3GPP TSG-SA WG3 Meeting #23
Victoria, BC, Canada, 14-17 May 2002

Tdoc S3-020221

CR-Form-v5.1

CHANGE REQUEST

⌘	**33.203**	**CR**	**0xx**	⌘ **rev**	**-**	⌘	Current version:	**5.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM □ ME/UE ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Removal of 2 separate Key derivation functions		
Source:	⌘	Ericsson		
Work item code:	⌘	IMS-ASEC	***Date:*** ⌘	2002-05-07
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)*

Reason for change:	⌘	TS 33.203 mandates that two different IPSec ESP integrity keys are derived from IK for the inbound and outbound SAs. Other that to avoid reflection attacks, this doesn't add extra security.
Summary of change:	⌘	It is specified that different SPI values shall be used in the P-CSCF and UE while negotiating the integrity protection. This makes unnecessary to have two derivation functions and separate integrity keys for each unidirectional SA.
Consequences if not approved:	⌘	The proposed change simplifies implementations while keeping the level of security.

Clauses affected:	⌘	Annex B		
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘	
Other comments:	⌘	HMAC-SHA-1-96 requires a 160-bit key. How this key is derived from IK is address in a separate CR.		

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.

Annex B (informative): Mechanisms for IPSec based solution

[Editors Note: If the IPSec solution is finally chosen the chapters below shall be moved into the main body of this TS in the corresponding sections.]

B.1 [6.2] Confidentiality mechanisms

IPsec ESP may optionally be implemented for providing confidentiality of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. If ESP confidentiality is used, it shall be applied in transport mode between UE and P-CSCF. If ESP confidentiality is provided, it is always provided in addition to ESP integrity protection.

The SAs that are required for ESP shall be derived from the 128-bit integrity key CK_{IM} generated through IMS AKA, as specified in chapter 6.1.

If confidentiality is required, for each direction, there is one ESP SA for both confidentiality and integrity that shall be used between the UE and the P-CSCF. The encryption ~~transform is~~algorithm and key are identical for the two SAs in either direction. ~~The encryption key for the SA inbound from the P-CSCF is CK.~~

The UE and the P-CSCF shall allocate different SPI values for each SA. This helps to mitigate the risk of reflection attacks.

~~The encryption key for the SA inbound from the P-CSCF is CK_{IM_in}. The encryption key for the SA outbound from the P-CSCF is CK_{IM_out}.~~

~~The encryption keys are derived as $CK_{IM\_in} = h1(CK_{IM})$ and $CK_{IM\_out} = h2(CK_{IM})$ using suitable key derivation functions h1 and h2.~~

The encryption key derivation on the user side is done in the ISIM. The encryption key derivation on the network side is done in the P-CSCF.

The method to set up ESP security associations during the SIP registration procedure is specified in chapter 7.

B.2 [6.3] Integrity mechanisms

IPsec ESP shall provide integrity protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. ESP integrity shall be applied in transport mode between UE and P-CSCF.

The SAs that are required for ESP shall be derived from the 128-bit integrity key IK generated through IMS AKA, as specified in chapter 6.1. The transform used for the ESP SA shall be negotiated as specified in chapter 7. ESP shall use two unidirectional SAs between the UE and the P-CSCF, one in each direction. The integrity algorithm and key is identical for both SAs.

The UE and the P-CSCF shall allocate different SPI values for each SA. This helps to mitigate the risk of reflection attacks.

~~The integrity key for the SA inbound from the P-CSCF is IK_{IM_in}. The integrity key for the SA outbound from the P-CSCF is IK_{IM_out}.~~

~~The integrity keys are derived as $IK_{IM\_in} = h1(IK_{IM})$ and $IK_{IM\_out} = h2(IK_{IM})$ using suitable key derivation functions h1 and h2. (They may be the same as those in section 6.2.)~~

The integrity key derivation on the user side is done in the ISIM. The integrity key derivation on the network side is done in the P-CSCF.

The method to set up ESP security associations during the SIP registration procedure is specified in chapter 7.