3GPP TSG-WG3 Meeting #31
Munich, Germany, 18th–21th November 2003

Tdoc ⌘S3-030725

CR-Form-v7

CHANGE REQUEST

⌘ **TS 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:	⌘	Removing anti-replay requirement from Confidentiality clause
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	18/07/2003
Category:	⌘	**D**
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:	⌘	The TS requires anti-replay services in the confidentiality section where it does not naturally belong to. The requirement is already captured in more natural place in the TS.
Summary of change:	⌘	The anti-replay requirement is removed from the confidentiality clause where it should not be specified. The requirement is already specified in the clause 6.3 under the Integrity requirements.
Consequences if not approved:	⌘	The requirement is defined two times which is not necessary and can create unnecessary confusion.

Clauses affected:	⌘	6.2

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

6.2 Confidentiality mechanisms

If the local policy in P-CSCF requires the use of IMS specific confidentiality protection mechanism between UE and P-CSCF, IPsec ESP as specified in [13] shall provide confidentiality protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. IPSec ESP general concepts on Security Policy management, Security Associations and IP traffic processing as described in reference [14] shall also be considered. ESP confidentiality shall be applied in transport mode between UE and P-CSCF.

The method to set up ESP security associations (SAs) during the SIP registration procedure is specified in clause 7. As a result of an authenticated registration procedure, two pairs of unidirectional SAs between the UE and the P-CSCF all shared by TCP and UDP, shall be established in the P-CSCF and later in the UE. One SA pair is for traffic between a client port at the UE and a server port at the P-CSCF and the other SA is for traffic between a client port at the P-CSCF and a server port at the UE. For a detailed description of the establishment of these security associations see section 7.

The encryption key CK_{ESP} is the same for the two pairs of simultaneously established SAs. The encryption key CK_{ESP} is obtained from the key CK_{IM} established as a result of the AKA procedure, specified in clause 6.1, using a suitable key expansion function.

[Editors Note: This key expansion function depends on the ESP encryption algorithm and should be specified in Annex I but is FFS.]

The encryption key expansion on the user side is done in the UE. The encryption key expansion on the network side is done in the P-CSCF.

~~The anti-replay service shall be enabled in the UE and the P-CSCF on all established SAs.~~