3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010099**

14 September, 2001

Sophia Antipolis, France

Source: **Siemens**

Title: **Requested changes to TS 33.203 v050**

Document for: **Discussion and Decision**

Agenda Item:

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. It implements the changes resulting from the proposals made in the companion contributions "IPsec for Integrity protection between UE and P-CSCF" and "IPsec SA setup procedures between UE and P-CSCF", also submitted to this meeting. To make the changes to TS 33.203 v050 proposed here visible all revisions in TS 33.203 v050 were accepted. The revision marks you find below indicate the changes proposed here.

5.1.1 Confidentiality protection

[Editor's note: This section shall deal with what confidentiality protection that is provided between different nodes both inter domain, intra domain and the UE]

IP-based services will get protection by the confidentiality protection defined in R'99 at the bearer level. In R'99 confidentiality protection is provided for signaling data and user data between the UE and the serving RNC. The serving RNC retrieves the cipher key CK from the SN. The ciphering protection for UMTS is optional to use.

For UMTS access confidentiality protection for SIP signaling can either rely on the confidentiality mechanisms provided by UMTS and mechanisms provided by Network Domain Security, cf. [5],~~.~~ or optionally implement end-to-end confidentiality at the IP level between UE and P-CSCF, as specified in section 6.2.

~~*[Editor's note: It is optional to implement confidentiality protection and it should be applied at the same level as the integrity protection.]*~~

5.1.2 Integrity protection

~~*[Editor's note: This section shall deal with what integrity protection that is provided between different nodes both inter domain, intra domain and the UE]*~~

Integrity protection shall be used end-to-end at the IP level 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 what integrity algorithm ~~that~~ shall be used for the session, specified in chapter 7.

2. The UE and the P-CSCF shall agree on an integrity key, IK_{IM} that shall be used ~~when calculating a MAC~~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 ~~make a MAC check to~~ verify that the data received originates from a node which has the agreed session key, IK_{IM}. This check is also used for detecting if the data has been tampered with by a man-in-the-middle.

~~[Editor's note: It is FFS at what layer the SIP signaling shall be protected. It can be placed from the IP-Level up to the SIP-level.]~~

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 security associations (SA) required for ESP shall use 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_{IM}. The encryption key for the SA outbound from the P-CSCF is CK_{IM_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.

6.3 Integrity mechanisms

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

~~[Editor's note: the following mechanisms are FFS:~~

~~data integrity protection method~~

~~etc]~~

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 security associations (SA) required for ESP shall use 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}. The integrity key for the SA outbound from the P-CSCF is IK_{IM_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.

7 Security association set-up procedure ~~mode set-up~~

~~*[Editor's note: the following mechanisms are FFS:*~~

~~*Key settings*~~

~~*Mechanisms for ciphering and integrity mode negotiation*~~

~~*Key lifetime*~~

~~*Key identification*~~

~~*When to start encryption and integrity protection]*~~

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 keys derived during the authentication process.

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

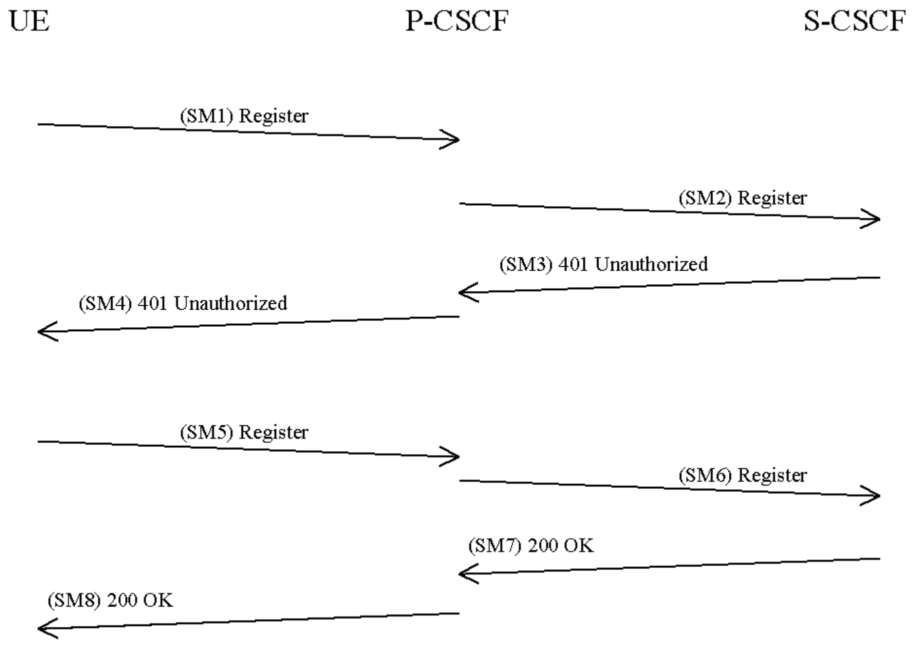
- REGISTER message with synchronization failure indication

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.]

7.2 Set-up of security associations ~~services~~ (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 the UE shall include a proposed set of security algorithms. In this case a list of n integrity algorithms and a list of m confidentiality algorithms are~~is~~ proposed.

The SPI_U shall be chosen in such a way that it uniquely identifies 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 algorithms list | [confidentiality algorithms list]| SPI_U*

~~Integrity-Algorithm-1, Integrity-Algorithm-2, …, Integrity-Algorithm-n~~

Content-Length: 0

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

The SPI_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. 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: esp | *integrity algorithm | [confidentiality algorithm] | SPI* _P | *unprotected_port*

~~Integrity-Algorithm-m~~

Content-Length: 0

The UE shall in SM5 start the integrity protection – and optionally the confidentiality protection - of the whole SIP-message by setting up ESP security associations according to the parameters negotiated in SM1 and SM4, and applying ESP to the message.~~using the Integrity-Algorithm-m and the IK and include a MAC.~~ Furthermore the Security-setup line ~~proposed set of algorithms that where~~ sent in SM1 shall be included:

SM5:

ESP(
REGISTER sip: ----
Via: ----
From: IMPI
To: IMPU
Call-ID: ----
Cseq: 1 REGISTER
Security-setup: *esp | integrity algorithms list | [confidentiality algorithms list]| SPI_U*

~~Security-setup: *integrity algorithms list | [confidentiality algorithms list |] SPI_U*~~
...
)
~~Integrity-Algorithm-1, Integrity-Algorithm-2, …, Integrity-Algorithm-n~~
~~MAC~~
Content-Length: 0

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.

~~*[Editors Note: The security mode setup shall be generic such that for future needs confidentiality algorithms can be negotiated and applied. At this the NULL algorithm shall be assumed to be the confidentiality algorithm i.e. the system will rely on existing confidentiality mechanisms defined for UMTS and R'99.]*~~

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

7.3 Error cases in the setup 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_{IM}. In this situation, the P-CSCF will receive IPsec 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 ESP integrity check and successfully completes the authentication, it is immediately processed. However, if during the registration timer the P-CSCF receives ESP 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.

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_{IM} and therefore the ESP 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 by an ESP SA, and is not already aware of any errors, the P-CSCF shall accept such REGISTER messages indicating network authentication failure on a different port, the unprotected port, 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.

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 unprotected port in the clear, indicating the synchronisation 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.

7.3.2 Error cases related to the Security-Setup

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: *esp | integrity algorithms list | [confidentiality algorithms list]| SPI_U*

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.]

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: *esp | integrity algorithms list | [confidentiality algorithms list]| SPI_U*

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.]

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. 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)

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.

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 association 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.

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.

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:

ESP (

   REGISTER sip: ----
   Via: ----
   From:  IMPI
   To: IMPU
   Call-ID: ----
   Cseq: 1 REGISTER
   Security-setup:  esp | integrity algorithms list | [confidentiality algorithms list ]|
   SPI_U

   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.]

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:

```
ESP (
    REGISTER sip: ----
    Via: ----
    From:  IMPI
    To: IMPU
    Call-ID: ----
    Cseq: 1 REGISTER
    Security-setup:  esp | integrity algorithms list | [confidentiality algorithms list ]|
    SPI_U

    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.]

~~7.2 Failures in the set-up process~~

~~Failures related to authentication failures and synchronization failures are specified in 6.1. However when a failure occurs the SIP failure messages shall not be integrity protected. The integrity algorithm shall only be applied in the successful cases.~~

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

~~7.2.1 Unacceptable proposal set~~

~~When the P-CSCF receives a proposal set in a SIP REGISTER message in SM1 that is not acceptable it shall modify the message such that the S-CSCF sends an error message back to the UE in SM3 and the registration process is finished.~~

~~SM2:~~

~~REGISTER sip: ----~~
~~Via: ----~~
~~From: IMPI~~
~~To: IMPU~~
~~Call-ID: ----~~
~~Cseq: 1 REGISTER~~
~~Security-setup: Integrity-Algorithm-1, Integrity-Algorithm-2, …, Integrity-Algorithm-n~~

~~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.]*~~

~~7.2.2 Failure of integrity check~~

~~When the P-CSCF receives a SIP message, which is integrity, protected and the integrity check fails the P-CSCF shall silently discard that message.~~

~~*[Editors Note: It is still FFS how failures related to MAC failures shall be handled in detail. This includes the behavior of both the P-CSCF and the UE.]*~~