3GPP TSG-SA3 Meeting #26
Oxford, UK, 19 – 22 November 2002

Tdoc ⌘S3-020627

CR-Form-v7

CHANGE REQUEST

⌘	**33.203**	**CR**	**CRNum**	⌘**rev**	**-**	⌘	Current version:	**5.3.0**	⌘

*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 ☒ Radio Access Network □ Core Network ☒

Title:	⌘	TCP and UDP share same SA		
Source:	⌘	Nokia		
Work item code:	⌘	IMS-ASEC	***Date:*** ⌘	12/11/2002
Category:	⌘	**F**	***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:	⌘	TCP and UDP sharing (SP-020583) is approved in by SA#17. The clause 6.3 which mention the separate SA for each transport protocol should be changed.
Summary of change:	⌘	The brief description of SA establishment in clause 'Integrity mechanisms' is changed according to SP-020583.
Consequences if not approved:	⌘	Inconsistent in the same specification.

Clauses affected:	⌘	6.3				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

6.3 Integrity mechanisms

IPsec ESP as specified in reference [13] shall provide integrity 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 integrity 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 the registration procedure, ~~two~~ a pair~~s~~ of unidirectional SAs between the UE and the P-CSCF, ~~one pair for~~shared by TCP ~~and one pair for~~and UDP, shall be simultaneously established in the P-CSCF and later in the UE. ~~Each pair consists of an~~One SA is for traffic from the UE to the P-CSCF (inbound SA at the P-CSCF) and an SA is for traffic from the P-CSCF to the UE (outbound SA at the P-CSCF).

The integrity key IK_{ESP} is the same for the ~~four~~ two simultaneously established SAs. The integrity key IK_{ESP} is obtained from the key IK_{IM} established as a result of the AKA procedure, specified in clause 6.1, using a suitable key expansion function. This key expansion function depends on the ESP integrity algorithm and is specified in Annex I of this specification.

The integrity key expansion on the user side is done in the UE. The integrity 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.