

TSG-Terminals Working Group 3 (USIM) meeting #1
Nice 25th - 27th January, 1999

TSGT3#1(99)003

Page 1

Source: SMG9 UMTS WP secretary

Title: Report from SMG9 UMTS meeting #7 (Dec 15 - 16, 1998)

**DRAFT Report of the
SMG9 UMTS Working Party, meeting #7
hosted by Nokia in
Copenhagen, 15.-16- December 1998**

Chairman: Günter Maringer (T-Mobil)
Secretary: Michael Sanders (ETSI)

List of participants: Annex A
List of documents: Annex B
Access to SMG9 UMTS documents Annex C
Approved Agenda Annex D

1 Opening of Meeting

The meeting was opened by Günter Maringer, the chairman of SMG9 UMTS working party. The meeting was hosted by Nokia in Copenhagen.

2 Roll call of delegates

The meeting was attended by 14 delegates. The list of delegates can be found in Annex A.

3 Input documents

Several input documents were noted and added to the agenda. A list of document can be found in annex B.

4 Approval of Agenda

The agenda in 98u060 was approved with some amendments. The approved agenda is appended as annex D.

5 Review of report from the 6th meeting

The report in 98u059 was approved.

6 Liaisons

It had been hoped that a draft version of the SMG10 document, UMTS 33.22, "UMTS Security Mechanism" would be available for the meeting. However, the last SMG10 plenary instead mandated the SMG10 WPC (UMTS) to continue work on the document and prepare it for presentation to SMG #28 as version 1.0.0 (i.e. for information).

6.1 LS from SMG10 on changes required to UMTS 21.11

98u061 is an LS from SMG10 regarding changes that they think are necessary to UMTS 21.11. It lists several requirements currently contained within UMTS 33.21. They are listed below along with the any discussion within SMG9 UMTS:

R5a A valid USIM shall be required to access any UMTS service except for emergency calls where the network should be allowed to decide whether or not emergency calls should be permitted without a USIM.

⇒ This requirement is already contained within UMTS 21.11.

R5b It shall be possible to prevent the use of a particular USIM to access UMTS services.

⇒ This requirement is already contained within UMTS 21.11.

R5c It shall be possible to control access to a USIM so that it can only be used to access UMTS services by the subscriber to whom it was issued or by users explicitly authorised by that subscriber.

⇒ This requirement is already contained within UMTS 21.11.

R5d It shall be possible to control access to data in a USIM. For instance, some data may only be accessible by an authorised home environment.

⇒ This requirement is fulfilled in the sense that 03.48 security is proposed for the USIM. However, there was some discussion within SMG9 UMTS as to which extent this requirement is covered. It was agreed that a more advanced method of access control may be useful (e.g. the EN726-3 "AUT" access condition) but also that there was not enough time left to elaborate a more detailed mechanism.

R5e It shall not be possible to access data in a USIM that is only intended to be used within the USIM, e.g. authentication keys and algorithms.

⇒ It was agreed that this requirement should be added into UMTS 21.11 in subclause 4.

R5f If a UICC contains more than one USIM (to access services from different home environments) then different home environments shall only have access to the USIMs of their own users.

⇒ As multiple USIMs per UICC will not be specified for phase 1 UMTS, it was agreed that this issue should be further examined at a later stage.

R5g If a UICC contains more than one USIM (to access services from different home environments) then security management data (e.g. authentication information) of each USIM shall be protected independently against unauthorised access and modification.

⇒ As multiple USIMs per UICC will not be specified for phase 1 UMTS, it was agreed that this issue should be further examined at a later stage.

R5h It shall be possible to control access to, and selection of, USIMs and other non-UMTS applications stored on the same UICC. In particular, it shall be possible to have shared directories between applications where appropriate.

⇒ This will be rediscussed at the 3GPP USIM meeting.

R5i It shall be possible to ensure that the origin and integrity of applications and/or data downloaded to the UICC can be checked. It may also be necessary to ensure that the confidentiality of downloaded applications and/or data can be ensured.

⇒ This requirement can be fulfilled by the functionality contained within GSM 03.48.

6.2 LS from SMG 10 on UMTS security context

98u063 is an LS from SMG10 requesting that SMG9 review UMTS 33.21 "UMTS Security Mechanism" for:

- referencing to SMG9-maintained specifications
- assumptions relating to the USIM and UICC.

Subclauses 5.1.5 and 5.3 were reviewed. It was concluded that assumptions related to USIM and UICC were correct, however

- the requirements listed as coming from UMTS 22.00 were no longer in line the latest version of UMTS 22.00,
- no references to SMG9 specifications are made.

In subclause 5.2.1,

- "User Service profile" should be "User profile"

A LS in reply to SMG10 was drafted in 98u071, this was further discussed and agreed as 98u072.

Comments to subclause 7.2.1 are contained within section 6.1 of this report.

6.3 LS from SMG10 on Security of ME-USIM interface

98u064 is an LS in reply to the SMG9 UMTS LS to SMG10 in 98u035. SMG9 UMTS had requested that SMG10:

- identify requirements to counter masquerading and eavesdropping at the ME/USIM interface;
- identify security problems that may arise due if the use of administration commands are standardised across the ME/USIM interface.

The LS was noted.

7 Report from 1st 3GPP meeting in Sophia Antipolis

The chairman reported from the first TSG meeting of 3GPP. Effectively the USIM work will move to 3GPP, where in the TSG-T (terminals working party), a subgroup dealing with the USIM was created. The first meeting of this group will be January, 25th to 27th. Any documents related to 3GPP can be found on the 3GPP server (www.3gpp.org).

8 ARIB status

98u067 is a report describing the status of the USIM work within ARIB and TTC in Japan. It deals with such issues as:

- Key Standardization Bodies and 3rd Generation Concept in Japan
- UIM in ARIB IMT-2000 System (status of permanent / removable USIM issue)
- UIM Standardization Work in ARIB and TTC
- Baseline Standards
- Evolution Points
- Status of ARIB documents including:
 - ARIB Volume 1: Requirements and Objectives for 3G Mobile Services and System
 - AIF-SWG7-7-3: UIM Functionality and Requirements for 3G Mobile System
 - AIF-SWG7-11-4: Study items for Evolution into UIM-MT interface for ARIB IMT-2000
 - Security Design Principle (version 1, November 1998)

Regarding the removable USIM, it was clarified that Japanese operators expected that their customers with a fixed (i.e. embedded) USIMs to be able to roam on to European UMTS networks.

It was commented that the existence of the SIM in GSM was one of the GSM success factors, because it contributes a dramatic increase in security, it allows for a worldwide market for mobile equipment, with the benefit of economies of scale, and, for the operator, a differentiation factor and direct link to the customer, in particular with the advent of advanced SIM-based services as the SIM application toolkit. In addition, operators benefit from the increased security (there have been no reported cases of a SIM being cloned) and increased revenue from their roaming customers, and roaming visitors to their own networks. It was noted that this issue would probably be addressed in the TSG-T and TSG-S of 3GPP.

It was stated that SWG7 will continue the smart card work for the ANSI based core network.

9 Review of UMTS 22.00 and 22.01

98u066 contains UMTS 22.00 v1.5.0 (11 December 1998). It was reviewed during the meeting with the following conclusion:

- a requirement that UMTS MEs shall not support 5 V SIMs is now made. UMTS 21.11 was updated accordingly.

98u065 contains UMTS 22.01 v3.3.0. It was reviewed during the meeting with the following conclusions:

- there is still no elaboration of the term "user profile". It was agreed that this item should be noted for future study within UMTS 21.11.
- the subclause dealing with the USIM has not undergone too many changes since the last review of UMTS 22.01 by SMG9-UMTS, and there are still pending CRs on UMTS 22.01, so a detailed review of the document will be appropriate at a later stage.

10 Draft UMTS 21.11

Note: Note that some paper copies of 98u070 available at the meeting in Copenhagen were incorrectly marked with the number "98u058". The correct 98u058 does not contain any revision marks. The documents as available on the ETSI server are the correct ones.

98u058 contains UMTS 21.11 v0.3.0. This incorporates all changes agreed at SMG9 UMTS #6.

98u070 contains some additions for UMTS 21.11 v0.3.0 proposed by the rapporteur. The more significant changes agreed during the meeting consisted of inclusion of relevant material from GSM 02.17, in line with action point AP6-1 from the previous meeting (see below). Discussion of these changes and further issues raised at the meeting as described below resulted in a new version of UMTS 21.11 in 98u0xx.

10.1 UICC size issues

98u057 is a modified version of 98u054 produced as result of discussions and conclusions at SMG9 UMTS #6.

One manufacturer stated that it may be difficult to meeting ISO mechanical standards for a combined ID-1/micro-SIM card.

It was noted that in Japan, they do not currently have a backward compatibility problem as although SIMs are specified for PDC, they are not actually used. However, to support roaming customers, it would be necessary.

It was proposed that the final decision about a new size could be delayed until April. This will give the SIM manufacturers a chance to make a more detailed investigation into the matter, and furthermore, it allows for further discussion on the issue at the TSG-T-SIM meeting in January and at the TSG-T meeting in March.

A discussion document will be produced by RL and MS and emailed to SMG9_UMTS within a week for comments. It would then be sent to SMG9 (and MOU, SERG/SCAG/TWG, SMG) and as an input from SMG9 UMTS.

10.2 USIM files

98u068 is an input document which proposes a list of GSM EFs and procedures that are mandatory in GSM. The recommendations in 98u068 were discussed and agreed with the following remarks:

In section 2:

- EF_{LP} (Language preference) - EF_{ELP} should be used instead
- EF_{BCCH} (Broadcast control channels) - this may not be required as there is minimal benefit in storing this information in the SIM.

In section 3:

- EF_{SDN}, EF_{FDN}, EF_{BDN}, should be moved to under the USIM.

10.2.1 ADNs

SMG9 were currently examining a way of extending the number of ADNs in a flexible manner. This involves creating an EF index (indicated in the SST). This would contain a list of the IDs for EF_{ADN1}, EF_{ADN2} etc., and further files which may carry additional information like grouping information. It was noted that there is a Japanese requirement to have two display names (in different character sets) per ADN entry. This requirement could be fulfilled in the same manner. It was agreed to add these requirements to UMTS 21.11.

10.3 Shared files access

No additional input arose during the joint session between SMG9 UMTS and SMG API during SMG9 #16bis.

98u056 contains the alternatives discussed during SMG9 UMTS #6. That meeting had agreed that method 3 appeared to be the most suitable. This method would require a user to select a user profile before entering the CHV if multiple USIMs were present on the UICC.

It was agreed that proposal 3 should be further elaborated and added to UMTS 21.11. The chairman undertook to write an input (within 2 weeks).

10.4 Next steps

UMTS 21.11 will be presented to SMG9#17 for information. The remaining outstanding issues and the SMG9-UMTS approval to present the document to SMG9 will be achieved at a SMG9-UMTS subgroup meeting to be held during SMG9#17. It is clearly identified that 21.11 is still incomplete with regard to the following matters:

- Security: 33.22 was not yet available
- The modifications to 22. 01 made at the last SMG1 plenary are not yet incorporated into version 3.3.0 and could not yet be considered.

11 AOB

During SMG9 #16bis, there was a joint session on SMG9 UMTS and SM9 API issues. The main discussion topic were the requirements for application downloading. It appeared that the requirements of both groups may be fulfilled by the VOP download mechanism. However, as this was not yet available to SMG9, further discussion would be required when it becomes available. VISA have stated that it will be available at the SMG9 #17. A joint meeting was proposed between SMG9 UMTS and SMG9 API during SMG9 #17. This will be held on the Wednesday.

Action points from previous meeting

- AP6-1: review GSM 02.17 for issues which should be mentioned in UMTS 21.11. **(GM)**
⇒ closed - see 98u070
- AP6-2: review UMTS 21.11 to convert GSM terminology into UMTS terminology. **(GM)**
⇒ closed - see 98u070
- AP6-3: collect a list of files that will be required. **(PV)**
⇒ closed - see 98u068
- AP6-4: delegates should inform their SMG10 and SMG1 delegates of the need for output from these groups on UICC related issues. **(all)**
⇒ Input from SMG10 is expected at the 1st 3GPP USIM meeting.
- AP6-5: develop a proposal to define the different application classes (internal / external) to prompt discussion on the issue at meeting #7. **(BB)**
⇒ open . BB to provide input to the 3GPP USIM working group.

AP6-6: review 98u056, method 3, for practical aspects and whether the multi-user concept is feasible in practice (everybody)
⇒ see clause 10.3 of this report.

New Action points from this meeting

AP7-1: Check ARIB meeting reports and make a summary of discussion and conclusions regarding whether or not a removable USIM should be mandatory.
(CN)

AP7-2: ARIB to provide input to the January 3GPP terminals USIM (JH)

12 Closing of the meeting

The meeting was closed at 15:30 and the chairman thanked Nokia for hosting the meeting and the delegates for their contributions. It was noted that this would be the last meeting of SMG9 UMTS and that further meetings would take place as part of the 3GPP.

ANNEX A List of delegates

NAME	Organisation	Tel	Fax	Email
AHLGREN Kristina	ERICSSON	+46 46 193923	+46 46 193136	kristina.ahlgren@ecs.ericsson.se
BASQUIN Bruno	GEMPLUS	+33 4 42 36 50 47	+33 4 42 36 64 15	bruno.basquin@gemplus.com
BAUDRU Geneviève	SFR / CEGETEL	+33 1 55 68 48 42	+33 1 55 68 47 03	genevieve.baudru@mail1.sfr.fr
BARNES Nigel	MOTOROLA	+44 1256 790 169	+44 1256 790 190	Nigel_Barnes@euro.css.mot.com
GEMME Paolo	ITALTEL	+39 02 4388 8502	+39 02 4388 7519	paolo.gemme@italtel.it
HECKMANNS Ulrich	Giesecke & Devrient	+49 89 4119 2545	+49 89 4119 2118	ulrich.heckmanns@gdm.de
HONDA Yoshio	ERICSSON NIPPON	+81 3 5216 9076	+81 3 5216 9047	yoshio.honda@ericsson.co.jp
JOLIVET Paul	DE LA RUE CARD SYSTEMS	+33 1 49 69 24 27	+33 1 49 69 25 02	paul.jolivet@fr.delarue.com
LINDHOLM Rune	NOKIA MOBILE PHONES	+358 10505 4477	+358 10505 4544	rune.lindholm@nmp.nokia.com
MARINGER Günter	T-MOBIL	+49 228 936 1249	+49 228 936 1257	guenter.maringer@t-mobil.de
NODA Chie	DoCoMo	+33 1 4076 0660	+33 1 4076 0015	noda@docomo.fr
SANDERS Michael	ETSI/PT SMG	+33 4 92 94 42 90	+33 4 93 65 28 17	michael.sanders@etsi.fr
VESTERGAARD Peter	NOKIA MOBILE PHONES	+45 33 29 21 96	+45 33 29 20 01	peter.vestergaard@nmp.nokia.com
WAKAKI Moto	TELECOM JAPAN	+81 3 5540 8420	+81 3 5540 8485	wakaki@japan-telecom.co.jp

ANNEX B List of documents

Tdoc	Title	Source	Status
98u058	UMTS 21.11, version 0.3.0	PT SMG	noted
98u059	Draft meeting report from UMTS #6(Sophia Antipolis, 4 - 5 Nov, 1998)	PT SMG	approved
98u060	Draft Agenda for SMG9 UMTS #7 (Copenhagen 15-16 December, 1998)	UMTS chairman	see annex in meeting report
98u061	LS from SMG10: changes required to 21.11 v0.1.0 clause 4	SMG10 (98P259)	noted
98u062	UMTS 33.21 (v1.0.4): UMTS Security Requirements	SMG10	noted
98u063	LS from SMG10: UMTS security context	SMG10 (98p261)	noted
98u064	LS from SMG10: Security of ME-USIM interface	SMG10 (98p331)	noted
98u065	UMTS 22.01 v3.3.0	PT SMG	noted
98u066	UMTS 22.00 v1.5.0	PT SMG	noted
98u067	UIM Standardization in ARIB SWG7	Nippon Ericsson	noted
98u068	Mandatory files from GSM	Nokia	discussed
98u069	LS to SMG1 on dual voltage issues	SMG9 UMTS	withdrawn
98u070	Proposed changes to UMTS 21.11 v0.3.0	21.11 rapporteur	discussed
98u071	LS to SMG10	SMG9 UMTS	revised - see 98u072
98u072	LS to SMG10	SMG9 UMTS	approved

ANNEX C Access to SMG9 UMTS documents

C.1 The ETSI FTP server

All Tdocs, meeting invitations or other relevant information available electronically will be placed on the ETSI server in an appropriate location under the directory:

http://docbox.etsi.org/tech-org/smg/document/smg9/sg_umts/

All SMG9 (in fact all GSM) specifications can be found under the directory:

<http://docbox.etsi.org/tech-org/smg/specs/>

(the subdirectories indicate the different releases i.e. phase 1, phase 2, Release 96 etc)

A username and password is required. Any ETSI member can obtain a username by contacting the ETSI help desk; email :helpdesk@etsi.fr or tel: +33 4 9294 4900 or fill out an on-line application form at:

<http://www.etsi.org/AccountRequest/form.idc>

C.2 ETSI listserver email groups

SMG9 have several discussion/information email groups on the ETSI email listserver. UMTS issues are discussed on SMG9_UMTS. In order to join these lists, you must send an email to LISTSERV@LIST.ETSI.FR with one or more of the following lines of text:

subscribe SMG9_UMTS YourFirstName YourLastName
subscribe SMG9_plenary YourFirstName YourLastName
subscribe SMG9_generics YourFirstName YourLastName
subscribe SMG9_toolkit YourFirstName YourLastName
subscribe SMG9_api YourFirstName YourLastName
subscribe SMG9_test YourFirstName YourLastName

You will then automatically receive (via email) further details about how the list operates.

All lists have an associated archive of every email sent via that list. Information on how to access the archive are sent to you when you subscribe to the list.

ETSI has many other email groups on the list server. A continuously updated list of these groups can be found at:

<http://www.lsoft.com/scripts/wl.exe?XH=LIST.ETSI.FR>

ANNEX D Approved agenda

1. Opening of the meeting
2. Roll call of delegates
3. Input documents
4. Approval of agenda 98u060
5. Review of report from previous meeting 98u059
6. Liasons 98u061, 98u062, 98u063, 98u064
7. Report from 1st 3GPP meeting in Sophia Antipolis
8. ARIB status 98u067
9. Review of UMTS 22.00 and 22.01 98u066, 98u065
10. Draft UMTS 21.11
11. AOB
12. Closing of the meeting