

14 - 17 May 2002

Victoria, Canada

CR-Form-v5
<b>CHANGE REQUEST</b>
⌘ <b>33.203 CR</b> ⌘ rev <b>-</b> ⌘ Current version: <b>5.1.0</b> ⌘

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

<b>Title:</b>	⌘ Update of SA handling procedures		
<b>Source:</b>	⌘ Hutchison 3G UK		
<b>Work item code:</b>	⌘	<b>Date:</b>	⌘ 10/05/2002
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ Rel-5
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> 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)

<b>Reason for change:</b>	⌘ Current security association (SA) handling procedures do not cover all the possible cases that can occur
<b>Summary of change:</b>	⌘ Update the way the P-CSCF handles security associations to deal with some cases that are not already covered. Also describes the behaviour of the UE and P-CSCF in isolation of each other. The SA handling procedures are also moved from a section describing error behaviour
<b>Consequences if not approved:</b>	⌘ Some behaviour of the P-CSCF is not described, which means that different P-CSCF may take different action possibly causing the UE to become unreachable.

<b>Clauses affected:</b>	⌘ 6.1, 7.3.3, 7.4		
<b>Other specs affected:</b>	⌘ <input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘	
<b>Other comments:</b>	⌘		

## 6.1 Authentication and key agreement

The scheme for authentication and key agreement in the IMS is called IMS AKA. The IMS AKA achieves mutual authentication between the ISIM and the HN, cf. Figure 1. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI, cf. [3]. The HSS and the ISIM share a long-term key associated with the IMPI.

The HN shall choose the IMS AKA scheme for authenticating an IM subscriber accessing through UMTS. The security parameters e.g. keys generated by the IMS AKA scheme are transported by SIP.

The generation of the authentication vector AV that includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in [1]. The ISIM and the HSS keep track of counters  $SQN_{ISIM}$  and  $SQN_{HSS}$  respectively. The requirements on the handling of the counters and mechanisms for sequence number management are specified in [1]. The AMF field can be used in the same way as in [1].

Furthermore a security association is established between the UE and the P-CSCF. The subscriber may have several IMPUs associated with one IMPI. These may belong to the same or different service profiles. Only one SA shall be active between the UE and the P-CSCF. This single SA shall be updated when a new successful authentication of the subscriber has occurred, cf. section 7.4.3.3.

It is the policy of the HN that decides if an authentication shall take place for the registration of different IMPUs e.g. belonging to same or different service profiles. Regarding the definition of service profiles cf. [3].

### 7.3.3 Error cases relating to aAuthenticated re-registration

If the registration is a re-registration, a pair of security associations between UE and P-CSCF is already active. The authenticated re-registration shall initially utilize the existing SA. This is the normal case. However, in the event the UE originates the (SM1) Register message using no protection, the P-CSCF shall still accept it and forward the request to the S-CSCF, indicating that the register message was not integrity protected. This shall trigger the S-CSCF to challenge the subscriber with the execution of a new IMS-AKA authentication procedure as described in clause 6.1.1.

[Editors Note: The exact mechanism for changing SAs is currently under investigation.]

Before SM7 is sent by the UE, both peers shall replace the existing SA by the new SA negotiated during these first two messages:

[Editors Note: The exact mechanism when to change SA1 to SA2 under certain error conditions is FFS.]

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

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 SM4 from the S-CSCF and then sends SM6 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 SM6 could be successfully processed by the UE, the UE also creates the new SAs SA11 and SA12 in its database. The UE then sends SM7 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. SM7 is protected with the new SA11.

- 4) The P-CSCF waits for the response SM10 from the S-CSCF and then sends SM12 to the UE, using the new SA 12.

- 5) After the reception of SM12 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.

#### ~~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 SM12, and SM12 is sent by the P-CSCF, but not received by the UE, then the UE has only the old 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.

### 7.3.3.13 Error cases related to IMS AKA

#### User authentication failure

The S-CSCF will send a 4xx Auth\_Failure message SM10, which will pass through the already established SA to the UE as SM12. 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 SM7 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 SM7, indicating the synchronisation failure, to the P-CSCF, using the already established SA. The P-CSCF deletes the new SA after receiving this message.

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

#### Unacceptable proposal set

The message SM6 shall respond to the first REGISTER message SM1 with a 4xx Unacceptable\_Proposal, 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 4xx Unacceptable\_Proposal message back to the UE in SM4 and SM6 and the registration process is finished.

#### SM2:

REGISTER(Security-setup = *integrity mechanisms list*, [*confidentiality mechanisms list*], *integrity algorithms list*, [*confidentiality algorithms list*], SA\_ID\_U, [*info*], Failure = NoCommonIntegrityAlgorithm, IMPI)

[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 SM7 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 SM7 do not match. In this case the P-CSCF shall respond to the UE by sending a 4xx Unacceptable\_Proposal message in SM12 using the already established SA. Both sides delete the new SAs.

The P-CSCF therefore shall modify the message SM8 such that the S-CSCF sends the 4xx Unacceptable\_Proposal message back to the UE in SM10 and SM12 and the registration process is finished.

#### SM8:

REGISTER(Security-setup = *integrity mechanisms list*, [*confidentiality mechanisms list*], *integrity algorithms list*, [*confidentiality algorithms list*], SA\_ID\_U, [*info*], Failure = NoCommonIntegrityAlgorithm), IMPI)

[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.]

## 7.4 Management and Use of Security Associations

Every successful registration procedure that includes a user authentication produces a new pair of security associations (SAs). These new SAs shall then replace the previous SAs. This section describes how the UE and P-CSCF shall handle this replacement and which SA to apply to which message. Security associations may be unidirectional or bi-directional. This section assumes that security associations are unidirectional, as this is the general case. Whenever a user is registered there is a **current SA** for each direction at both the P-CSCF and the UE. In addition there may be either a **registration SA** for each direction or an inbound **old SA** at the UE and either a **registration SA** or a **valid SA** for each direction or rarely both at the P-CSCF. They are denoted as follows:

SA\_in\_cur        current inbound SA  
SA\_out\_cur      current outbound SA  
SA\_in\_reg       registration inbound SA  
SA\_out\_reg      registration outbound SA  
SA\_in\_old       old inbound SA (in UE only)  
SA\_in\_val       valid inbound SA (in P-CSCF only)  
SA\_out\_val      valid outbound SA (in P-CSCF only)

This notation has local significance only. That means that SA\_in\_cur at the UE is not always the same as SA\_out\_cur at the P-CSCF and similarly for other SAs. The SAs shall be distinguished by different SA\_IDs.

### 7.4.1 Management of security associations in the UE

The UE shall be involved in only one registration procedure at a time. Upon starting a new registration procedure, any existing registration SAs are deleted. The UE shall delete any SA whose expiry time is exceeded. If the wrong SA is used to protect any message, the message should be discarded.

A successful registration with authentication proceeds in the following steps:

- The UE sends the initial message to register with the IMS. It should be integrity-protected using SA\_out\_cur if it exists.
- The UE receives an authentication challenge in a message from the P-CSCF. This message shall be integrity-protected using SA\_in\_cur if the UE's initial message was integrity-protected.
- If this message can be successfully processed by the UE, the UE creates the new SAs, SA\_in\_reg and SA\_out\_reg, which are derived according to section 7.2. The expiry time of the registration SAs should be set to allow enough time to complete the registration procedure. The UE then sends its response to the P-CSCF, which shall be protected with SA\_out\_reg.
- The UE receives a registration successful message from the P-CSCF, which shall be protected using SA\_in\_reg.
- After the successful processing of the registration successful message by the UE, the registration is complete. The UE sets the expiry time of the registration SAs equal to the registration timer in the message. SA\_in\_cur becomes the new SA\_in\_old, SA\_out\_reg becomes the new SA\_out\_cur and SA\_in\_reg becomes the new SA\_in\_cur.

A failure in the registration means the UE should delete SA\_in\_reg and SA\_out\_reg. If the first message in a registration procedure is protected, the UE shall protect all other outbound messages in that registration procedure with SA\_out\_cur or ensure that SA\_in\_cur was applied to protect all other inbound messages in that registration procedure, for example synchronization failure messages. If the first message was not protected, then no protection shall be applied to the other messages.

When a SIP message protected with SA\_in\_cur is successfully received from the P-CSCF, the UE shall delete SA\_in\_old if it exists.

Outside registration procedures, the UE shall use SA\_out\_cur to protect all outbound traffic. Furthermore the UE shall ensure that all inbound traffic is protected with either SA\_in\_cur or SA\_in\_old.

## 7.4.2 Management of security associations in the P-CSCF

The P-CSCF shall delete any SA whose expiry time is exceeded. If the current SAs are deleted and there exist valid SAs, then the P-CSCF makes the SA\_out\_val the new SA\_out\_cur and SA\_in\_val the new SA\_in\_cur, and removes the valid SAs. If the wrong SA is used to protect any message, the message should be discarded.

The P-CSCF associates the IMPI and IMPU given in the registration procedure with the registration SAs created during that registration procedure. The P-CSCF associates the IMPI given in the registration procedure and all the successfully registered IMPUs related to that IMPI with current and valid SAs.

A successful registration with the first message protected proceeds in the following steps:

- The P-CSCF receives the first register message. If it is protected, it should be integrity-protect using SA\_in\_cur or SA\_in\_val.
- The P-CSCF forwards the message containing the challenge to the UE. This shall be integrity-protected using SA\_out\_cur, if the initial message was protected.
- The P-CSCF then creates the new SAs, SA\_in\_reg and SA\_out\_reg, which are derived according to section 7.2. The expiry time of the registration SAs should be set to allow just enough time to complete the registration procedure.

Editor's note: there can exist 3 sets of SAs at this point.

- The P-CSCF receives the message carrying the response from the UE. It shall be protected using SA\_in\_reg.
- The P-CSCF forwards the successful registration message to the UE, which shall be protected using SA\_out\_reg. This completes the registration procedure for the P-CSCF. The P-CSCF sets the expiry time of the registration SAs equal to the registration timer in the message. If the first register message was protected, then SA\_out\_reg becomes SA\_out\_val and SA\_in\_reg becomes SA\_in\_val (overwriting any previous valid SAs). If the first register message was unprotected, then SA\_out\_reg becomes SA\_out\_cur and SA\_in\_reg becomes SA\_in\_cur, and all valid and registration SAs are deleted.

A failure in the registration means the P-CSCF should delete SA\_in\_reg and SA\_out\_reg. If the first message in a registration procedure is protected, the P-CSCF shall protect all other outbound message in a registration procedure with SA\_out\_cur or ensure that SA\_in\_cur was applied to protect all other inbound messages in a registration procedure, for example synchronization failure messages. If the first message was not protected, then no protection shall be applied to the other messages.

When the P-CSCF successfully receives a SIP message protected with SA\_in\_val from the UE, then SA\_in\_val and SA\_out\_val becomes the new SA\_in\_cur and SA\_out\_cur respectively, and there are no more valid SAs.

Outside registration procedures, the P-CSCF shall use SA\_out\_cur to protect outbound traffic. Furthermore the P-CSCF shall ensure that inbound traffic is protected with either SA\_in\_cur or SA\_in\_val. If the wrong SA is used, the message should be discarded.