

Technical Specification Group Services and System Aspects
Meeting #20, Hämeenlinna, Finland, 09-12 June 2003

TSGS#20(03)0222

Source: SA WG3
Title: 1 CR to 33.203: Annex H: Alignment of Authentication algorithm handling with RFC 3329 (Rel-5)
Document for: Approval
Agenda Item: 7.3.3

The following CR was approved by SA WG3 meeting #28 and is hereby presented to TSG SA#20 for approval.

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-030222	33.203	040	-	Rel-5	Annex H: Alignment of Authentication algorithm handling with RFC 3329	F	5.5.0	IMS-ASEC	S3-030207

CR-Form-v7	
CHANGE REQUEST	
# TS 33.203 CR 040 # rev - #	Current version: 5.5.0 #

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: Alignment of Authentication algorithm handling with RFC3329		
Source:	# SA WG3		
Work item code:	# IMS-ASEC	Date:	# 25/4/2003
Category:	# F	Release:	# Rel-5
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	<i>F</i> (correction)		2 (GSM Phase 2)
	<i>A</i> (corresponds to a correction in an earlier release)	R96	(Release 1996)
	<i>B</i> (addition of feature),	R97	(Release 1997)
	<i>C</i> (functional modification of feature)	R98	(Release 1998)
	<i>D</i> (editorial modification)	R99	(Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

Reason for change:	# Appendix H of TS 33.203 is incomplete and inconsistent with RFC3329		
	1) RFC 3329 (sip-sec-agree) specifies in Appendix A. <i>Algorithm: This parameter defines the used authentication algorithm. It may have a value of "hmac-md5-96" for HMAC-MD5-96 [13], or "hmac-sha-1-96" for HMAC-SHA-1-96 [14]. The algorithm parameter is mandatory</i>		
	2) TS 33.203 specifies in Annex H <i>Algorithm: If present, 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].</i>		
	→ The specification in TS 33.203 is incomplete as no default value has been defined.		
Summary of change:	# Correct the incomplete specification by aligning Annex H with RFC3329.		
Consequences if not approved:	# Incompatible implementations may appear.		

Clauses affected:	# Annex H		
Other specs affected:	#	#	
	#	#	Other core specifications
	#	#	Test specifications
	#	#	O&M Specifications
Other comments:	#		

***** FIRST 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 / port1 / port2 )
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                 = "spi" EQUAL spivalue
spivalue            = 10DIGIT; 0 to 4294967295
port1               = "port1" EQUAL port
port2               = "port2" 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".

Preference: As defined in [21].

Algorithm: ~~Diff present,~~ 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: 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 destination port number for inbound messages that are protected.

Port2: Defines the 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 CHANGES *****
