3GPP TSG SA WG3 Security **S3-020223**

May 14 – May 17, 2002

Victoria, Canada

Agenda Item: TBD

Source: Ericsson

Title: The use of SHA-1 in IMS and IPSec ESP

Document for: Discussion and decision

1. Scope and objectives

This CR proposes that the IK derived from IMS AKA which is 128 bit long should be expanded to 160 bit since this is required by an IPSec implementation as defined in [RFC 2404]. The proposed scheme is that the key K, which is fed into the HMAC, is IK padded with 4 zero bytes 0x00:

K=IK||0x00||0x00||0x00||0x00

Hence K is a 160 bit key with entropy equal to the entropy of IK.

References

[RFC 2404] RFC 2404 “The use of HMAC-SHA-1-96 within ESP and AH, IETF, November 1998

CR-Form-v5

CHANGE REQUEST

⌘	**33.203**	**CR**		⌘ **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:	⌘	The definition of the key to be used for HMAC-SHA1-96 within ESP		
Source:	⌘	Ericsson		
Work item code:	⌘	IMS-ASEC	***Date:*** ⌘	06/05/2002
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)*

Reason for change:	⌘	Currently it is not specified how the IMS AKA IK is to be used with HMAC SHA1 within the IPSec ESP framework
Summary of change:	⌘	Proposes how to expand IK from 128 bit to 160 bit
Consequences if not approved:	⌘	IMS cannot use HMAC SHA1 as specified by IPSec

Clauses affected:	⌘	2,	
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments:	⌘		

************* FIRST CHANGED SECTION **************

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.

There are two cases:

1. If the negotiated integrity algorithm is HMAC-MD5-96 the input key is the 128 bit key IK which is stored in the IPSec SA
2. If the negotiated integrity algorithm is HMAC-SHA-1-96 the 128 bit key IK has to be expanded with 4 zero bytes 0x00 i.e.

   IK=IK||0x00||0x00||0x00||0x00

   which is stored in the IPSec SA

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 is identical for both SAs.

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.