3GPP TSG-SA3 Meeting #29
San Francisco, USA, July 15-18, 2003

Tdoc ⌘S3-030404

CR-Form-v7

CHANGE REQUEST

⌘	**33.210**	**CR**	**CRNum**	⌘**rev**	**-**	⌘	Current version:	**5.4.0**	⌘

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:	⌘	Update draft-ietf-ipsec-sctp-03.txt reference to new standard RFC: RFC3554		
Source:	⌘	Siemens		
Work item code:	⌘	SEC-NDS-IP	***Date:*** ⌘	09/07/2003
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:	⌘	draft-ietf-ipsec-sctp-06.txt has been accepted by the IETF as a standard RFC: RFC3554
Summary of change:	⌘	Replacement of referenced draft-ietf-ipsec-sctp-03.txt by RFC3554 Removal of remaining editors note.
Consequences if not approved:	⌘	The specification will reference to an old expired IETF-draft

Clauses affected:	⌘	2, Annex C				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*** first change ***

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] RFC-3554: “On the Use of Stream Control Transmission Protocol (SCTP) with IPsec”~~Internet Draft: "On the Use of SCTP with IPsec ", available as "draft-ietf-ipsec-sctp-03.txt"~~

[27] RFC-1750: “Randomness Recommendations for Security".

**** next change ****

Annex C (normative): Security protection of IMS protocols

This section details how NDS/IP shall be used to protect IMS protocols and interfaces.

C.1 The need for security protection

The security architecture of the IP multimedia Core Network Subsystem (IMS) is specified in 3GPP TS 33.203 [10]. 3GPP TS 33.203 [10] defines that the confidentiality and integrity protection for SIP-signalling are provided in a hop-by-hop fashion.

The first hop i.e. between the UE and the P-CSCF through the IMS access network (i.e. Gm reference point) is protected by security mechanisms specified in 3GPP TS 33.203 [10].

The other hops, within the IMS core network including interfaces within the same security domain or between different security domains are protected by NDS/IP security mechanisms as specified by this Technical Specification.

3GPP TS 23.002 [3] specifies the different reference points defined for IMS.

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.~~