3GPP TSG SA WG3 Security — S3#33 *Tdoc ⌘S3-040429*
10 - 14 May 2004, Beijing, China

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.203** **CR** **CRNum** ⌘ **rev** ⌘ Current version: **6.2.0** ⌘

*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⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	SIP Privacy mechanism when IMS interworking with non-IMS (foreign) network
Source:	⌘	Nokia
Work item code:	⌘	IMS-ASEC
Date:	⌘	14/5/2004
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	*(G<SM 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:	⌘	This CR adds the handling of user privacy feature in SIP, when the IMS interworking with a non-IMS network.
Summary of change:	⌘	The privacy handling is added with modification to Rel-5 handling for Rel-6 IMS.
Consequences if not approved:	⌘	It is impossible to guarantee IMS interworking security.

Clauses affected:	⌘	5.3, 6.5			
Other specs affected:	⌘	**Y** / **N**	Other core specifications	⌘	TS 24.229, TS 24.228
		X /	Other core specifications		
		/ **X**	Test specifications		
		/ **X**	O&M Specifications		
Other comments:	⌘				

5.3 SIP Privacy handling in~~for~~ IMS Networks

Privacy may in many instances be equivalent with confidentiality i.e. to hide the information (using encryption and encryption keys) from all entities except those who are authorized to understand the information. The SIP Privacy Extensions for IMS Networks do not provide such confidentiality. The purpose of the mechanism is rather to give an IMS subscriber the possibility to withhold certain identity information of the subscriber as specified in [22] and [23].

NOTE 1: It is useful that the privacy mechanism for IMS networks does not create states in the CSCFs other than the normal SIP states.

Editor's note: the exact mechanism for building the trust relation for privacy handling is ffs.

*** NEXT CHANGE ***

6.5 CSCF interoperating with proxy located in ~~non-IMS~~a foreign network

SIP signalling protected by TLS specified in RFC 3261 [6] may be used for protecting the SIP interoperation between an IMS CSCF with a proxy/CSCF located in ~~non-IMS~~a foreign network. The CSCF may request the TLS connection with a foreign Proxy by publishing sips: URI in DNS server, that can be resolved via NAPTR/SRV mechanism specified in RFC 3263 [23]. When sending/receiving the certificate during the TLS handshaking phase, the CSCF shall verify the name on the certificate against the list of the interworking partners.

Editor's note: A “foreign network” is currently defined as a non-IMS network. It may extend to also IMS network which is ffs.

The TLS session could be inititiated from either ~~the CSCF or the foreign proxy~~network. A TLS connection is capable of carrying multiple SIP dialogs.

Applying this method is to prevent attacks on SIP level, but it does not prohibit other security methods to be applied so as to strengthen the security for IP based networks. This part is specified in Annex A of TS 33.210 [5].

NOTE 1: The key management and certificate management for TLS is out of scope of the present specification.

NOTE 2: The security mechanism between the CSCFs within IMS is covered by NDS/IP security specified in TS 33.210 [5].

*** END OF CHANGE ***