Technical Specification Group Services and System Aspects **TSGS#19(03)0111**

Meeting #19, Birmingham, UK, 17-20 March 2003

Source: **SA WG3**

Title: **1 CR to 33.203: Correction of the Port 2 definition for SA establishment**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CR was approved by e-mail after SA WG3 meeting #27 and is hereby presented to TSG SA#19 for approval.

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-030111	33.203	039	-	Rel-5	Correction of the Port 2 definition for SA establishment	F	5.4.0	IMS-ASEC	S3-030170

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **039** ⌘**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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Correction of the Port 2 definition for SA establishment
Source:	⌘	SA3 WG
Work item code:	⌘	IMS-ASEC
Date:	⌘	06/03/2003
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:	⌘	Missing link between symbolic name in main body and syntax definition in Annex H. Misleading rule for selection of source port number at P-CSCF.
Summary of change:	⌘	Provides missing link between main body and Annex H. Provides clear rule for selection of source port number at P-CSCF. Reference RFC3329 is updated.
Consequences if not approved:	⌘	Specification may be incomplete and lead to implementation errors.

Clauses affected:	⌘	1.2, 7.1, 7.2, Annex H

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

**********the first change**********

1. 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] IETF RFC 3310 (2002): "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 2451 (1998): "The ESP CBC-Mode Cipher Algorithms ".

[21] ~~Draft-ietf-sip-sec-agree-05 (October 2002): "Security Mechanism Agreement for SIP Sessions".~~ IETF RFC 3329 (2002): " Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

**********the second change**********

7.1 Security association parameters

For protecting IMS signaling between the UE and the P-CSCF it is necessary to agree on shared keys that are provided by IMS AKA, and a set of parameters specific to a protection method. The security mode setup (cf. clause 7.2) is used to negotiate the SA parameters required for IPsec ESP with authentication, but without confidentiality.
The SA parameters that shall be negotiated between UE and P-CSCF in the security mode set-up procedure, are:

- **Integrity algorithm**

NOTE: What is called "authentication algorithm" in [13] is called "integrity algorithm" in this specification in order to be in line with the terminology used in other 3GPP specifications and, in particular, to avoid confusion with the authentication algorithms used in the AKA protocol.

The integrity algorithm is either HMAC-MD5-96 [15] or HMAC-SHA-1-96 [16].

Both integrity algorithms shall be supported by both, the UE and the P-CSCF as mandated by [13]. In the unlikely event that one of the integrity algorithms is compromised during the lifetime of this specification, this algorithm shall no longer be supported.

NOTE: If only one of the two integrity algorithms is compromised then it suffices for the IMS to remain secure that the algorithm is no longer supported by any P-CSCF. The security mode set-up procedure (cf. clause 7.2) will then ensure that the other integrity algorithm is selected.

- **SPI (Security Parameter Index)**

The SPI is allocated locally for inbound SAs. The triple (SPI, destination IP address, security protocol) uniquely identifies an SA at the IP layer. The UE shall select the SPIs uniquely, and different from any SPIs that might be used in any existing SAs (i.e. inbound and outbound SAs). The SPIs selected by the P-CSCF shall be different than the SPIs sent by the UE, cf. section 7.2.

NOTE: This allocation of SPIs ensures that protected messages in the uplink always differ from protected messages in the downlink in, at least, the SPI field. This thwarts reflection attacks. When several applications use IPsec on the same physical interface the SIP application should be allocated a separate range of SPIs.

The following SA parameters are not negotiated:

- Life type: the life type is always seconds;
- SA duration: the SA duration has a fixed length of 2^{32}-1;

NOTE: The SA duration is a network layer concept. From a practical point of view, the value chosen for "SA duration" does not impose any limit on the lifetime of an SA at the network layer. The SA lifetime is controlled by the SIP application as specified in clause 7.4.

- Mode: transport mode;
- Key length: the length of the integrity key IK_{ESP} depends on the integrity algorithm. It is 128 bits for HMAC-MD5-96 and 160 bits for HMAC-SHA-1-96.

Selectors:

The security associations (SA) have to be bound to specific parameters (selectors) of the SIP flows between UE and P-CSCF, i.e. source and destination IP addresses, transport protocols that share the SA, and source and destination ports.

- IP addresses are bound to a pair of SAs, as in clause 6.3, as follows:
  - inbound SA at the P-CSCF:
    The source and destination IP addresses associated with the SA are identical to those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.
  - outbound SA at the P-CSCF:
    the source IP address bound to the outbound SA equals the destination IP address bound to the inbound SA;
    the destination IP address bound to the outbound SA equals the source IP address bound to the inbound SA.

NOTE: This implies that the source and destination IP addresses in the header of the IP packet in which the protected SIP REGISTER message was received by the P-CSCF need to be the same as those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

- The transport protocol selector shall allow UDP and TCP.
- Ports:

1. The P-CSCF receives messages protected with ESP from any UE on one fixed port (the"protected port") different from the standard SIP port 5060. The number of the protected port is communicated to the UE during the security mode set-up procedure, cf. clause 7.2. No unprotected messages shall be sent to or received on this port. From a security point of view, the P-CSCF may receive unprotected messages from any UE on any port which is different from the protected port.

NOTE: The protected port is fixed for a particular P-CSCF, but may be different for different P-CSCFs.

2. For protected or unprotected outbound messages from the P-CSCF (inbound for the UE) any source port number may be used at the P-CSCF from a security point of view.

3. For each security association, the UE assigns a local port to send or receive protected messages to and from the P-CSCF ("protected port"). No unprotected messages shall be sent to or received on this port. The UE shall use a single protected port number for both TCP and UDP connections. The port number is communicated to the P-CSCF during the security mode set-up procedure, cf. clause 7.2. When the UE sends a re-REGISTER request, it shall always pick up a new port number and send it to the network. If the UE is not challenged by the network, the port number shall be obsolete. Annex H of this specification gives detail how the port number is populated in SIP message. From a security point of view, the UE may send or receive unprotected messages to or from the P-CSCF on any ports which are not the protected ports.

4. The P-CSCF is allowed to receive only REGISTER messages on unprotected ports. All other messages not arriving on the protected port shall be discarded by the P-CSCF.

5. The UE is allowed to receive only the following messages on an unprotected port:

   - responses to unprotected REGISTER messages;

   - error messages.

   All other messages not arriving on a protected port shall be discarded by the UE.

The following rules apply:

1. For each SA which has been established and has not expired, the SIP application at the P-CSCF stores at least the following data: (UE_IP_address, UE_protected_port, SPI, IMPI, IMPU1, ... , IMPUn, lifetime) in an "SA_table".

NOTE: The SPI is only required when initiating and deleting SAs in the P-CSCF. The SPI is not exchanged between IPsec and the SIP layer for incoming or outgoing SIP messages.

2. The SIP application at the P-CSCF shall check upon receipt of a protected REGISTER message that the source IP address in the packet header coincides with the UE's IP address inserted in the Via header of the protected REGISTER message. If the Via header does not explicitly contain the UE's IP address, but rather a symbolic name then the P-CSCF shall first resolve the symbolic name by suitable means to obtain an IP address.

3. The SIP application at the P-CSCF shall check upon receipt of an initial REGISTER message that the pair (UE_IP_address, UE_protected_port), where the UE_IP_address is the source IP address in the packet header and the protected port is sent as part of the security mode set-up procedure (cf. clause 7.2), has not yet been associated with entries in the "SA_table". Furthermore, the P-CSCF shall check that, for any one IMPI, no more than three SAs per direction are stored at any one time. If these checks are unsuccessful the registration is aborted and a suitable error message is sent to the UE.

NOTE: According to clause 7.4 on SA handling, at most three SAs per direction may exist at a P-CSCF for one user at any one time.

4. For each incoming protected message the SIP application at the P-CSCF shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by the pair (UE_IP_address, UE_protected_port) in the "SA_table". The SIP application at the P-CSCF shall further check that the IMPU associated with the SA in the "SA_table" and the IMPU in the received SIP message coincide. If this is not the case the message shall be discarded.

5. For each SA which has been established and has not expired, the SIP application at the UE stores at least the following data: (UE_protected_port, SPI, lifetime) in an "SA_table".

NOTE: The SPI is only required to initiate and delete SAs in the UE. The SPI is not exchanged between IPsec and the SIP layer for incoming or outgoing SIP messages.

6. When establishing a new pair of SAs (cf. clause 6.3) the SIP application at the UE shall ensure that the selected number for the protected port, as well as SPI number, do not correspond to an entry in the "SA_table".

NOTE: Regarding the selection of the number of the protected port at the UE it is generally recommended that the UE randomly selects the number of the protected port from a sufficiently large set of numbers not yet allocated at the UE. This is to thwart a limited form of a Denial of Service attack. UMTS PS access link security also helps to thwart this attack.

7. For each incoming protected message the SIP application at the UE shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by UE_protected_port in the "SA table". The source port selector is set to be a wildcard in the UE's IPsec database.

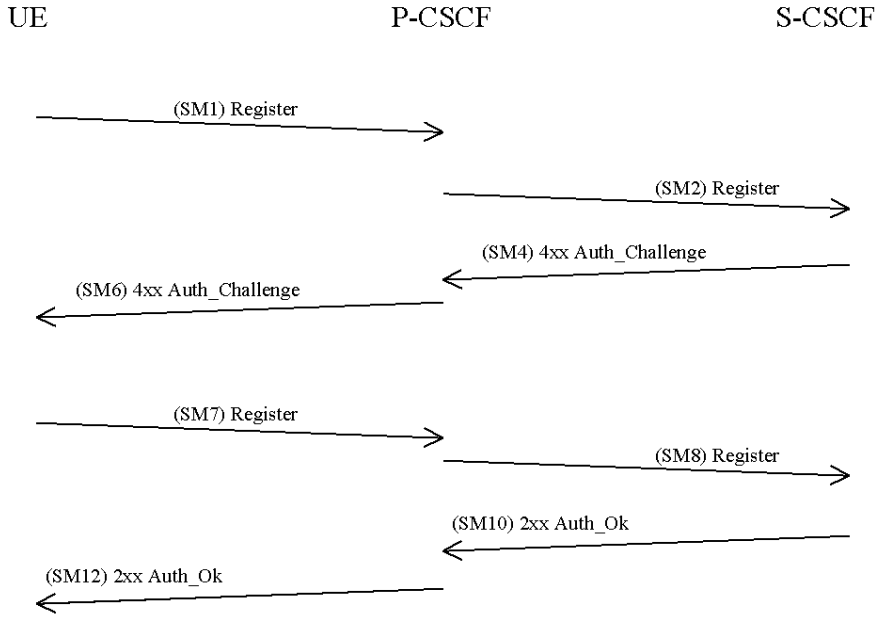
NOTE: If the integrity check of a received packet fails then IPsec will automatically discard the packet.

8. The lifetime of an SA at the application layer between the UE and the P-CSCF shall equal the registration period.

**********the third change**********

7.2 Set-up of security associations (successful case)

The set-up of security associations is based on [draft-IETF-sip-sec-agree21]. Annex H of this specification shows how to use [draft-IETF-sip-sec-agree21] for the set-up of security associations.
In this section the normal case is specified i.e. when no failures occurs. Note that for simplicity some of the nodes and messages have been omitted. Hence there are gaps in the numbering of messages, as the I-CSCF is omitted.



The UE sends a Register message towards the S-CSCF to register the location of the UE and to set-up the security mode, cf. clause 6.1. In order to start the security mode set-up procedure, the UE shall include a *Security-setup*-line in this message.
The *Security-setup-line* in SM1 contains the SPI numbers Security Parameter Index value and the protected port selected by the UE. It also contains a list of identifiers for the integrity algorithms which the UE supports.

SM1:
REGISTER(Security-setup = *SPI_U, Port_U, UE integrity algorithms list)*

SPI_U is the symbolic name of the SPI value (cf. section 7.1) spi that the UE selects. The syntax of spi is defined in Annex H.

Port_U is the symbolic name of a pair of port numbers (port1, port2) where port1 defines the destination port number for inbound messages at the UE that are protected, and port2 defines the source port number for outbound messages at the UE that are protected. The syntax of port1 and port2 is defined in Annex H.

Upon receipt of SM1, the P-CSCF temporarily stores the parameters received in the *Security-setup-line* together with the UE's IP address from the source IP address of the IP packet header, the IMPI and IMPU. Upon receipt of SM4, the P-CSCF adds the key IK_{IM} received from the S-CSCF to the temporarily stored parameters. The P-CSCF then selects the SPI for the inbound SA. The P-CSCF shall define the SPIs such that they are unique and different from any SPIs as received in the *Security-setup-line* from the UE.

NOTE: This rule is needed since the UE and the P-CSCF use the same key for inbound and outbound traffic.

In order to determine the integrity algorithm the P-CSCF proceeds as follows: the P-CSCF has a list of integrity algorithms it supports, ordered by priority. The P-CSCF selects the first integrity algorithm on its own list which is also supported by the UE.

The P-CSCF then establishes another pair of SAs in the local security association database.

The *Security-setup*-line in SM6 contains the SPI assigned by the P-CSCF and the fixed number of the protected port at the P-CSCF. It also contains a list of identifiers for the integrity algorithms which the P-CSCF supports.

SM6:
4xx Auth_Challenge(Security-setup = *SPI_P, Port_P, P-CSCF integrity algorithms list)*

SPI_P is the symbolic name of the SPI value (cf. section 7.1) spi that the P-CSCF selects. The syntax of spi is defined in Annex H.

Port_P is the symbolic name of the port number port1, where port1 defines the destination port number for inbound messages at the P-CSCF that are protected. The port number port2 of the P-CSCF shall be absent in Port_P. The syntax of port1 is defined in Annex H.

Upon receipt of SM6, the UE determines the integrity algorithm as follows: the UE selects the first integrity algorithm on the list received from the P-CSCF in SM 6 which is also supported by the UE.
The UE then proceeds to establish another pair of SAs in the local SAD.
The UE shall integrity-protect SM7 and all following SIP messages. Furthermore the integrity algorithms list received in SM6 shall be included:

SM7:
REGISTER(Security-setup = *P-CSCF integrity algorithms list)*

After receiving SM7 from the UE, the P-CSCF shall check whether the integrity algorithms list received in SM7 is identical with the integrity algorithms list sent in SM6. If this is not the case the registration procedure is aborted. The P-CSCF shall include in SM8 information to the S-CSCF that the received message from the UE was integrity protected. The P-CSCF shall add this information to all subsequent REGISTER messages received from the UE that have successfully passed the integrity check in the P-CSCF.
SM8:
REGISTER(Integrity-Protection = *Successful*, IMPI*)*

The P-CSCF finally sends SM12 to the UE. SM12 does not contain information specific to security mode setup (i.e. a Security-setup line), but with sending SM12 not indicating an error the P-CSCF confirms that security mode setup has been successful. After receiving SM12 not indicating an error, the UE can assume the successful completion of the security-mode setup.

********** the fourth change **********

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

The BNF syntax of [~~draft-ietf-sip-sec-agree~~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 [~~draft-ietf-sip-sec-agree~~21].

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].

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 ~~port1 is also used for outbound messages~~it is set to be a wildcard by the receiver.

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

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.