Source: **ARIB SWG7**

Title: **Proposed Evolution Points for USIM Specifications**

---

1. Introduction

This document describes the proposed evolution points for the initial draft USIM-MT specifications, which should be completed in April 1999. The evolution points mean items for which the existing GSM SIM should be evolved into USIM. The following GSM SIM specifications are assumed.

- GSM 11.11 version 7.1.0 (1998-11)
- GSM 11.12 version 4.3.1 (1998-03)
- GSM 11.14 version 7.1.0 (1998-11)

A list of the evolution points for USIM is described in section 3 and 4, based on an investigation in the UMTS development in ETSI and requirements from ARIB and TTC. The section 3 includes descriptions of the evolution points, and the section 4 summaries each point with its priority.

2. References

Following materials are referred in the document.

[1] UIM functionality and requirements for a 3G mobile system (it is based on ARIB Volume 1, MPT interim report in May 1998, ITU-T Q.1701 and Q.1711) (AIF/SWG7-7-3)
[2] UMTS22.01: Service Aspects; Service Principles v3.2.1, Chap.11:UMTS IC Cards and User Service Identity Module, and Cha.14.2.Provision and evolution of services within UMTS
[3] UMTS22.05: Services and Service Capabilities v3.1.0, Chap.9.2. Execution Environment
[4] UMTS22.07:Terminal and Smart card concepts v3.0.0 , Whole parts
[5] UMTS22.10:Service Aspects of UMTS Terminals and IC cards v0.0.4, Whole parts
[6] UMTS22.20:Service Aspects; Service Management v0.0.3 Chap.6.Subscriber profiles
[7] UMTS22.24:Charging and Accounting Mechanisms v3.0.0, Chap.8.3.Low-cost Chargeable Events, and Chap.10.Impacts on Standardization
[8] UMTS22.60: Mobile multimedia services including mobile Intranet and Internet services v3.0.0 Chap.7.Impact on Standardization.
[9] UMTS22.70:Service aspects; VHE v3.0.0, Chap.4.VHE concepts and requirements, Chap.5.Recommendations for realization of VHE concept, Chap.6.Standardization
[10] UMTS33.20:Security Principles for UMTS v0.4.0 Whole part
[11] UMTS22.00:UMTS Phase1 Ver.1.3.0, Chap.5.USIM
[12] UMTS21.11:USIM and IC Card Requirements V0.4.0

3. Evolution Points

3.1 General/High-level point of view

(1) Support of USIM Portability [1]:USIM Portability is an integral capability within the 3G networks that supports mobility of USIM devices among the 3G terminals which support removable USIM. This functionality should be achieved even on the another family member.

(2) UIM version management : It is necessary for ME to identify UIM version like EF_{PHASE} in GSM specification (e.g. First version(initial draft specifications) or Version 1).

3.2 Logical characteristics point of view

(1) Support of multiple mobile applications [2][5]: It shall be possible for the 3G IC Card to host other applications in addition to the USIM. Each application on an IC card shall reside in its own domain (physical or logical). It shall be possible to manage each application on the card separately. And each application should be able to be activated simultaneously.

(2) Possibility to have shared applications/files (e.g. phone books, call barring table, etc) between multiple subscriptions [4]: This should be standardized as desirable optional functionality for IC card.

(3) Possibility for some applications/files to be restricted to one or some of the subscriptions [4]: This should be standardized as desirable optional functionality for IC card.

(4) File•@ structure and access conditions for multiple mobile applications [12]: Since 3G ICC may contain multiple applications a flexible method of controlling file access will be required.

3.3 Multiple applications point of view

(1) Access rights control to SIM application [3]: A standardized certification scheme and security model with several levels of trusts in order to control the scripts access rights to the platform resources and capabilities. This would be used to allow e.g. the SP and the SP only to access to USIM data.

(2) Support of plastic roaming with the existing 2G systems (PDC, cdmaOne): It shall be possible to roam into the existing 2G NW by using multiple mobile applications (3G+PDC /USIM, 3G+cdmaOne/USIM).

(3) Support of GSM-3G roaming on the USIM basis [2]: Figure5 (in UMTS22.01) shows two types of examples to achieve roaming between GSM and 3G by using IC card. One is named 'USIM roaming' which enable for USIM to roam into GSM NW.

(4) Support of GSM-3G roaming on the GSM SIM basis [2]: Figure5 (in UMTS22.01) The other case is named 'SIM roaming' which enable for GSM SIM to roam into 3G NW.

(5) Variable-length parameter of authentication algorithm (RAND, Kc and SRES): It is necessary to control the length of security parameter for diversification of algorithm and strength, life of security.

3.4 Physical characteristics point of view

(1) Eliminate 5V SIM [11]: 3G mobile terminals do not have to support 5V SIMs.

(2) 1.8V ICC: Current studying Item in ETSI SMG9.

(3) USIM-ME interface speed enhancement: Current working Item in ETSI SMG9.

(4) T=1 transmission protocol: Current working Item in ETSI SMG9.

(5) Smaller size ICC: Current working Item in ETSI SMG9.

3.5 Service provisioning point of view

(1) Support of Profile exchange [1][9]: This function provides a mechanism for the MT, the USIM and the Core Network to exchange service capability information.

(2) Support of Application Data Transfer [1][9]: This function provides a mechanism for the MT, the USIM and the Core Network to exchange applications and associated data.

(3) Support of Proactive Applications [1][5][9]: This function gives a mechanism whereby applications can initiate actions to be taken by the MT. These applications may reside in the USIM, MT or external device or may be downloaded from the Core Network.

(4) Support of Screening service [1]: The USIM has the ability to allow, bar or modify the call, the supplementary service operation or the service data operation.

(5) Support of secure data downloading [1][4][5][8][9]:

(6) Support of Over the Air Service Provisioning [1]: 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.

3.6 Common files point of view

(1) Enhancement of ADN file (Users group, Two names for one number, etc) [12]: From the user's perspective, ADNs is one of the most important visible functionality delivered by the ICC. The GSM ADN should be enhanced e.g. by being able to group users in order to separate them into business and private numbers, or by assigning a class identifier to users in order to associate them with a particular mode of alerting.

(2) Store incoming call records, last call time / charge: To display incoming call records that include caller's phone numbers, reception date/time and status (answered or unanswered).

(3) URL List for internet services: Store URL list for internet services like BOOKMARK or FAVORITES of web browser.

4. Prioritization of each Evolution Point

In this section, the evolution points are evaluated whether they are necessary to be included as work items in TSG-T WG3 that should be completed in April March 1999.

A… High
B… Middle

ID	Subject	Priority	Remarks
3.1-(1)	Support of USIM Portability (including between another family member network)	A	
3.1-(2)	UIM version management	A	
3.2-(1)	Support of Multiple Mobile Application	A	
3.2-(2)	Possibility to have shared applications/files	A	
3.2-(3)	Possibility for some applications/files to be restricted to one or some of the subscriptions	A	
3.2-(4)	File structure and access conditions for multiple mobile applications	A	
3.3-(1)	Access rights control to SIM application	A	
3.3-(2)	Support of plastic roaming with the existing 2G systems (PDC, cdmaOne)	A	
3.3-(3)	Support of GSM-3G roaming on the USIM basis	A	
3.3-(4)	Support of GSM-3G roaming on the GSM SIM basis	A	
3.3-(5)	Variable-length parameter of authentication algorithm (RAND, Kc and SRES)	A	
3.4-(1)	Eliminate 5V SIM	A	
3.4-(2)	1.8V ICC	A	
3.4-(3)	USIM-ME interface speed enhancement	A	
3.4-(4)	T=1 transmission protocol	A	
3.4-(5)	Smaller size ICC	B	
3.5-(1)	Support of Profile exchange	A	For VHE
3.5-(2)	Support of Application Data Transfer	A	For VHE
3.5-(3)	Support of Proactive Applications	A	For VHE
3.5-(4)	Support of Screening service	A	For VHE
3.5-(5)	Support of secure data downloading	A	For VHE
3.5-(6)	Support of Over the Air Service Provisioning	A	

3.6-(1)	Enhancement ADN file (Users group, Two names for one number, etc)	A	
3.6-(2)	Store incoming call records , last call time / charge ,	A	
3.6-(3)	URL List for internet services (e.g. Bookmark , Favorites)	B	

5. Conclusion

The evolution points for the initial draft USIM specifications are presented. It is essential for ARIB to decide solutions for most of the points until April 1999, in order to start the IMT-2000 commercial services in Japan around April 2001. TSG-T WG3 is kindly required to decide its work plan and procedure considering the above evolution points.