

Technical Specification Group Services and System Aspects
Meeting #21, Frankfurt, Germany, 22-25 September 2003

TSGS#21(03)0485

Source: SA WG3
Title: CR to 33.203: Annex H in 33.203 (Rel-5)
Document for: Approval
Agenda Item: 7.3.3

Meet	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SAWG3 Doc
SP-21	SP-030485	33.203	044	-	Rel-5	F	Annex H in 33.203	5.6.0	5.7.0	S3-030445

CR-Form-v7	
CHANGE REQUEST	
⌘ 33.203 CR 044 ⌘ rev - ⌘ Current version: 5.6.0 ⌘	

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:	⌘ Annex H in 33.203		
Source:	⌘ SA WG3		
Work item code:	⌘ IMS-ASEC	Date:	⌘ 07/07/2003
Category:	⌘ F	Release:	⌘ Rel-5
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)	R96	(GSM Phase 2)
	A (corresponds to a correction in an earlier release)	R97	(Release 1996)
	B (addition of feature),	R98	(Release 1997)
	C (functional modification of feature)	R99	(Release 1998)
	D (editorial modification)	Rel-4	(Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-5 (Release 4)
		Rel-6	(Release 5)
			(Release 6)

Reason for change:	⌘ Annex H needs to be updated if the current solution in 33.203 related to the behaviour of SIP over TCP is changed.
Summary of change:	⌘ The syntax in Annex H is suggested to be modified in the following way: <ol style="list-style-type: none"> 1. The Security-Client header is repeated with Security-Verify header. 2. New SPI parameter is added. 3. Semantics of port number parameters is updated.
Consequences if not approved:	⌘ Implementation of potential new requirements in 33.203 main body is not possible with the current syntax in Annex H.

Clauses affected:	⌘ Annex H										
Other specs affected:	<table border="1" style="font-size: x-small;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"> </td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"> </td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"> </td> <td style="padding: 2px;">N</td> </tr> </table>	Y	N		N		N		N	Other core specifications	⌘ 24.228, 24.229
	Y	N									
		N									
	N										
	N										
		Test specifications									
		O&M Specifications									
Other comments:	⌘										

***** Begin of Change *****

Annex H (normative): The use of "Security Mechanism Agreement for SIP Sessions" [21] for security mode set-up

The BNF syntax of [21] is defined for negotiating security associations for semi-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- 3gpp"
mech-parameters	= (preference / algorithm / protocol / mode / encrypt-algorithm / spi-c / spi-s / port1-port-c / port2-port-s)
preference	= "q" EQUAL qvalue
qvalue	= ("0" ["." 0*3DIGIT]) / ("1" ["." 0*3("0")])
algorithm	= "alg" EQUAL ("hmac-md5-96" / "hmac-sha-1-96")
protocol	= "prot" EQUAL ("ah" / "esp")
mode	= "mod" EQUAL ("trans" / "tun")
encrypt-algorithm	= "ealg" EQUAL ("des-ede3-cbc" / "null")
spi-c	= " spi-c " EQUAL spivalue
spi-s	= " spi-s " EQUAL spivalue
spivalue	= 10DIGIT; 0 to 4294967295
port1-port-c	= " port1-port-c " EQUAL port
port2-port-s	= " port2-port-s " EQUAL port
port	= 1*DIGIT

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

Mechanism-name: For manually keyed IPsec, this field includes the value "ipsec- 3gpp". "[ipsec- 3gpp](#)" [mechanism extends the general negotiation procedure of \[21\] in the following way:](#)

- [1. The server shall store the Security-Client header received in the request before sending the response with the Security-Server header.](#)
- [2. The client shall include the Security-Client header in ~~to~~ the first protected request. In other words, the first protected request shall include both Security-Verify and Security-Client header fields.](#)
- [3. The server shall check that the content of Security-Client headers received in previous steps \(1 and 2\) are the same.](#)

Preference: As defined in [21].

Algorithm: Defines the authentication algorithm. May have a value "hmac-md5-96" for algorithm defined in [15], or "hmac-sha-1-96" for algorithm defined in [16]. The algorithm parameter is mandatory.

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-ede3-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.

Spi-c: Defines the SPI number of the inbound SA used for inbound messages at the protected client port.

~~NOTE: The SPI number will be used for outbound messages for the entity which did not generate the "spi" parameter~~

Spi-s: Defines the SPI number of the inbound SA at the protected server port.

~~Port1~~Port-c: Defines the protected client port ~~destination port number for inbound messages that are protected~~.

~~Port2~~Port-s: Defines the protected server port ~~source port number for outbound messages that are protected. If no Port2 parameter is present it is set to be a wildcard by the receiver~~.

It is assumed that the underlying IPsec implementation supports selectors that allow all transport protocols supported by SIP to be protected with a single SA.

***** End of Change ****