

CR-Form-v5

CHANGE REQUEST

⌘ **33.210 CR CRNum** ⌘ 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:	⌘ Removal of reference to Internet draft <i>draft-ietf-ipsec-sctp-03.txt</i>		
Source:	⌘ Ericsson/Telenor		
Work item code:	⌘ SEC-NDS-IP	Date:	⌘ 22.04.2002
Category:	⌘ F Use <u>one</u> 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.	Release:	⌘ REL-5 Use <u>one</u> 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:	⌘ Dependency on Internet draft that may never become an RFC.
Summary of change:	⌘ To remove all references to Internet draft <i>draft-ietf-ipsec-sctp-03.txt</i>
Consequences if not approved:	⌘ The specification would be ambiguous/misleading in Annex C Protection of IMS protocols over the Cx interface. Note that the removal of the reference to Internet draft <i>draft-ietf-ipsec-sctp-03.txt</i> does not preclude NDS/IP from protecting the Cx interface.

Clauses affected:	⌘ Clause 2 References Annex C.2
Other specs affected:	⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications
Other comments:	⌘

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TS 21.133: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements".
- [2] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".
- [3] 3GPP TS 23.002: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture".
- [4] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2".
- [5] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".
- [6] 3GPP TS 29.060: "3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".
- [7] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".
- [8] 3GPP TS 33.103: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Integration guidelines".
- [9] 3GPP TS 33.120: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Principles and Objectives".
- [10] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Access security for IP-based services".
- [11] RFC-2393: "IP Payload Compression Protocol (IPComp)".
- [12] RFC-2401: "Security Architecture for the Internet Protocol".
- [13] RFC-2402: "IP Authentication Header".
- [14] RFC-2403: "The Use of HMAC-MD5-96 within ESP and AH".
- [15] RFC-2404: "The Use of HMAC-SHA-1-96 within ESP and AH".
- [16] RFC-2405: "The ESP DES-CBC Cipher Algorithm With Explicit IV".
- [17] RFC-2406: "IP Encapsulating Security Payload".
- [18] RFC-2407: "The Internet IP Security Domain of Interpretation for ISAKMP".
- [19] RFC-2408: "Internet Security Association and Key Management Protocol (ISAKMP)".

- [20] RFC-2409: "The Internet Key Exchange (IKE)".
- [21] RFC-2410: "The NULL Encryption Algorithm and Its Use With IPsec".
- [22] RFC-2411: "IP Security Document Roadmap".
- [23] RFC-2412: "The OAKLEY Key Determination Protocol".
- [24] RFC-2451: "The ESP CBC-Mode Cipher Algorithms".
- [25] RFC-2521: "ICMP Security Failures Messages".
- [26] ~~Internet Draft: "On the Use of SCTP with IPsec", available as "draft-ietf-ipsec-setp-03.txt"~~

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.

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-setp-02.txt" shall be replaced by the corresponding RFC reference when this draft reaches RFC status.~~