Technical Specification Group Services and System Aspects
Meeting #16, Marco Island, Florida, 10-13 June 2002

TSGS#16(02)0355

Source: **SA WG3**

Title: **CR to 33.210: NDS/IP Confidentiality protection for IMS session keys (Rel-5)**

Document for: **Approval**

Agenda Item: **7.3.3**

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-020355	33.210	001		Rel-5	NDS/IP Confidentiality protection for IMS session keys	F	5.0.0	SEC-NDS-IP	S3-020229

3GPP TSG SA-WG3 Meeting #23 **S3-020229**
Victoria Island, Canada, 14th–17th May 2002

CR-Form-v5

CHANGE REQUEST

⌘ **33.210** **CR** **001** ⌘ **rev** **-** ⌘ Current version: **5.0.0** ⌘

*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:	⌘	NDS/IP Confidentiality protection for IMS session keys.
Source:	⌘	SA WG3
Work item code:	⌘	SEC-NDS-IP
Date:	⌘	13.05.2002
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: ⌘

In the scope of IMS, session keys are transported in SIP over the Mm interface between I-CSCF and P-CSCF. This communication may take place between security domains and according to 33.210, IMS operators shall route this traffic via SEGs and operate NDS/IP Za-interface between SEGs in this case.

Currently, within the NDS/IP framework, ESP will be tipically used with both encryption and authentication/integrity on Za interfaces but an authentication/integrity only mode is also allowed.

The confidentiality of the IMS session keys will be compromised in the event that the IMS operator chooses to operate Za-interface between SEGs with an integrity-only mode.

Since protecting only those messages which carry session keys would imply knowledge at the IPSec layer of the content of the SIP message, it is considered an acceptable simplification to mandate encryption for all messages crossing security domain boundaries.

Summary of change: ⌘ ESP shall be always used with both encryption and integrity (i.e. integrity-only mode is NOT permited).

Consequences if not approved: ⌘ Confidentiality of IMS session keys is compromised if NDS-IP framework is applied over Mm interface (I-CSCF – P-CSCF) with no encryption.

Clauses affected: ⌘ Annex C.2

Other specs affected: ⌘
☐ Other core specifications ⌘
☐ Test specifications
☐ O&M Specifications

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.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.

C.2 Protection of IMS protocols and interfaces

IMS control plane traffic within the IMS core network shall be routed via a SEG when it takes place between different security domains (in particular over those interfaces that may exist between different IMS operator domains). In order to do so, IMS operators shall operate NDS/IP Za-interface between SEGs.

IPSec ESP shall be used with both encryption and integrity protection for all SIP signalling traversing inter-security domain boundaries.

It will be for the IMS operator to decide whether and where to deploy Zb-interfaces in order to protect the IMS control plane traffic over those IMS interfaces within the same security domain.

Diameter messages over the Cx interface shall make use of SCTP. Additional guidelines on how to apply IPSec in SCTP are specified in [26]. This RFC shall also apply to NDS/IP if IMS operator chooses to deploy Zb-interface at Cx interface.

Editor's Note; The reference to I-D "draft-ietf-ipsec-sctp-02.txt" shall be replaced by the corresponding RFC reference when this draft reaches RFC status.