CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: 6.3.0 ⌘

*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 [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	Forwards compatibility to TLS based access security
Source:	⌘	Ericsson
Work item code:	⌘	IMS-SEC ***Date:*** ⌘ 23 June 2004
Category:	⌘	**F** ***Release:*** ⌘ Rel-6

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 IMS specification is not forward compatible to one potential deployment mode of TLS based access security.
Summary of change:	⌘	Adds one potential solution.
Consequences if not approved:	⌘	One potential TLS deployment mode cannot be used when UE is roaming in visited network.

Clauses affected:	⌘	8.2			
Other specs affected:	⌘	Y: Other core specifications	⌘	23.003	
		N: Test specifications			
		N: O&M Specifications			
Other comments:	⌘				

***** Begin of Change ****

8.1 Requirements on the ISIM application

This clause 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.

Domain and realm names used in IMPI, IMPU(s) and Home Network Domain Name shall contain IMS Trust Domain Name.

NOTE: The exact content and format of IMS Trust Domain Name is out of the scope of this specification. It could be, for example, “ims.com” or “3gppnetwork.com”.

NOTE: This requirement guarantees that TLS can be used for IMS access security between UE and P-CSCF in the future.

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.

***** End of Change ****