Technical Specification Group Services and System Aspects
Meeting #16, Marco Island, Florida, 10-13 June 2002

TSGS#16(02)0351

Source: SA WG3

Title: CR to 33.203: Requested Changes for SIP integrity (Rel-5)

Document for: Approval

Agenda Item: 7.3.3

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-020351	33.203	008		Rel-5	Requested Changes for SIP integrity	C	5.1.0	IMS-ASEC	S3-020317

3GPP TSG SA WG3 Security — S3#23 **S3-020317**

14 - 17 May 2002

Victoria, Canada

CR-Form-v5

CHANGE REQUEST

⌘ **33.203** **CR** **008** ⌘ **rev** **-** ⌘ Current version: **5.1.0** ⌘

*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 ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Requested Changes for SIP integrity
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	17 May, 2002
Category:	⌘	**C**
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:	⌘	The CR implements SA3's decision to use IPsec without IKE as the mechanism for SIP integrity. It also reflects changes in draft-IETF-sip-sec-agree on which the mechanism for SIP integrity relies. It further resolves some open issues and provides clarifications and editorial changes.
Summary of change:	⌘	The requested changes are described in detail in a companion contribution by Siemens to SA#23. The main changes are: - move Annexes B and D to main body; - replace generic text in section 7 with text specific for IPsec; - revise section 7.2 to reflect changes in draft-IETF-sip-sec-agree; - delete most of the text SA handling in section 7.3 as it is now contained in section 7.4 - treat security associations for TCP and UDP independently; - counter reflection attacks by unidirectional SPIs; - propose a key expansion function for HMAC-SHA-1-96; - update references.
Consequences if not approved:	⌘	The specification will not be complete, and not in line with the IETF.

Clauses affected:	⌘	2, 5.1.4, 6.3, 7.1, 7.2, Annex B, Annex D, Annex X(new), Annex Y(new)		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	TS 24.228, TS 24.229
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".

5 Security features

5.1.3 Confidentiality protection

~~Confidentiality mechanism need not be required for the first hop between the UE and the P-CSCF~~Confidentiality protection shall not be applied to SIP signalling messages between the UE and the P-CSCF. It is recommended to offer

encryption for SIP signalling at link layer i.e. between the UE and the RNC using the existing mechanisms as defined in [1].

Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [5].

5.1.4 Integrity protection

Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signaling, as specified in section 6.3. The following mechanisms are provided.

1. The UE and the P-CSCF shall negotiate the integrity algorithm that shall be used for the session, as specified in chapter 7.

2. The UE and the P-CSCF shall agree on ~~a~~ security associations, which include ~~identifyies~~ the integrity keys, ~~IK~~ that shall be used for the integrity protection. The mechanism is based on IMS AKA and specified in chapter 6.1.

3. The UE and the P-CSCF shall both verify that the data received originates from a node, which has the agreed ~~session~~ integrity key~~, IK~~. This verification is also used to detect if the data has been tampered with.

4. ~~The UE and the P-CSCF shall both verify the freshness of the message such that both r~~Replay attacks and reflection attacks ~~are~~ shall be mitigated.

Integrity protection between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [5].

6.2 Confidentiality mechanisms

No confidentiality mechanism is provided in this ~~version of the~~ specification, cf. section 5.1.3.

6.3 Integrity mechanisms

~~*[Editor's note: At this stage both Annex B and Annex C provides with potential measures for integrity protection. One of these solutions will be the normative solution.]*~~

IPsec ESP as specified in reference [13] shall provide integrity protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. IPSec ESP general concepts on Security Policy management, Security Associations and IP traffic processing as described in reference [14] shall also be considered. ESP integrity shall be applied in transport mode between UE and P-CSCF.

The method to set up ESP security associations (SAs) during the SIP registration procedure is specified in section 7. As a result of the registration procedure, two pairs of unidirectional SAs between the UE and the P-CSCF, one pair for TCP and one pair for UDP, shall be simultaneously established. Each pair consists of an SA for traffic from the UE to the P-CSCF (inbound SA at the P-CSCF) and an SA for traffic from the P-CSCF to the UE (outbound SA at the P-CSCF).

The integrity key IK_{ESP} is the same for the four simultaneously established SAs. The integrity key IK_{ESP} is obtained from the key IK_{IM} established as a result of the AKA procedure, specified in chapter 6.1, using a suitable key expansion function. This key expansion function depends on the ESP integrity algorithm and is specified in Annex Y of this specification.

The integrity key expansion on the user side is done in the UE. The integrity key expansion on the network side is done in the P-CSCF.

The anti-replay service shall be enabled in the UE and the P-CSCF on all established SAs.

7 Security association set-up procedure

The security association set-up procedure is necessary in order to decide what security services ~~that~~ to apply and when the security services start. In the IMS, authentication of users is performed during registration as specified in Section 6.1. Subsequent signaling communications in this session will be integrity ~~and optionally confidentiality~~ protected based on the keys derived during the authentication process.

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. section 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].

  Note: this, in particular, excludes the use of the NULL integrity algorithm.

  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 algorithm 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. section 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 most significant bit of any SPI allocated by the P-CSCF shall be "0" and the most significant bit of any SPI allocated by the UE shall be "1".

  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 section 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 protocol, and source and destination ports.

- IP addresses are bound to a pair of SAs, as in section 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 is either TCP or UDP.

- 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. section 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 port number may be used at the P-CSCF from a security point of view.

3. For each security association, the UE assigns a 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 may use different protected port numbers for TCP and UDP. The numbers of these ports are communicated to the P-CSCF during the security mode set-up procedure, cf. section 7.2. 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 protected ports.

[Editor's note: The condition that the UE sends and receives protected messages on the same port is not necessary from a security point of view. These ports could be made different, at the expense of one more parameter to be negotiated in the security mode set-up procedure, but they have to be fixed in the registration procedure.]

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, transport protocol, 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 given in the contact header of the protected REGISTER message. If the contact 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, for each transport protocol, the triple (UE_IP_address, UE_protected_port, transport protocol), 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. section 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 and per transport protocol 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 section 7.4 on SA handling, at most three SAs per direction and per transport protocol need to 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 section 7.4 on SA handling has been used. The SA is identified by the triple (UE_IP_address, UE_protected_port, transport protocol) 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, transport protocol, 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 two new pairs of SAs (cf. section 6.3) the SIP application at the UE shall ensure that, for each transport protocol, the selected number for the protected port does 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 section 7.4 on SA handling has been used. The SA is identified by the pair (UE_protected_port, transport protocol) in the "SA table"

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.

~~For protecting IMS signaling between the UE and the P-CSCF it is necessary to agree on shared keys provided by IMS AKA, on certain protection methods (e.g. an integrity protection method) and a set of parameters specific to a protection method, e.g. the cryptographic algorithm to be used. The parameters negotiated are typically part of the security association to be used for a protection method.~~

~~The security mode setup shall support the negotiation of different protection mechanisms. It shall be able to negotiate or exchange the SA parameters required for these different protection mechanisms. Although the supported protection mechanisms could be quite different, there is a common set of parameters that have to be negotiated for each of them. This set of parameters includes:~~

- ~~Authentication (integrity) algorithm, and optionally encryption algorithm;~~
- ~~SA_ID that is used to uniquely identify the SA at the receiving side;~~

~~- Key length: the length of encryption and authentication (integrity) keys is 128 bits.~~

~~Parameters specifically related to certain protection methods are kept in the annexes describing the protection methods.~~

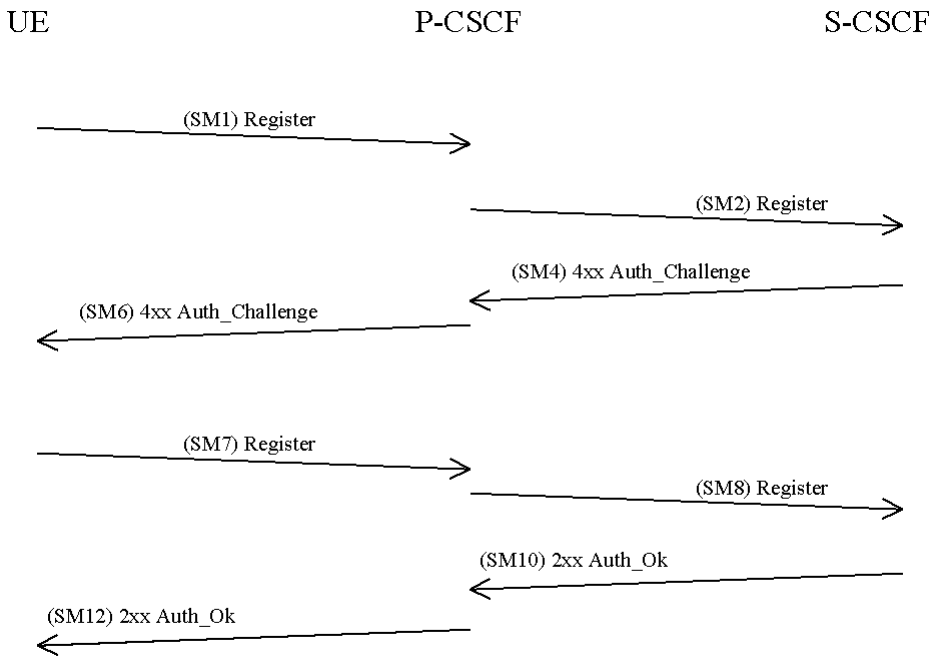
~~The SA between the UE and the P-CSCF will have a limited lifetime. The lifetime timer shall be the same as the registration timer, which is defined per contact address. When the UE registers the registration timer will be negotiated between the UE, the P-CSCF and the S-CSCF. The S-CSCF will be able to accept, decrease or increase the proposed expiration time from the UE and the final value is sent in the response to the UE. The expiry time in the UE will be shorter than the expiry time in the S-CSCF, such that the UE is able to re-register. For each new successful authentication the SA shall be updated. The S-CSCF shall align the expiration of subsequent registrations with any existing registration timer. The SA is deleted if the registration timers expires in the P-CSCF or in the S-CSCF.~~

~~[Editors Note: The support of different mechanisms is FFS.]~~

7.2 Set-up of security associations (successful case)

The set-up of security associations is based on [draft-IETF-sip-sec-agree]. Annex X of this specification shows how to use [draft-IETF-sip-sec-agree] 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. section 6.1. ~~This has been described in 6.1.~~ In order to start the security mode set-up procedure the UE shall include a *Security-setup-: line* in this message.~~,~~ ~~including the protection method, the proposed set of integrity algorithms, the proposed set of confidentiality algorithms (optional), the SA_ID and an optional *info* field. The *info* field is reserved for method specific use, so any method supported by the security mode set-up must specify whether and how to use the *info* field. The SA_ID_U shall be chosen so that it uniquely identifies the (unidirectional) inbound SA at the UE side.~~

The *Security-setup-line* in SM1 contains the SPIs and the numbers of the protected ports assigned by the UE for the SAs for TCP and UDP. It also contains a list of identifiers for the integrity algorithms which the UE supports.

~~Elements in [...] are optional.~~

SM1:
REGISTER(Security-setup = *SPI_U_TCP, SPI_U_UDP, Port_U_TCP, Port_U_UDP, UE integrity algorithms list)*
~~integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info]), IMPI, IMPU)~~

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 SPIs for the inbound SAs for TCP and UDP.
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 the two pairs of SAs in the local security association database.
~~The P-CSCF shall choose exactly one of the proposed mechanisms respectively and exactly one of the proposed algorithms respectively based on the policies that applies and send the selected mechanisms and algorithms to the UE in SM6.~~

~~The SA_ID_P shall be chosen in such a way that it uniquely identifies the (unidirectional) inbound SA at the P-CSCF side, within the P-CSCF.~~

~~[Editors Note: It is FFS if the HN shall take part in the negotiation of algorithms.]~~

The *Security-setup-:* line in SM6 contains the SPIs assigned by the P-CSCF for the SAs for TCP and UDP 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:
~~401 Unauthorized response~~ 4xxAuth_Challenge~~4xx Auth_Challenge~~(Security-setup = *SPI_P_TCP, SPI_P_UDP, Port_P, P-CSCF integrity algorithms list)*
~~*integrity mechanism, [confidentiality mechanism], integrity algorithm, [confidentiality algorithm], SA_ID_P, [info],* IMPI)~~

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 the two pairs of SAs in the local SAD.

The UE shall ~~in~~ integrity-protect SM7 and all following SIP messages.~~start the integrity protection – and optionally the confidentiality protection – of the whole SIP-message by setting up security associations according to mechanisms and the parameters negotiated in SM1 and SM6, and applying the corresponding protection to the SIP-message.~~
Furthermore the integrity algorithms list ~~Security-setup: line sent~~ received in SM6~~1~~ shall be included:

SM7:
REGISTER(Security-setup = *P-CSCF integrity algorithms list)*
~~*integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info],* IMPI)~~

After receiving SM7 from the UE, the P-CSCF shall ~~compare~~ check whether the integrity algorithms list ~~the Security-Setup line of~~ received in ~~this message~~SM7 is identical with the integrity algorithms list ~~Security-Setup line received~~ sent in SM6~~1.~~. If this is not the case the registration procedure is aborted. The P-CSCF shall include in SM8 ~~include~~ 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 set-up (i.e. a Security-setup- line), but with sending SM12 not indicating an error the P-CSCF confirms that security mode set-up has been successful. After receiving SM12 not indicating an error, the UE can assume the successful completion of the security-mode setup.

~~[Editors Note: It is FFS if the HN shall take part in the negotiation process.]~~

Annex B (informative): Mechanisms for IPSec based solution

[Editors Note: If the IPSec solution is finally chosen the chapters below shall be moved into the main body of this TS in the corresponding sections.]

B.1 [6.2] Confidentiality mechanisms

IPsec ESP may optionally be implemented for providing confidentiality of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. If ESP confidentiality is used, it shall be applied in transport mode between UE and P-CSCF. If ESP confidentiality is provided, it is always provided in addition to ESP integrity protection.

The SAs that are required for ESP shall be derived from the 128-bit integrity key CK_{IM} generated through IMS AKA, as specified in chapter 6.1.

If confidentiality is required, for each direction, there is one ESP SA for both confidentiality and integrity that shall be used between the UE and the P-CSCF. The encryption transform is identical for the two SAs in either direction. The encryption key for the SA inbound from the P-CSCF is CK.

The encryption key for the SA inbound from the P-CSCF is CK_{IM_in}. The encryption key for the SA outbound from the P-CSCF is CK_{IM_out}.

The encryption keys are derived as $CK_{IM\_in} = h1(CK_{IM})$ and $CK_{IM\_out} = h2(CK_{IM})$ using suitable key derivation functions h1 and h2.

The encryption key derivation on the user side is done in the ISIM. The encryption key derivation on the network side is done in the P-CSCF.

The method to set up ESP security associations during the SIP registration procedure is specified in chapter 7.

B.2 [6.3] Integrity mechanisms

IPsec ESP shall provide integrity protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. ESP integrity shall be applied in transport mode between UE and P-CSCF.

The SAs that are required for ESP shall be derived from the 128-bit integrity key IK generated through IMS AKA, as specified in chapter 6.1. The transform used for the ESP SA shall be negotiated as specified in chapter 7. ESP shall use two unidirectional SAs between the UE and the P-CSCF, one in each direction. The integrity algorithm is identical for both SAs.

The integrity key for the SA inbound from the P-CSCF is IK_{IM_in}. The integrity key for the SA outbound from the P-CSCF is IK_{IM_out}.

The integrity keys are derived as $IK_{IM\_in} = h1(IK_{IM})$ and $IK_{IM\_out} = h2(IK_{IM})$ using suitable key derivation functions h1 and h2. (They may be the same as those in section 6.2.)

The integrity key derivation on the user side is done in the ISIM. The integrity key derivation on the network side is done in the P-CSCF.

The method to set up ESP security associations during the SIP registration procedure is specified in chapter 7.

Annex D (informative): Set-up procedures for IPSec based solution

[Editors Note: If the IPSec solution is finally chosen the chapters below shall be moved into the main body of this TS in the corresponding sections.]

This section is based on section 7 and provides additional specification for the support of IPsec ESP.

D.1 Security association parameters

The SA parameters, identifiers and attributes that shall be negotiated between UE and P-CSCF, are

- ESP transform identifier
- Authentication (integrity) algorithm
- SPI

Further parameters:

- Life type: the life type is always seconds
- SA duration: the SA duration has a fixed length of 2^{32}-1.
- Key length: the length of encryption and authentication (integrity) keys is 128 bits.

Selectors:

The security associations (SA) have to be bound to specific parameters (selectors) of the SIP flows between UE and P-CSCF, i.e. IP addresses and ports. Both sides have to use the same policy here, but since the required selectors will be known from the SIP messages, there is no need to negotiate them. However, it is critical to keep the source IP address and source port number, the selector pair unique in P-CSCF. The P-CSCF must reject any REGISTER message sent from a valid SA's selector pair corresponding to a different IMPI than the one that is bound to this selector pair. The only parameter that shall be negotiated, is a fixed port for specific unprotected SIP messages at the P-CSCF:

1. For the inbound SA at the P-CSCF (outbound for the UE) the P-CSCF shall use a fixed port. This may be port 5060 as the standard SIP port, or any other fixed port where the server accepts SIP messages from the UE. In addition, another port for specific unprotected SIP messages from the UE to the server is fixed.
   For the outbound SA at the P-CSCF (inbound for the UE) ANY port number shall be allowed at the P-CSCF.
2. On the UE side, the SIP UAs shall use the same port for both sending and receiving SIP signalling to the P-CSCF.
3. If there are multiple SIP UAs belonging to different ISIMs in one UE they shall use different SAs and bind them to different ports on the UE side.
4. The UE may send only the following messages to the fixed port for unprotected messages:
   - initial REGISTER message;
   - REGISTER message with network authentication failure indication;
   - REGISTER message with synchronization failure indication.

   All other messages incoming on this port must be discarded by the SIP application on the P-CSCF.

[Editors' note:It is ffs whether case 3 can actually occur.]

For each incoming message the SIP application must verify that the correct inbound SA associated with the public ID (IMPU) given in the SIP message has been used. This shall be done by verifying that the correct source IP address and source port bound to the public ID (IMPU) of the SIP message have been used for sending the message.

~~D.2 Security mode setup for IPsec ESP~~

~~This section describes how the security mode setup described in chapter 7 shall be used for negotiating ESP as protection mechanism and setting up the parameters required by ESP.~~

~~D.2.1 General procedures specific to the ESP protection mechanism~~

~~The integrity and encryption mechanisms both have the value "esp". The fields SA_ID_U and SA_ID_P carry the SPI values to be exchanged, to identify the ESP SAs.~~

~~The P-CSCF shall use an unprotected port to be able to receive specific unprotected messages. This unprotected port has to be communicated to the UE, by using the *info* field of message SM6. This unprotected port is required, when an IPsec SA is already in place at the P-CSCF, but the UE due to any reason is not able to use this SA. In this case, the UE shall send error messages or a new REGISTER message in the clear to the P-CSCF port received in the *info* field within SM6. Otherwise at the P-CSCF side, ESP would simply drop all IP packets from the UE that fail the integrity check.~~

~~The error messages that shall be sent in the clear from the UE to the P-CSCF are these for network authentication failures (sections 7.3.1.2) and synchronization failures (section 7.3.1.3).~~

~~D.2.2 Handling of user authentication failure~~

~~(This extends the content of chapter 7.3.1.1 and 7.3.3.3 for IPsec ESP)~~

~~In the case of a user authentication failure, the user will usually not be able to use a security association with the correct key material. Therefore, when using ESP for integrity protection and encryption, this will cause SM7 to be dropped at the P-CSCF IP(sec) layer due to a failed integrity check within ESP processing.~~

~~As SM7 will not reach the P-CSCF IMS application, the P-CSCF shall implement a timer for the authentication process. When a message is received that passes the integrity-check and successfully completes the authentication, it is immediately processed. However, if during the registration timer the P-CSCF receives packets that cannot be verified, it discards them. At the end of the registration timer, it reports an authentication failure back to the home network.~~

~~D.2.3 Authenticated re-registration procedures specific to the ESP protection mechanism~~

~~The new security associations SA11 and SA12 shall be bound to a new port on the UE side. This new port shall be communicated by the UE in the *info* field of the first REGISTER message SM1.~~

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

tba

Annex Y (normative): Key expansion functions for IPsec ESP

If the selected authentication algorithm is HMAC-MD5-96 then $IK_{ESP} = IK_{IM}$.

If the selected authentication algorithm is HMAC-SHA-1-96 then IK_{ESP} is obtained from IK_{IM} by appending the 32 most significant bits of IK_{IM} to IK_{IM}.