**3GPP TSG SA WG3 Security — S3#20** **S3-010504**

**16 - 19 October, 2001**

**Sydney, Australia**

**Source:** **Siemens**

**Title:** **Requested changes to TS 33.203 v060 concerning security mode set-up**

**Document for:** **Discussion and Decision**

**Agenda Item: 7.3**

**Abstract**

*TS 33.203 is not yet under change control. This contribution is nevertheless written in the form of a change request to facilitate inclusion in TS 33.203. The sections given in this contribution replace chapter 7, "Security mode set-up procedure" and both annexes B and D.*

*The goal of the proposed changes is to have a* ***generalised security mode set-up procedure in the main body of TS 33.203*** *that supports the negotiation of different mechanisms for integrity protection and encrpytion, and is independent of any specific mechanism (SIP layer protection or IPsec ESP). So what basically has been done is that all text specific to IPsec ESP has been moved from chapter 7 to the informative annex D.*

*The updated chapter 7 now specifies this generalised security mode set-up procedure.*

*Annex D has been updated to specify the parts of security mode setup specific to the integrity/encryption method IPsec ESP.*

*Besides these changes the updated annex B replaces the current proposal for deriving different keys for the different SAs in place between UE and P-CSCF.*

*To make the changes to TS 33.203 v060 proposed here visible all revisions in TS 33.203 v060 were accepted. The revision marks you find below indicate the changes proposed here.*

# 7 Security mode set-up procedure

The security mode setup procedure is necessary in order to decide when and how the security services start. In the IM CN SS authentication of users is performed during registration as 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 mode supported parameters

For protecting IMS access network signaling between the UE and the P-CSCF it is necessary to agree, in addition to the 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:~~Parameters, identifiers and attributes that shall be negotiated between UE and P-CSCF, are~~

- Authentication (integrity) algorithm, and optionally encryption algorithm

~~-Life type: the life type is always seconds~~

- SA lifetime~~duration~~: ~~the SA duration has a fixed length of $2^{32}$-1.~~

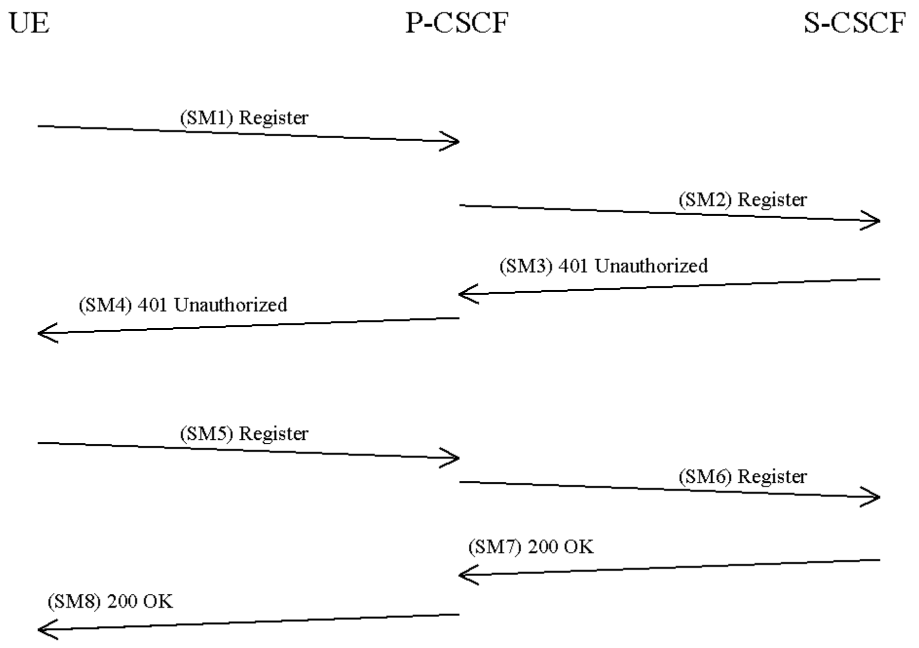
- SA_ID, that is used to uniquely identify the SA at the receiving side.

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

~~*[Editors Note:*~~ Parameters specifically related to ~~IPSec~~certain protection methods are kept in ~~Annex D~~the according annexes describing the protection methods. ~~*-and should be moved into this section if that solution is finally chosen.]*~~

# 7.2 Set-up of security associations (successful case)

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.



The UE sends a Register message towards the S-CSCF for authentication purposes. This has been described in 6.1. In order to ~~setup the security services~~start security mode setup the UE shall include a *Security-setup:* line in this message, including the protection method, the proposed set of integrity~~security~~ 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. ~~In this case a list of n integrity algorithms and a list of m confidentiality algorithms are proposed.~~ The SA_ID_U~~PI_U~~ shall be chosen in such a way that it uniquely identifies~~y~~ the (unidirectional) inbound SA at the UE side, within the UE.

Elements in [...] are optional.

SM1:

REGISTER sip: ----

Via: ----
From: IMPI

To: IMPU

Call-ID: ----

Cseq: 1 REGISTER

...

Security-setup: ~~*esp*~~ *integrity mechanism | [confidentiality mechanism] | integrity algorithms list | [confidentiality algorithms list ]| SA_ID*~~*PI*~~*_U | [info]*

Content-Length: 0

~~*[Editors Note: The parameters esp and SPI_U are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_U should probably defined for the SIP-level protection solution]*~~

The P-CSCF shall choose exactly one of the proposed mechanisms, respectively, and exactly one of the proposed algorithms, respectively, based on the policy that applies and send the selected mechanisms and algorithms to the UE in SM4.

The SA_ID_P~~PI_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: The unprotected port specifies the port where the P-CSCF is willing to accept unprotected error messages sent by the UE.]*~~

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

SM4:

SIP/2.0 401 Unauthorized
Via: ----
From: IMPI

To: IMPU

Call-ID: ----

Cseq: 1 REGISTER

...

Security-setup: *integrity mechanism | [confidentiality mechanism]*~~esp~~ | *integrity algorithm | [confidentiality algorithm] | SA_ID*~~*PI*~~ _P ~~*| unprotected_port*~~*| [info]*

Content-Length: 0

~~*[Editors Note: The parameters esp and SPI_P are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_P should probably defined for the SIP-level protection solution. The unprotected port is only valid for the IPSec solution and shall be removed if Sip-level protection is chosen. The unprotected port for IPSec specifes what port shall be used for error messages sent from the UE.]*~~

The UE shall in SM5 start the integrity protection – and optionally the confidentiality protection -of the whole SIP-message by setting up security associations according to the mechanisms and parameters negotiated in SM1 and SM4, and applying the corresponding protection to the SIP-message. Furthermore the *Security-setup*: line sent in SM1 shall be included:

SM5:

REGISTER sip: ----

Via: ----
From: IMPI

To: IMPU

Call-ID: ----

Cseq: 1 REGISTER

Security-setup: *integrity mechanism | [confidentiality mechanism]* ~~*esp*~~ | *integrity algorithms list | [confidentiality algorithms list ]| SA_ID_U*~~*PI_U*~~ *| [info]*

...

Content-Length: 0

~~*[Editors Note: The parameters esp and SPI_U are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_U should probably defined for the SIP-level protection solution]*~~

After receiving SM5 from the UE, the P-CSCF shall compare the Security-Setup line of this message with the Security-Setup line received in SM1.

The P-CSCF finally sends SM8 to the UE. SM8 does not contain information specific to security mode setup (i.e. a Security-setup line), but with sending SM8 not indicating an error the P-CSCF confirms that security mode setup has been sucessful. After receiving SM8 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.]*

## 7.3 Error cases in the set-up of security associations

Whenever an expected message is not received after a time-out the receiving entity considers the registration to have failed.

*[Editor's note: Clarify, how SIP registration handles the inconsistent state that is created by a lost SM8 message]*

## 7.3.1 Error cases related to IMS AKA

Errors related to IMS AKA failures are specified in section 6.1. However, this section additionally describes how these shall be treated, related to security setup.

*[Editors Note: It is FFS if this is appropriate taking DoS attacks into account.]*

### 7.3.1.1 User authentication failure

In this case the authentication of the user fails in the network due an incorrect RES. The S-CSCF will send a 401 Unauthorized message SM7, which will pass through the already established SA to the UE as SM8.

Note, that this failure will already occur in SM5, when the UE does not use the correct integrity key IK. In this situation, the P-CSCF will receive protected packets that cannot be verified.~~ and therefore will be discarded.~~

~~In order to handle this situation, 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.~~

It may seem from the above discussion that there is no requirement to check the RES at the S-CSCF since a false RES sent by a UE will never reach the S-CSCF. However, it is still necessary to check RES at the S-CSCF since this prevents a P-CSCF from registering a UE without performing user authentication. It therefore reduces S-CSCF trust in the P-CSCF.

### 7.3.1.2 Network authentication failure

If the UE is not able to successfully authenticate the network, the UE is not able to create the key IK and therefore the SA with the P-CSCF, such that it is not possible to send SM5 in a protected way. Since the P-CSCF already expects SIP messages from the UE to be protected, and is not already aware of any errors, the P-CSCF shall accept such REGISTER messages indicating network authentication failure in the clear.

So the UE sends a new register message SM5, indicating a network authentication failure, to the P-CSCF, without protection. SM5 should not contain the security-setup line of the first message.

~~*[Editors Note: For IPSec failure messages due to a netowork authentication failure shall be sent on a different port, the unprotected port. This text shall be moved into the main body if IPSec is finally chosen.]*~~

### 7.3.1.3 Synchronisation failure

In this situation, the UE observes that the AUTN sent by the network in SM4 contains an out-of-range sequence number. The UE shall sends a new register message SM5 to the P-CSCF in the clear, indicating the synchronization failure. SM5 should not contain the Security-Setup line of the first message, and the P-CSCF shall keep the security-setup state created after receiving SM1 from the UE.

~~*[Editors Note: For IPSec failure messages due to synchronization failures shall be sent on a different port, the unprotected port. This text shall be moved into the main body if IPSec is finally chosen.]*~~

## 7.3.2 Error cases related to the Security-Set-up

### 7.3.2.1 Unacceptable proposal set

In this case the P-CSCF cannot accept the proposal set sent by the UE in the Security-Set-up command of SM1. SM4 shall respond to SM1 with indicating a failure, by sending a 403 Forbidden error message.

The P-CSCF therefore shall modify the message SM2 such that the S-CSCF sends a 403 Forbidden error message back to the UE in SM3/4 and the registration process is finished.

SM2:

REGISTER sip: ----

Via: ----
From: IMPI

To: IMPU

Call-ID: ----
Cseq: 1 REGISTER

Security-setup: *integrity mechanism | [confidentiality mechanism]~~ esp~~ | integrity algorithms list | [confidentiality algorithms list ]| SA_ID~~PI~~_U | [info]*

Failure: *NoCommonIntegrityAlgorithm*

Content-Length: 0

~~*[Editors Note: The parameters esp and SPI_U are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_U should probably defined for the SIP-level protection solution]*~~

*[Editors Note: It is FFS how the exact mechanism shall be for the Unacceptable proposal set case. The editor believes that the S-CSCF is the registrar and hence the P-CSCF should only be able to modify the headers and not send back responses. The failure response should be sent by the S-CSCF. This however has not been agreed.]*

### 7.3.2.2 Unacceptable algorithm choice

If the P-CSCF sends in the security-setup line of SM4 an algorithm that is not acceptable for the UE (i.e. has not been proposed), the UE shall not continue to create a security association with the P-CSCF and shall terminate the registration procedure.

### 7.3.2.3 Failed consistency check of Security-Set-up lines

This is the case if the Security-Setup line in SM5 from the UE to the P-CSCF cannot be verified, so the Security-Setup line of the unprotected SM1 and the Security-Setup line of the protected SM5 do not match. The P-CSCF shall respond to the UE by sending a 403 Forbidden error message in SM8. The P-CSCF therefore shall modify the message SM6 such that the S-CSCF sends a 403 Forbidden error message back to the UE in SM7/8 and the registration process is finished.

SM6:

REGISTER sip: ----

Via: ----
From:  IMPI

To: IMPU

Call-ID: ----
Cseq: 1 REGISTER

Security-setup: *integrity mechanism | [confidentiality mechanism]* ~~*esp*~~ *| integrity algorithms list | [confidentiality algorithms list ]| SA_ID*~~*PI*~~*_U | [info]*

Failure: *NoCommonIntegrityAlgorithm*

Content-Length: 0

~~*[Editors Note: The parameters esp and SPI_U are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_U should probably defined for the SIP-level protection solution]*~~

*[Editors Note: It is FFS how the exact mechanism shall be for the Unacceptable proposal set case. The editor believes that the S-CSCF is the registrar and hence the P-CSCF should only be able to modify the headers and not send back responses. The failure response should be sent by the S-CSCF. This however has not been agreed.]*

## 7.3.3 Authenticated re-registration

If the registration is a re-registration, a pair of security associations between UE and P-CSCF is already active.

*[Editors Note: It is FFS if these SAs shall protect the first two messages of the authenticated re-registration, i.e. SM1 and SM4.]*

Before SM5 is sent by the UE, both peers shall replace the existing SA by the new SA negotiated during these first two messages.

### 7.3.3.1 Handling of security associations in authenticated re-registrations (successful case)

~~*[Editors Note: The following part of the description is independent of the particular mechanism for integrity and confidentiality protection.]*~~

Before re-registration begins the following SAs exist:

- SA1 from UE to P-CSCF
- SA2 from P-CSCF to UE

The re-registration then is as follows:

1) The UE sends SM1 to re-register with the IMS, using the existing SA1 to the P-CSCF. As in the case of a new registration, a list of parameters to be negotiated in a security association set-up is included.

*[Editors Note: It is FFS if the SA1 shall be used for SM1 or not]*

2) The P-CSCF waits for the response SM3 from the S-CSCF and then sends SM4 to the UE, using SA2. As in the case of a new registration, the parameters selected for the new security associations are included. The P-CSCF then creates two new security associations, in parallel to the existing ones, in its database:

- SA11 from UE to P-CSCF

- SA12 from P-CSCF to UE

3) If SM4 could be successfully processed by the UE, the UE also creates the new SAs SA11 and SA12 in its database. The UE then sends SM5 to the P-CSCF. As in the case of a new registration, the authentication response and the list of parameters repeated from message 1 are included. SM5 is protected with the new SA11.

4) The P-CSCF waits for the response SM7 from the S-CSCF and then sends SM8 to the UE, using the new SA 12.

5) After the reception of SM8 by the UE, the re-registration is complete.

The UE now uses the new SAs for all subsequent messages. The old (outbound) SA1 is deleted. The old (inbound) SA2 must be kept until a further SIP message protected with the new inbound SA12 is successfully received from the P-CSCF.

The P-CSCF keeps all four SAs with the UE active until a further SIP message protected with the new inbound SA11 is successfully received from the UE. In the meantime, the P-CSCF continues to use the old SA2 for outbound traffic to the UE.

*~~Aspects specific to the use of IPsec/ESP:~~*

~~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 first REGISTER message SM1 in the list of parameters to be negotiated in a security association set-up.~~

*~~[Editor's note: If it is desired to use identical messages for new registrations and re-registrations then a new port can also be included in the first message for new registrations although it is not strictly needed there.]~~*

### 7.3.3.2 Error cases related to authenticated re-registration

Whenever an expected message is not received after a time-out the receiving entity considers the registration to have failed. The receiving entity then deletes any new security associations it may have established and continues to use the old ones if they have not yet expired.

If the registration protocol goes well up to the last message SM8, and SM8 is sent by the P-CSCF, but not received by the UE , then the UE has only the olds SAs available (after the time-out), but the P-CSCF cannot know this. Therefore, the P-CSCF continues to use the old SA2 for outbound traffic to the UE, but keeps both, old and new SAs. The new SAs are deleted when a message is received from the UE which is protected with the old SA, or if a REGISTER message is received on the port where the P-CSCF accepts specific unprotected messages.

### 7.3.3.3 Error cases related to IMS AKA

User authentication failure

The S-CSCF will send a 401 Unauthorized message SM7, which will pass through the already established SA to the UE as SM8. Afterwards, both, the UE and the P-CSCF delete the new SAs.

Network authentication failure

If the UE is not able to successfully authenticate the network, it does not establish a new SA. The UE sends a REGISTER message SM5 indicating a network authentication failure to the P-CSCF, using the already established SA. The P-CSCF deletes the new SAs after receiving this message.

Synchronisation failure

If the UE notices a synchronisation failure it does not establish a new SA. The UE sends a message SM5, indicating the synchronisation failure, to the P-CSCF, using the already established SA. The P-CSCF deletes the new SA after receiving this message.

### 7.3.3.4 Error cases related to the Security-Setup

Unacceptable proposal set

The message SM4 shall respond to the first REGISTER message SM1 with a 403 Forbidden, using the already established SA. Neither side establishes a new SA.

The P-CSCF therefore shall modify the message SM2 such that the S-CSCF sends the 403 Forbidden error message back to the UE in SM3/4 and the registration process is finished.

SM2:

REGISTER sip: ----

Via: ----
From: IMPI

To: IMPU

Call-ID: ----
Cseq: 1 REGISTER

Security-setup: *integrity mechanism | [confidentiality mechanism] ~~esp~~ | integrity algorithms list | [confidentiality algorithms list ]| SA_ID~~PI~~_U | [info]*

Failure: *NoCommonIntegrityAlgorithm*

Content-Length: 0

*[Editors Note: It is FFS how the exact mechanism shall be for the Unacceptable proposal set case. The editor believes that the S-CSCF is the registrar and hence the P-CSCF should only be able to modify the headers and not send back responses. The failure response should be sent by the S-CSCF. This however has not been agreed.]*

*~~[Editors Note: The parameters esp and SPI_U are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_U should probably defined for the SIP-level protection solution]~~*

Failed consistency check of Security-Set-up lines

This is the case if the Security-Setup line in SM5 from the UE to the P-CSCF cannot be verified, so the Security-Setup line of the unprotected SM1 and the Security-Setup line of the protected SM5 do not match. In this case the P-CSCF shall respond to the UE by sending a 403 Forbidden error message in SM8 using the already established SA. Both sides delete the new SAs.

The P-CSCF therefore shall modify the message SM6 such that the S-CSCF sends the 403 Forbidden error message back to the UE in SM7/8 and the registration process is finished.

SM6:

REGISTER sip: ----

Via: ----
From: IMPI

To: IMPU

Call-ID: ----
Cseq: 1 REGISTER

Security-setup: *integrity mechanism | [confidentiality mechanism] ~~esp~~ | integrity algorithms list | [confidentiality algorithms list ]| SA_ID~~PI~~_U | [info]*

Failure: *NoCommonIntegrityAlgorithm*

Content-Length: 0

*[Editors Note: It is FFS how the exact mechanism shall be for the Unacceptable proposal set case. The editor believes that the S-CSCF is the registrar and hence the P-CSCF should only be able to modify the headers and not send back responses. The failure response should be sent by the S-CSCF. This however has not been agreed.]*

*~~[Editors Note: The parameters esp and SPI_U are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_U should probably defined for the SIP-level protection solution]~~*

Annexes are only to be used where appropriate:

# Annex <A> (normative): <Normative annex title>

# 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

~~*[Editor's note: This section shall deal with cipher algorithms]*~~

~~For access to IMS through UMTS no cipher algorithms are specified for IM CN SS other than those provided by UMTS R´99 i.e. [1] and Network Domain Security [5].~~

~~*[Editor's note: No other accesses than UMTS are within the scope of R5. Since it is optional to implement the text above seems too stringent. Hence the editor believes that it would be good if also confidentiality mechanisms where defined.]*~~

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 ~~use~~ 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 encryption key for the SA outbound from the P-CSCF is CK$_{MOD}$~~

~~[Note: CK$_{MOD}$ is a suitable modification of CK. An example of a suitable modification is a rotation of the key bits by n bits, where n remains to be determined.]~~

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 ~~use~~ be dervied from the 128-bit integrity key IK$_{IM}$ 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 integrity key for the SA inbound from the P-CSCF is IK. The integrity key for the SA outbound from the P-CSCF is~~ ~~$IK_{MOD}$~~

~~[Note:~~ ~~$IK_{MOD}$~~ ~~is a suitable modification of IK. An example of a suitable modification is a rotation of the key bits by n bits, where n remains to be determined.]~~

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

# Annex C (Informative): Mechanisms for SIP-level solution

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

## C.1 6.2 Confidentiality mechanisms

*[Editor’s note: This section shall deal with cipher algorithms]*

For access to IMS through UMTS no cipher algorithms are specified for IM CN SS other than those provided by UMTS R´99 i.e. [1] and Network Domain Security [5].

*[Editor’s note: No other accesses than UMTS are within the scope of R5. Since it is optional to implement the text above seems too stringent. Hence the editor believes that it would be good if also confidentiality mechanisms where defined.*

## C.2 6.3 Integrity mechanisms

# 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 chapter is based on chapter 7 and provides additional specification for the support of IPsec ESP.

## D.1 ~~7.1~~ 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 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. The only parameter that shall be negotiated, is a 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.

[Note: It is ffs whether case 3 can actually occur.]

# 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 mechanism 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 SM4. 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 SM4. 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 SM5 to be dropped at the P-CSCF IP(sec) layer due to a failed integrity check within ESP processing.

As SM5 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.