Source: **ARIB SWG7**

Title: **USIM Functionality and Requirements in ARIB**

The attachment is an approved document in SWG7 describing the UIM functionality and requirements in ARIB and TTC. It is provided for reference.

Attachment: UIM functionality and requirements for a 3G mobile system (AIF-SWG7-7-3)

AIF/SWG7-7-3
Revised version of AIF/SWG7-4-2

UIM functionality and requirements for a 3G mobile system

September 28, 1998

KDD, JT, Ericsson

1. Introduction

This document describes UIM functionality and related requirements for a 3G mobile system which are collected from following referenced materials;

[1] Volume1 : Requirements and Objectives for a 3G Mobile Services and System, ARIB version 0 (December 18, 1997)
[2] MPT : Interim report of the Next generation mobile system WG , MPT (May 25, 1998)
[3] ITU-T Q.1701 : Framework for IMT-2000 Network
[4] ITU-T Q.1711 : IMT-2000 Functional Network Architecture

2. UIM functionality and requirements based on ARIB Volume1 and MPT interim report

2.1 UIM Functionality

(1) Originating and terminating calls should require a UIM as physical device or as a functionality to be present in the mobile terminal, subject to legal constraints concerning the requirement for UIM functionality in order to place an emergency call.
[The capability to record user and terminal identities should be provided. Whether such recording capability is actually used and the information provided to emergency service authorities is subject to national regulations.] [Volume1 5.1.1.4]

2.2 UIM Requirement

2.2.1 Information Storage requirement

2.2.2 Network Service Requirement

(1) Service access possibility from different terminals by using UIM [MPT 1.5.1(4)]
(2) UIM indication as a condition to access services other than for emergency

communications (within the legislative permissible range) [MPT 1.5.1(7)]

(3) With consideration to emergency call to police or fire department, it is desired that the terminal can access to the network without a radio terminal identification authentication and user identification authentication. [MPT 2.2.7(8)]

(4) User mobility refers to the capability that allows for access to services without dependence on a specific radio terminal. It is a UIM (User Identity Module: logical entity to manage the user identifier on the user-side) base mobility. If a UIM is implemented in the radio terminal as a function, then terminal mobility and user mobility is fixed and actualized on a one-to-one basis. To actualize true user mobility there is a need to standardize the UIM function, logical and physical interface between the UIM and radio terminal, and logical interface between the UIM and core network. [MPT 2.2.2(1)]

(5) UIM portability is the capability incorporated in the next generation mobile communication network that supports portability of UIM device over terminals. It is actualized with a detachable UIM device. To actualize UIM portability there is a need to standardize the physical interface between the detachable UIM and radio terminal. However, provision of UIM portability shall be an optional service by the operator, and it is desirable that the operator can select either detachable UIM or terminal-integrated-UIM. [MPT 2.2.2(2)]

(6) The user mobility is conferred by the flexibility of access by users to telecommunication services which are available at any terminal, in such a way that the user gives its identity and related profiles by means of detachable UIM to the mobile terminal and/or network to be accessed, and may configure any one of these terminals, fixes or mobile, to meet its service requirements. The user mobility involves the network capability to locate a user with reference to a unique user identity (i.e. IMT-2000 number) for the purpose of addressing, routing and charging of calls. [Volume1 5.3.2]

(7) In order to support the requirements of these location services, the addition of new location network functions and network entities will be required. New and modified interfaces to the existing wireless network will also be required. The necessary signaling should be studied for services user such as FCC enhanced 911 emergency rule-making(FCC's Report and Order, CC Docket No.94-102), e.g. cell ID(currently used in spite of more Accurate location information in future), calling MS ID, call back function, tracking of calling MS, accept roaming MS, MS without authentication. The use of MS for making emergency call to the

police without a valued UIM should be studied. [Volume1 Annex6 5.4]

(8) Supplementary services [Volume1 5.1.7]

2.2.3 Terminal Service Requirement

2.2.4 Service Specific Requirement

(1) The 3G Mobile System radio interface(s) shall be designed in such a way that operational flexibility is maximised. Operational flexibility may include modification of operational data in the mobile station via the radio interface described bellow;

- Over the Air Service Provisioning (IS-53) :
  The over the air service provisioning feature allows a potential service subscriber to activate (i.e., become authorized for) new service without the intervention of a third party (e.g., authorized dealers). The feature consists of over-the-air programming of certain mobile station indicators and electronic key agreement for secure transfer of the A-key to authorize telecommunication services with a specific service provider.
- Network Based Mobile Unit Software Download (IS-53) :
- Enable new services and applications to be delivered to subscribers via mobile unit;
- Provide capabilities and functions that complement existing services to simplify their use;
- Extend the functionality of mobile units to add value for customers without significantly affecting the weight, size, cost and battery life of these devices;
- provide carriers with a mechanism to activate and configure mobile units.

Implementation of this requirement in mobile stations is subject to the capabilities of the mobile stations. [Volume1 6.3.2.12]

2.2.5 UIM Data Access Requirement

2.2.6 Interoperability/Multiapplication Requirement

2.2.7 Security Requirement

(1) To allow for a detachable UIM reflecting the style to prioritize compactness for exclusive use of mobile communication services, remain compatible with various multimedia terminal standards, and permit several styles such as ISO standard styles, etc. that suit co-use for other purposes, it is desired to ensure a security mechanism that can be issued for multiple detachable UIMs of the same user dial-up number. [MPT 2.2.7(6)]

(2) To further strengthen protection of the security information stored in UIM, it is

necessary to prepare a UIM authentication mechanism of the network/service provider. [MPT 2.2.7(10)]

(3) There is a need for a user check mechanism such as a password check, etc. to verify the user using the UIM. For this reason, there is a need to standardize the logical interface between the UIM and radio terminal. [MPT 2.2.7 (12)]

(4) A 3G Mobile System aim to achieve the following secondary technical objectives: **Identification of Entities :** procedures used in a 3G Mobile System should be based on the unique identification of the entities (e.g. service providers, network operators, etc.) involved. [Volume1 3.2]

(5) A 3G Mobile System aim to achieve the following primary operational objectives: **a) Authentication and Identification of user**

- to provide for the required user authentication and billing functions;
- to provide for unique user identification and numbering in accordance with appropriate ITU-T Recommendations;
- to provide for a unique equipment identification scheme; [Volume1 3.3]

(6) Security keys and possible devices, such as the UIM, distributed to the 3G Mobile System users should be easily and securely managed and updated; [Volume1 6.5.1]

(7) A 3G Mobile System shall provide User identity authentication feature which provides a means by which the identity of the 3G Mobile System user is verified to be the one claimed in order for the service not to be compromised by the fraud use. [Volume1 6.5.2.2]

(8) A 3G Mobile System shall provide UIM holder verification feature which provides a means by which the human user of the UIM is authenticated to the UIM in order for the service not to be accessed by theft or unauthorised person. This feature may be locally implemented without interaction with the network. [Voluem1 6.5.2.3]

(9) A 3G Mobile System shall provide User data confidentiality feature which provides the privacy of communication by protecting the data of the 3G Mobile System user against interception over the 3G Mobile System radio interfaces. The feature applies to voice, or any other type of user data. [Volume1 6.5.2.4]

(10) A 3G Mobile System shall provide User identity confidentiality feature which provides a means by which the identity of the 3G Mobile System user is protected against disclosure over the 3G Mobile System radio interfaces. [Volume1 6.5.2.6]

(11) A 3G Mobile System shall provide Network operator/service provider

authentication feature which provides a means by which the identity of the 3G Mobile System network operator/service provider is verified to be the one claimed. This feature may effectively be achieved by authenticating the network operator to which the user is accessing. [Volume1 6.5.2.8]

(12) A 3G Mobile System shall provide Version control of security data and mechanism which provides a means by which security data and mechanisms can be updated and controlled between the parties involved. [Volume1 6.5.2.11]

3. **UIM requirements based on ITU-T Q.1701/1711**

3.1 Framework for IMT-2000 Networks(Q.1701)

3.1.1 Service Concepts and Network Capabilities(quoted from Q.1701 Section7)

3.1.1.1.Capability Set concept

IMT-2000 functionality will be defined in Capability Sets. The requirements documents will follow such an approach.

3.1.1.1.1.Capability Set 1

The first IMT-2000 Capability Set (Capability Set 1) is intended to show a significant improvement over second generation system capabilities in order to make the change worth while in terms of customer perception. Therefore, IMT-2000 Capability Set 1 is intended to provide more service and network capabilities than are available in existing second generation systems.

IMT-2000 Capability Set 1 contents are those capabilities, and the interfaces functionality to support those capabilities which are to be included in Q.1711, etc. (See Appendix A.)

Table 1/Q.1701 shows the capabilities to be supported by IMT-2000 Capability Set 1. It is anticipated that additional Capability Sets for IMT-2000 systems will continue to accumulate capabilities.

Note: In the following table, the term “network” refers to the access and/or the core network, if not otherwise stated.

Table1 Capability set-1 for IMT-2000

Category	Capabilities
Q) Network Services/Features - Terminals & User	1. Network model to support: 1.1. network with uploading and downloading of user profiles, data information, etc., to support UIM functionality via functional communication channels 1.2. software configurable terminals, for operational flexibility (e.g., to support pro-active applications)

Interface Modules (UIM)	1.3. flexible enough to support future enhancements in software-defined radios, for operational flexibility 2. Mobiles and UIM with downloading capabilities over the air for data and applications. Appropriate procedures should set in place to protect sensitive and confidential information transferred over the air. 3. Multiple calls on a single terminal. 4. Support terminal roaming with removable or integrated UIM and provide information needed from UIM to associate a subscriber with the MT and to personalize the MT. 5. Personal mobility based on a UIM separate from the terminal (IC card). 6. Multiple registration of one user on several terminals for different services

3.1.2.Interfaces for study(quoted from Q.1701 section 8)

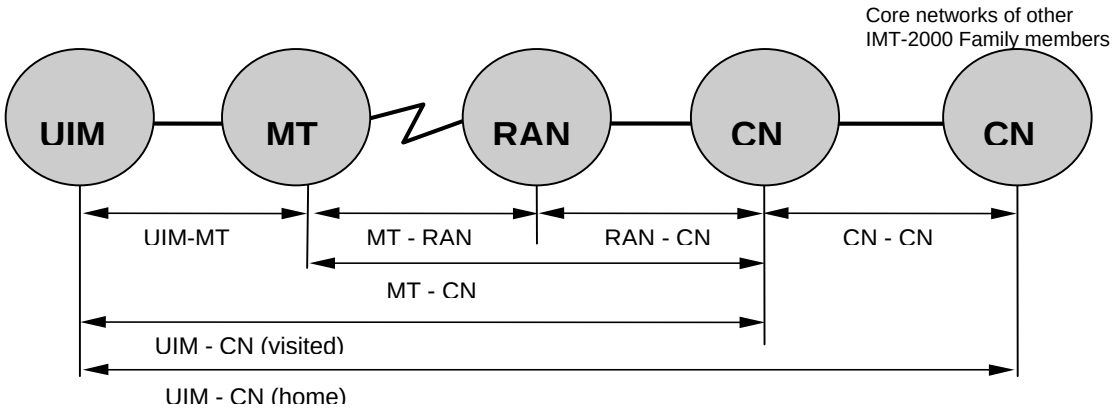

Figure 1-1 Functional communications of an individual IMT-2000 family member

3.1.2.1.The UIM to MT interface(quoted from Q.1701 section 8.3)

This is the physical interface between the user removable UIM and the Mobile Terminal and is a single, clearly defined interface. The definition of this interface includes a secure physical (ISO compliant) specification (e.g., size, contacts, electrical specification, voltage, basic information exchange protocols.)

The UIM may be physically removable from the MT or it may be integrated into the MT (non-removable.) A non-removable UIM is functionally equivalent to a removable UIM. Standards for UIM physical interconnection to the MT do not apply to a non-removable UIM. Some UIM functionalities may be uploadable and downloadable.

3.1.2.1.1.UIM-MT and UIM-CN functional communications

Information is passed from the UIM to the MT for processing in the MT or for transfer to the CN. The MT may use the information in subsequent communication with the CN in the MT-CN functional communication. Information such as the following non-exhaustive examples may be exchanged:

- UIM access control (e.g., PIN transfer to authenticate the user to the UIM);
- identity management (e.g., transfer of internationally unique subscriber or user identity);
- authentication control (e.g., transfer of challenges and responses for authentication);
- service control (e.g., transfer of user service profiles or user service logic); and
- man-machine interface control (e.g., transfer of user-specific MMI configuration).

The UIM-MT functional communication will allow for the establishment of family-specific information exchange between the UIM and the MT.

The UIM-CN functional communication is used to support services where software objects in the UIM relates to Software in the Network. These may be, e.g., profile services and data services. This may be used for downloading software tools or objects over a pseudo-transparent (connection) data path established across the network.

The UIM-CN functional communication will allow for the establishment of family-specific information exchange between the UIM and the (home) CN.

3.1.3. Structure of IMT-2000 documentation in ITU-T (quoted from appendix A)

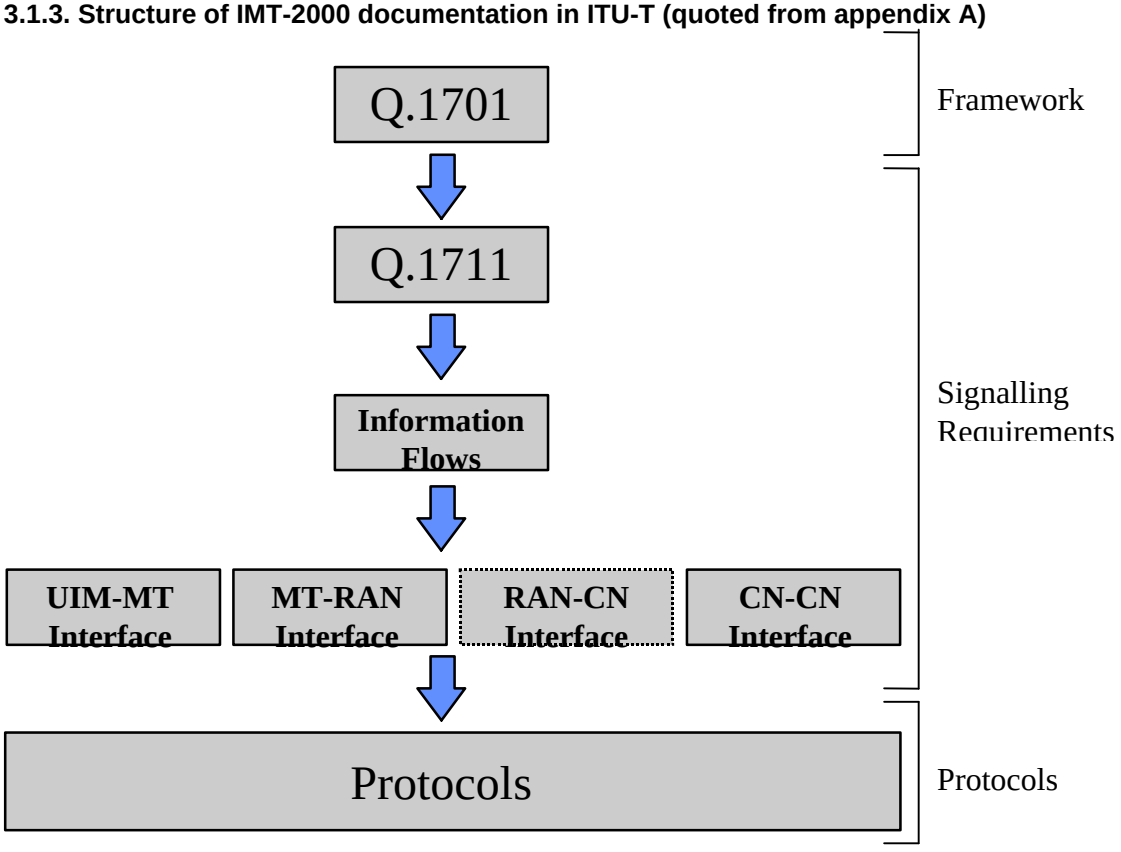

Figure 1-2 - Structure of IMT-2000 documentation in ITU-T

3.2.Functional Network Architecture(Q.1711)

3.2.1.IMT-2000 Specific and UIM related Functions

3.2.1.1.Additional Functions related to global roaming (quoted from section4.9)

The functions in this subsection are used to support global roaming in addition to other functions described.

For IMT-2000 CS1, two alternatives for global roaming are envisaged:

Roaming of UIM (UIM Portability) : a UIM provided by the home network is used with an MT available by the visited network.

Roaming of UIM and MT (terminal mobility) : a UIM provided by the home network is used with an MT available in the home and the visited network.

Figure 4-1 depicts the above two global roaming alternatives.

UIM and MT Global Roaming
UIM-MT, MT-RAN, and NNI are IMT-2000 interfaces

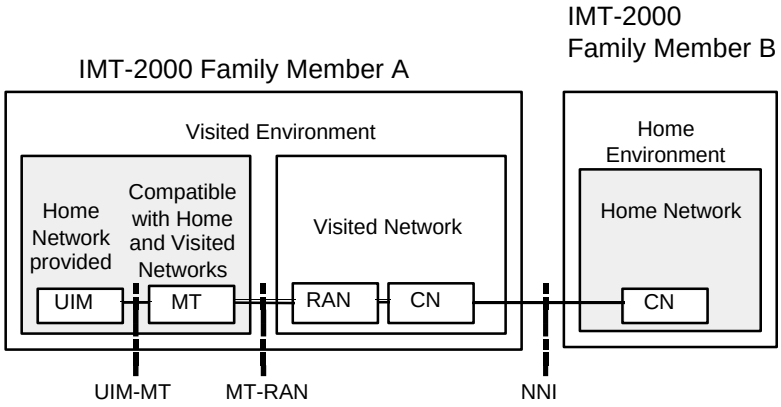

Figure2-1a UIM and MT Global Roaming Alternative 1

UIM Global Roaming
UIM-MT and NNI are IMT-2000 interfaces

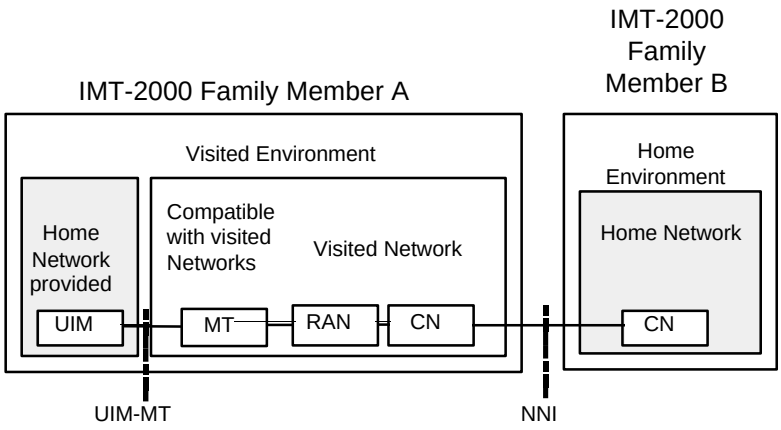

Figure 2-1b UIM Global Roaming Alternative 2

Selection of service providers allows mobile terminals to roam between networks supported by the same or different service providers/operators. This may include the use of mechanisms to preferentially select certain service providers/operators where multiple service providers/operators provide coverage in the same area.

Functions related to interworking includes the mechanisms to provide, for example, charging, fraud, and problem resolution. These mechanisms may be used in "real time" cases.

3.2.1.2.Functions supporting IMT-2000 users(quoted from section4.13)

UIM Portability is an integral capability within the IMT-2000 networks that supports mobility of UIM devices among the IMT-2000 terminals. In this context, UIM portability requires a physical separated device from the terminal. Therefore, this capability is an optional capability since IMT-2000 supports a physical separated UIM as well as an integrated UIM within the terminal.

IMT-2000 Personal Mobility is a function which enables a user to transfer her/his identity between IMT-2000 mobile terminals. It is implicit in this definition that the IMT-2000 Personal Mobility is to access the telecommunication services delineated in the user's service profile, on any IMT-2000 mobile terminal. Every IMT-2000 user has a User Identity Module (UIM) which can interface and be associated with any IMT-2000 terminal.

3.2.1.3.Functions related to software configurable terminals(quoted from section 4.16.)

The software configurable terminals capability provides the mechanisms which allow applications to interact and operate with any MT. The applications and related data can permanently reside within the UIM, the MT, or external device or can be downloaded by the Core Network.

Capability Profile Exchange: This function provides a mechanism for the MT, the UIM and the Core Network to exchange service capability information. For example, the following types of exchanges may occur:

- MT services capability may be provided to the UIM or Core Network;
- UIM services capability may be provided to the MT or Core Network;
- Core Network services capabilities may be provided to the UIM.

Application Data Transfer: This function provides a mechanism for the MT, the UIM and the Core Network to exchange applications and associated data. For example, the following types of exchanges may occur:

- MT data may be provided to the UIM or Core Network;
- UIM data and applications may be provided to the MT or Core Network;
- Core Network data and applications may be provided to the UIM or MT.

Proactive Applications: This function gives a mechanism whereby applications can initiate actions to be taken by the MT. These applications may reside in the UIM, MT or external device or may be downloaded from the Core Network. Examples of these actions include:

- display text from the UIM or Core Network to the MT;
- send a short message;
- set up a voice call to a number held by the UIM, MT or external device;
- set up a data call to a number and bearer capabilities held by the UIM, MT or external device;
- send a supplementary service control or service data;
- play tone in earpiece;
- initiate a dialogue with the user;
- provide local information from the MT to the UIM or to the Core Network;
- provide help information on each command involved in the dialogue with the user.

Screening service by UIM: This function allows that when this screening service is activated by the UIM, all dialed digit strings, supplementary service control service data are first passed to the UIM before the MT sets up the call, the supplementary service operation or the service data operation. The UIM has the ability to allow, bar or modify the call, the supplementary service operation or the service data operation. For example, a call request can be replaced by a supplementary service operation or a service data operation, and vice-versa.

Security: This function allows that applications designed using the features in this capability can use the methods to ensure data confidentiality, data integrity, and data sender validation, or any subset of these.

3.2.2.The IMT-2000 Functional Models

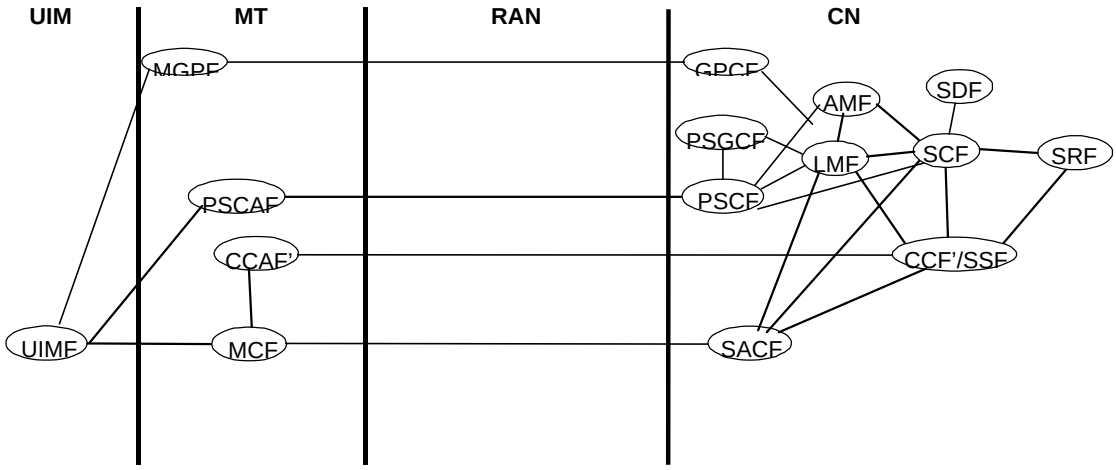

Figure 2-2 Communication and Service Control Related Functional Entities

3.2.2.1.Functional Entities related to UIMF on the Mobile Side of the Radio Interface

This section describes the communication and service control related FEs in the UIM and mobile terminal subsystems.

MCF - Mobile Control Function: This FE provides the overall service access control logic and processing at the mobile side of the radio interface. Specifically, it interacts with the network for mobility management. It includes functions to:

g)interact with the UIMF to retrieve user identification information, location management related information (e.g. location area identity), security and privacy related information (e.g. temporary mobile user identity);

h)interact with the UIMF to exchange application information with the applications that are allocated within the UIMF, MCF, or external device;

j)interact with SCF (utilising the relationship with the SACF) for service control purposes, for example to download and store service logic and application data (this can also be done by the UIMF);

m)interact with UIMF to perform serving system selection;

UIMF - User Identification Management Function: This FE provides the means to identify both the IMT-2000 user and the mobile terminal to the network and/or to the service provider, and contains processing capability for authentication and service handling in the UIM. It includes functions to:

a) store IMT-2000 user-related information such as IMT-2000 user identification information both to identify the IMT-2000 user and to address the mobile terminal, location management related information and security and privacy related information;

b) interact with MCF to provide IMT-2000 user identification information, location management related information (e.g. location area identity), security and privacy related information (e.g. temporary mobile user identity);

c) interact with MCF to exchange application information with the applications that are allocated within the MCF, UIMF, or external device;

d) interact with MCF to provide serving system selection information based on e.g. location area identity, service availability, and service preferences;

e) interact with the AMF (utilising the relationship with the MCF or PSCAF) for IMT-2000 user authentication and ciphering key generation (e.g. calculation of authentication response and generation of ciphering key);

f) perform and control authentication of the network to the user in case of mutual authentication, and update authentication parameters in the UIM in interaction with the AMF, utilising the relationship with the MCF or PSCAF;

g) interact with the SCF to exchange application information, utilising the relationship with the MCF or PSCAF, for example to support proactive applications;

h) store, process and/or work with Man Machine Interface (MMI) functionality in the MT to display application data or other types of data downloaded from the network or loaded into the UIMF by other means;

i) execute service logic required to handle service attempts in the UIM, both related to a call and not related to a call.

The connection control agent function may be either contained in the call control agent functional entity or a separate functional entity. The CCAF' functionality is mostly the same in either case, however, the differences are noted below the CCAF' FE description.

MGPF - Mobile Geographic Position Function: This FE provides the overall control for the geographic position finding function on the mobile terminal side. It includes functionality to:

g) interact with UIMF in support of user identification, authentication and privacy.

PSCF - Packet Service Control Function: This FE provides the packet service control functionality in the IMT-2000 core network. It includes functionality to:

j) interacts with SCF to support the transfer of information between SCF and UIMF

3.2.3.Network Reference Points

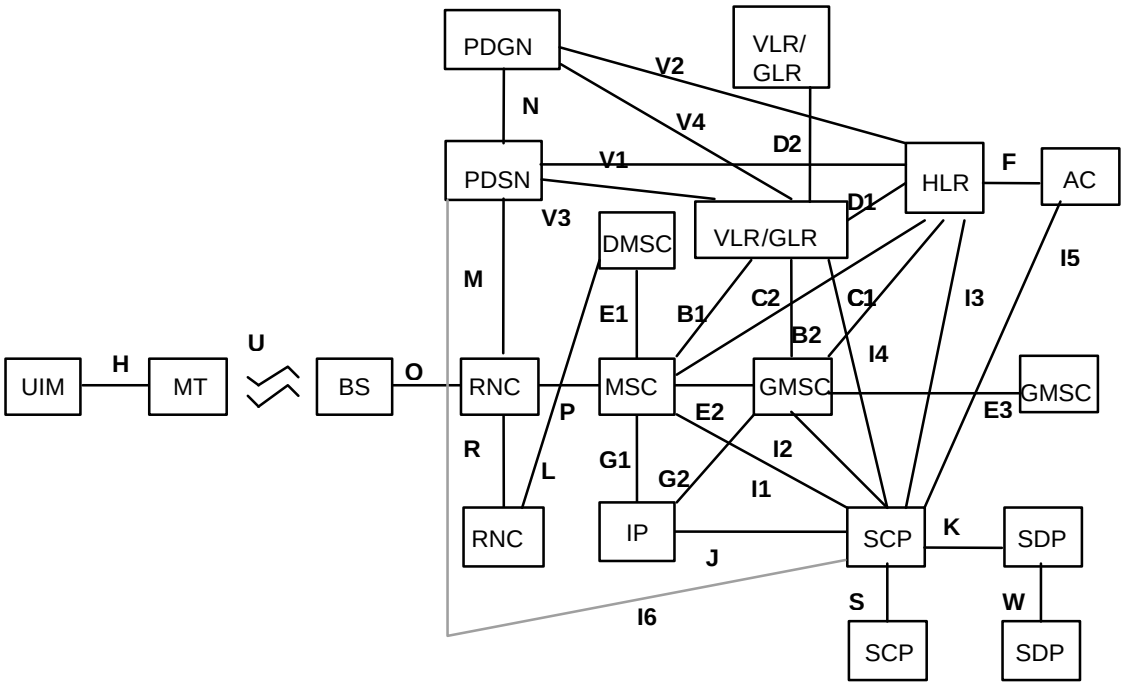

FIGURE2-3 **Reference Points in IMT-2000 Reference Model**

3.2.4. Global Roaming and Interworking Scenarios (quoted from section 7)

3.2.4.1.Network interconnections to support the interaction between UIM and Home SCF (quoted from section 7.2.2.8)

The interaction between UIMF and home SCF for service control purposes will be supported across network boundaries. In this case the SACF or the PSCF of the serving network as well as the MCF or PSCAF support the transparent exchange of information between SCFh and UIMF, for example to download and store service programs and/or application data.

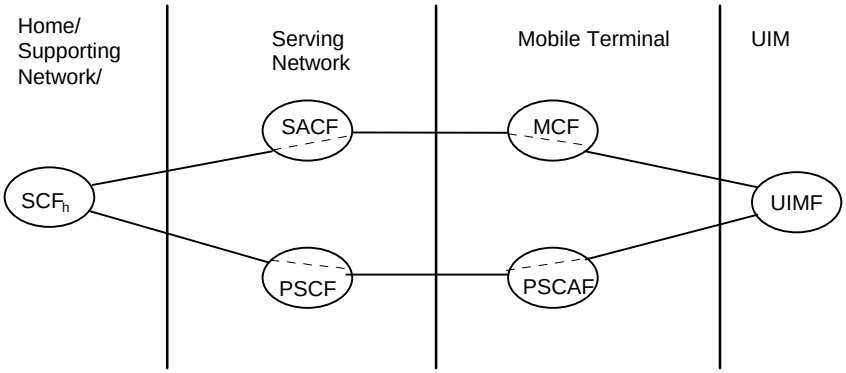

Figure 2-4 Network interconnections: UIMF-SCFh relationships

3.3 Functional Information Flows

[TBD]