3GPP TSG-T3 #28 **Tdoc T3-030693**
Marseille, France 19-22 August 2003

Title: LS on the effects of USIM services 27 and 38
Response to: LS (S3-030474) on Effects of Services 27/38 on 2G/3G Interworking and Emergency Calls from S3
Release:
Work Item:

Source: T3
To: S3, CN1
Cc:

Contact Person:
Name: Stefan Kaliner
Tel. Number: +49 228 936 31255
E-mail Address: stefan.kaliner@t-mobile.de

Attachments: T3-030694

---

1. Overall Description:

T3 thanks S3 for their LS (S3-030474) on Effects of Services 27/38 on 2G/3G Interworking and Emergency Calls and is pleased to state that TR 31.900 was updated according to the related changes in TS 33.102. Now it points out explicitly that a disabled USIM service n° 27 prevents access to a 2G BSS only if that requires ciphering. It is also mentioned that in this case the ME does not derive the ciphering key Kc.

In regard to the effects on emergency calls when services 27 and/or 38 are not available, T3 agreed to add a generic statement into 31.900 rather than a list of all possible scenarios that may fail. T3 thinks that TR 31.900 may not be the best place for more explicit statements and suggests rather including these into the core specifications. T3 leave it open to S3 and CN1 to decide about the most suitable location.

The changes to TR 31.900 can be seen from the attached CR, which was agreed by T3.

2. Actions:

none

3. Date of Next TSG-T3 Meetings:

Meeting	Date	Location
T3#29	18-21 November 2003	New York, US (tbc)
T3#30	10-13 February 2004	Sophia Antipolis, France

CR-Form-v7

CHANGE REQUEST

⌘ 31.900 CR 011 ⌘rev - ⌘ Current version: 5.2.0 ⌘

*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:	⌘	Consequences if USIM services n° 27 and n° 38 are not available.
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 20/082003
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:	⌘	It was clarified in TS 33.102 that a disabled USIM service n° 27 prevents access to a 2G BSS only if that requires ciphering. Further, the negative impact of access restrictions by unavailability of the optional USIM services n° 27 and n° 38 on emergency calls needs to be mentioned.
Summary of change:	⌘	The explanations on services n° 27 and n° 38 are extended to cover the reasons for change.
Consequences if not approved:	⌘	TR 31.900 may not completely reflect the core specifications.

Clauses affected:	⌘	Section 5.1			
Other specs affected:	⌘	**Y**	**N**		⌘
		[ ]	[ ]	Other core specifications	
		[ ]	[ ]	Test specifications	
		[ ]	[ ]	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.1 3G ME and UICC

A 3G ME has to support the UICC. 3G TS 31.101 [1] and 3G TS 31.102 [2] apply.

According to 3G TS 21.111 [3] a 3G ME does not support a 5V ME/UICC interface. This is valid even when it accesses the SIM application on the UICC. According to the same specification, a UICC does always support at least two voltage classes, i.e. a 5V only UICC cannot exist.

In case of a UICC inserted in a 3G ME, nothing but the 3G command set (as defined in 3G TS 31.101 [1] and 3G TS 31.102 [2]) can be used by the ME. In particular, the 2G command RUN GSM ALGORITHM is not available.

To support a 2G/3G dual mode ME in a 2G radio access network, the USIM may provide functions for 2G backward compatibility. Two particular USIM services are defined for such purposes:

1. **Service n° 27:** "GSM Access". This service is essential when a 2G BSS is involved and ciphering is active in the BSS. The USIM additionally generates the 2G ciphering key Kc required by the 2G air interface. From the security point of view, this behaviour can be characterised as "**3G + Kc mode**" (see below). Further, the USIM supports some additional 2G data storage elements that are necessary for 2G radio access. If service n° 27 is not available in the USIM, the lack of Kc prevents operation with a 2G BSS when ciphering is active. No ciphering key derivation is done by the ME.

2. **Service n° 38:** "GSM Security Context". This service is required when a 2G VLR/SGSN and/or a 2G HLR/AuC is involved. The USIM performs 2G AKA, i.e. it accepts 2G input data and generates 2G output data. From the security point of view, this behaviour can be characterised as "**virtual 2G mode**" (see below). If service n° 38 is not available in the USIM, 2G AKA is not supported and network access is impossible with a 2G VLR/SGSN and/or a 2G HLR/AuC.

   A 2G VLR/SGSN never goes with a 3G BSS. Hence when a 2G VLR/SGSN is involved, then a 2G BSS is always part of the transmission chain and service n° 27 is additionally required, i.e. services n° 27 and n° 38 have to be available at the same time.

If services n° 27 and n° 38 are not supported by the USIM (which the ME can detect from the USIM Service Table during the USIM activation procedure) network access is impossible in a mixed 2G/3G environment, even if a SIM application is available on the UICC. A 3G ME only accesses the USIM application on the UICC.

From the security point of view, the compatibility services are connected to up to three different operation modes (see also Annex B):

- **Normal 3G mode:** The results of the 3G algorithm are sent to the ME without any change. The USIM receives RAND and AUTN and responds with RES, CK and IK. This mode applies if service n° 27 is not available.

- **3G + Kc mode:** The 2G ciphering key Kc (derived from CK, IK) is additionally included in the response. The USIM receives RAND and AUTN and responds with RES, CK, IK and Kc. This requires conversion function c3 to be supported by the USIM. If service n° 27 is available in the USIM, this mode is always active and the ME picks the relevant values from the USIM response according to the present network situation.

- **Virtual 2G mode:** The USIM receives a 2G authentication request with RAND and returns a 2G authentication response with SRES (derived from RES) and ciphering key Kc (derived from CK, IK). This requires a particular algorithm execution mode plus conversion functions c2 and c3 to be supported by the USIM. If service n° 38 is available in the USIM, this mode is not always active. The ME may switch the USIM from normal 3G mode or 3G + Kc mode to virtual 2G mode by sending a particular command parameter according to the present network situation.

The services n° 27 and n° 38 are both optional. Network operators can decide whether to include them into their USIMs and hence to allow network access with lower security level. It should be noted that this access limitation also affects emergency call set-up and handover.