

## CHANGE REQUEST

⌘ **TS 33.203 CR CRNum** ⌘ rev ⌘ Current version: **6.0.0** ⌘

For [HELP](#) on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** UICC apps  ME  Radio Access Network  Core Network

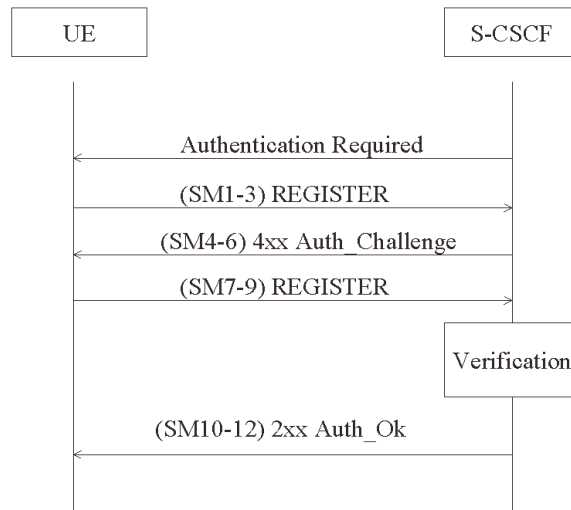
<b>Title:</b>	⌘ Clarifying formulation and notation related to protected port numbers		
<b>Source:</b>	⌘ Alcatel		
<b>Work item code:</b>	⌘ IMS-ASEC	<b>Date:</b>	⌘ 29/09/2003
<b>Category:</b>	⌘ <b>D</b>	<b>Release:</b>	⌘ Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	<b>F</b> (correction)	<b>2</b> (GSM Phase 2)	
	<b>A</b> (corresponds to a correction in an earlier release)	<b>R96</b> (Release 1996)	
	<b>B</b> (addition of feature),	<b>R97</b> (Release 1997)	
	<b>C</b> (functional modification of feature)	<b>R98</b> (Release 1998)	
	<b>D</b> (editorial modification)	<b>R99</b> (Release 1999)	
	Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<b>Rel-4</b> (Release 4)
			<b>Rel-5</b> (Release 5)
			<b>Rel-6</b> (Release 6)

<b>Reason for change:</b>	⌘ Parts of the document are inaccurate about the use of protected port numbers by the UE
<b>Summary of change:</b>	⌘ Some sentences related to protected port number pair in section 7.1 are reformulated to avoid misunderstanding and be more in line with the formulation in section 7.2
<b>Consequences if not approved:</b>	⌘ Unclear section 7.1

<b>Clauses affected:</b>	⌘ 6.1.4, 7.1						
<b>Other specs affected:</b>	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Test specifications			
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	O&M Specifications			
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
<b>Other comments:</b>	⌘						

## 6.1.4 Network Initiated authentications

In order to authenticate an already registered user, the S-CSCF shall send a request to the UE to initiate a re-registration procedure. When received at the ~~UES-CSCF~~, the re-registration shall trigger a new IMS AKA procedure that will allow the S-CSCF to re-authenticate the user.



## 7.1 Security association parameters

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

The SA parameters that shall be negotiated between UE and P-CSCF in the security mode set-up procedure, are:

### - Integrity algorithm

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

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

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

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

### - SPI (Security Parameter Index)

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

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

**The following SA parameters are not negotiated:**

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

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

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

**Selectors:**

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

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

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

- The transport protocol selector shall allow UDP and TCP.
- Ports:
  1. The P-CSCF receives messages protected with ESP from any UE on one fixed port (the "protected port") different from the standard SIP port 5060. The number of the protected port is communicated to the UE during the security mode set-up procedure, cf. clause 7.2. For every protected request towards UE, the P-CSCF shall insert the protected port into Via header. No unprotected messages shall be sent from or received on this port. From a security point of view, the P-CSCF may receive unprotected messages from any UE on any port which is different from the protected port.

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

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

4. The P-CSCF is allowed to receive only REGISTER messages on unprotected ports. All other messages not arriving on the protected port shall be discarded by the P-CSCF.
5. For every protected request, the UE shall insert the protected port pair of the corresponding SA into Via header. 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 pair, 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 pair (source IP address, source port) in the packet headers coincide with the UE's address pair (IP address, source port) inserted in the Via header of the protected REGISTER message. If the Via header does not explicitly contain the UE's address pair, but rather a symbolic name then the P-CSCF shall first resolve the symbolic name by suitable means to obtain an address pair.

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

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

4. For each incoming protected message the SIP application at the P-CSCF shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by the pair (UE\_IP\_address, UE\_protected\_port) in the "SA\_table". The SIP application at the P-CSCF shall further check that the IMPU associated with the SA in the "SA\_table" and the IMPU in the received SIP message coincide. If this is not the case the message shall be discarded.
5. For each SA which has been established and has not expired, the SIP application at the UE stores at least the following data: (UE\_protected\_port, SPI, lifetime) in an "SA\_table".

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

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

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

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

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

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

