

CR-Form-v7

CHANGE REQUEST

⌘ **33.203 CR CRNum** ⌘ rev **-** ⌘ Current version: **5.6.0** ⌘

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 ME Radio Access Network Core Network

Title:	⌘ Clarification to USIM based access to IMS				
Source:	⌘ Vodafone				
Work item code:	⌘	Date:	⌘ 17/07/03		
Category:	⌘ F	Release:	⌘ Rel-5		
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:		
	F (correction)		2 (GSM Phase 2)		
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)		
	B (addition of feature),		R97 (Release 1997)		
	C (functional modification of feature)		R98 (Release 1998)		
	D (editorial modification)		R99 (Release 1999)		
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)		
			Rel-5 (Release 5)		
			Rel-6 (Release 6)		

Reason for change:	⌘ The current specification of USIM-based access to IMS could be interpreted to mean that the USIM application on the UICC has to be IMS aware. This was never intended so the specification should be clarified.
Summary of change:	⌘ It is made clear that USIM-based access to IMS does not require the USIM application on the UICC to be IMS aware.
Consequences if not approved:	⌘ It could be incorrectly interpreted that the USIM application has to be enhanced with IMS-specific features.

Clauses affected:	⌘									
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="width: 20px; text-align: center;"><input type="checkbox"/></td> <td style="width: 20px; text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td style="width: 20px; text-align: center;"><input type="checkbox"/></td> <td style="width: 20px; text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td style="width: 20px; text-align: center;"><input type="checkbox"/></td> <td style="width: 20px; text-align: center;"><input type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Other core specifications ⌘ Test specifications ⌘ O&M Specifications ⌘
Y	N									
<input type="checkbox"/>	<input type="checkbox"/>									
<input type="checkbox"/>	<input type="checkbox"/>									
<input type="checkbox"/>	<input type="checkbox"/>									
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.

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 [non IMS aware](#) 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.

8.1 Requirements on the ISIM application

This section identifies requirements on the ISIM application to support IMS access security. It does not identify any data or functions that may be required on the ISIM application for non-security purposes.

The ISIM shall include:

- The IMPI;
- At least one IMPU;
- Home Network Domain Name;
- Support for sequence number checking in the context of the IMS Domain;
- The same framework for algorithms as specified for the USIM applies for the ISIM;
- An authentication Key.

The ISIM shall deliver the CK to the UE although it is not required that SIP signaling is confidentiality protected.

At UE power off the existing SAs in the MT shall be deleted. The session keys and related information in the SA shall never be stored on the ISIM.

8.2 Sharing security functions and data with the USIM

When an ISIM is used for IMS access, only the following options for sharing security functions and data are permitted:

- No security functions or data are shared;
- Only the sequence number checking mechanism is shared;
- Only the algorithm is shared;
- Only the algorithm and sequence number checking mechanism are shared;
- The authentication key, authentication functions and the sequence number checking mechanism are shared.

When a USIM is used for IMS access, only the following option is applicable:

- The authentication key, authentication functions and the sequence number checking mechanism are shared.

NOTE: If the authentication keys and functions are shared, the cipher/integrity key sets generated during authentication are used with different cipher/integrity algorithms in CS/PS domain and IMS. Note that the same cipher/integrity key set is never used for both CS/PS domain and IMS because the authentication and key agreement protocol is run independently between CS/PS domain and IMS. Therefore there is no danger that the compromise of the cipher/integrity algorithm in one domain would lead to vulnerabilities in the other domain.

If the mechanism and data for checking sequence numbers are shared then it shall be required for the authentication failure rate due to synchronization failures to be kept sufficiently low. In particular, the mechanism shall be required to support interleaving authentication in three domains (CS, PS and IMS). Example methods to achieve this are described in Annex G.