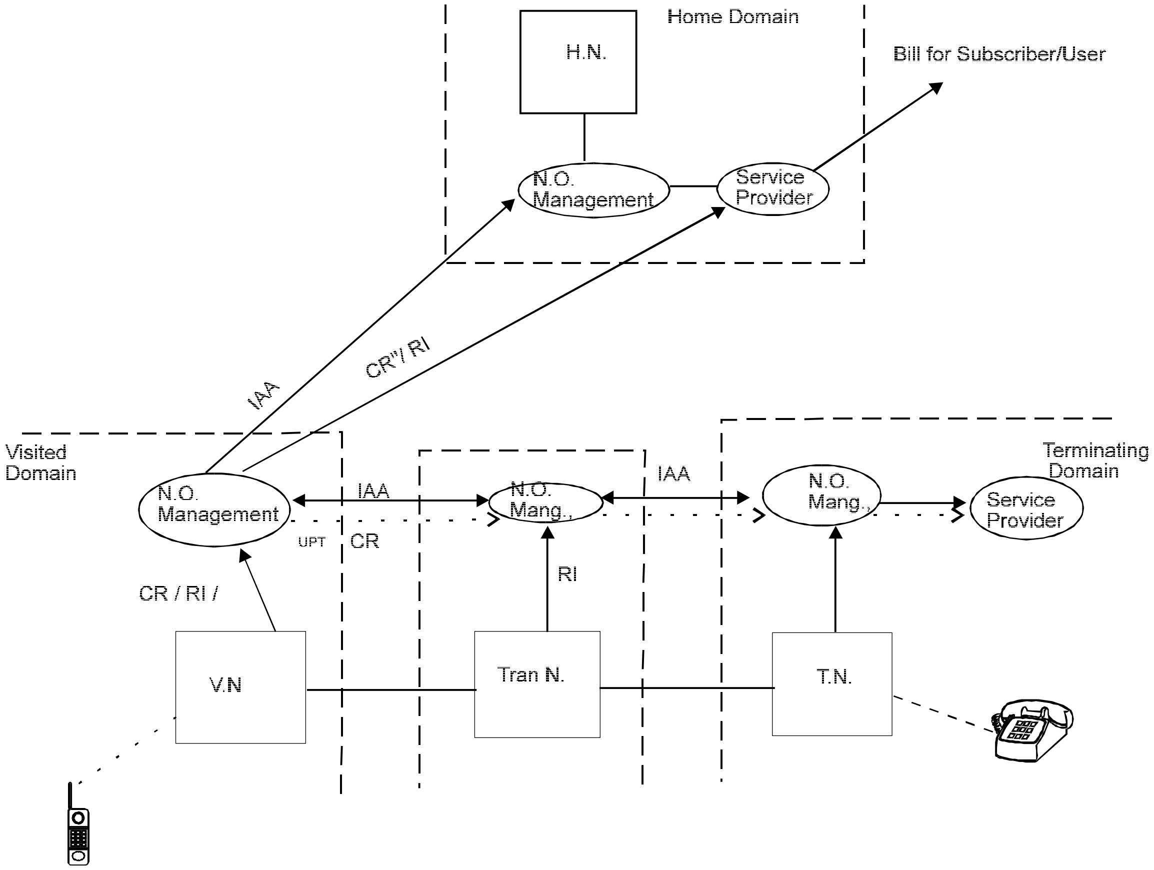


**Fig 21: Expanded version of figure 20, for Outgoing and Incoming Calls**

It is proposed that an international clearing house should be used for accounting records (IAA) between (UPT) service providers and network operators.

### 5.6.2 Incoming Calls

In UPT incoming calls to a user would create a call record and hence a Charge Record not dissimilar to a GSM mobile users 'split charging'. The UPT user as the called party, would be charged for that portion of the communication from his Home Location to the location he is at as illustrated in Figures 21, 23 and 24.

Charge Records will be sent to both the calling and called service providers.

If the called party however, is in his home domain then there is no charge for the receipt of incoming. Nevertheless a Charge Record will be raised indicating no charge.

The items within CR & IAA are needed not just for charging but for statistical analysis by the network operators and service providers.

### 5.6.3 Registration/De-registration for UPT user

It is assumed that the chosen scenarios for UMTS or FPLMTS must be similar in operation. Thus in the same way as incoming calls to a user in his home domain, Charge Records are raised for registration and de registration. This is shown in Figure 22.

The content of CR/RI may contain items such as:

- IMUI, TMUI, IMUN or CLI
- Originating network identifier
- Account identifier
- Supplementary service (or service feature) used.

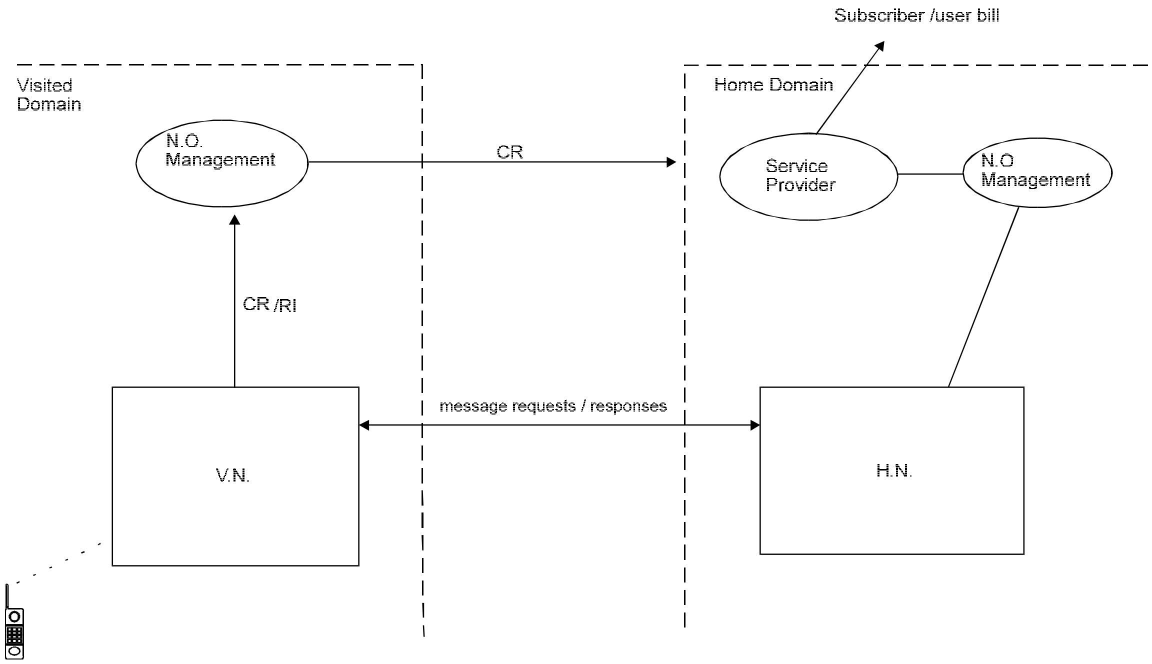


**Fig 22: Location Registration/Dereigistraion**

### 5.6.4 Location Registration

Location registration charges are related to the actual locations of the communicating parties. Charges are decided by the service provider/network operator or by the national regulatory body.

Possible factors establishing charges are:

- the duration of the communication
- time of day
- day of year
- the calling and called user locations.

These factors are represented as items of information appearing in the Charge Record (CR) and IAA.

The tariffs used by a given service provider in the case of user location, generally depend on:

- originating access network
- the intermediate or transit network
- the terminating access network;

and whose general characteristics of Quality of Service, bearer capability access type, etc., and the calling and called parties relative location to ‘home’ affect the tariffs.

The service provider tariffs, held in the charging management functionality, are assumed to be operated by the different network operator with the methods internationally agreed.

For UPT and UMTS, the service provider must have a mutual agreement with other service providers and network operators so that location related charges can be applied to the called and calling party depending on their respective locations see [29]. Figure 23 depicts a UPT call made by a mobile to another mobile with the Charge and IAA records being generated and supplied to the concerned parties.

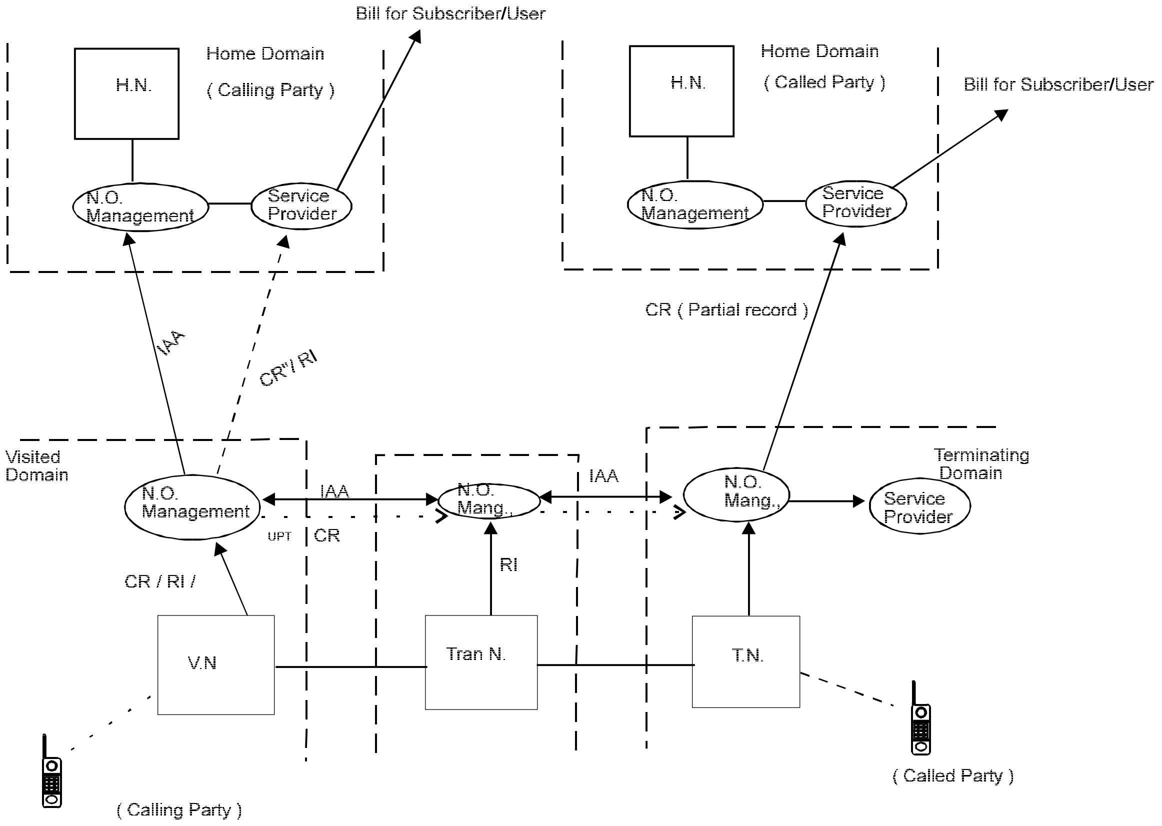


**Fig 23: Location Oriented Charging**

The partial record CR, in GSM split charging is generated by the called party terminating domain, and sent to the called party home domain. However, in practice, most networks will (because the call is routed via the home domain) generate the record themselves for their roamed subscribers/users, as it saves time in creating billing records for network use.

In figure 23, it shows the partial records going to the service providers. However, the terminating and originating network operator management, could send the records to the Home network operator management systems from which, the providers could be supplied.

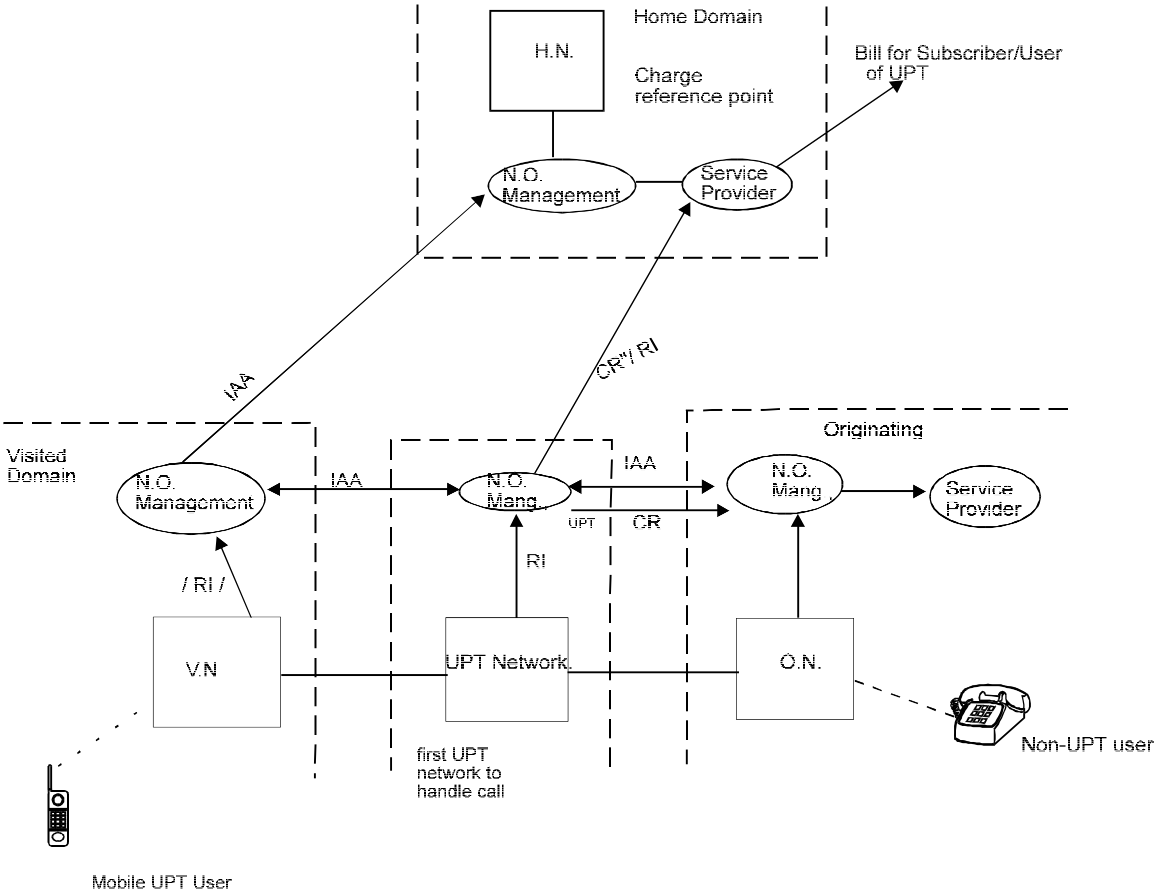


**Fig 24: Incoming UPT calls to a mobile user**

### 5.6.5 Record Content

The two general record types (IAA & CR/RI) do not necessarily contain the same information, as stated in GSM [30].

The elemental charges of 'Network Access' (a GSM tariffing component) are based on data registered in the subscription by the subscriber/user. These access charges are not included in the IAA accounts between network operators.

The access charges are collected by the Home PLMN (domain) or Service Provider and would appear in CR/RI.

The charges for 'Network Utilisation' (the other GSM tariffing component) do appear in the IAA as well as in the Charge Record to the Service Provider.

For UPT ETSI [29], the types of charges should in principle map to the GSM tariffing component elements.

The types of UPT charge are:

- subscription related charges
- service management related action charges
- personal mobility related action charges
- call related signalling charges
- location related charges

It is not clear if all the charge elements of UPT will map to UMTS. It is suggested in ITU [31], ( Baseline doc., Req., for UPT), that new accounting arrangements between UPT and UMTS providers will be required.

#### 5.6.5.1 *IAA Record Elements*

The IAA may contain information on:

- Date and time a circuit is seized for incoming and outgoing routes
- Date and time User (calling party) clear
- Date and time called party clear
- Date and time of signalling message 'Address Complete'
- Time of 'Answer' (used to start charging)
- Time discontinuity
- incoming network Route number (Port address)
- Outgoing network Route number (Port address)
- Called Number
- Originating network Identifier (Visited identity)
- Logging exchange identifier
- Point-of-entry type of access
- Answer indication
- Charge Band (i.e. destinations with common charge rates)
- Call clearing cause
- Call type i.e. Incoming or Outgoing
- Bearer service indication
- Teleservice indicator
- Number of data units

#### 5.6.5.2 *Charge Record Elements*

The Charge record may contain the following information:

- User Identifier
- Public User Number
- Date and time of Authentication
- Date and time of start of call
- Date and time of end of call
- Call duration
- Origin
- Called number (i.e. Dialled number)
- Default charging reference location (i.e. home or temporary home)
- Routing address (where the mobile user is now i.e. IC/OG network routing number)
- Re-routing number (data item shown if service feature is active e.g. call forwarding, call transfer).
- Supplementary service indicator (i.e. service feature)
- Bearer service indicator
- Number of data units (for volume charges)
- Teleservice indicator
- Surcharges (i.e. fixed fees)
- Account identifier
- Partial output record
- Correlation identification
- Access category ('normal line', coin box, hotel, office, mobile etc.,)
- Visited network identity

### 5.7 *Ownership*

Ownership of charging information is categorised for convenience into two types - Variables and Parameters.

Variables :
The contents of the IAA and CR have information which does not necessarily belong to any specific organisation or user, but is needed for the operation of the telecommunications system. Such variables, for

example, date, time, address complete, time of answer, are used by administrations in their call charging calculations, not only for the subscriber/user but also network operator to network operator, network operator to service provider. The integrity of this information is therefore important for charging purposes.

Parameters :
The other items in the records are 'owned' i.e. their values are controlled and may be specified by their owners within certain bounds. These parameters, may be considered as private data thus requiring confidentiality and integrity security features in their storage and transmission to other NOs and SPs.

The following tables attempt to classify the items that are likely to be sent in IAA and CR [32].

| Variables | Used By | | | | |
|---|---|---|---|---|---|
| Items in IAA & Charge Record | NO | SP | Sub. | User | |
| - Date | * | * | | | |
| - Time | * | * | | | |
| - Calling Party Clear (date & time) | \| | \| | | | |
| - Called Party Clear (date & time) | \| | \| | | | |
| - Address Complete | \| | \| | | | |
| - Answer | \| | \| | | | |
| - Time Discontinuity | \| | \| | | | |
| - Correlation identification | \| | * | | | |
| - Answer indication | \| | \| | | | |
| - Answer charge/no-charge | \| | \| | | | |
| - Partial output record | \| | \| | | | |
| - Call clearing cause | \| | \| | | | |
| - Bearer service indication | \| | \| | | | |
| - Teleservice indication | V | V | | | |
| - No. of data units etc. | * | | | | |

Table 3

| Parameters | Ownership | | | | |
|---|---|---|---|---|---|
| Items in IAA | NO | SP | Sub. | User | |
| - IC/OG Circuit Identifier | * | | | | |
| - IC/Network Route Number (port address) | \| | | | | |
| - OG/Network Route Number (port address) | \| | | | | |
| - Called Number | * | * | | | |
| - Originating Network Identifier | \| | | | | |
| - Charge Band (charge rates) | \| | * | | | |
| - Point of Entry # etc., | V | | | | |

Table 4

| Parameters | Ownership | | | | |
|---|---|---|---|---|---|
| Items in Charge Record | NO | SP | Sub. | User | |
| - Origin (CLI or IMSI/TMSI) | * | * | | | |
| - Called Number | * | * | | | |
| - Default Charging Reference Location | *? | * | | | |
| - Routing Address | * | | | | |
| - Re-routing Address (service) | | * | | | |
| - Surcharge | * | * | | | |
| - Account Identifier # | | * | | | |
| - Access Category etc., | * | | | | |

Table 5.
***Note:***_: * - - - - - ->   = from -too, all the same_

It appears from the classification that only network operator's and service provider's information are in the records, thus the security requirements may only need to consider a two role arrangement for any instance of transfer.

# 6. Information Flows

There are two ways of representing the information flows for authentication mechanisms with respect to the two different models used by 3GS3 i.e. a role model and the functional model [1.2] which have been adopted by the project. The general information flow options for the authentication processes can be found in the technical report, TR2 [2].

Specific functional model cases are applied to mobility management flows to show the support of authentication procedures in UMTS or FPLMTS.

## 6.1 *Support of Authentication procedures*

### 6.1.1 Assumptions

Firstly, core network functional structures are as in Figure 4, and such a functional network structure map to IN physical node types :

| Functional entities | Node types |
|---|---|
| SCAF, CCF/SSF | SSP+ (service switch +non-call associated cap.) |
| SCF | SCP |
| SDF | SDP |

also these entities are used by UMTS network operator to provide the network mobility capabilities. and the other role model entities map to the functional model as indicated in figure 25.

Secondly, when a UMTS user via an access network, uses a UMTS core network in which the service provider/network operator does not directly hold the user's master profile, the network is referred to in the paper as the Visited network. The Home network is a UMTS core network in which a user's master profile is kept and maintained by the subscriber and service provider.

Thirdly, it is assumed that the subscriber service provider transfers the subscribers user's service profile information into the home UMTS network operators SCP/SDP by agreement.

### 6.1.2 Access Network Signalling

Access network signalling will not be considered in this paper. Those in the core network will be investigated.

### 6.1.3 Functional Structure in core network

There are three basic IN network entity relationship structures for the core network in the service control plane, in which the UMTS network operator and service provider may have different entities. These structures are illustrated in figure 25. The authentication procedures performed would obviously be under different role ownership.

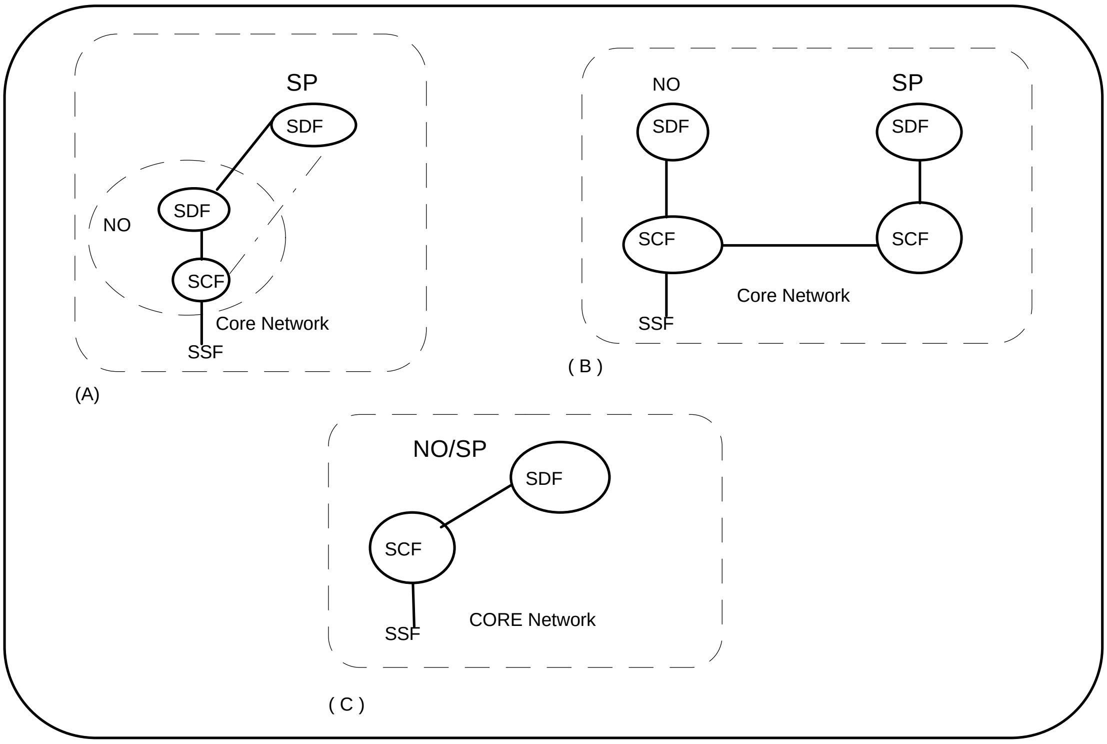


**Figure 25: Optional structures for core network - NO/SP functional relationships**

The three options indicate the relationship between FEs for UMTS network operators and service providers. In the structures the user authentication capability is possibly divided between the network operator (NO) and service provider (SP) for the different options which are applicable during the mobility registration function; see [24].

In option (A) the Registration/de-registration (RDH) feature using assumption 1,is located in the NO SCP with the authentication (Acc) capability in the SP SDP.
Or
the RDH in NO SCP and Acc in NO SDP with user profile data in SP SDP.

Option (B), RDH is in NO SCP and Acc is in SP SCP.

Whilst in option (C) RDH is in NO/SP SCP and Acc is in NO/SP SDP; using assumption 3. Option c functional structure would then represent the service control plane of the ‘visited’ UMTS network operator, and the ‘home’ UMTS network operator and service provider.

Options (A &B) will not be considered in this paper since the information flows and signalling interfaces between SCF<--> SCF, and SDF<-->SDF are unstable.

Option (C) for authentication at registration time will be considered in the following text for user or terminal.

**Note:** certain assumed operations are made between networks.

### 6.1.3.1 *Security Protocols in the core network*

The security protocols chosen for option (c) are from 3GS Technical Report 2 [2], and SMG ETR 50901 ver 2.2.0 [24], those of Mutual Authentication which combines mechanisms as detailed in the general authentication information flows of [2]. There are two mechanisms applicable at Registration times, one for current registration and another for new registration. The current registration has a three message structure, while the new registration has a five message structure. The information flows for these registration methods are shown in figures 26, and 27 respectively. Only the start and authentication flows are shown between the main physical entities e.g. networks/ UIM.

The notation and abbreviations in the following figures and text of this section of the report, can be found in TR2 [2].

### 6.1.4 Mutual Authentication Information flows

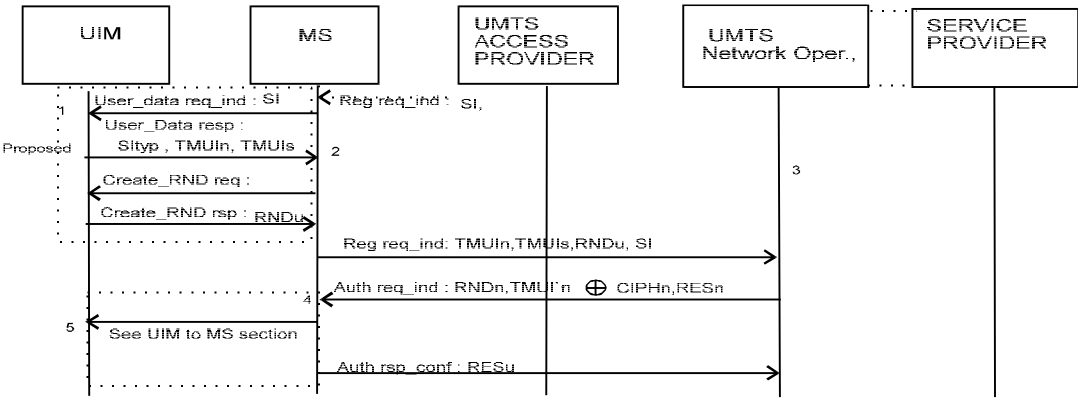


**Figure 26: Network information flow to network operator.**

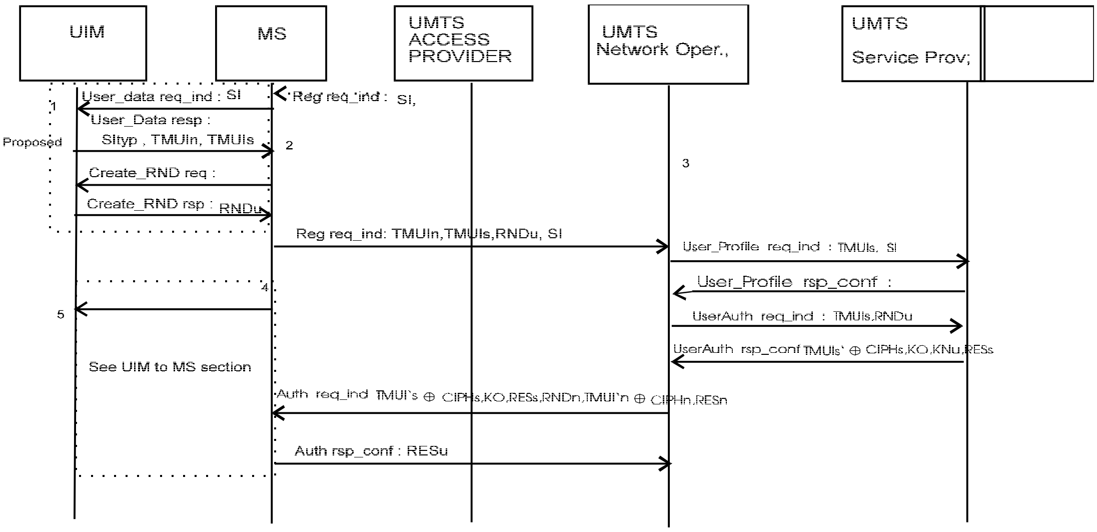

UIM
MS
UMTS ACCESS PROVIDER
UMTS Network Oper.,
UMTS Service Prov;
User_data req_ind : SI
Reg req_ind : SI,
1
User_Data resp : SItyp , TMUIn, TMUIs
Proposed
2
3
Create_RND req :
Create_RND rsp : RNDu
Reg req_ind: TMUIn,TMUIs,RNDu, SI
User_Profile req_ind : TMUIs, SI
User_Profile rsp_conf :
4
5
UserAuth req_ind : TMUIs,RNDu
UserAuth rsp_conf TMUIs' ⊕ CIPHs,KO,KNu,RESs
See UIM to MS section
Auth req_ind TMUI's ⊕ CIPHs,KO,RESs,RNDn,TMUI'n ⊕ CIPHn,RESn
Auth rsp_conf : RESu

**Figure 27: Network information flow to service provider**

The abbreviations used in the protocols above are defined in TR2 [2].
Figures 24 and 25, for the ‘visited’ and or ‘home’ service control plane structure follows option (c), in figure 25.

The following observations are made :
1. It should be possible, as shown in figure 27, to allow the flows between network operator and service provider to be swapped around with authentication taking place first followed by the supply of the user service data.
**Note:** these transactions could be SCP to SCP.

2. Another possibility is that, the operations of User_profile and User_auth., be combined in a single request message with a single response message to the requester.

The remainder of this document refers to the new registration sequence as shown in 27, with expansions of the network operator and visited networks in terms of option (c) and the functional model entities.

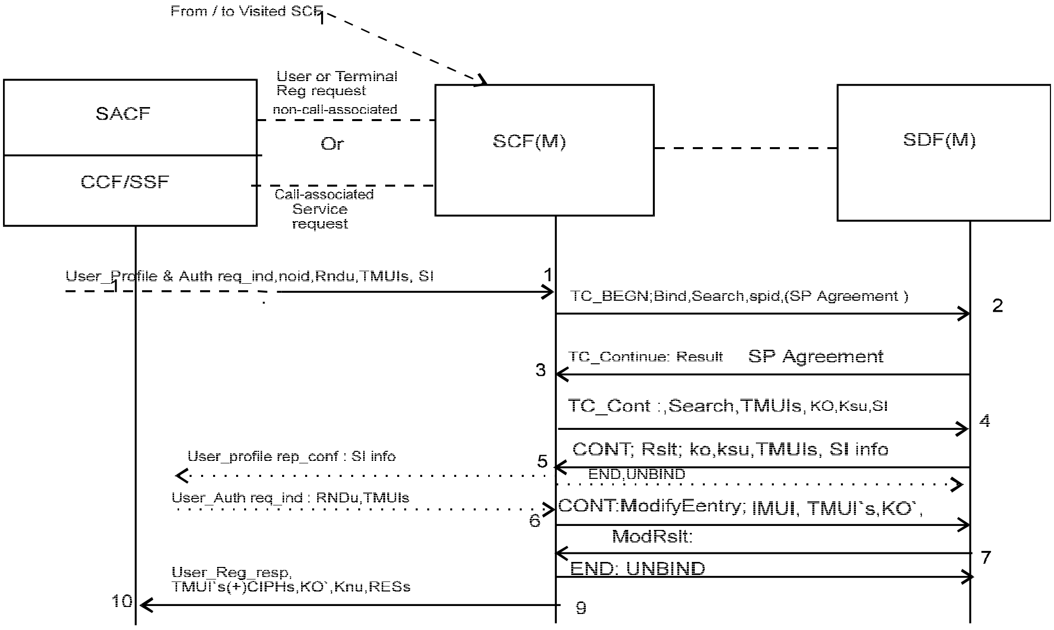

From / to Visited SCF
User or Terminal
Reg request
non-call-associated
Or
Call-associated
Service
request
SACF
CCF/SSF
SCF(M)
SDF(M)
User_Profile & Auth req_ind,noid,Rndu,TMUIs, SI
1
TC_BEGN;Bind,Search,spid,(SP Agreement )
2
TC_Continue: Result SP Agreement
3
TC_Cont :,Search,TMUIs, KO,Ksu,SI
4
CONT; Rslt; ko,ksu,TMUIs, SI info
User_profile rep_conf : SI info
5
END,UNBIND
User_Auth req_ind : RNDu,TMUIs
6
CONT:ModifyEentry; IMUI, TMUI`s,KO`,
ModRslt:
7
END: UNBIND
User_Reg_resp,
TMUI`s(+)CIPHs,KO`,Knu,RESs
10
9

**Figure 28: Information flow between functional entities**

### 6.1.4.1 *Service Provider Information flows*

The figure 28 above indicates the possible transactions in a ‘home’ network as a consequence of a new Registration request occurring in a ‘visited’ network.

The following statements describe likely behaviour in the SCF and SDF. Only information elements associated with security are considered.

#### 6.1.4.1.1 Procedures

1. A request indication arrives at the SCF(M) from SCAF or from another SCF. The request carries the temporary mobile user identity (TMUIs ), a random ‘challenge’ RNDu supplied from the user UIM and the visited network operator’s identity (NOID).

2. A BIND and Search operation is performed on the SDF. The specific Service Provider agreement is obtained in the SDF using the SPid which was computed from TMUIs.

3. The received noid is checked against the agreement noid to establish validity. If the identity cannot be verified an error message is returned. If the identity is OK, the SP agreement is returned which allows the SCF(M) proceeds to verify the user and obtain the security parts from the user service profile in SDF

4. Perform a search on the SDF with TMUIs.

5. The search result returns IMUI, KO, Ksu. and TMUIs.

The following functions may be performed at the SCF either in parallel or in serial between transactions 5&6.

a) Generate a new TMUI's value. See 3GS3 TR2 [2]

b) Generate a Key-Offset KO'

c) Call a key generation function. Inputs to the function are Ksu and a concatenated data string of NOID || KO' giving a computed output secret key Kn.

d) Call a key Generation function. Inputs to the function are Ksu, and a data string composed of KO', the RNDu and TMUI's concatenated. This function gives an output referred to as RESs **-** the 'challenge response' to the user.

e) Call a cryptographic check function (or hiding function ) this function will protect the integrity and verify the origin of the data string used to produce it. Its inputs will be Ksu and the RNDu received from the user giving the output CIPHs which is exclusively Ored with TMUI's.

6. Modify the user service profile security parts using the IMUI to address and store TMUI's, KO' and Kn

7. Check the result.

8. End the association with the SDF

9. Create a return message from the SCF to SACF or SCF which will be destined for the visited network and the user.

#### 6.1.4.1.2 Constraints

1. Time limitations

Between the arrival message (1), and the response (10) in figure (c) there is an imposed time limit of between 1 and 10 seconds. The actual value used is selected by the national administration. See [36]. This limits the computation time available for the home network (i.e. Authentication Server)

2. TMUI structure

Secondly the possible structure of TMUIs. If a user is to roam into different networks then the structure of TMUI must be:

CC--NDC--SN - an ITU-T E.164 structure, where CC = Country code, NDC= Network ID + SCPID + SPID and SN = subscriber (user) number.

The maximum number of digits for international use will be 15digits, therefore the variable user part of TMUI is quite limited.

**Issue:** does this limitation of TMUI reduce the security of the Mutual Authentication?

Another way of addressing the message during registration is to use the MSISDN number (Mobile Station ISDN Number) i.e. the diallable number which could be held in the UIM, to get to the user Home carrying TMUI as data in the message. This would enable a larger variable number set for users.

3. Bandwidth Limitations

On the SCF interface to other SCFs, SDFs and SSFs there is a protocol limitation of 272 octets (this restriction is as a consequence of MTS etc.). However, the bandwidth could be solved by using a broad band stack e.g. ATM.

4. Secure Links

See Network Operator information flow constraints.

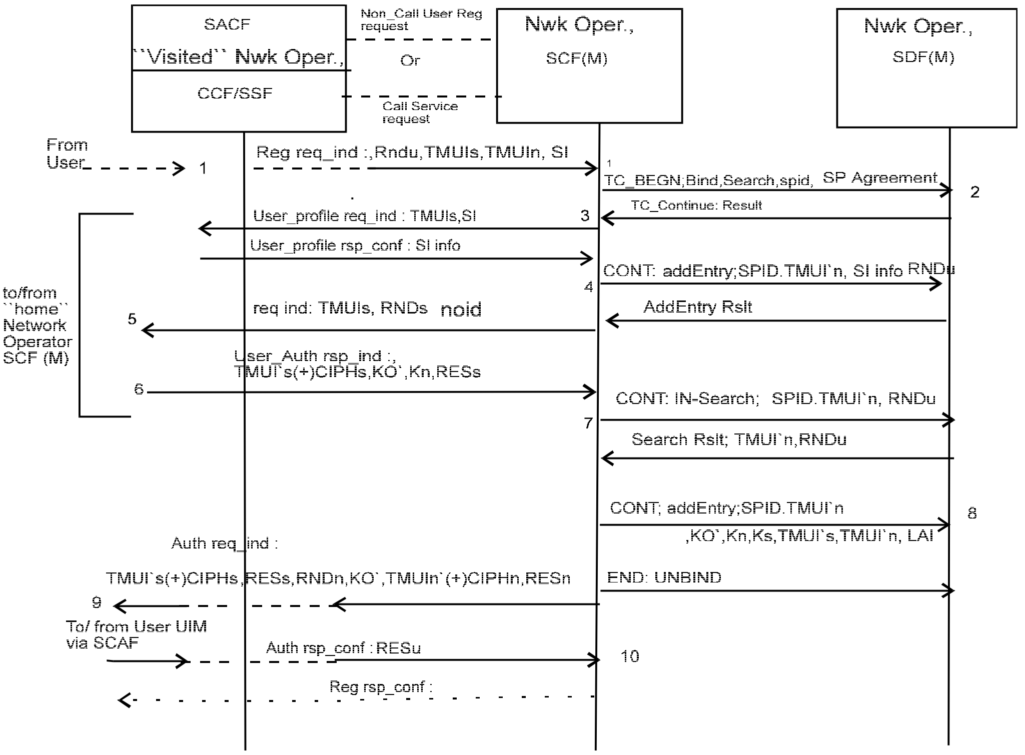

SACF
``Visited`` Nwk Oper.,
CCF/SSF
Non_Call User Reg request
Or
Call Service request
Nwk Oper.,
SCF(M)
Nwk Oper.,
SDF(M)
From User
1
Reg req_ind :,Rndu,TMUIs,TMUIn, SI
1
TC_BEGN;Bind,Search,spid, SP Agreement
2
TC_Continue: Result
3
User_profile req_ind : TMUIs,SI
User_profile rsp_conf : SI info
CONT: addEntry;SPID.TMUI`n, SI info RNDu
4
to/from ``home`` Network Operator SCF (M)
5
req ind: TMUIs, RNDs noid
AddEntry Rslt
User_Auth rsp_ind :, TMUI`s(+)CIPHs,KO`,Kn,RESs
6
CONT: IN-Search; SPID.TMUI`n, RNDu
7
Search Rslt; TMUI`n,RNDu
CONT; addEntry;SPID.TMUI`n ,KO`,Kn,Ks,TMUI`s,TMUI`n, LAI
8
Auth req_ind :
TMUI`s(+)CIPHs,RESs,RNDn,KO`,TMUIn`(+)CIPHn,RESn
END: UNBIND
9
To/ from User UIM via SCAF
Auth rsp_conf : RESu
10
Reg rsp_conf :

**Figure 29: Registration Request by User to a Visited Network**

### 6.1.4.2 *Network Operator information flows*

The figure 29 above shows the security information flows between the mobile IN functionality in the visited core network for a Registration request by a user. The additional elements within the flow, e.g. TMTI, LAI, SI etc. are not shown.

The identified operations performed by the SCF(M) and SDF(M) for the security aspects are described in the following statements :

#### 6.1.4.2.1 Procedures

1. On receipt of the user request indication, the SCAF triggers and sends the message on to the SCF. The SCF determines the provider Id from TMUIs and opens a dialogue with its own SDF.

2. A bind and Search operation for the SP agreement and Route information is requested from the SDF.

3. The result is returned - SPID, Route data and Agreement data.

The following transactions may be performed between transactions 3 and 4.

a) A temporary mobile user ID TMUI'n is generated [see section 2].

b) A request is made for a new visited object to be created in the SDF, with objectid of Spid.TMUI'n and with RNDu and TMUI'n as attributes.

4. An addEntry operation is requested of the SDF,with the appropriate results returned.

5. The route is selected and a request (authenticate user) is sent to the user's home network.
**Note:** the dialogue between the SCF(M) and the SDF(M) is kept open while waiting for the response from the home network.

6. On receipt of the response the data is searched for KO', Kn and held.

7. Using the original spid.TMUI'n the content is requested.

The following operations may be performed between transactions 7 and 8:

a) Generate a Random number RNDn.

b) Call a hiding function, (Cu). The input uses key Kn, and a data string RNDu, giving the output CIPHn ,which is exclusively Ored with TMUI'n.

c) Call the User Authentication Function. This function uses key Kn and a data string of concatenated data items of RNDn, RNDu and TMUI'n. The output RESn is the challenge response from the visited network.

d) A session Key generation function is called, with inputs of Kn and a data string of RNDn, RNDu and TMUI'n the output of which gives the session key Ks.

**Note:** operations c and d could be performed in parallel.

8. The created and received data items are now added to the visited object spid.TMUI'n in the SDF(M). These items being KO', Kn, Ks and TMUI'n.

If the results are satisfactory, the SDF is unbound from the SCF and the dialogue closed.

9. The user response message is created and returned via the SACF. The security message elements being: TMUI's exclusive Ored CIPHs, RESs, RNDn, KO', TMUI'n exclusive Ored CIPHn and RESn.

This message contains the 'challenge responses' from the service provider and the visited network operator, including an additional 'challenge' from the visited network operator.

10. This message is the response from the user UIM to the challenge:

$$RESu = Akn [RNDu \| RNDn.$$

where A is a user authentication algorithm in the UIM. A new value of RESu is computed at the SCF(M) and compared with RESs for equality.

**Note:** It is assumed that the A algorithm is standardised.

### 6.1.4.2.2 Constraints

The constraints are not dissimilar to those of the home network stated above.

#### 6.1.4.2.3 Secure Links

A secure signalling link is required between the Visited Network and the Home Network. In figure 29 transactions 6 and 9 require such a facility. This inter-network security requirement is imposed by the mutual authentication protocols on the network operators infrastructures.

The need for Confidentiality and Integrity security services on such links would require standardisation.

## 6.2 *Support for UIM data and UIM management*

An initial study was made of information flows for the mutual authentication mechanism between User Identification Module (UIM) and Terminal (MS) at their interface. The aim was to establish where each of the algorithms should be implemented and where information should be stored. To this end a scenario is presented in figure 30. This is not the only possibility. The algorithms are identified in Technical Report 2 [2].

### 6.2.1 **Assumptions**

The following assumptions have been applied to the scenario :

- The user-service provider key Ksu is stored securely on the UIM, and never leaves the UIM, in particular never passes over the UIM/Terminal interface. Therefore, all algorithms which use Ksu must be executed on the card, these are :
    - the identity algorithm Cu using for calculating CIPHs
    - the network operator generation algorithm An.

  It is assumed that the algorithm Cu for calculating CIPHs and that for CIPHn are different and can be implemented in different entities. If this is not the case then Cu is implemented on the UIM.

- The temporary identities TMUIs and TMUIn are stored on the UIM, as they are user specific and require retention between user UIM sessions.

- At the start of any UIM session it can be assumed that the UIM has the current TMUIs and TMUIn stored.

- It is also assumed that the encryption algorithm will be implemented on the terminal since no other information is given in [2].

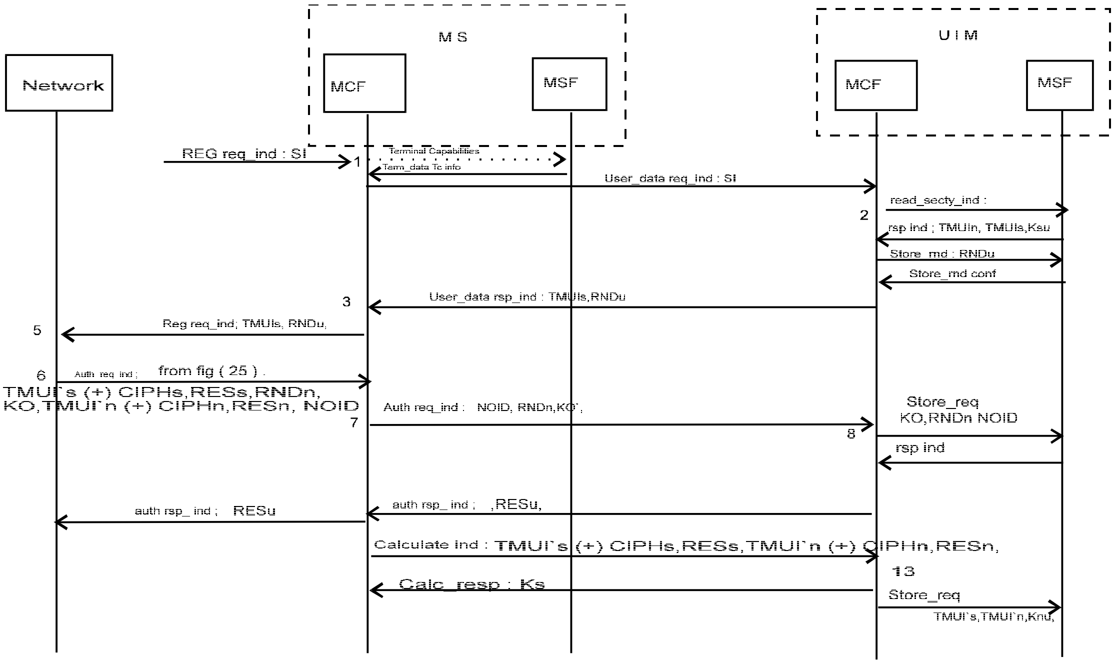


**Figure 30: Information flows between an MS, UIM and network**

### 6.2.2 UIM and Mobile Station Interaction

Figure 30 above shows a proposed information flow between the user information module (UIM) and the mobile station terminal (MS).

The authentication of Service provider and network operator is performed on the UIM, including the recovery of the temporary identities and session key generation, the latter being passed to the MS.

Operations are defined in 3GS3 TR [2] ‘A mutual authentication mechanism for UMTS’.

The identified operations performed by the MS and UIM for the security aspects are described in the following statements:
**Note:** The numbers appearing in the following text at the start of a statement refer to figure 30.

1. On receipt of a registration request from the User the MS passes the message to the UIM.

2. The MCF function of the UIM calculates a random number RNDu , stores the number local then sends a Read_request for the TMUIn and TMUIs to the MSF of the UIM. The MSF responds with the required information plus Ksu.

3 The registration response is returned to the MS containing the TMUIs, RNDu.

5. A request  indication is sent to the network containing the random challenge TMUIs, RNDu.

Between steps 5 and 6 the information flows as described for figure 28 may be performed.

6. An Authentication request is sent from the network. The MS selects the appropriate parameters NOID, RNDN, KO and passes them on.

7. A user request authorisation message is sent from the MS to the UIM containing the selected parameters where it is received by the UIM MCF

8. The UIM MCF performs the following calculations :
Calc., Knu = An(Ksu,KO,NOID) ; Calc., RESu = Au(Knu,RNDu | | RNDn), and locally stores KO, RNDn, NOID. A response is returned to the MS -RESu.

10. On receipt of RESu the MS sends to the UIM the remainder of the original message of - TMUI`s(+)CIPHs,RESs,TMUI`n(+)CIPHn,RESn.

13. The UIM calculates - CIPHs = Cu(Ksu,KO,RNDu ) and exclusively-or with --(TMUI’s(+)CIPHs) to recover the new temporary identity TMUI’s.
It then, using the service provider algorithm ( As ) it creates RESs such that
RESs = As(Ksu,RNDu|| KO || TMUI’s) : it then proceeds to compare the received RESs with the generated RESs If OK, similar calculations to recover and test RESn are performed. e.g. Calc., CIPHn = Cu(Knu,RNDu)
If OK,
the next action is to create the session key Ks. This is calculated as follows :
Ks = Ak(Knu, RNDu || RNDn || TMUI’n ) ; where Ak is the session key generation algorithm.
The session key is then passed to MS for use until further change.
In addition the UIM stores by overwriting TMUIs and TMUIn with TMUI’s & TMUI’n in the MSF.

**Note:** If any of the checks were to fail a message is returned to the MS and to the network.

### 6.2.3 **UIM/Terminal Interface Issues**

The following is a list of discussion points which will allow an initial definition of the UIM/Terminal interface to be made:

1. The user - service provider key $K_{SU}$ is analogous to the subscriber key Ki in GSM except that Ki is never updateable, and therefore can be physically protected as a result of the manufacturing process. If the $K_{SU}$ is to be up datable during the life of the UIM it will have to be logically protected and therefore careful consideration should be given to how this will be achieved.

2. If encryption is implemented on the terminal then the UIM/Terminal interface is clear, and therefore it is probable that a further algorithm will be required on the UIM to support secure messaging for certain applications between the UIM and external world. Secure messaging would of course not be required if the encryption algorithm is implemented on the card. The first option could be achieved, and in fact is specified for the TE9 card. The second option requires close study, especially with respect to timing and would not be compatible with GSM.

3. If secure messaging is required then the ETSI TE9 specifications should be studied. These specifications define telecommunications IC cards and terminals. Secure messaging within these specifications is defined between an external secure module and the card. In the pay phone environment the secure model is usually placed within the call box, this being possible because the pay phone operator owns the call box. This is of course different in the mobile environment, and the secure module is more likely to be within a network/application entity.

4. A working assumption is required as to whether backwards compatibility with GSM is to be supported, and if so, for how long. The present GSM SIM does not allow radical enhancements to its logic during its lifetime. It is almost certain that this will not be the case for future generation cards, and this fact has to be considered with respect to migration and the design of the card.

### 6.2.4 **Summary**

It is difficult to guess exactly what the UIM will support in the future, and how quickly the UIM/Terminal interface will perform being dependent on the protocol used. The scenario used tries to create the response to the MS and hence network as quickly as possible and utilise the time while waiting for the conformation that registration was successful. It is clear that a number of fundamental questions as stated in the sub-section ‘UIM/Terminal Interface Issues’ need addressing before protocol constraints are established.

## 6.3 *Support for Identity passing*

### 6.3.1 **Scenarios for transmitting line identities.**

In current systems, a number of relationships exist between operators and other players.

Logically Network Operators have differing roles:

The Visited Network Operator,
A number of Transit Network Operators,
The Call Originating Network Operator.

Other Players will in future include the Service Providers of both parties and the Authorised Parties who will receive Malicious Call Identification service (MCId).

The normal operation of the Calling Line Identity Presentation service (CLIP) is the number of the calling line, in mobile telephony the calling party, is delivered by the call set-up to enable the called party to evaluate who is calling them before the call is answered.

They may as a result chose not to answer the call. In future call screening systems will be able to intercept the incoming call and automatically, block or divert unwanted calls. Also the called users equipment, or destination switch, may be able to use the calling number information for ring-back.

The requirement for calling party number to be delivered to the called switch will soon be a UK standard for all users and interconnection. The goal of these changes is to remove the intrusion the telephone makes into our private homes.

The Calling User may of course subscribe to Calling Line Identity Presentation/Restriction which will instruct the destination switch to not present the identity to the called terminal/user. So the user cannot chose to not answer the call since they do not know who it is from. Though the called user will realise that the identity has been restricted.

The delivery of the calling party number across the network is performed irrespective of the subscribed restriction presentation service is for two reasons :

1. the information may be required by interconnected networks, and Independent Service Providers, to collate bills for the user and for each other.

In addition, the Routing Address is required by the billing centre to add to event records. This is normally displayed in partial form on the users bill so that they can see where calls were made from and where calls were received that incurred an excess charge.

2. the called user may also have invoked the MCId service. The MCId allows a concerned Called Party to dial a Special Access Code at their terminal which will cause the Calling Party's Number to be printed out along with the event record for the call at an authorised location which may monitor calls. This must happen whether or not the Calling Party subscribes to number presentation restriction. The purpose of this is to discourage malicious and nuisance calls, and aid toward catching the offending parties.

Authorised Parties are normally the local police station to the fearful called user. Clearly, the registration of the MCId service requires some initial effort by the authorising party and network operator, hence, users will need to register their need for this service prior to their malicious calls being registered.

In principle, for mobile users the Calling Line Identity is the Users Number not the Routing Number of the port (base station) where the call is routed from. This preserves the confidentiality of the mobile users location. However, in this case the routing number (base station port address) must also be delivered to the destination switch to assist the MCId service, with the calling party's number. This Routing Number is used by the Authorised Party to discover the location the call was made from, and is never presented to the end user.

Hence the calling party’s number must, in future, be transmitted with the call set-up across the network. If the calling party subscribes to Number Presentation Restriction an indication is also to be sent with the call set-up to instruct the destination switch to not present the identity.

Malicious Call Identity (MCId) for called mobile terminals is being investigated by the GSM committees, clearly it is no longer rational that destination switch is likely to be the local switch to the authorised party.

## 6.4 *Support for legal interception requirements*

### 6.4.1 Introduction

The EC has published a document which details the requirements for Legal Interception of Communications [39]. Although that document does not explicitly mention mobile communications it must be assumed that the requirements contained within it apply in the same way to mobile communications as to fixed line communications. There is also another report which highlights concerns that exist about the ability or the lack of ability to intercept communication to and from satellites [40].

The purpose of this document is to show where there may be possible problem areas when legal intercept is an issue and the affects that interception could have on the network. All the effects are subjective and will depend in reality on the actual implementation involved.

### 6.4.2 Problems and Effects on the Network

Interception in the fixed network is relatively straight forward **-** the line that the suspect uses is known which makes it easy to intercept at the exchange or elsewhere within the network (for example at the street cabinet or at a remote concentrating unit). A mobile network presents a number of problems **-** this is valid as much for GSM and analogue networks as it will be for UMTS. These include: not knowing on which MSC the suspect will appear, handover, large satellite footprints, roaming, encryption etc.

The amount of information required by an intercept authority could also potentially cause problems, particularly as a lot of this information is required in real-time or as soon as possible afterwards. The information required includes: the communication itself, the calling number, the called number, any subsequent called numbers, the time and duration of the call, the location of the suspect and it may be necessary to obtain names, addresses and numbers of the suspect and his correspondents. This could be of particular concern where the intercept requirement is placed on one operator but the user is registered with another. The additional information required could place pressure of increased traffic on the network, especially where names and addresses need to be sent.

All intercepted traffic has to be passed to the requesting agency en clair (i.e. not encrypted). This means that additional processing has to be done to achieve this and it will also be necessary for the network operator who has to provide the intercept to have access to the keys. The network operator providing the service may not be the one on which the suspect is registered (i.e. the suspect has roamed) and may also not be in the country where the agency requesting the intercept is situated (see diagram below). This in itself could cause an increase in traffic, in addition to all the political decisions that have to be considered.

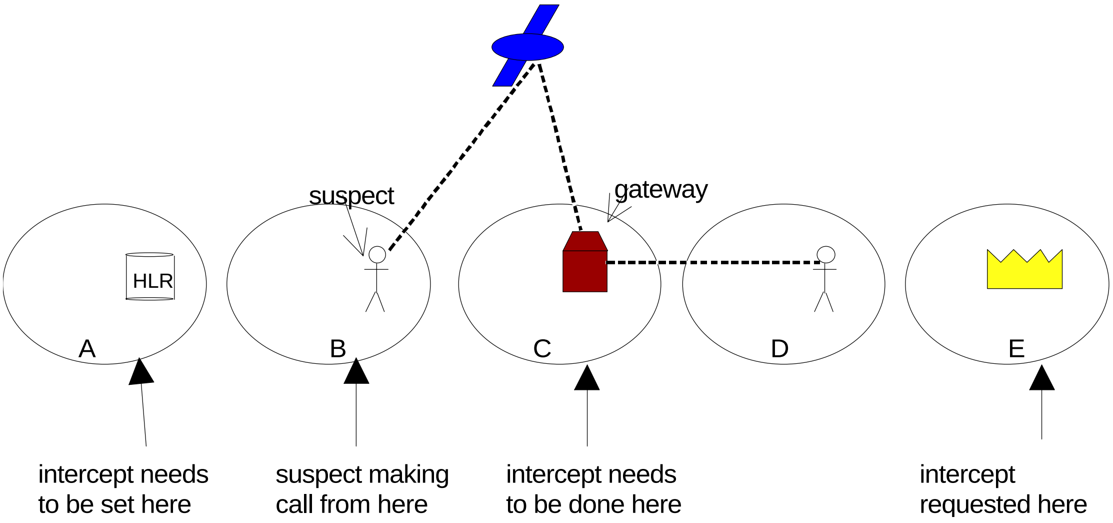

suspect
gateway
HLR
A
B
C
D
E
intercept needs to be set here
suspect making call from here
intercept needs to be done here
intercept requested here

Figure 31: Example of Legal Interception Problem

It would be expected that a three party bridge (or something similar) be inserted at call set up time and traffic also sent down this leg. This increases the amount of traffic, although this third leg may not touch the mobile network (i.e. it may only be necessary to use the fixed trunk networks) but signalling will be required in order to set it up. There are problems associated with this solution in that if handover between MSCs occurs the MSC containing the bridge has to be kept in the call for the duration, again potentially increasing the amount of traffic to be carried. The three party bridge is a relatively clumsy solution and it is likely that there are more elegant solutions which would allow handover to take place easily without increasing the traffic volumes and without tying up resources

It is envisaged that the agency wishing to insert an intercept would have to set a flag in the suspect’s user profile. Whether this could be done automatically by signalling or whether it has to be done by the suspect’s network operator is to be determined, but is likely to depend on trusted third party type relationships. If done automatically, some form of authentication would need to be carried out and new signalling messages defined. With an automatic setting of flags this opens up other areas of possible security breaches - if the HLR could be changed in one way it must surely be possible to change it (hack) in other ways.

When the suspect started to make a call, relevant information would be retrieved from his home location register - including the intercept flag. The MSC would recognise the set flag and automatically set the interception mechanism in process assuming that the necessary authentication has been done. As the call progresses all the information would be relayed to the interception agency which may or may not be in the same country.

With respect to satellite communications, it has been reported that interception cannot happen unless the country containing the suspect has a gateway to the satellite. However, this may not be entirely true. This method would involve serious problems with handover, but could be used if all else fails. Continually having to change the intercept or to keep the base station in existence for the call without being detected could cause signalling overheads.

### 6.4.3 Conclusion

It is inevitable that interception will increase the traffic through the network but the amount of increase is dependent on the method used and the number of intercepts used. Intercept is not as straightforward as it would appear to be - technically it is possible to do the intercept and there are various ways in which it could be done. It would appear that the main questions concern the political, legal and security issues.

# 7. Fraud Indicators

## 7.1 *Introduction*

This section identifies and classifies potential indicators of fraud in cellular mobile telecommunications systems. The origins of this work lie in studies concerned with characterising *technical* fraud (i.e. usage of cloned mobile phone equipment) on analogue i.e. first generation networks. This should be remembered when reading the section. Some, but not all, of the indicators referenced may also be useful for the detection of *commercial* fraud (i.e. that committed using false subscriptions) and for the detection of fraud in general in second and third generation cellular systems. However, it is entirely possible that other indicators not referenced in this document may be useful for the detection of fraud in these other cases.

There are many different types of technical and commercial fraud e.g. direct call selling, PABX fraud, personal use of clones. Each has its own idiosyncrasies and can thus be characterised by unique combinations of indicators. Groups of indicators for each known type of technical fraud are identified in this section.

The section also discusses which of the highlighted indicators can be measured easily in existing networks and which cannot. Future work should address the measurement of these indicators by placing requirements on future systems e.g. UMTS and FPLMTS, and developing mechanisms to facilitate the measurements. Finally, a sub-section detailing how second and third generation systems may differ from first generation systems in terms of fraud detection is included.

It should be noted that the original LINK 3GS3 working paper on fraud indicators has been edited substantially for obvious commercial and security reasons in order to produce this section for public dissemination.

## 7.2 *Identification of Potential Fraud Indicators*

The objective of the following sections is to identify and classify potential indicators of fraud in cellular mobile telecommunication systems.

Two classifications of potential indicators and their interrelationship are considered:

- Classification by type of indicator (Section 7 3).
- Classification by use of indicator (Section 7 4).

## 7.3 *Classification of Indicators by Type*

In terms of a classification of indicators by type, we consider three categories:

- Usage indicators
- Mobility indicators
- Deductive indicators

### 7.3.1 **Usage Indicators**

A usage indicator is defined by some criterion relating to the way in which a mobile is used. For example, the number of mobile originating calls made in a defined time interval by an individual subscriber may potentially be such an indicator. Some types of fraud are characterised by unusually high usage.

In this document, we only consider usage characteristics of mobile originating calls or other mobile originating transactions. This is reasonable in first generation systems such as AMPS and TACS because incoming calls do not in general incur any charges (for the receiving party), and hence it is difficult to understand how mobile terminating calls on their own can be used to commit fraud. This stance is harder to justify in second and third generation systems where in particular roaming can lead to charges for a receiving mobile party. Thus, indicators based upon the usage characteristics of mobile terminating calls may also be appropriate in these newer systems.

The actual number of basic usage criteria is extremely small. As illustrated in Table 6, most can be represented in *absolute* and *differential* form. For subscriber specific analysis, only the absolute form is required; the differential form only complicates the analysis. However, for blanket or global analysis, there is a possible advantage in using differentials. Suppose for the purposes of argument that the usage (however this is defined) corresponding to any individual genuine subscriber over a given time period is constant, with differences in the usage existing from subscriber to subscriber. Then the variation in usage of a subscriber from one time period to the next i.e. the difference, is zero for all subscribers irrespective of whether they are low or high usage subscribers. Thus, in such a scenario, we have effectively mapped the different usage levels of different genuine subscribers into a single profile **-** any deviations from this unique profile imply suspicious activity. This is far preferable to the use of absolute criteria in which the genuine subscriber with highest usage determines the threshold level for all subscribers and a fraudulent mobile associated with a low usage subscriber can operate for a significant time period without detection. However, in practice, genuine subscribers can exhibit large variations in their usage from one defined time period to the next. In a worst case scenario, the use of differentials can then lead to significantly poorer fraud detection capability relative to absolutes for blanket analysis. We will thus concentrate on the use of absolute usage criteria for fraud detection in this document. The adoption of a differential form of usage criteria is also complicated by the fact that there are a number of ways that 'differences' can be formed (the standard first order difference, formed by subtracting the current measure from the corresponding previous measure, may not always be the optimum choice)

| **Absolute Usage Criteria for Mobile Originating Calls and Other Transactions (per subscriber)** |
|---|
| Number of transactions within a defined time interval |
| Total time usage within a defined time interval |
| Total time required for a defined number of transactions or total time usage to occur (from the inception of the first call within the defined time interval) |
| Duration of individual transactions |
| |
| **Differential Usage Criteria for Mobile Originating Calls and Other Transactions (per subscriber)** |
| 'Differences' between the number of transactions within corresponding defined time intervals |
| 'Differences' between the total time usage within corresponding defined time intervals |
| 'Differences' between the total time required for a defined number of transactions or total time usage to occur within corresponding defined time intervals |

*Table 6: Basic Usage Indicators for the Detection of Fraud*

The basic usage criteria can be classified into distinct categories in a number of different ways to yield a vast array of possible indicators. It is useful to allocate these classifications into one of four groups, as illustrated in Table 7. So, for example, in addition to the number of calls made by an individual subscriber in a defined time interval being a potential indicator, we also have the number of calls made by an individual subscriber in a defined time interval to national destinations and the number of calls made by an individual subscriber in a defined time interval to international destinations as potential indicators.

It is also possible to combine two or more of these classifications to yield hybrid classifications. For example, we may classify usage criteria into the following categories:

mobile originating calls to national destinations from inside switch area A.
mobile originating calls to international destinations from inside switch area A.
mobile originating calls to national destinations from outside switch area A.
mobile originating calls to international destinations from outside switch area A.
all other mobile originating transactions

| |
|---|
| **1. Classification by Geographic Source of Mobile Originating Transactions** |
| Classification by cell site(s) or switch area(s) |
| |
| **2. Classification by Destination of Mobile Originating Transactions (B-Number Analysis)** |
| **Geographic** |
| Classification by national/regional/international calls |
| **Non-geographic** |
| Classification by repeated calls to a single number |
| Classification by calls to fixed/mobile numbers |
| Classification by calls to premium rate/non-premium rate numbers |
| Classification by calls to freefone/non-freefone numbers |
| |
| **3. Classification by Temporal Factors** |
| Classification by time of day (e.g. 0700-1900hrs, 1900hrs-0700hrs) |
| Classification by time of week (e.g. week day, weekend) |
| Classification by special periods or events (e.g. Christmas, bank holidays) |
| |
| **4. Classification by Type of Mobile Originating Transaction** |
| Classification by mobile originating call, enquiry calls/flash requests, conference calls, activation/deactivation of supplementary services, operation of diverts |

*Table 7: Four Possible Generic Classifications of Basic Usage Indicators*

### 7.3.2 **Mobility Indicators**

A mobility indicator is defined by some criterion relating to the mobility of a mobile. For example, the number of successful ‘rescue’ handovers[1] performed during all mobile originating calls made in a

---

3 In general terms, there are several different types of handover. A ‘rescue’ handover is the most common type and is one which is mandatory in order to maintain acceptable signal quality during a conversation usually because of the mobility of a subscriber. However, there are other generic types: ‘confinement’ (to reduce local interference and thus improve QoS) and ‘traffic’ (to redistribute local traffic in order to improve capacity) being two. Not all these types may relate to mobility to the same extent.

defined time interval by an individual subscriber may potentially be such an indicator. Some types of fraud are characterised by unusually low mobility.

Measurement of mobility in a terrestrial cellular network is difficult because there is no precise position location capability. The resolution is limited to cells during calls and to location areas (i.e. sets of contiguous cells) between calls. Mobility indicators must therefore be defined differently, or at least in different contexts, for the in-call and out-of-call cases. Table 8 illustrates an example set of basic mobility indicators for these two different scenarios. Note that it is possible to define many other basic mobility indicators as a consequence of the fact that mobility is difficult to measure precisely, though the ones illustrated are probably the most useful.

The potential weighting of many of these indicators by cell or location area size as appropriate is a reflection of the fact that cell and location area sizes fluctuate significantly with geographical position in accordance with the expected offered traffic. Exactly how such weightings can be applied in practice is a topic for further study. For the out-of-call case, location updates can in principle occur for a variety of reasons e.g. on movement from one location area to an adjacent one, after a defined time interval, as commanded by the appropriate base station. Only those which correspond to a movement from one location area to an adjacent one need to be considered as these are the only type which are a measure of mobility.

| **In-Call Mobility Criteria** |
|---|
| Number of successful handovers within a defined time interval |
| Number of successful handovers within a defined time interval weighted by cell size |
| Number of successful handovers which do not return a mobile to the previous cell within a defined time interval |
| Number of successful handovers which do not return a mobile to the previous cell within a defined time interval weighted by cell size |
| Number of distinct cells visited within a defined time interval |
| Number of distinct cells visited within a defined time interval weighted by cell size |
| Geographical separation of cells visited within a defined time interval |
| |
| Number of successful handovers for individual transactions |
| Number of successful handovers for individual transactions weighted by cell size |
| Number of successful handovers which do not return a mobile to the previous cell for individual transactions |
| Number of successful handovers which do not return a mobile to the previous cell for individual transactions weighted by cell size |
| Number of distinct cells visited for individual transactions |
| Number of distinct cells visited for individual transactions weighted by cell size |
| |
| **Out-of-Call Mobility Criteria** |
| Number of successful mobility based location updates within a defined time interval |
| Number of successful mobility based location updates within a defined time interval weighted by location area size |
| Number of successful mobility based location updates which do not return a mobile to the previous location area within a defined time interval |
| Number of successful mobility based location updates which do not return a mobile to the previous location area within a defined time interval weighted by location area size |
| Number of distinct location areas visited within a defined time interval |
| Number of distinct location areas visited within a defined time interval weighted by location area size |
| Geographical separation of location areas visited within a defined time interval |

*Table 8: Basic Mobility Indicators for the Detection of Fraud*

For the in-call case, there are at least two reasons for considering indicators other than the number of successful handovers (whether weighted by cell size or not):

To take account of the fact that cells can be revisited.

To take account of the mobility characteristics of subscribers who make or receive calls in many cells during a defined time interval but do not tend to move across cell boundaries while making calls.

Analogous arguments exist for considering indicators other than the number of successful mobility based location area updates (whether weighted by location area size or not) for the out-of-call case.

Clearly, the values of in-call and out-of-call mobility criteria depend not only upon mobility considerations but also upon the relative times for which a mobile is in the in-call and out-of-call states.

The basic in-call mobility indicators can be classified as illustrated in Table 9.

| |
|---|
| **1. Classification by Type of Transaction** |
| Classification by mobile originating/mobile terminating transaction |
| |
| **2. Classification by Type of Handover (Handover related indicators only)** |
| Classification by rescue/confinement/traffic etc. handovers |

*Table 9: Two Possible Classifications of Basic In-Call Mobility Indicators*

### 7.3.3 **Deductive Indicators**

A deductive indicator is an indicator which arises as a by-product of fraudulent behaviour. For example, the presence of overlapping calls other than enquiry or conference calls (i.e. between two or more clones or between a genuine mobile and one or more clones all with the same identity) may potentially be such an indicator.

Table 10 illustrates the set of basic deductive indicators.

| |
|---|
| Control and traffic channel congestion in cells |
| Overlapping calls or overlapping calls and location updates |
| Overlapping mobile originating calls with b-number comparison |
| Velocity checks |
| Recent history of alarms associated with mobile |
| Calls to and/or from other mobiles which have a recent history of alarms or have subsequently raised alarms |

Table 10: Basic Deductive Indicators

## 7.4 ***Classification of Indicators by Use***

In terms of a classification of indicators by use, we again consider three categories:

- Primary indicators
- Secondary indicators
- Tertiary indicators

*Primary indicator*s are those which in principle can be employed in isolation to detect fraud.

*Secondary indicator*s are those from which in principle useful information can be gained if they are considered in isolation, but which should not be employed in isolation to detect fraud.

*Tertiary indicator*s are those from which no useful information can be gained if they are considered in isolation, but which in principle can provide ancillary information in connection with the detection of fraud.

Note that this classification of indicators by use into primary, secondary and tertiary indicators does not imply anything about the value or reliability of a particular indicator at a particular point in time. In fact, this classification is independent of the value or reliability of indicators and is purely conceptual. An indicator classed as primary may well be completely unreliable at a particular time and therefore should not be employed. Conversely, an indicator classed as tertiary may be very reliable at a particular time **-** the fact that it is tertiary simply implies that it must by definition be employed in conjunction with other (reliable) indicators.

Table 11 illustrates a classification of all the (absolute) indicators we considered in section 7.3.1 according to use

| |
|---|
| **Primary Indicator**s |
| Number of mobile originating transactions within a defined time interval (unclassified or classified by the destination of mobile originating transactions i.e. b-number analysis) |
| Total time usage of mobile originating transactions within a defined time interval (unclassified or classified by the destination of mobile originating transactions i.e. b-number analysis) |
| Duration of individual mobile originating transactions (unclassified or classified by the destination of mobile originating transactions i.e. b-number analysis) |
| |
| **Secondary Indicator**s |
| Number of mobile originating transactions within a defined time interval (classified by the geographic source of mobile originating transactions, temporal factors or type of MO transaction) |
| Total time usage of mobile originating transactions within a defined time interval (classified by the geographic source of mobile originating transactions, temporal factors or type of MO transaction) |
| Duration of individual mobile originating transactions (classified by the geographic source of mobile originating transactions, temporal factors or type of MO transaction) |
| Total time required for a defined number of transactions or total time usage to occur (from the inception of the first call within the defined time interval) (classified or unclassified) |
| Overlapping calls or overlapping calls and location updates (with or without geographic source comparison) |
| Overlapping mobile originating calls with b-number comparison (with or without geographic source comparison) |
| Velocity checks |
| |
| **Tertiary Indicator**s |
| All mobility indicators (classified or unclassified) |
| Control and traffic channel congestion in cells |
| Recent history of alarms associated with mobile |
| Calls to and/or from other mobiles which have a recent history of alarms or have subsequently raised alarms |

*Table 11: Classification of Indicators by Use into Primary, Secondary and Tertiary Categorie*s

Some of the assignments in Table 11 perhaps need some clarification. In particular, it may not be clear why some of the indicators have been assigned to the secondary rather than primary category. For example, all usage criteria classified according to the geographic source of transactions are considered to be secondary indicators. In order to explain why this is so, suppose that an arbitrary subscriber is allowed to make 300 minutes of mobile originating calls in total within any period of 24 hours before raising an alarm. Now, it would be quite reasonable to suggest, for example, that only 90 minutes of these calls could be to international destinations. This is because the calling profiles (i.e. the types of numbers called) of genuine subscribers are generally quite stable on a day-to-day basis and it would be very unlikely that a genuine subscriber would make more than 90 minutes of international calls within any period of 24 hours, although they may make up to 300 minutes of calls in total. This is why usage criteria classified according to destination are assigned primary status. However, it would be quite unreasonable to suggest, for example, that only 90 (or even say 270) minutes of all calls could be made from an arbitrary switch area. The mobility patterns of genuine subscribers will fluctuate a great deal on a day-to-day basis and it is quite likely that a subscriber could make a large proportion of calls from a single switch area, particularly as a switch area is a very artificially defined region. Thus, although usage criteria classified according to geographic source do provide useful information about the likelihood of fraud (since fraudulent activity does tend to occur in certain geographical areas), it would be very unwise to use them in a primary capacity.

What about some of the deductive indicators which are assigned to the secondary category ? One reason why we cannot assign for example detection of overlapping calls and similar indicators to the primary category is because of the presence of extension mobiles (i.e. clones of a subscriber's own mobile for personal (‘legitimate’) use of that subscriber) on analogue networks. Thus, because these indicators cannot distinguish legitimate’ from illegitimate clones, they cannot be given primary status. Switch boundary effects are also influential in this decision.

### 7.5 ***Summary of Useful Indicators***

Table 12 summarises indicators which appear to be useful in principle for detecting certain types of fraud. Note from Table 12 that it is extremely difficult to universally characterise and hence devise indicators to reliably detect the personal use of fraudulent mobiles. This is probably because such mobiles are used by different people for a wide range of reasons including calling friends, relatives abroad, other members of a drug ring etc.

| **Basic Indicator** | **Classification/Type** | **Type of Fraud** | | | | | |
|---|---|---|---|---|---|---|---|
| | | **Direct Call Selling** | **PABX Fraud** | **Freefone Fraud** | **Mobile-to-Mobile Fraud** | **Premium Rate Line Fraud** | **Personal Use** |
| **Primary** | | | | | | | |
| Total MO time usage | Unclassified | √√ | √√ | √√ | √√ | √√ | √ |
| | Geographic destination | √√ | | | | | √ |
| | Repeated calls to a single b-number | | √√ | √√ | √√ | √√ | |
| | Calls to UK freefone numbers | | | √√ | | | |
| | Calls to UK mobile numbers | | | | √√ | | √ |
| | Calls to UK premium rate numbers | | | | | √√ | √ |
| MO call duration | Unclassified | √√ | √√ | √√ | √√ | √√ | √ |
| **Secondary** | | | | | | | |
| Total MO time usage | Geographic source | √√ | √√ | √√ | √√ | √√ | |
| | Temporal factors | √√ | √√ | √√ | √√ | √√ | |
| | Type of transaction | | | | | √√ | |
| Time to surpass thresholds | All thresholds | √√ | √√ | √√ | √√ | √√ | √ |
| Overlapping `calls’ | All types | √√ | √√ | √√ | √√ | √√ | √√ |
| Velocity checks | Unclassified | √√ | √√ | √√ | √√ | √√ | √√ |
| **Tertiary** | | | | | | | |
| Mobility | All types and classifications | √√ | √√ | √√ | √√ | √√ | |
| Cell congestion | Unclassified | √√ | √√ | √√ | √√ | √√ | |
| Recent alarms | Unclassified | √ | √ | √ | √ | √ | √ |
| Calls to/from other fraudulent mobiles | Unclassified | √ | √ | √ | √ | √ | √ |

*Table 12 : Summary of Useful Indicators at the Present Time as a Function of Type of Fraud*

(√√ = useful in the majority of cases, √ = useful in isolated cases)

## 7.6 *Measurement of Indicators*

Many of the indicators cited in Section 7.3 are measured as a normal part of existing cellular system operation. For instance, all usage indicators can be derived from billing information. This fact facilitates the rapid and efficient introduction of a comprehensive fraud detection system.

However, there are some indicators for which this is not true, for example mobility indicators. For the out of call case, it is true that the number of mobility based location updates can be deduced simply from the HLR/VLR network entities. However, for the in-call case, there is no reason for operators to record the number of handovers made by each individual subscriber unless operators plan to charge for handovers which is generally not the case. This needs to be addressed by placing requirements on future systems e.g. UMTS and FPLMTS, and developing mechanisms to facilitate the measurements.

## 7.7 *Fraud detection in GSM and UMTS/FPLMTS*

### 7.7.1 **GSM Fraud Detection**

The two most significant differences with respect to fraud detection between a second generation system such as GSM and first generation systems are:

- The ability to differentiate easily between different tele- and bearer services in GSM.
- The ability to roam between different networks in GSM.

The former feature allows usage indicators to be classified according to the exact tele- or bearer service.

The latter feature implies that the fraud engines (i.e. the systems that perform fraud management) of different network operators must co-operate in order to facilitate efficient fraud detection. This is not simply a case of the visited network operator monitoring a subscriber’s behaviour in isolation. For example, if cloning of SIM cards were possible, this approach would not detect simultaneous use of a subscription on different GSM networks.

### 7.7.2 **UMTS/FPLMTS Fraud Detection**

Three fundamental system requirements of UMTS/FPLMTS are that they be:

- multi-service
- multi-environment
- multi-operator

The multi-service aspect of UMTS/FPLMTS allows usage indicators to be classified according to the exact service being used.

The multi-environment feature of UMTS/FPLMTS should allow greater resolution to the process of monitoring subscribers mobility in urban/office environments where microcells/picocells are in existence.

As far as the third requirement is concerned, a multitude of operators, some small, some large, some localised, some nation-wide may be in existence. The fraud detection architecture for such a scenario requires careful consideration. It is unlikely that the smaller localised operators will be able to afford to operate dedicated fraud engines, and, in any case, a multitude of ‘fraud engines’ in any arbitrary region is bound to be counter-productive in terms of signalling and effectiveness.

At this stage we consider two advanced fraud detection mechanisms:

*Dynamic Location Areas*

The size of location areas for individual subscribers suspected of being fraudulent can be dynamically reduced in order to observe their mobility patterns with greater resolution. Whilst obviously a long term measure, this can be compared to developments expected in third generation systems in which the size of location areas will be dynamically adjusted on a per subscriber basis in accordance with their mobility history in order to minimise signalling load on the network. It is also possible that this approach could be adopted in GSM as an evolutionary measure at some stage: the BCCH already broadcasts the cell identity which is required in order for cell rather than location area based location updates.

*Handset Intelligence*

Certain information, such as a list of the last *n* b-numbers called or mobility information, can be stored in the handset or smart card as appropriate. This information could be retrieved by the network/fraud engine as appropriate for the purposes of fraud detection. This corresponds in part to a distributed archive. A problem with this approach is lack of storage space particularly in a smart card.

# 8. References and Bibliography

[1] LINK PCP, 3GS3, Technical Report 1: *Security features for third generation systems,* Final Version, 14th February 1996
[2] LINK PCP, 3GS3, Technical Report 2: *Security mechanisms of third generation systems,* Final Version, 14th February 1996
[3] ITU-T I.312 / Q1201 Principles of Intelligent Network Architecture
[4] ITU-T I.328 / Q1202 Intelligent network service plane architecture
[5] ETSI TC-TR/NA 61201, Ver 2 1/95, Network Aspects; Security Requirements for Global IN Systems
[6] ITU-T Q1204 Intelligent network distributed functional plane architecture
[7] ITU Draft 1. FNA Ver 0.1.0 Jan 1995 - FPLMTS Functional Architecture
[8] ITU-T Q1205 IN Physical Plane Architecture
[9] see [27]
[10] ITU-R 687-1 FPLMTS Baseline Document
[11] CCITT COMX1-R209 Final Report of SG11 from 9 to 20 March 1992
[12] ETSI Draft Technical Report DTR/NA-6001 Ver 2 9/1990 Intelligent Networks Framework
[13] see [5]
[14] see [12]
[15] ETSI DTR/NA - 43308 Ver 3 9/1992 Baseline document on the integration of IN and TMN
[16] ITU Rec. M3010 Principles for Telecommunications Management Network
[17] ISO/IEC DIS 10745 Feb 1992 OSI Upper Layers Security Model
[18] ETSI DTR/NA-70401 Ver 0.6.1 2/93 General UPT Security Architecture
[19] ECMA TR-46 Section 3.2 Security in Open Systems: A Security Framework
[20] ITU Rec. X700| OSI 7498-4 Management Framework
[21] ISO [7498-2] 1989 - Open system interconnection - Basic Reference Model, Part 2: Security Architecture
[22] D-ETR/SMG-50501- Objectives and Framework for the TMN of the UMTS
[23] D-ETR/SMG-50201- Framework for services to be supported by UMTS
[24] D-ETR/SMG-50901, Version 2.2.0 , June 1995 - Security principles for the UMTS
[25] see [2 ]
[26] deleted
[27] D-ETR/SMG-50301 - Framework of Network requirements Inter working and Integration for UMTS
[28] IEEE Network - May/June 1994 - Security considerations in a Network Management Environment - Donal O'Mahony
[29] ETSI ETR 055-3 UPT Service Concept Part 3: Service Aspects of Charging, Billing and Accounting
[30] GSM [02.20] Collection Charges
[31] ITU Q7/11 - Baseline document. Requirements for UPT
[32] ETSI NA 72305 Ver 0.1.0 1994
[33] ITU-T Rec M3400 TMN Management Functions
[34] ETSI TC-TR NA-60801, Ver 7a IN intra domain management requirements for CS-2
[35] DTR/ NA 43308- Baseline document of Integration of IN and TMN.
[36] ITU-T Rec., Q.1218 - Interface Recommendation For Intelligent Network CS-1.
[37] Draft ITU-T Rec., Q. FNA ,Version 1.1.0, September 1995. - Network Functional Models For FPLMTS.
[38 ] Draft ETSI NA - 61301 - Joint NA6/SMG5 doc., Version 8.1.0, Sept., 1995. IN/UMTS Framework Document.
[39] International Requirements for the Lawful Interception of Telecommunications - European Union Council Resolution - January 1995
[40] Legal Interception on Telecommunications Systems provided outside National Boundaries - Report of Expert Sub Group to the Police Cooperation Working Group (Interception) - Paris 5 May 1995

## 9. Abbreviations

| | |
|---|---|
| BCAF | Bearer Control Access Function |
| BCF | Bearer Control Function |
| BCFr | see RBCF |
| BRCF | Bearer Control Function |
| BSC | Base Station Controller |
| BTS | Base Transmitting Station |
| CCAF | Connection Control Access Function |
| CCF | Connection Control Function |
| CLI | Calling Line Identity |
| CPN | Customers Private Network |
| CR | Charge Record |
| CS-1 | Capability Set 1 |
| ECMA | European Computer Manufacturers Association |
| ETSI | European Telecommunications Standards Institute |
| FCAPS | Fault, Configuration, Accounting, Performance and Security (management) |
| FE | Functional Entity |
| FPLMTS | Future Public Land Mobile Telecommunications System |
| GSM | Global Standard for Mobility |
| IAA | Inter Administration Accounting |
| IMTI | International Mobile Terminal Identity |
| IMUI | International Mobile User Identifier |
| IMUN | International Mobile User Number |
| IN | Intelligent Network |
| INCM | IN Conceptual Model |
| ISDN | Integrated Services Digital Network |
| ISO | International Standards Organisation |
| ITU | International Telecommunications Union |
| MBCF | Mobile Bearer Control Function |
| MCCF | Mobile Connection Control Function |
| MCF | Mobile Control Function |
| MF | Mediation Function |
| MRRC | Mobile Radio Resource Control |
| MRTR | Mobile Radio Transmission and Reception |
| MS | Mobile Station |
| MSC | Mobile Switching Centre |
| MSF | Mobile Storage Function |
| MTU | Mobile Termination Unit |
| N-OSF | Network Management Layer OSF |
| NE | Network Element |
| NEF | Network Element Function |
| NIST | National Institute of Standards and Technology |
| NO | Network Operator |
| OS | Operating System |
| OSF | Operations System Function |
| PBX | Private Branch Exchange |
| PIN | Personal Identification Number |
| PLMN | Public Land Mobile Network |
| PSTN | Public Switched Telephone Network |
| PTN | Private Telephone Network |
| QAF | Q Adapter Function |
| RBCF | Radio Bearer Control Function |
| RFTR | Radio Frequency Transmission and Reception |
| RRC | Radio Resource Control |
| RRCP | Radio Resource Control Plane |

| | |
|---|---|
| S-OSF | Service Management Layer OSF |
| SACF | Service Access Control Function |
| SCE | Service Creation Environment |
| SCEF | Service Creation Environment Function |
| SCEP | Service Creation Environment Point |
| SCF | Service Control Function |
| SCP | Service Control Point |
| SDF | Service Data Function |
| SDP | Service Data Point |
| SMAF | Service Management Access Function |
| SMF | Service Management Function |
| SMP | Service Management Point |
| SP | Service Provider |
| SRF | Special Resource Function |
| SSCP | Service Switching and Control Function |
| SSF | Service Switching Function |
| STP | Signalling Transfer Point |
| TACAF | Terminal Access Control Agent Function |
| TACF | Terminal Access Control Function |
| TMN | Telecommunications Management Network |
| UIM | UMTS Identity Module |
| UMTS | Universal Mobile Telecommunications System |
| UPT | Universal Personal Telecommunication |
| WSF | Workstation Function |

**Additional Notations and Abbreviations**

The notation and abbreviations used in this section are taken from TR2 [2].

CIPHx: It is the output used to conceal an identity. It is from the identity hiding algorithm (Cu).

KO’: It is a key offset, which is used in conjunction with the user secret key Ksu to generate the key Kn.

Kn: The network operator secret key. It is known to the mobile user and the ‘current’ network operator.

Ks: User session key. It is known to the mobile user and ‘current’ network operator and is generated as a result of every use of the authentication mechanism.

RESx: This is a check value, acting as the ‘challenge response’ to the mobile user’s ‘challenge request’. The responses come from the service provider RESs, network operator RESn, and the mobile user RESu.

RNDx: They are random ’challenges’ generated by the user RNDu and Network operator RNDn.

TMUI’x: They are temporary identities generated by the service provider TMUI’s and the network operator TMUI’n supplied to the mobile user for current use.

# 10. Appendix

## APPENDIX A Security Requirements of Co-operating IN Entities inside a Managed Domain

ETSI has produced a set of security requirements [5], these are summarised in the table.

The security requirements apply to the IN relationships as existing in the Distributed functional plane. The IN must be protected against :

- unauthorised use of services and resources
- unauthorised disclosure of stored or transferred data
- unauthorised modification, replay and deletion of data
- denial of service.

They can be met by applying security features in the IN architecture.

The table below is a summary of these requirements for each IN-relation.

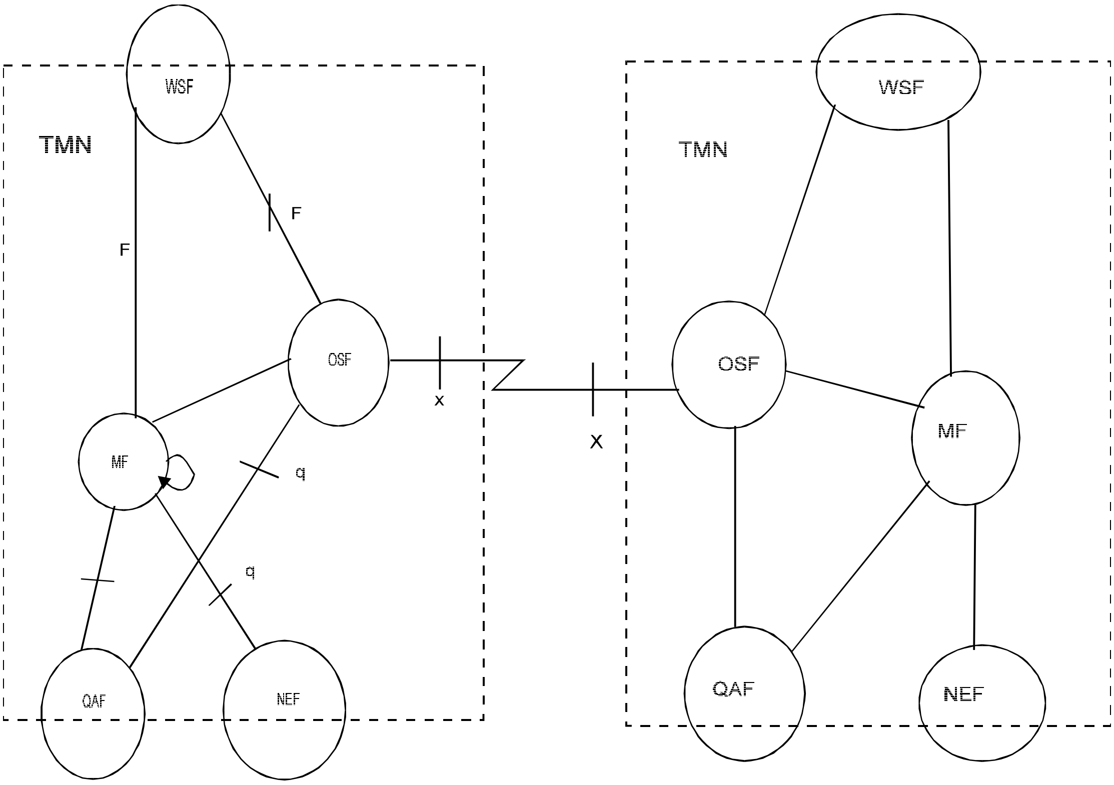
| | **data orig authent** | **peer-entity authent** | **audit & alarm** | **data integrit** | **access control** | **selecti confid** | **non-repudit** |
|---|---|---|---|---|---|---|---|
| **SCF-SCF** | x | - | x | x | x | x | - |
| **SCF-SDF** | x | - | x | x | x | x | - |
| **SDF-SDF *** | x | - | x | x | x | x | - |
| **SCF-SRF** | x # | - | x | - | - | x | - |
| **SCF SSF** | x # | - | x | - | - | - | - |
| **SCF-OSF *** | x | - | x | x | x | x | x |
| **OSF-SDF *** | x | - | x | x | x | x | - |
| **OSF-SRF *** | x | - | x | - | - | x | - |
| **OSF-SCEF** | x | - | x | x | x | x | x |

Table 13: Requirements for each IN-relation

# = It is important in the case of inter domain relations
* = From a security point of view this relation is not recommended for inter domain communication.
**Note:** peer entity authentication is being studied by the ITU.

## APPENDIX B Reference Points between the Management Function Blocks

This is obtained from ITU-T Rec., M.3010. [16].



TMN Relationships

TMNs need to co-operate to provide the overall end-end service as seen by network operators and providers. This often involves and in third generation systems will involve, the transfer of management information relating to specific interfaces or specific links, events on the different links e.g. subscriber charging, inter administration accounting , and may be security violations .

The management information will be exchanged via the x reference point supported by the X interface between the TMNs.

Access to a TMN for a user (NO, or SP) is via the WSF function.

The reference points q, and f are internal to a TMN and do not go between different administrations. These reference points are supported by the Q interface and the F interface in physical structures. see [16].

## APPENDIX C Document History

| Date | Version | Changes |
|---|---|---|
| 12 December 1994 | V1 Draft A | Initial draft |
| 23 March 1995 | V2 Draft B | Major revision by GPT based on comments from all partners. |
| 13 April 1995 | V3 Draft C | Minor revision by GPT based on comments from Vodafone |
| 5 May 1995 | Version 1 | Minor revision by GPT based on comments from Vodafone |
| 20. December 1995 | V2 Draft A | Initial draft |
| 17 January 1996 | V2 Draft B | Revision by GPT- new sections added based on comments from partners. |
| 14 February | Final Version | |