3GPP TSG-T (Terminals) Meeting #13
Beijing, China, 19 - 21 September, 2001

Tdoc TP-010205

Source: T3

Title: Change Request on SIM/USIM inter-working report (TR 31.900)

Document for: Approval

This document contains a change request to TR 31.900 as agreed by T3.

T3 Doc	Spec	CR	Rel	Cat	Subject
T3-010580	31.900	001	R99	F	Sharing of enabling/disabling procedure between SIM and USIM

3GPP T3 (USIM) Meeting #20
Marseille, France, 03 - 05 September, 2001

Tdoc T3-010580
(revised version of T3-010568)

CR-Form-v3

CHANGE REQUEST

⌘ **31.900** **CR** **001** ⌘ rev **-** ⌘ Current version: **3.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Sharing of enabling/disabling procedure between SIM and USIM.
Source:	⌘	*T3*
Work item code:	⌘	***Date:*** ⌘ 2001-09-05
Category:	⌘	**F** ***Release:*** ⌘ R99

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)*

Reason for change:	⌘	Enabling/disabling of FDN and BDN services are different in USIM and SIM and this point should be highlighted in the TR.
Summary of change:	⌘	Mention that enabling/disabling procedure can be shared between SIM and USIM.
Consequences if not approved:	⌘	The TR would not cover all potential implementation difficulties.

Clauses affected:	⌘	7.7		
Other specs affected:	⌘	[ ] Other core specifications [ ] Test specifications [ ] O&M Specifications	⌘	
Other comments:	⌘			

7 Interworking between a SIM application and a USIM application on a UICC

A SIM application and a USIM application which are implemented together on a single UICC can never be active at the same time. Neither can they be switched from one to the other. Their activity solely depends on the type of ME in which they are inserted: A 2G ME will always activate the SIM application, while a 3G ME only uses the USIM application. Hence a direct way of interworking does not exist.

However, both applications may share certain elements, either to enable an intended basic subscription mode of the UICC (single or double subscription) or to optimise memory consumption, but still both applications have to be virtually independent from a functional point of view. This means that a 2G ME can interwork with the SIM application without any influence from the USIM, while a 3G ME finds all the mandatory characteristics of the USIM application. Naturally, independence ends if one application changes shared data which is later accessed by the other application because the UICC was inserted into another type of ME. This has to be taken into account.

The following sections describe the possible options.

7.1 IMSI, secret key and authentication algorithm

In the HLR/AuC, a single subscription is identified by a particular IMSI, which is connected to a particular secret key (given by "Ki" for 2G, "K" for 3G) and to one type of authentication algorithm ("A3/A8" for 2G, "f1-f5" for 3G). At no time, a single IMSI may be connected to more than one secret key or algorithm. This is valid for both 2G and 3G contexts. Further, it applies that

- Length and Format ($IMSI_{2G}$) = Length and Format ($IMSI_{3G}$)

- Length (Ki) = Length (K)

- 2G-Type Algorithm = Part of 3G Algorithm + Conversion Functions c2, c3

For the third "equation" see Annex B2 or 3G TS 31.102 [2] and 3G TS 33.102 [6]. This 2G behaviour of the 3G algorithm is the same as the virtual 2G mode described in section 5.1. If it is always active, e.g. in a SIM application or in a 2G HLR/AuC, it shall in the following be called a fixed virtual 2G mode. Then, in fact, it is a 2G algorithm.

There are three possible options for the UICC:

1. **Separate IMSI & Separate Secret Key:** This case applies if the network operator - for some reason - wants to administrate the 2G and the 3G subscription, i.e. the usage of a 2G or 3G ME, fully independent. The two subscriptions can be maintained in either in a single 2G or 3G HLR/AuC or in different dedicated 2G and 3G HLR/AuCs. Then USIM and SIM applications also have to keep separate IMSIs, i.e. $IMSI_{3G} \neq IMSI_{2G}$. The secret keys have to be different as well, i.e. $K \neq Ki$. Of course, the algorithms in the UICC have to correspond to the algorithms associated with the IMSIs in the HLR/AuCs. The USIM application needs a 3G algorithm, while for the SIM application it can either be

    - a 2G algorithm on its own or

    - a 3G algorithm in fixed virtual 2G mode. In that case the UICC needs to implement a 3G algorithm only, which from the SIM application is executed in 2G mode. The HLR/AuC must support this option accordingly.

2. **Separate IMSI & Shared Secret Key:** From a functional point of view, this option is identical to option 1, except that the UICC saves 128 bits for the storage of a second secret key. On the other hand, the deliberate assignment of the same secret key to two different IMSIs would require particular solutions during secret key generation and pre-personalization.

3. **Shared IMSI & Shared Secret Key:** This case applies if the network operator wants to have one single subscription for a user, independent of the usage of a 2G or 3G ME. Consequently the UICC has to carry the same identification details, i.e. IMSI and secret key, in both SIM and USIM applications. On the network side there is a single entry consisting of one IMSI and one secret key in either a 2G or a 3G HLR/AuC, i.e. $IMSI_{3G} = IMSI_{2G}$ and $K = Ki$. In a 2G HLR the algorithm has to be a 3G-type in fixed virtual 2G mode (a 3G algorithm

does not fit into a 2G HLR and a 2G algorithm does not fit with the USIM application on the UICC) while in a 3G HLR the algorithm is a 3G-type. On the UICC side there is not much choice: The USIM application essentially needs a 3G algorithm while for the SIM application it can only be a 3G-algorithm in (fixed) 2G mode as there is no 2G-type in the network. Again this has the advantage of having only one shared 3G algorithm on the UICC, which from the SIM application is executed in 2G mode.

The fourth theoretical combination, namely shared IMSI & separate secret keys, is not a valid option as a single IMSI cannot be associated with more than one secret key simultaneously.

7.2 File mapping

When comparing the file structure of a SIM in GSM TS 11.11 [7] with that of a USIM in 3G TS 31.102 [2] it strikes that many not only have the same name and file identifier (although under different DFs) but are entirely equal by size and content parameters. This generally allows for memory efficient implementation of a SIM together with a USIM as these files can be shared by both applications, i.e. necessary storage capacity is only required once. Further, shared files speed up the pre-personalization process as they save valuable programming time.

Therefore files should be mapped as far as possible, i.e. in all cases where basic properties are equal and identical contents do not conflict with the access by either a 2G or a 3G ME or with intended subscription differences when separate IMSIs are used (cases 1 or 2 in section 7.1). Mapping is not possible, when the content is clearly subscription dependent like in case of IMSI, Kc, KcGPRS or MSISDN in a double subscription UICC.

Annex C gives an overview on the SIM and USIM files that potentially can be mapped. A case by case decision should be conducted by the network operator / card manufacturer for each UICC implementation.

7.3 Access conditions

If a EF or DF is accessible in both 2G and 3G operation modes (e.g. in the MF: EF-PL in the UICC can be identical to EF-ELP in the SIM), then independent 2G and 3G access conditions may be defined for the file. The UICC does not check the consistency of the access conditions in both modes.

Therefore it is possible that the same EF or DF has different security attributes in 2G and 3G operation mode. It is the responsibility of the network operator and the card manufacturer to ensure at the personalisation stage that the security attributes for 2G and 3G session are the same, if necessary.

7.4 Secret codes

In 3G mode, 8 Application PINs with global key references are available and the UICC also supports up to 8 Local PINs with specific key references. Local PINs can only be used within an ADF. Further, up to 10 administrative PINs can be defined. A replacement PIN, called Universal PIN, may also exist.

In 2G mode, only CHV1 and CHV2 are available. They apply to files in DF-GSM and DF-TELECOM. Additionally, up to 11 administrative PINs can be defined.

Mapping of PINs between 2G and 3G operation modes, so that activation, deactivation or changing of a PIN in one operation mode has the same effect in the other operation mode, follow the following principles:

- **Mapping of CHV1**

  CHV1 in the SIM application can be mapped to any USIM application PIN with a global key reference (or to the Universal PIN), but to only one at a time.

- **Mapping of CHV2**

  CHV2 in the SIM application can be mapped to the corresponding local key reference belonging to the USIM application to which the CHV1 is mapped. In the 2G operation mode, this PIN is considered to be global, in the 3G operation mode, it is seen as a being local. If mapped, then, with respect to the requirement in TS GSM 11.11 [7] for CHV2, this PIN cannot be disabled in either operation mode. The UICC will return an appropriate error condition in that case.

- **Mapping of Local PINs**

  A SIM does not support Local PINs, hence there is no correspondence in 2G operation mode. Local PINs cannot be mapped.

- **Mapping of administrative PINs**

  The mapping of administrative PINs between the 2G and 3G operation modes is fully under the discretion of each network operator and card manufacturer.

7.5 Activation of 2G and 3G operation modes

After a cold reset has been performed (i.e. during UICC activation), the ATR sent by the UICC is compliant to 3G TS 31.101 [1]. No particular operation mode is active at this stage. The selection and activation of either 2G operation mode (i.e. the SIM application) or 3G operation mode, is implicitly done by the ME when sending the first command. The following table describes the different possible cases.

ICC / ME Combination	Class Byte of First Command	Resulting Operation Mode	Remark
UICC with or without a SIM application in a 3G or 2G/3G dual mode ME	'0X' or '8X'	3G	The USIM application shall reject commands with class byte = 'A0'. First command right after ATR can be SELECT or STATUS.
UICC with a SIM application in a 2G ME	'A0'	2G	The SIM application may reject commands with class byte = '0X' or '8X'. First command right after ATR can be SELECT, STATUS or GET RESPONSE.
UICC without a SIM application in a 2G ME	'A0'	No operation!	All further commands with class byte = 'A0' will be rejected.

A 3G or 2G/3G dual mode ME will only send commands with class byte = '0X' or '8X'. A 2G ME will only send commands with class byte = 'A0'. The operation mode selection takes place regardless of the result of the command (i.e. if it was successful or not).

7.6 Selection of cyclic files

As the SIM application and the USIM application are based on individual specifications, a particular difference applies for the selection of cyclic files.

For the SIM, GSM TS 11.11 [7] specifies that "After selection of a cyclic file (for either operation), the record pointer shall address the record updated or increased last.", whereas for the USIM it is required in 3G TS 31.101 [1] that "After a successful selection the record pointer is undefined.". In the latter case, the record pointer is set implicitly by the subsequent access command.

Therefore, in the case of a selection of cyclic files, the UICC will behave corresponding to its current operation mode, i.e. comply to 2G requirements when the SIM application is active and to 3G requirements when the USIM application is active.

A 3G ME shall handle this situation accordingly, i.e. depending on whether a SIM or a UICC is inserted.

7.7 Enabling/disabling procedures for dialling numbers

Enabling/disabling procedures of restricted dialling numbers services (e.g. FDN or BDN) are different between SIM and USIM. Nevertheless, if a dialling number file is mapped between a SIM and a USIM, the corresponding enabling/disabling procedures can also be linked. When an enabling/disabling procedure is shared between a SIM and a USIM, the enabling/disabling of a restricted dialling numbers service in one mode (SIM or USIM) is reflected in the other mode (respectively USIM or SIM).