3GPP TSG-SA3 Meeting #24 ***S3-020436***
Helsinki, Finland, Date

CR-Form-v5.1

CHANGE REQUEST

⌘ **33.203** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*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 **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	Draft-ietf-sip-sec-agree syntax for manually keyed IPsec
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	2002-07-04
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:	⌘	[draft-ietf-sip-sec-agree] does not have detail on how it will be used with manually keyed IPsec. For this missing information, 33.203 has an empty annex (H) to be included later. This CR proposes text for annex H.
Summary of change:	⌘	This document defines the syntax for [draft-ietf-sip-sec-agree] so that the mechanism can be used to negotiate IPsec security associations. The syntax is defined in annex H. Some additions and editorial changes to the references are also included.
Consequences if not approved:	⌘	Security mode setup procedure will not work before the exact syntax of the [draft-ietf-sip-sec-agree] for manually keyed IPsec is defined.

Clauses affected:	⌘	2, Annex H
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ 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 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[2] 3GPP TS 22.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for the IP Multimedia Core Network".

[3] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem".

[4] 3GPP TS 21.133: "3rd Generation Partnership Project; T Technical Specification Group Services and System Aspects; Security Threats and Requirements ".

[5] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

[6] IETF RFC 3261 "SIP: Session Initiation Protocol".

[7] 3GPP TS 21.905: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Vocabulary for 3GPP specifications".

[8] 3GPP TS 24.229: "3rd Generation Partnership Project: Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP".

[9] 3GPP TS 23.002: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, Network Architecture".

[10] 3GPP TS 23.060: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, General Packet Radio Service (GPRS); Service Description".

[11] 3GPP TS 24.228: "3rd Generation Partnership Project: Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP".

[12] IETF RFC 2617 (1999) "HTTP Authentication: Basic and Digest Access Authentication".

[13] IETF RFC 2406 (1998) "IP Encapsulating Security Payload (ESP)".

[14] IETF RFC 2401 (1998) "Security Architecture for the Internet Protocol".

[15] IETF RFC 2403 (1998) "The Use of HMAC-MD5-96 within ESP and AH".

[16] IETF RFC 2404 (1998) "The Use of HMAC-SHA-1-96 within ESP and AH".

[17] Draft-ietf-sip-digest-aka-01: "HTTP Digest Authentication Using AKA". April, 2002.

[18] IETF RFC 3041 (2001) "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[19] IETF RFC 2402 (1998) "IP Authentication Header".

[20] IETF RFC 2405 (1998) "The ESP DES-CBC Cipher Algorithm With Explicit IV".

Annex H (normative): The use of [draft-IETF-sip-sec-agree] for security mode set-up

~~[To be added]~~

The BNF syntax of [draft-ietf-sip-sec-agree] is defined for negotiating security associations for manually keyed IPsec in the following way:

security-client = "Security-Client" HCOLON sec-mechanism *(COMMA sec-mechanism)

security-server = "Security-Server" HCOLON sec-mechanism *(COMMA sec-mechanism)

security-verify = "Security-Verify" HCOLON sec-mechanism *(COMMA sec-mechanism)

sec-mechanism = mechanism-name *(SEMI mech-parameters)

mechanism-name = "ipsec-man"

mech-parameters = (preference / algorithm / protocol / mode / encrypt-algorithm / spi / port1 / port2 / transport)

preference = "q" EQUAL qvalue

qvalue = ("0" ["." 0*3DIGIT]) / ("1" ["." 0*3("0")])

algorithm = "alg" EQUAL ("hmac-md5-96" / "hmac-sha-1-96" / "null")

protocol = "prot" EQUAL ("ah" / "esp")

mode = "mod" EQUAL ("trans" / "tun")

encrypt-algorithm = "ealg" EQUAL ("des-cbc" / "null")

spi = "spi" EQUAL spivalue

spivalue = 10DIGIT; 0 to 4294967295

port1 = "port1" EQUAL port

port2 = "port2" EQUAL port

port = 1*DIGIT

transport = "transport" EQUAL ("TCP" / "UDP")

The parameters described by the BNF above have the following semantics:

Mechanism-name: For manually keyed IPsec, this field includes the value “ipsec-man”.

Preference: As defined in [draft-ietf-sip-sec-agree].

Algorithm: If present, defines the authentication algorithm. May have a value “hmac-md5-96” for algorithm defined in [15], “hmac-sha-1-96” for algorithm defined in [16] or “null” if authentication is not used. If no Algorithm parameter is present, the algorithm will be “null”.

Note: According to clause 7.1 the “null” algorithm is not allowed for use in IMS.

Protocol: Defines the IPsec protocol. May have a value “ah” for [19] and “esp” for [13]. If no Protocol parameter is present, the value will be “esp”.

Note: According to clause 6 only “esp” is allowed for use in IMS.

Mode: Defines the mode in which the IPsec protocol is used. May have a value “trans” for transport mode, and value “tun” for tunneling mode. If no Mode parameter is present, the value will be “trans”.

Note: According to clause 6.3 ESP integrity shall be applied in transport mode i.e. only “trans” is allowed for use in IMS.

Encrypt-algorithm: If present, defines the encryption algorithm. May have a value “des-cbc” for algorithm defined in [20] or “null” if encryption is not used. If no Encrypt-algorithm parameter is present, the algorithm will be “null”.

Note: According to clause 6.2 no encryption is provided in IMS i.e. only Encrypt-algorithm “null” is allowed for use in IMS.

Spi: Defines the SPI number used for inbound messages.

Note: The SPI number will be used for outbound messages for the entity which did not generate the “spi” parameter

Port1: Defines the port number for inbound messages

Port2: Defines the port number for outbound messages. If no Port2 parameter is present port1 is also used for outbound messages.

Note: According to clause 7.1, Port2 parameter is not used in IMS.

Transport: If present, defines the transport layer protocol. May have a value “TCP” for TCP, or value “UDP” for UDP. If not present, any transport protocol can be used (cf. transport = “wildcard” as in [14]).