Technical Specification Group Services and System Aspects
Meeting #20, Hämeenlinna, Finland, 09-12 June 2003

TSGS#20(03)0207

3GPP TSG SA WG3 Security — S3#28 **S3-030275**
06 - 09 May 2003
Berlin, Germany

Title: **LS on clarification of USIM-based access to IMS**
Release: **Rel-5**
Source: **SA 3**
To: **SA, SA 1, SA 2, T 3**

Contact Person:
Name: Stefan Schröder
Tel. Number: +49 882 936 33312
E-mail Address: stefan.schroeder@t-mobile.de

Attachments: **S3-030199, S3-030276**

---

1. Overall Description:

The attached paper S3-030199 was discussed at S3#28. It intends to clarify the access possibility to IMS with a USIM, based on its release version.

SA3 delegates who attended the joint T3/SA3 meeting in 2001 believe that (interpretation 2) was agreed in that meeting, and TS 33.203 reflects that decision.

However, SA3 acknowledges that the paper raises some technical issues and business consequences related to (interpretation 2). Therefore, the decision for the correct interpretation has to be made before closing Rel-5, and this should be clearly reflected in all relevant specifications.

SA3 proposes to make the decision at SA level, taking into account input from all relevant groups. It might be necessary to postpone the Rel-5 freeze for this particular issue in order to account for any CRs that are needed to reflect that decision.

2. SA3 position:

(Interpretation 1) can be ruled out, as it was not considered valid. SA3 sees no security reasons to prefer either (interpretation 2) or (interpretation 3). This decision can be based on business consequences and on the potential impact on technical specifications.

- In case SA prefers (interpretation 2), no SA3 TS needs to be changed, but other TSes may need to address the technical issues raised.
- In case SA prefers (interpretation 3), the attached CR S3-030276 has to be applied to TS 33.203 and the interpretation of other 3GPP groups specifications shall be checked. This CR, not based on security arguments, has been just conditionally approved by SA3 in case SA makes the decision for (interpretation 3).

3. Actions:

The addressed groups are kindly asked to

1) **state their position to SA in order to enable the decision**
2) **consider the impact of any SA decision on their Rel-5 specifications**
3) **align their TSes according to the SA decision, if necessary**

4. Date of Next SA 3 Meetings:

SA3 #29	15 - 18 July 2003	San Francisco, USA
SA3 #30	07 - 10 Oct 2003	Europe

TSG-SA WG3 #28 **S3-030199**
Berlin, Germany, 6th–9th May 2003 **Agenda Item:**

Title: **Clarification of USIM-based access to IMS**

Source: **T-Mobile, Vodafone**

Contact: Hans Hauser, T-Mobile Deutschland
Tel. +49 171 549 0399
hans.hauser@t-mobile.de

---

1. Introduction

TS 33.203 version 5.5.0 *Access security for IP-based services* states in section 8 *ISIM*:

> For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on a UICC. The following implementation options are permitted:
>
> - Use of a distinct ISIM application on a UICC which does not share security functions with the USIM;
> - Use of a distinct ISIM application on a UICC which does share security functions with the USIM;
> - Use of a R99/Rel-4 USIM application on a UICC.
>
> NOTE: For later releases other implementations of ISIM are foreseen to be permitted.
>
> If there is an ISIM and a USIM application on a UICC, then the ISIM application shall always be used for IMS authentication.
> ...

There seem to be different understandings of the third bullet point around:

(interpretation 1) with UICCs based on Release *6* (and later) specs carrying a USIM application but not an ISIM application access to an IMS is not possible. Consequently, a 3G operator is obliged to install an ISIM application on a Rel6 (and later) based UICC with USIM in case the user wants to access an IMS;

(interpretation 2) with UICCs based on Release *5* (and later) specs carrying a USIM application but not an ISIM application access to an IMS is not possible. Consequently, a 3G operator is obliged to install an ISIM application on a Rel5 (and later) based UICC with USIM in case the user wants to access an IMS;

(interpretation 3) UICCs with USIMs based on any USIM release from R'99 onwards can be used for IMS access in case no ISIM application is present.

Seemingly, there is a need to clarify this.

2. Discussion

2.1 USIM ↔ terminal interface

A Rel5 (and onwards) terminal has to check whether an ISIM application is available or not on the UICC. In case no ISIM is present IMS relevant parameters are to be derived from the USIM application. There is however no possibility for a Rel5 (and onwards) terminal to check the spec version on which the USIM application is based. And even in case a Rel5 (and onwards) terminal could find out about this nothing is specified how to signal the IMS access denial to the terminal.

2.2 Mandatory use of an ISIM

At SA#20, a CR to TS 33.203 Rel5 (SP-030100) was approved mandating the use of an ISIM for IMS access in case an ISIM exists on the UICC. Obviously, this CR makes only sense if the presence of an ISIM on a UICC is not mandatory.

2.3 Operators not or not yet running an IMS

It might well be the case that a network operator is interested to make use of the latest USIM specification available but has not yet made a decision to introduce an own IMS. One could of course argue that such operator is free to start with issuing Rel5 based UICCs with USIMs but no ISIMs since TS 22.101 version 5.8.0 requests in section 13.1.5:

> It shall be possible to update ISIM specific information via the air interface, in a secure manner.

However, given the sensitive character of ISIM data it can be doubted whether heavily security related information such as (cf. TS 33.203)

- support for sequence number checking in the context of the IMS Domain,
- the same framework for algorithms as specified for the USIM [applicable] for the ISIM or
- an authentication key

really should be downloaded over the air. For the time being, no standardized secure manner how to accomplish this is available.

For later releases the mandatory use of an ISIM for IMS access may be considered.

3. Conclusions

- Interpretations 1 and 2 are not applicable.
- Interpretation 3 is correct: Using IMS access parameters derived from the USIM application in case no ISIM is present on the UICC should be possible.

It has to be emphasized that this proposal does not intend to encourage the use of IMSI derived parameters for IMS access at the expense of an ISIM introduction.

4. Proposal

It is proposed to remove “R99/Rel-4” in the third bullet point in TS 33.203 section 8 so that it would read then:

- Use of a USIM application on a UICC.

3GPP TSG-WG3 Meeting #28
Berlin, Germany, 6th–9th May 2003

Tdoc ⌘S3-030276

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.203** **CR** **CRNum** ⌘**rev** ⌘ Current version: **5.5.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarification on USIM-based access to IMS
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	06/05/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Current TS forbids IMS access with a Rel-5 onwards UICC without an ISIM.
Summary of change:	⌘	Remove limitation of IMS access to R99/Rel-4 USIMs.
Consequences if not approved:	⌘	It would not be possible to access IMS with a Rel-5 onwards UICC without an ISIM.

Clauses affected:	⌘	8.			
		Y	**N**		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

8 ISIM

For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on a UICC. The following implementation options are permitted:

- Use of a distinct ISIM application on a UICC which does not share security functions with the USIM;
- Use of a distinct ISIM application on a UICC which does share security functions with the USIM;
- Use of a ~~R99/Rel-4~~ USIM application on a UICC.

NOTE: For later releases other implementations of ISIM are foreseen to be permitted.

If there is an ISIM and a USIM application on a UICC, then the ISIM application shall always be used for IMS authentication.

There shall only be one ISIM for each IMPI. The IMS subscriber shall not be able to modify or enter the IMPI. The IMS subscriber shall not be able to modify or enter the Home Domain Name.