3GPP TSG SA WG3 Security — S3#18 **S3-010224**

21 - 24 May, 2001

Phoenix, USA

3GPP T3 Meeting #19
St John, US VI, 8 - 11 May, 2001

Tdoc T3-010316

Meeting Report

TSG-T3 Ad Hoc Meeting #37 (Joint with TSG-S3)

Hosted by Giesecke & Devrient

in Munich, Germany

3 May 2001

Contents

Chairman: Stefan Kaliner (Deutsche Telekom MobilNet GmbH)
Host: Giesecke & Devrient, Munich, Germany

1 Opening of the Meeting

The T3 Vice-Chairman, Nigel Barnes, opened the 37th ad hoc meeting of the 3GPP TSG-T WG3, this time joint with 3GPP TSG-SA WG3, at 09:15 on 3rd of May 2001. The goal of the meeting was to clarify between T3 and S3 some important issues related to TR 31.900 – SIM/USIM Internal and External Interworking Aspects.

After his arrival the ad hoc chairmanship was handed over to Stefan Kaliner, rapporteur of TR 31.900, who held this task until the end of the meeting.

2 Roll Call of Delegates

The T3 ad hoc meeting #37 was attended by 18 delegates from 5 countries. The list of delegates can be found in Annex A of this report. Apologies of absence were received from the T3 Secretary, Michael Sanders

3 Input Documents / Agenda

T3z010500 contains the draft agenda. The agenda was approved with the addition of 2 new documents. It can be found in Annex B of this report.

4 Notification of IPR obligations

The chairman drew the attention of the delegates to the fact that 3GPP Individual Members have the obligation under the IPR policies of their respective Organisational Partners to inform their respective Organisational Partners of Essential IPRs they become aware of. They were asked to take note that they had been invited to:

- investigate in their company whether their company does own IPRs which are, or are likely to become Essential in respect of the work of the Technical Specification Group.
- notify the Chairman, or the Director-General of their respective Organisational Partners, at the earliest opportunity, of all potential IPRs that their company may own, by means of the IPR Statement and the Licensing declaration forms.

5 Review of Scenario Involving 2G Security Over UTRAN

T3z010503 contains a LS from S3 to T3 cc S1 on TR 31.900 – SIM/USIM Internal and External Interworking Aspects. It is a response to a LS on the same subject from T3 to S3 cc S1, see T3-010187. In their LS S3 agree with T3 that a 3G subscription can be installed in a 2G HLR/AuC. However, they insist on the requirement in TS 33.102 that a "*R99+ ME with a USIM inserted and attached to a UTRAN shall only participate in UMTS AKA and shall not participate in GSM AKA"*. If this requirement is not satisfied, false base station attacks in a pure 3G environment (i.e. scenario A in TR 31.900) could no longer be prevented. It was therefore found impossible by S3 to modify this requirement in order to allow the potential use cases as pointed out in the initial LS from T3.

The S3 delegates were asked to explain the security risk connected to the case in question: In scenario F (all components = 3G, except HLR/AuC = 2G) the overall security level is 2G as the HLR/AuC is only able to deliver triplets and only RAND is delivered to the ME in the authentication request. If this was a valid scenario, then a false base station in the pure 3G case (scenario A) could take a valid triplet (RAND, SRES, Kc) of the target user (however this was obtained), send only RAND and derive CK and IK from Kc. As the ME would not reject an authentication request with only RAND (as mandated by said requirement) it would execute the 3G algorithm in virtual 2G mode in the USIM, derive CK and IK from Kc and return SRES. CK and IK would now be available on both sides, yet the base station is false. This way, at least some faked communication, potentially enough to track a 3G user or to eavesdrop a data call, could be established.

After a short discussion this explanation was recognised and understood by the T3 delegates. It was agreed to delete case F as an operational scenario from TR 31.900 and to fully reflect the related requirement in TS 33.102. A note should be included into TR 31.900 to point out the primary consequence: A network operator who issues UICCs to enable his customers to use 3G networks (UTRAN) at home or while roaming, shall have a 3G HLR/AuC installed. Otherwise authentication will fail with a 3G ME complying to the standards.

It was also mentioned and generally agreed, that as a result of the exclusion of scenario F, there may be further need to maintain GSM SIM specifications even past R4, to let 2G operators, who – due to the risk of rejection when accessing a 3G network – do not want to issue UICCs, participate from new card features.

The question was raised, how the reaction of the ME in scenario F is defined. TS 33.102 requires that it shall not "participate in 2G AKA", i.e. authentication would somehow fail in this case. The meeting agreed that

a) any further reaction of the ME appears to be undefined, and

b) there is no means to prevent a ME with a USIM subscription in a 2G HLR/AuC to access 3G networks (in order to save the user from disappointing display messages and the accessed network from unwanted signalling load).

After a short discussion of possible solutions (e.g. usage of something like the Forbidden-PLMN List – with the risk of Denial-of-Service attacks, or an appropriate entry in the USIM that generally forbids 3G access – it would have to be maintained via OTA), it was agreed that this issue be highlighted to the T3 plenary. A possible way forward could be a LS to T2 and S1 to make them aware of the problem.

6 Other issues within TR 31.900

T3z010502 is a proposal to modify and extend some of the definitions included in TR 31.900 and align them with TS 33.102. It was stressed that the definitions in TR 31.900 have been deliberately chosen to be different (but certainly not incorrect!) from those in other specifications in order to help understand the meaning of the terms from another point of view. However, no problem was seen in adding further definitions as long as they are beneficial to the reader of the document. After some discussion that included several changes to the proposal, it was agreed to include the results into TR 31.900.

During the course of the meeting the question was raised as to what exactly is a "3G subscription" or a "USIM subscription". Both terms are used in TR 31.900. After some discussion, it was concluded that a "3G subscription" is identical to a "USIM subscription" and is defined by the total of all mandatory and optional features defined in the 3G USIM specifications, in particular is connected to a 3G algorithm.

Finally, it was agreed that the rapporteur updates TR 31.900 by the results of the meeting. The new version 1.1.0 of TR 31.900 shall be presented to T3 plenary during T3#19 in St. John. Subsequently it could be given to TSG-T for approval and – as requested by the S3 delegates – to S3 for information.

7 Any Other Business

There was no other business related to the issues of this meeting.

8 Closing of the Meeting

The ad hoc chairman thanked the hosts for the excellent facilities and organisation of the meeting, and the delegates of the two groups S3 and T3 for their attendance. He then closed the meeting at 15:30 h.

ANNEX A List of delegates

This table lists all delegates who attended the T3 ad hoc meeting #37 (joint with S3).

TITLE	Firstname	Lastname	Organization	Partner
Mr.	Ramin	AFCHAR	Cetecom GmbH	ETSI
Mr.	Nigel	BARNES	Motorola Ltd	ETSI
Mr.	Stefan	ECKHARD	Giesecke & Devrient GmbH	ETSI
Mr.	Timothy	EVANS	Vodafone Group Plc	ETSI
Mr.	Christian	HEIM	Giesecke & Devrient GmbH	ETSI
Mr.	Pascal	HUBBE	Alcatel Telecom SA	ETSI
Mr.	Günther	HORN	Siemens AG	ETSI
Mr.	Edgar	JANSSEN	Vodafone D2 (Mannesmann)	ETSI
Mr.	Paul	JOLIVET	DoCoMo Europe SA	ETSI
Mr.	Stefan	KALINER	Deutsche Telekom MobilNet GmbH	ETSI
Mr.	Kai	KITTEL	Siemens AG	ETSI
Ms.	Ileana	LEUCA	AT&T Wireless Services, Inc.	T1
Mr.	Valteri	NIEMI	Nokia Mobile Phones	ETSI
Dr.	Stefan	PUETZ	Deutsche Telekom MobilNet GmbH	ETSI
Mr.	Jens	RUEDINGER	Vodafone D2 (Mannesmann)	ETSI
Mr.	Hartmut	STEINEGGER	Giesecke & Devrient	ETSI
Mr.	Michael	WALKER	Vodafone Group Plc	ETSI
Mr.	Heinz	ZOELLNER	Orga Kartensysteme GmbH	ETSI

Those delegates with an ETSI server username and password can obtain the full/updated contact information for any delegate by going to the URL for the delegates' database at:
http://webapp.etsi.org/teldir/TelDirectory.asp

They are also able to update their own information (new address / tel. / fax / email etc) by using the URL:
http://webapp.etsi.org/teldir/PersonalInfo.asp

ANNEX B Approved Agenda

1 Opening of the meeting .....**document(s)**
2 Roll call of delegates
3 Input documents / Agenda..... 500
4 Notification of IPR obligations
5 Review of scenario involving 2G security over UTRAN 503, 501
6 Other issues within TR 31.900..... 502
7 Any Other Business
8 Closing of the meeting

ANNEX C Document list

The documents listed below can be found on the 3GPP server at the location:

ftp://www.3gpp.org/TSG_T/WG3_USIM/adhocs/37-0105-Munich/

Number	Title	Source	status
T3z010500	Agenda for T3 ad hoc #37 (joint with SA3) on SIM/USIM interworking	31.900 rapporteur	revised – see report
T3z010501	TR 31.900 v1.0.0 "SIM/USIM internal and external interworking"	T3 secretary	
T3z010502	Terminology in TR31.900 & TS 33.102	Siemens Atea	discussed
T3z010503	LS from S3 to T3 cc S1 "re: TR 31.900 - SIM/USIM Internal and External Interworking Aspects"	S3	noted
T3z010504			
T3z010505			
T3z010506			