Technical Specification Group Terminals
Meeting #6, Nice, France, 13-15 December 1999

TSGT#6(99)257

Source: ITU-T SG11 WP3

Agenda item: 5

Document for: Information

Subject: Common mobile telecommunications smart card standard

---

This document contains two documents relating to the organisation mobile telecommunication smart card standardisation work.

The first document is the output of the 2G/3G SIM, USIM & R-UIM officials meeting meeting held in early November.

The second document is a LS in response from the ITU-T SG11 WG3 to ETSI SMG9.

Both documents are registered to the TSG-T meeting for information.

Doc 99-006

(editorially updated version of 99-005)

Committee Correspondence

Source: 2G/3G SIM, USIM & R-UIM officials meeting [1]

To: 3GPP-PCG, 3GPP2-SC, GAIT, SMG9, T1P1, TR45, UWCC-PDFG

CC: 3GPP-TSG-T3, 3GPP2-TSG-C/S/N, CDG, GSM Association, GSM-NA, TR45.2, TR45.3, TR45.5

Subject: Common mobile telecommunications smart card standard

Delegates to the 2G/3G SIM, USIM & R-UIM officials meeting held November 1st 1999 in Austin, Texas, would like to make the following proposal regarding the mobile telecommunication smart card management across all wireless technologies of the groups addressed above.

The group concluded that, with the increasing activities of several different committees, there was a danger that the resulting telecommunications smart cards standards would diverge, thereby preventing the inter-operation of several systems on one card. It was proposed that the best way to avoid this situation was to have one committee responsible for the top-level common aspects of mobile telecommunications smart cards.

It was agreed that a harmonized smart card for all next generation telecommunication technologies is a strong requirement.

Considering that SMG9 has years of experience as the custodian of a widely used mobile telecommunications smart card specification, it is proposed that SMG9 extends its role to act as the central focus point for all next generation telecommunications smart cards.

SMG9 should be invited to extend its scope and take the role of managing common aspects of mobile telecommunication smart card in the following areas:

- physical interface specifications
- the common logical interface
- file ID allocation (DFs) at the common level, respecting existing directory structures
- shared data that is technology independent (e.g. the phone book).

The specification of the structure and content of the technology specific files, procedures and protocols will remain in the domain of the formulating standards committee.

The meeting realizes that there are open issues that need to be addressed, such as:

- the derivation of technology independent service requirements
- common inter-technology requirements such as multiple subscriptions, multi-technology roaming
- Toolkit related functionality
- a notification process with the various SDOs.

This group is planning a follow up meeting to address these issues, possibly in Rome on the 17th of January 2000.

It is requested that the addressed organizations ratify the approach outlined above before the 17th of January 2000, and inform SMG9 via the SMG9 Chairman, Dr. Klaus Vedder (klaus.vedder@gdm.de) and the SMG9 Secretary, Michael Sanders (michael.sanders@etsi.fr).

---

[1] see attached attendees list

List of attendees at the 2G/3G SIM, USIM & R-UIM officials meeting (Austin, Tx, 1st Nov, 1999)

Name	Organisation	Email	Official position
AEBI Paul	Swisscom	paul.aebi@swisscom.com	Chair GSM Assocation SCAG
BARNES Nigel	Motorola	nigel.barnes@motorola.com	Vice-chair ETSI SMG9
BROWNLEY Jane	Lucent Technologies	jbrownley@lucent.com	Secretary TR-45
COURSEY Cameron	SBC	coursey@tri.sbc.com	Co-chair GAIT
DENNETT Steve	Motorola	qa1404@email.mot.com	Chair 3GPP2
FERGUSON Ron	Sprint PCS	rfergu01@sprintspectrum.com	Chair 3GPP2 TSG-S UIM focus group
GOGIC Aleksandar	Vodafone Airtouch	alex.gogic@airtouch.com	Co-chair 3GPP2 TSG-C UIM focus group
HABBAL Omar	Schlumberger	ohabbal@san-jose.tt.slb.com	Meeting host
HAYES Stephen	Ericsson	eussrh@am1.ericsson.se	Chair T1P1 GTI
HOSFORD Mark	LG Infocomm	mhosford@lginfocomm.com	Chair T1P1.2
SANDERS Michael	3GPP & SMG support team	michael.sanders@etsi.fr	Secretary ETSI SMG9 & 3GPP T3
SENNET DeWayne	AT&T Wireless	dewayne.sennett@attws.com	Chair of UWCC PDFG SIM ad hoc group
TSENG Mitch	Nokia	mitch.tseng@nokia.com	Co-chair 3GPP2 TSG-C UIM focus group
VEDDER Klaus	Giesecke & Devrient	klaus.vedder@gdm.de	Chair ETSI SMG9 & 3GPP T3
WATTS Terry	SBC	watts@tri.sbc.com	Chair TR-45 UIM/ESN ad hoc group
WILLHOFF Steve	Nokia	steve.willhoff@nokia.com	Chair TR-45.3.6

ITU - Telecommunications Standardization Sector **Temporary Document PL/11 129R1**

STUDY GROUP 11

Geneva, 22 November – 10 December

Questions: Plenary SG11

SOURCE: WP3/11 Vice Chairman

TITLE: Liaison Statements to be sent to technical bodies outside SG11

---

1. Introduction

This document contains the liaison statements to be sent to other technical bodies outside ITU-T SG11 from SG 11 WP3 prepared in the meeting that took place from the 22nd November to the 2nd December 1999 in Geneva. These liaison statements were agreed in the plenary of WP3 on the 2nd December.

2. Contents

Liaison no.	FROM:	TO:	Subject:
1	WP3/11	29/13	Intelligent Mobility for the GII, IMT 2000
2	8/11	SG's 7 and 13	Study on new areas of interworking under SG7 involving the internet and IMT 2000 networks
3	8/11	13/2	Comments to draft recommendation F116
4	8/11	ETSI SMG 9	UIM requirements and ongoing standardisation work.

3. proposal

These liaisons were presented for agreement at the SG11 plenary on 3rd December 1999.

LIAISON 4

ITU - Telecommunication Standardization Sector

STUDY GROUP 11

Geneva, Switzerland, November 22 - December 10, 1999

QUESTION: 8/11

SOURCE: ITU-T SG 11 (Geneva, November 22 - December 10, 1999)

TITLE: UIM REQUIREMENTS AND ONGOING STANDARDIZATION WORK

LIAISON STATEMENT

TO: ETSI SMG9

APPROVAL: SG 11 meeting 3rd December 1999.

FOR: Action

DEADLINE: May 31, 2000

CONTACTS: Masami Yabusaki
NTT DoCoMo
Washington Plaza
40, rue Washington
75408 Paris Cedex 08, France

Tel: +33 1 56 88 30 30
Fax: +33 1 56 88 30 45
Mobile: +33 6 8259 4358
E-mail: yabusaki@docomo.fr

Introduction

SG 11 is the lead SG in ITU-T on IMT-2000. We have been working on all aspects of this diverse and complex system, which aims to achieve a significant step forward in the global mobile telecommunications infrastructure. As part of this, we have been interacting with a number of regional standards bodies that are doing work related to the goal of specifying a global mobile telecommunications system.

Status of Work on IMT-2000 Specifications in SG 11

Specifically, SG 11 has been addressing and has completed the work on the first IMT-2000 Capability Set with respect to the requirements for IMT-2000 (Recommendation Q.1701) and the functional architecture for IMT-2000 (Recommendation Q.1711), both of which were finalized at our March, 1999 meeting. At our November 22 - December 10, 1999 meeting, we reached

Resolution 1 Determination on the information flows for the UIM-MT, MT-RAN and CN-CN (NNI) interfaces (draft new Recommendation Q.1721.) (At this meeting, we also reached Resolution 1 Determination for draft new Recommendations Q.1731, "Radio-technology Independent Requirements for IMT-2000 Layer 2 Radio Interface." and Q.1751, "Inter network Signalling Requirements for IMT-2000 Capability Set 1.")

Along with the above, we are working on a Supplement to the Q.1700-series of Recommendations which is intended to provide a roadmap of IMT-2000 standards developed in ITU and other standards developing partnership projects and organizations (3GPPs and SDOs). The scope includes any relevant standards that are targeted toward the specification of IMT-2000 systems.

Evolution of Work on UIM-MT Interface

SG 11 has been made aware of the meeting of ETSI SMG9, 3GPP T3, 3GPP2 TSG C, GAIT, UWCC, PDFG, TIA TR45.3, TIA TR45, T1.P1 and the GSM Association[2]. We would ask for confirmation of this meeting and its outcome. We note the cooperation emerging among interested parties with respect to developing standards for UIMs and their physical realization, and the view that ETSI SMG9 is well positioned to progress this work.

SG 11 acknowledges and recognizes the work being done in ETSI SMG9, and we have been informed of the intention to extend the mandate of SMG9 towards setting global standards in this area. Since ITU-T is the pre-eminent global standards organization, we are prepared to support efforts in the development of UIM standards to avoid any duplication of effort in this area. To this end, while not complete in all respects, we wish to provide to you our current views on UIM to MT Interface Requirements, via a draft Supplement progressed at the November 22 - December 10, 1999 SG 11 meeting, and intended for finalization in 2000, as an attachment to this liaison statement.

We would ask that you inform us of your plans and work program in this area so that we may be fully aware of the work that is being done.

Ongoing Involvement of ITU-T SG 11

SG 11 wishes to maintain a role in this work, and to monitor its progress. We therefore request that you keep ITU-T, and specifically SG 11 (and the organization that will be continuing the work on IMT-2000 post the WTSA decisions in the fall of 2000) regularly and frequently informed as you progress the work in this area.

ATTACHMENT

[2] We are encouraging participants in our meeting who are also involved in the listed bodies and any other relevant bodies to bring this liaison statement to their attention.

ATTACHMENT

(Temporary Document TD3/11- 34 to the SG11 meeting)

ITU - Telecommunication Standardization Sector

STUDY GROUP **11**
Geneva, 22 November – 10 December 1999

Question(s): 23/11

Source* **:** EDITORS - Q.FSU (Jan Oudelaar, Lucent NL, Dr. Shila Heeralall, Lucent USA)

TITLE: ITU-T DRAFT RECOMMENDATION Q.1741 (Q.FSU) VERSION 7.1

Abstract:

This temporary document provides Version 7.1 of draft recommendation Q.1741(formerly Q.FSU), IMT-2000 Functionality and Signalling Requirements for UIM. It includes the amendments made during the SG 11 Plenary meeting held in Geneva, 22 November – 10 December 1999.

*CONTACTS : Mr. Jan Oudelaar
Lucent Technologies NL B.V.
P.O.Box 1168
1200 BD Hilversum, The Netherlands
Tel +31 35 687 1736
Fax +31 35 687 5810
Email: oudelaar@lucent.com

Dr. Shila Heeralall
Lucent Technologies Inc.
Room 3A-334, 67 Whippany Road
Whippany, NJ, 07981 USA
Tel: +1 973 581 6981
Fax: +1 973 386 4555
Email: shila@lucent.com

ITU - T Recommendation Q.FSU Version 7.1

IMT-2000 Functionality and Signalling requirements for UIM

Summary

This recommendation describes the functionality and requirements of the UIM (User IdentityModule) used within IMT-2000 mobile terminals and the UIM - MT signalling requirements. . This includes functional communications (e.g. UIM-CNv and UIM-CNh) across the UIM-MT interface. Only the requirements necessary to support global roaming and inter-operability between different family members of IMT-2000 are specified here.

Requirements which are related only to individual family members are outside the scope of this recommendation.

The User IdentityModule (UIM), provides functions to support user security and services. These functions may either reside in a removable physical device for a mobile terminal or be integrated into the physical mobile terminal. A non-removable UIM is functionally equivalent to a removable UIM.

Keywords

IMT-2000

Third Generation systems

FPLMTS

User Identity Module

Mobile Terminal

Contents

1. Scope

This recommendation describes the functionality and requirements of the UIM (User IdentityModule) used within IMT-2000 mobile terminals and the UIM - MT signalling requirements. This includes functional communications (e.g. UIM-CNv and UIM-CNh) across the UIM-MT interface. Only the requirements necessary to support global roaming and inter-operability between different family members of IMT-2000 are specified here.

Requirements which are related only to individual family members are outside the scope of this recommendation.

The User IdentityModule (UIM), provides functions to support user security and services. These functions may either reside in a removable physical device for a mobile terminal or be integrated into the physical mobile terminal. A non-removable UIM is functionally equivalent to a removable UIM.

2. References

1. ITU-T [draft recommendation] Q.1702, Framework for IMT-2000 networks
2. ITU-T [draft recommendation] Q.1711, Network Functional Model for IMT-2000
3. ITU-T [draft recommendation] Q.1721, IMT-2000 Information Flows

8. ISO 7816-1, 1987: "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics"
9. ISO 7816-2, 1988: "Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and locations of the contacts"
10. ISO 7816-3, 1997: "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols"
11. ISO 7816-4, 1995: "Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange"
12. *(Other ISO Specifications may need to be added)*
13. SG 2 Recommendation on E.212 (Revised) *(add title etc.)*
14. SG 2 Recommendation on E.164 (Revised) *(add title etc.)*

3. Definitions

This is a list of definitions of special terms used in this recommendation.

Authentication: a process by which the correct identity of an entity or party is established with a required assurance. The party being authenticated could be a user, subscriber, service provider or network operator.

Authentication algorithm parameters: Input parameters to the authentication algorithm used in the computations to produce the authentication response. If this response computed in the UIM (whether permanent or removable) matches the corresponding response computed in the AMF (Authentication Management Function), the authentication passes, otherwise authentication fails.

Authentication key: A user secret data used for authentication.

Cipher key: a code used in conjunction with a security algorithm to encode and decode user and/or signalling data.

Confidentiality: the avoidance of disclosure of information without the permission of its owner.

IC Card: a card holding an Integrated Circuit containing user, authentication and/or application data for one or more applications.

IMUI: International Mobile User Identity (e.g. IMSI), used to address a mobile terminal and the mobile user uniquely to a service provision function.

Integrity: (in the context of security) is the avoidance of unauthorized modification of information.

LAI: The Local Area Identifier identifies the area in which the mobile terminal is located in the visited network.

PIN: Personal Identification Number used toby the Mobile Terminal and the UIM for the verification of the identity of the user before giving access to the subscribed services if the PIN feature is activated. The PIN feature can be activated and deactivated by the user.

PIN Error Counter: The number of retries that the user can present or enter the PIN incorrectly before the PIN is blocked. Once the PIN is blocked, the service provider can instruct the user of how to unblock the PIN. **PUK:** A PIN unblocking code that is to be used to re-validate the PIN when the PIN is blocked.

Security: the ability to prevent fraud as well as the protection of information availability, integrity and confidentiality.

Service: set of functions offered to a user by an organisation.

Service Provider: an organisation which has a contractual relationship with the subscriber for overall provision of service capabilities, and directly bills the subscriber for them. Services include basic telecommunications facilities from network operators and value added services from both network operators and third party value added service providers.

Status of UIM (blocked, unblocked)

TMUI: A unique, temporary number that is assigned to a subscriber during each session, for user confidentiality and data length reduction.

IMT-2000 number: A number that uniquely identifies an IMT-2000 user and is used to place, or forward, a call to a user, or to identify a user upon call origination.

(Note: E.164 MS ISDN Number may be applied for this.)

4. Abbreviations and Acronyms

CN	Core Network
IMUI	International Mobile User Identity
ISO	International Organisation for Standardisation
LAI	Location Area Identity
MMI	Man Machine Interface
MT	Mobile Terminal
NO	Network Operator
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
PUK	PIN Unblocking Code
RAN	Radio Access Network
SP	Service Provider
TMUI	Temporary Mobile User Identity
UIM	User Identity Module

5. Functional Communications of the UIM

The User Identification Module (UIM), provides functions to support user security and services. These functions may either reside in a removable physical device for a mobile terminal or be integrated into the physical mobile terminal. A non-removable UIM is functionally equivalent to a removable UIM.

In the figure below the functional communications across the UIM-MT interface are shown in an overall IMT-2000 system. The UIM communicates with the Mobile Terminal, the visited Core Network and the home Core Network.

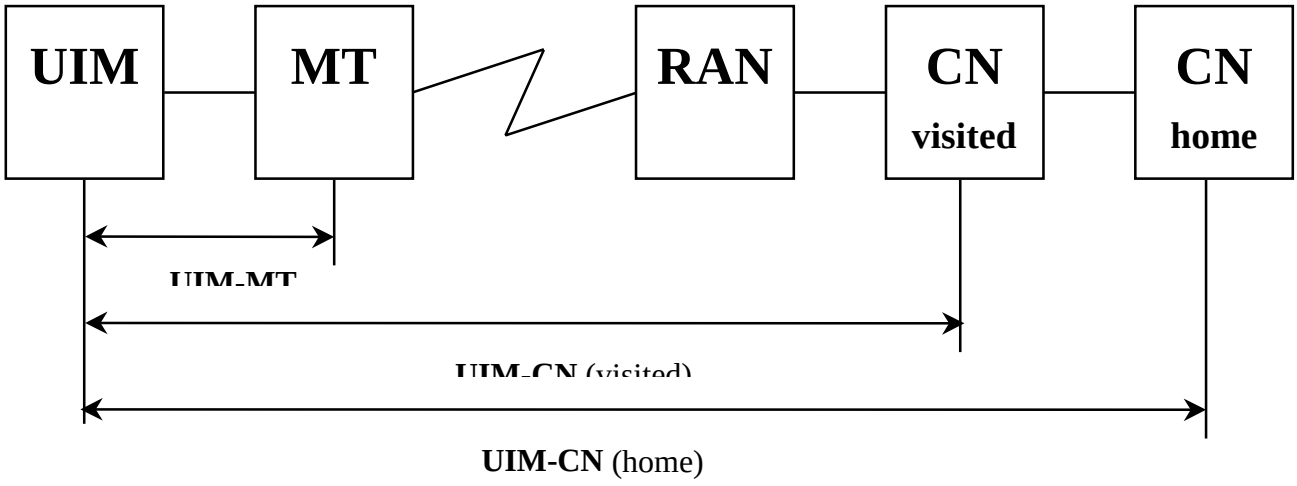


Figure 1/Q.1741 – Functional Communications of the UIM in a IMT-2000 system

6. Functions to be supported by the UIM

The UIM shall support the following functions:

6.1 Security related functions

This section provides some general security functions in the list below, and then it provides further security functions that are classified into three areas.
The general security functions are:

- Authentication between the UIM and the network. One or more authentication algorithms and their associated parameters may be supported. A valid UIM shall be present in the Mobile Terminal to access services in an IMT-2000 network with the exception of making emergency calls.
- Value-added-services application security, e.g. authentication of prepaid services
- Ciphering parameters to prevent eavesdropping
- Temporary Mobile User Identity to ensure privacy of the user
- Multiple access privileges that are configurable by the service provider for each information file stored in the UIM

Further security functionsfor the UIM areseparated into three areas. Security functions related to the presence of the UIM, security functions related to data access, and the security functions performed by the UIM.

A) SECURITY FUNCTIONS RELATED TO THE PRESENCE OF THE UIM

- The user shall be unambiguously identified, therefore the UIM shall be physically present in order to make use of any services except for emergency calls and totally free services which do not acquire user identification.

- If the UIM is removed from the mobile terminal during a call or calls, the call(s) shall be immediately terminated.

B) SECURITY FUNCTIONS RELATED TO DATA ACCESS

Data in the UIM falls into 5 categories and access to each category of data is controlled by suitable means. Data access control is discussed fully in section 7 together with data storage requirements.

C) SECURITY FUNCTIONS PERFORMED BY THE UIM

- Storage of Information related to security
- Storage and execution of cryptographic algorithms
- Verification of the results of cryptographic algorithms
- Authentication by the service provider/network operator of the user when required
- Authentication of the service provider/network operator.
- Ciphering of user traffic when required

6.2 Network related functions

- Procedures that are not clearly user dependent and may be directly caused by the interaction of the MS and the network shall be supported.
- Procedures that are automatically initiated by the MS, (eg some forms of location updating) shall be supported.
- Service profiles shall be owned by the service provider/network operator who can delegate or authorise the user to read or modify certain service parameters in the service profile. The user's service profiles stored on the UIM will contain parameters associated with the services that may be used. These parameters are required by the terminal, the network/or the service provider to ensure that the services are provided and in particular that they are presented in a uniform manner to the user. These service profiles may be stored on the UIM and/or transmitted by the service provider and the user shall be able to modify parameters in the service profiles.
- Over-the-air service provisioning and updating may be supported.

6.3 Functions related to other UIM Applications

- Also other applications than the UIM can be hosted, like e.g. applications like UPT, credit service and electronic banking. Each application shall reside in its own domain (physical or logical). It shall be possible to manage each application separately. The security and operation of an application in any domain shall not be compromised by an application running in a different domain.
- Applications should be able to share some information such as a common address book
- The UIM will be capable of multitasking, such as sending or receiving data from the terminal whilst also engaged in a call.
- It shall be possible for entities either within or outside of the serving network to communicate directly with the UIM. These communications shall be two way and initiated from either end with or without user interaction. The information passed may be informative data, executable code, service parameters etc. . An example of the use for such data would be in the support for software defined radio.

After powering on the Mobile Terminal (or after inserting the UIM) the capabilities of the terminal and of the UIM (especially related to the Service Profiles) shall be negotiated. If the terminal can not satisfy (all of) the requirements of the UIM, this shall be indicated to the user.

Examples of multi-applications are databases (e.g. telephone books), service profiles (e.g. controlling divert information), users preferences (e.g. short dialling codes) and SP- specific parameters inside a UIM application (e.g. call barring tables).

7 Multi purpose UIM Model

7.1 Introduction

The functionality of the UIM corresponds with the functionality of an IC card ("SIM") as defined in ETSI SMG9 for UMTS. The UIM may be an IC card (a removable UIM) but can as well be implemented as an integrated part of the terminal (a non-removable UIM); both versions are functionally equivalent.

A UIM may be multi-purpose in its capability. Figure 2/Q.1741 shows a multiple purpose UIM functional model comprising of components for supporting multiple service providers (UIM-SP), multiple User Profiles, and multiple service applications. A UIM capable to accommodate UIMs for multiple service providers as well as applications other than the UIM is called a **Multi Purpose UIM**.

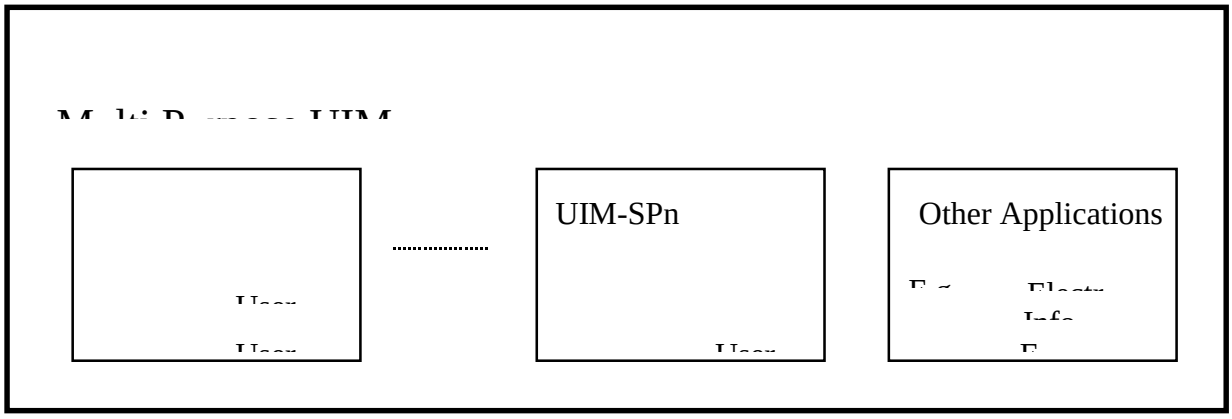


Figure 2/Q.1741 – Model of the Multi purpose UIM

7.1 Multiple Service Providers

A **UIM-SP** is a UIM related to a specific Service Provider. A UIM-SP has unique identity and is associated with one and only one Service Provider . A multiple service provider UIM will support multiple UIM-SPs for "mobility services" when those UIM-SPs are associated with different mobility service providers (Home Networks) as well as different VHE/IN services providers (Supporting Networks).

In order to support "plastic roaming", it should be possible to accommodate not only UIMs of different service providers, but also UIMs of different family members in a single UIM. A terminal should be able to read the UIMs of all IMT2000 family members and pass this information to the visited network.

In light of the security problems which may be caused by the coexistence of multiple UIM-SPs on a UIM, in the short term, it is expected that only one UIM-SP will be implemented on a UIM. Therefore, for Capability Set 1 of IMT2000 only a single Service Provider capability on a UIM is required.

7.3 Multiple User Profiles

A UIM-SP may support multiple **User Profiles**. The user profile contains information which may be used to personalize services for the user. A user may be associated with one or more user profiles. A user may select and activate his/her profile on a per call basis

It should be possible for one or more user profiles associated with the same user to be simultaneously active so that the user may make or receive simultaneous calls associated with different profiles . Activation of profiles should be done in a secure manner (e.g., with the use of a PIN).

For terminating calls the correct profile should be indicated by the user address used (e.g. IMUN). Each profile will have at least one unique user address associated with it. For originating calls the user should be able to choose from the available profiles, the appropriate one for the call. A profile identity will need to be associated with the call for accounting and billing purposes. User profile identities need not be standardized but a standardized means is required for indicating that a particular profile is being used.

Simultaneous use of the same user profile on multiple terminals for the same type of service should not be allowed.

User profiles associated with different home environments (home networks and/or supporting networks) should not share the same user address.

7.4 Other Applications

It should be possible for a Multiple Purpose UIM to host **other applications** in addition to the UIM-SPs, see figure 2. Service providers, subscribers or users may need to establish additional data or processes on a Multi Purpose UIM. Each application on an IC card should reside in its own domain (physical or logical). It should be possible to manage each application on the card separately. The security and operation of an application in any domain should not be compromised by running an application in another domain. Each application may need to use its own security mechanisms which are separate from those specified for UMTS e.g. electronic commerce applications.

Examples of other UIM applications are: off-line user applications like UPT, electronic banking, credit service, etc.

Applications should be able to share some information such as a common address book.

It should be possible to **address applications** which reside on the card in a secure manner **via the air interface**.

7.5 Support of Service Provisioning

It should be possible to **download a UIM-SP over the air-interface** to a (Multi Purpose) UIM. As an integrated UIM and a removable UIM are functionally equivalent, this should be possible for integrated and removable UIMs. This includes Over the Air Service Provisioning (OTASP) as detailed in Recommendation Q.1721, Section 12.

7.6 Phased Introduction

For Capability Set 1 of IMT2000 is shall be possible to accommodate at least one Service Provider and one User Profile on a UIM, the use of a Multi Purpose UIM is optional.

For CS2 a Multi Purpose UIM shall be mandatory, enabling multiple Service Provider applications on a MP-UIM, multiple User Profiles per Sevice Provider, Multiple other Applications, and support of Service Provisioning.

8 UIM Data Storage Requirements and Data Access Control

8.1 DataStorage Requirements

The UIM should provide memory to store the recommended data as listed in the four tables below. The four tables correspond to the four categories of data storage requirements which are:

(a)data required for UIM management, (b) data required for accessing the network, (c) data required for the user's subscribed services, and (d) data required for UIM applications. Sophisticated UIMs can support part or all of the UIM applications. The mandatory data elements will be populated for all subscribers. The optional data elements may be populated on a per-subscription basis.

Table 1: Data required for UIM Management

Data elements	Requirements
1) UIM Identification Note: This is a unique card identification number	Mandatory
2) UIM phase identification (also called Protocol revision number) Note: This indicates the standards release that the UIM is programmed to conform to	Mandatory
3) Value-added-service application identifications list Note: This indicates the value-added-service applications that the user has subscribed to	Optional
4) Personal Identification Number (PIN) #1 Note: Maintained by user	Mandatory
5) PIN #1 Error Counter and Unblocking Code (PUK1) Note: Unblocking code is maintained by the service provider	Mandatory
6) PIN #2 Note: Maintained by service provider	Mandatory
7) PIN2 #2 Error Counter and Unblocking Code (PUK2) Note: Unblocking code is maintained by the service provider	Mandatory
8) UIM access status (blocked/unblocked)	Mandatory
9) UIM general programming lock (UIM-GPL) Note: This is a code which locks any programming of any data on the UIM	Mandatory
10) UIM general programming lock owner Note: This is a code which uniquely identifies the owner of the UIM-GPL	Mandatory

11) UIM mobile network data programming lock (UIM-NDL) Note: This is a code which locks any programming of mobile network related data	Mandatory
12) UIM mobile network data programming lock owner Note: This is a code which uniquely identifies the owner of the UIM-NDL	Mandatory
13) Administrative Codes (up to 5) Note: This is a set of codes that can be assigned between the service provider and the card manufacturer to administer the UIM content	Optional
14) Over-the-air service provisioning and updating security parameters Note: The set of security parameters that are required by over-the-air procedures. These required parameters are unique to each air-interface OTA mechanism.	Optional

Table 2: Data required for accessing the Network

Data	**Requirements**
1) International Mobile UserIdentity (IMUI)	Mandatory
2) Temporary Mobile UserIdentity (TMUI) Note: A unique, temporary number that is assigned to a subscriber during each session, for user confidentiality and data length reduction	Mandatory
3) TMUI assignment source ID Note: This identifies the SDF which assigned the TMUI	Mandatory
4) TMUI expiration timer Note: This provides enhanced user confidentiality	Optional
5) Optional services list Note: This is a list of all the optional services the UIM supports (e.g. support download of applets)	Mandatory
6) UIM service table Note: A table that contains the list of services that the user has subscribed and/or activated such as the Abbreviated Dialing Number (AND) and PIN access	Mandatory
7) Specific PLMN programming lock (SPPL)	Mandatory
8) Specific PLMN programming lock owner Note: This is a code which uniquely identifies the owner of the SPPL	Mandatory
9) Language preference Note: A list of all the languages that the service provider can offer to the user for selection of a language to be used for entering using the handset keypad or for displaying on the screen. Examples of languages are English, French, Spanish, German, etc.	Mandatory
10) Preferred language Note: This is the language selected by the user	Optional
11) Ciphering key	Mandatory
12) Home PLMN	Mandatory
13) Preferred PLMN roaming list and associated parameters	Optional
14) Home PLMN search period	Mandatory
15) Network access control class (regular subscriber, emergency services, operator maintenance staff)	Mandatory

16) Access overload class	Mandatory
17) Forbidden PLMNs Note: Memory is allocated but default initialization is optional	Optional
18) Subscribed to User Zones Note: Serving zones to which the user has subscribed for service (it might be only a fraction of the operator's PLMN coverage area). It can also be used for serving zones with a discounted tariff	Optional
19) Network Identity of the last network accessed before power off	Mandatory
20) Location area of the last network accessed before power off	Mandatory
21) Cell ID of the last cell accessed before power off	Mandatory
22) Last geographical position (in geographical coordinates) of the MT before power off	Mandatory
23) Last RF configuration before MT power off Note: RF configuration = Frequency or carrier number of the last RF carrier used by the mobile before power off, as well as other relevant data defining the RF channel used by the mobile (e.g. PN offset). When powered on, the mobile should retrieve these parameters from the UIM and tune its RF receiver on this same channel first, to attempt to reacquire the network it was registered on at the time of the power off. This is used as a first network acquisition attempt. If the mobile can not acquire the previous network (e.g. because the mobile moved while it was powered off), the mobile will have to scan the whole RF band (and may be several bands if it is a multi-band mobile) to look for available PLMNs.	Optional
24) Location information Note: This file contains the previous successful registered network. It may include the TMSI, Location Area Identification (LAI), Cell Identity (CI), TMSI Timer	Mandatory
25) Administrative data Note: This parameter contains information concerning the mode of operation according to the type of UIM, such as normal, type approval, cell testing, or manufacturer specific	Mandatory
26) Authentication key for data services Note: This data services dedicated key might not be required if the authentication key for voice services can be used instead.	Optional
27) Data services ciphering key	Mandatory
28) Data services location information	Mandatory
29) Advice of charge counters, price, and currency (an option for implementing a prepaid service)	Optional
30) Authentication algorithm parameters Note: The set of parameters such as secret key(s) that are required by the authentication algorithms. One or more authentication algorithms may be supported. Therefore there may be more than one set of authentication algorithm parameters. It is mandatory to have at least one. One example requires these two keys as Mandatory: a) Secret key Ku (for user authentication) b) Secret key Ku' (for ciphering key generation)	Mandatory
31) Mobile manufacturer identity	Optional
32) Mobile Terminal electronic serial number (ESN)	Optional

Note: A number that uniquely identify each handset (mobile equipment)	
33) Service provider name	Optional
34) Group identity Note: A coding that allows the service provider to assign to a user when subscribed to special applications that are applicable to group(s).	Optional
35) Message Category Note: Identify the category of the cell-broadcast messages. The user may select the type of cell-broadcast messages to be received and/or accepted.	Optional
36) Broadcast control channel	Mandatory
37)	

Table 3: Data required for User's Subscribed Services

(This table contains only optional data)

Data	Requirements
1) Abbreviated dialing number list Note: This record is optional because it might not be used in phones which are not operated by human beings (e.g. a phone installed in an Automatic Teller Machine (ATM) and which is used for telemetry purpose such as reporting a low amount of cash in the ATM, or other alarms, etc.	Optional
2) Call screening	Optional
3) Pre-paid service information (i.e. remaining amount to be used)	Optional
4) Fixed dialing number	Optional
5) Short messages (SMS) storage	Optional
6) Bearer capabilities configuration parameters	Optional
7) Mobile Station International Mobile Dialing Number	Optional
8) Short message parameters	Optional
9) Short message status	Optional
10) Last number dialed	Optional
11) Service dialing number	Optional
12) Barred dialing number	Optional
13) Mobile IP parameters	Optional
14) Fixed IP address	Optional
15) Dynamic IP address	Optional
16) Information of last N successful incoming calls (e.g. phone number, duration, cost) Note: May be used for special billing	Optional
17) Information of last N successful outgoing calls (e.g. phone number, duration, cost Note: May be used for special billing	Optional

Table 4: Data required for UIM applications

(This table contains only optional data)

1) Cell broadcast screening parameters	Optional
2) Applet Note: The support of applets by the UIM requires the environment necessary to execute the applet (e.g. the virtual machine for JavaCard) to be present on the UIM	Optional
3) Other information or algorithms not related to the wireless network (e.g. encrypted storage of banking or other services passwords/PINs, Social Security Number; long distance calling card; credit/debit card information; electronic purse; public transportation access card; toll road toll card; etc.)	Optional

Editor's note: This section is alligned with table C.1 (Data elements in UIM re. Q.FIF) of appendix D of Q.FIF.NB: Appendix D will be transferred to Q.FSU.

8.2 UIM Data Access Control

External access to the data and functions within the UIM can be controlled in different ways. A conventional method is that using PINs but with evolving technologies a number of biometric techniques could be used to authenticate the user and allow access to particular areas of the UIM. Verification of the all accesses shall be performed by the UIM itself and not delegated to another entity (for example the terminal).

Different types of data that could be stored on the UIM include :

TABLE 1/Q.FSU - UIM DATA CLASSIFICATIONS

Type	**Description**
1	Data that only has to be used within the UIM and therefore never accessed from an external source eg data for authentication of a user (keys, cryptographic algorithms,...)
2	Data that are permanent identities or other values/parameters that are not allowed to be changed eg permanent user identities which must remain fixed for a period of time like IMUI.
3	Data that are temporary identities or other information that only are allowed to be changed by the service provider / network operator eg (TMUI), user profile, services/applications (for telecommunication), other non-telecommunication applications.
4	Data that are temporary identities or other information that are allowed to be changed by the service provider / network operator or delegated to the user eg some user profile parameters, services/applications (for telecommunication), other non-telecommunication applications parameters
5	Data that the user himself has stored on the UIM and is only allowed to change eg PIN for authentication to the UIM, telephone numbers/addresses, abbreviated dialling numbers

These data may be provided by the service provider/network operator at the time of provision of the UIM or over the air if new services, additional data, processes and security mechanisms need to be established.

These different kinds of data shall be protected by corresponding security measures to protect the stored information against unauthorised access, modification, manipulation e.g. :

- Physical/logical techniques for type 1 data
- Logical measures such as access rights, PINs or authentication for types 2 - 5.
- Authentication of the network/service provider if type 1 - 4 data is accessed by the network/service provider.

Applications in the UIM shall reside in their own domains (physical or logical). It shall be possible to manage each application on the card separately and the security and operation of an application in any domain shall not be compromised by an application running in a different domain.

The extensive functionality of the UIM will require significant amounts of data to pass across the UIM - terminal interface. This interface shall be protected against unauthorised access, manipulation, modification of the data passing across the interface and manipulation of the interface itself.

9. The UIM-MT interface

9.1 UIM-MT layers 1 and 2

9.1.1Electrical Interface and Transmission Protocol

The electrical interface and transmission protocol shall be in accordance with the ISO specifications [9,10].

9.1.2 Mechanical Interface

The mechanical interface (physical characteristics, dimensions and location of the contacts) shall be in accordance with the ISO specifications [8, 9].

9.1.3.Transport Protocol

Editor's Note :

9.2 UIM-MT layer 3

Editor's note: This covers layer 3 UIM-MT interactions. It relates to Q.FIF for signalling requirements across both UIM-MT and UIM-CN functional paths.

9.2.1 Sequence of states for interoperability

(Editor's note: Placeholder for agreed topic)

9.2.2 The UIM-MT signalling procedures

(Editor's note: Placeholder for signalling requirements that complement Q.FIF procedures)
The UIM-CNv information flows that support the attachment, subscription and authentication processes can be found in Q.1721.

9.2.3 Service provider access

For the information types 1 - 4 in Table 1 above, only service providers shall be allowed read or modification access, (after authentication of the accessing party by the UIM) to the data. Mechanisms shall be provided to ensure that while UIM data is being modified data read from the UIM is valid (lock out mechanisms).

9.2.3.1 Uploading of Data to the Network

When the user modifies data on the UIM (type 4/5 data), mechanisms shall be provided to guarantee alignment of corresponding data in the network. This may require mutual authentication.

9.2.3.2 Downloading of Data from the Network

9.2.3.3 Identities and Profiles

A number of functions will require non-volatile storage on the UIM. The requirements on the functions are as follows:

- The network may need to establish the identity of a service provider providing service(s) to the user. The UIM shall contain sufficient information to allow the network to perform this.
- The UIM shall contain sufficient information to allow the service provider to identify the subscriber and/or user.
- The UIM shall contain sufficient information to allow it to identify the service provider/network operator. Where services are obtained from different service providers, provision shall be made for each service provider to be identified separately.
- Where there is more than one subscription to the same service provider for the same service, e.g. business and personal, provision shall be made for the user or the UIM or the terminal to select the appropriate identity for the call based upon service capability.
- It should be possible to update UIM specific information over the air, e.g. service profile information, algorithms, etc.

Editor's Note : Multiple instances of the UIM may be required. This will impose additional security requirements which are for further study.

9.2.4 UIM-MT Interaction

The UIM shall support the standard protocol defined in ITU-T for the communication with the MT.

For sophisticated UIM supporting applets, the UIM might actively interact with the MT, requesting services from the MT such as:

- to dial a phone number provided by the UIM
- to obtain/send data information from/to a given IP address
- to display data on the handset display, to emit a given sound through the phone loud speaker (e.g. alarm sound)

Other approaches for UIM/MT interaction are under study.

These features will require extensions to the basic communication protocol between the UIM and the MT. The extensions will not be supported by all UIMs or all MTs. Capability descriptors in the UIM and the MT (e.g. the UIMN Optional Services List in the UIM) allow the two devices to learn about their respective capabilities.

In some cases, the MT might not be able to support services requested by the UIM. For instance, let's consider a UIM containing a stock trading applet which requires a Wireless Application Protocol (WAP) connection to the stockbroker server to perform trades. If this UIM is plugged in a voice only MT which does not have any WAP capability, any attempt by the subscriber to trade stocks using the UIM resident applet, will have to be rejected, because of the absence of the necessary capability in the MT.

Temporary Annex B: Living list of issues for joint Q.FIF and Q.FSU work*(Editor's note: This will form the basis to populate section 9.2.2)*

Q.FIF 6.1.1: UIM holder verification: UIM data storage: PIN. Explain how PIN is first entered into UIM? In what type of processes is this procedure used? I.e. When does MT request "PIN verification" to user? Explain activation and deactivation of the PIN feature. Verify if PIN is a Mandatory or Optional IE.

Q.FIF 6.1.2: User authentication procedure: UIM data storage: IMUI, TMUI, triplets or Authentication Key. How does UIM get supply of triplets? Status of IMUI data, is it different from the user-known directory number or is it a hidden data? Any description of authentication calculation etc. in Q.FSU (Security section)?

TMUI assignment: This requires TMUI update in UIM.

SSD update: Q.FSU security should indicate how SSD is updated and managed, in more detail than in Q.FIF. See note in section 3 of Q.FSU.

Call History Count: Verify this data storage.in UIM.

Q.FIF 6.2.2 Subscriber data management: Is user profilestored in UIM?

6.2.5 Identity retrieval and update: Verify that UIM stores TMUI, LAI & IMUI

6.2.8.1 Terminal location registration: Is there any UIM-CN interaction? If so, verify LAI data update in UIM.

6.2.8.4 Detach: This modifies MT status in UIM & CNh. Verify that UIM data storage has MT status.

6.2.9 Location data fault recovery: Appears to overlap with 6.2.4. What about location data in UIM, could it be unreliable or is it a master data?

Q.FIF 7.1.1 Mobile outgoing call: Need to clarify the role of the UIM at o/g call, e.g. how is speed dialling provided? Does UIM data storage include speed dialling data?

7.1.4 Mobile incoming call: Does UIM store a data called "roaming number", if so what exactly is this?

Q.FIF 8.1.1 Change of service: Verify how, if at all, UIM is involved in this procedure.

8.1.2 Adding a medium during a call: Initiated by MT to CNv. MT later updates UIM. Why does this involve the UIM? Any data storage required in UIM?

8.1.3 Removing a media during an active multimedia call: This involves MT updating UIM. Verify what data is updated.

8.2.3 Packet data service session termination (MT or ntwk initiated): Can be either MT or CN initiated. Verify if there is any role for the UIM here.

Q.FIF 9.2 Direct Home Command: All IFs are shown across CN's. Are there interactions with MT and UIM also. If so, what UIM data is involved?

Q.FIF SECTION 10: Messaging Service Applications

It is assumed that UIM has memory to store received messages. Verify UIM storage for SMS.

10.1.1 SMS Notification Transfer: In this procedure what happens if UIM memory is full?

10.1.2 MT originated short message: Short message may originate from UIM. Is this from a menu of short messages? Verify if UIM has a menu of short messages. Need to distinguish between this menu and memory for received short messages. Confirmation of message delivery to destination MC is returned to MT (and UIM also if appropriate), verify what UIM data this changes.

10.1.3 MT terminated short message: Explain how UIM message storage is involved.

10.3 Message Waiting Notification: (MWN) When is MWN stored in UIM & in that case, is it text or voice?

Q.FIF 11.1 Supplementary Services Control Procedures

11.1.1 Get password SS: CNh asks for password via CNv to MT and on to UIM. UIM responds with password. Why is UIM involved in this? Is it not that user enters password by key strokes & these are sent to CNh, as indicated on pg 11:192 FEA22? Does UIM data include password?

11.2 Remote SS control: Involves CNv – CNh interactions, with tone announcements to MT/UIM. Is this included in UIM functions? And what does UIM do with received tone announcements?

Q.FIF SECTION 12: Inter-system fault recovery (empty) Is this expected to include MT and or UIM? If so, what UIM data are involved? And in which procedures?

Q.FIF SECTION 13: Charging Information Handling

This is to provide advice of charge, call duration etc. to user from CNh via CNv. Details are empty. This is awaiting inputs from JQG6. Is this the UIM advice of charge data?

Q.FIF SECTION 14: Definition of Information Elements (IEs). Ensure that UIM data storage includes all IEs that reside in UIM.

Appendix C: Transferred to Q.23/11 to be considered in Q.FSU. This is data storage requirements at UIM & is better placed in Q.FSU.

Appendix D: Move to Q.23/11 for Q.FSU, deals with Identities in UIM (IMUI, TMUI) & is relevant for Q.FSU.

Appendix F: A-key generation for shared secret data (SSD) based authentication. This requires A-key generation in both UIM & CNh (LMF/AMF). Verify that Q.FSU covers A-key generation adequately.

Appendix G: Signalling function: OTASP (This may be included in the body of Q.FIF, e.g. under Service Activation).

OTASP (Over The Air Service Provisioning) is one of the OTA (Over The Air) services, to activate new subscribers. It uses the UIM data Init-IMUI provided at manufacturing time, clarify if this applies only to new integrated UIMs. Explain status of the Init-IMUI data, Is it confidentially stored inside the UIM? or is it advertised on the package? How does CNh identify this IMUI for A-key generation? Does UIM data storage include a separate field for Init-IMUI or is it just the IMUI field?

Once a user has bought a new MT (& UIM), there are 4 main steps:

A.1 Invocation of Activation with desired service provider (i.e CNh): User dials OTASP feature service code + CSC tel no. of CNv, as advertised on MT package. CNh sends Activation IMUI to MT. UIM returns Init-IMUI again for A-key generation. Explain what UIM does throughout this procedure, especially which UIM data are changed.

A.2 A-key generation for initial UIM authentication: This UIM authentication is done by sending a special secure authentication key (using Diffie-Helman public encryption algorithm) to the UIM. (Need to clarify this sentence relative to the next one which appears elsewhere in App. G). The A-key is never sent over the air. The A-key is derived from the Initial-IMUI and SSD. (Explain how UIM gets its initial SSD).Verifydetails with A-key generation procedures in section 6.1. The main security goal in OTASP is to ensure that user is not evesdropped during activation and that no one else gets fraudulently activated.

A.3 UIM re-authentication for voice & signalling ciphering: (Usual authentication procedure & UIM data used)

A.4 Exchange of OTASP data: This is for the actual activation of subscriber, once authentications are completed. CNh downloads to UIM via CNv, using OTA functionality, with ciphering of data over the radio channel turned-on. Data includes new permanent IMUI, information on supplementary services. The new IMUI is committed to UIM memory. Explain how UIM data storage handles this.

Regarding the question of how to enter "preferred roaming list" to integrated UIM, this could be downloaded during activation. If so, ensure that UIM data storage includes this.

After receiving data, MT does a terminal registration to re-register user & acknowledge data received. The secure voice path is used to obtain user's inputs for activation (service profile, financial information etc.). Clarify if service profile is stored in the UIM, if so ensure that UIM data storage includes this field. Is this Table 3 of Q.FSU Annex?

Temporary Annex C: Material moved to Q.FSU from Q.FIF Appendix C & D for consideration and inclusion within Q.FSU:

Q.FIF Appendix C: Data elements in UIM (User Identification Module)

(Editor's note: This should be considered in the finalization of sections8.1 and 8.2)

C.1 General

This appendix shows data elements in UIM (User Identification Module) regarding Q.1721 and their usages to ease readers understanding of information flows and information elements in Q.1721.

C.2 Data elements in UIM

TABLE C.1 Data elements in UIM regarding Q.1721

	Data elements	**Usage**	**Read/ Write**	**IMT-2000 user case**
1.	Authentication algorithm	Algorithm for User authentication	(Inaccessible)	M
2.	Ciphering key generation algorithm	Algorithm for Ciphering key generation	(Inaccessible)	M
3.	IMUI	Identity of a IMT-2000 user	R	M
4.	Ku	Secret key for User authentication	(Inaccessible)	M
5.	Ku'	Secret key for Ciphering key generation	(Inaccessible)	M
6.	LAI	Location Area Identity is stored / updated after Terminal location registration / updating is completed and is compared with current broadcasted one if a location update procedure needs to be executed	R/W	M
7.	TMUI	TMUI is assigned / updated after User authentication is completed and is formulated into UNI messages instead of IMUI to keep confidentiality and data length reduction of IMUI over radio interface. And TMUI is compared with TMUI in PAGING message to distinguish if it is paged	R/W	M
8.	TMUI assignment source ID	TMUI assignment source ID is assigned / updated together with TMUI after Terminal location registration / updating is completed and is formulated into Terminal location registration / updating message to identify SDF which assigned the TMUI	R/W	M
9.	TMUI expiration timer	TMUI expiration timer is assigned/updated, when appropriate, together with TMUI in order to provide enhanced user confidentiality	R/W	O
10.	Bearer capability	Designated bearer capability for a call is stored and is formulated into SETUP message	R/W	O
11.	QOS parameter	Designated QOS parameter for a call is stored and is formulated into SETUP message	R/W	O
12.	Transit network selection	Designated Transit network selection for a call is stored and is formulated into SETUP message	R/W	O
13.	Service ID	Designated Service ID for a User registration is stored and is formulated into User Registration Request message	R/W	-

14.	A-key	User/Home Service Provider Secret	Inaccessible	See Note 1
15.	SSD	User/Authenticating Network Secret	Inaccessible	See Note 1
16.	Authentication Algorithm for "A-key" based technique	Algorithm for User Authentication	Inaccessible	See Note 1
17.	Ciphering key Generation Algorithm for "A-key" based technique	Algorithm for Ciphering key Generation	Inaccessible	See Note 1
18.	Call History Count (CHCNT)	"Clone" detection Parameter	R/W	See Note 2

M: Mandatory, O: Optional, -: Don't care

Note 1: Necessary for the support of some security signalling protocols that utilize the "global challenge" authentication technique.

Note 2: Necessary for support of "clone detection." May be used with either "unique challenge" based authentication and ciphering key generation protocols or "global challenge" based authentication and ciphering key generation protocols.

Q.FIF Appendix D: Allocation and Usage of Identities

(Editor's noteRelevant points should be captured within Q.FSU sections and then delete this Appendix)

D.1 General

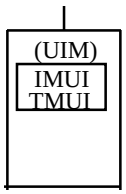
This appendix shows allocation and usage of identities to ease readers understanding of information flows and information elements in Q.1721.

D.2 Allocation and usage of identities

Allocation and usage of identities are as follows (see FIGURE D.1):

• The mobile terminal is activated when it is connected to a User Identification Module (UIM) which includes an International Mobile User Identity (IMUI). The UIM may be implemented as a functionality embedded into a mobile terminal or as a detachable module. When the UIM is detachable, it can be attached to any compatible IMT-2000 terminal.

• The IMUI or associated Temporary Mobile User Identity (TMUI) is used both to address a mobile terminal and to identify a IMT-2000 user.



IMUI: International Mobile User Identity

TMUI: Temporary Mobile User Identity

UIM: User Identification Module

FIGURE D-1/Q.1721

Allocation and usage of identities