Technical Specification Group Services and System Aspects **TSGS#21(03)0487**

Meeting #21, Frankfurt, Germany, 22-25 September 2003

Source: **SA WG3**

Title: **CR to 33.203: Introducing Confidentiality Protection for IMS (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

Meet	SA Doc	TS No.	CR No	Rev	Rel	Cat	Subject	Vers. Current	Vers New	SAWG3 Doc
SP-21	SP-030487	33.203	046	-	Rel-6	B	Introducing Confidentiality Protection for IMS	5.6.0	6.0.0	S3-030455

3GPP TSG-WG3 Meeting #29
San Francisco, USA, 15th–18th July 2003

Tdoc ⌘S3-030455

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.203** **CR** **046** ⌘**rev** ⌘ Current version: **5.6.0** ⌘

*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 ☒

Title:	⌘	Introducing Confidentiality Protection for IMS
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	29/06/2003
Category:	⌘	**B**
Release:	⌘	Rel-6

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)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Currently there is no confidentiality protection for Release 5 IMS between the UE and the P-CSCF. The mechanism in place in Relase 5 is the use of protection as defined in TS33.102 between the UE and the RNC. The aim for the access security was to create a framework that is independent of underlying security. Since the confidentiality mechanisms are missing in Release 5 this CR will close an existing gap for Release 6.
Summary of change:	⌘	The change introduces the possibility to have confidentiality protection in IMS.
Consequences if not approved:	⌘	There is no confidentiality protection for IMS and hence the dependency with lower layers for encryption will remain

Clauses affected:	⌘	5.1.3, 6.2, 7.1, 7.2			
Other specs affected:	⌘	**Y**	**N**		
		X		Other core specifications	⌘ TS24.229, TS24.228
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	There is another CR to TS33.203 from Ericsson on the key expansion function. This CR introduces the already agreed requirements in the Presence TR for Security and is directly copied from that TR with editorial changes.			

5.1.3 Confidentiality protection

Possibility for IMS specific confidentiality protection shall be provided to SIP signalling messages between the UE and the P-CSCF. Mobile Operators shall take care that the deployed confidentiality protection solution and roaming agreements fulfils the confidentiality requirements presented in the local privacy legislation. The following mechanisms are provided at SIP layer:

1. The UE shall always offer encryption algorithms for P-CSCF to be used for the session, as specified in clause 7.

2. The P-CSCF shall decide whether the IMS specific encryption mechanism is used. If used, the UE and the P-CSCF shall agree on security associations, which include the encryption key that shall be used for the confidentiality protection. The mechanism is based on IMS AKA and specified in clause 6.1.~~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].

6.2 Confidentiality mechanisms

If the local policy in P-CSCF requires the use of IMS specific confidentiality protection mechanism between UE and P-CSCF, IPsec ESP as specified in [13] shall provide confidentiality 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 confidentiality 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 clause 7. As a result of an authenticated registration procedure, two pairs of unidirectional SAs between the UE and the P-CSCF all shared by TCP and UDP, shall be established in the P-CSCF and later in the UE. One SA pair is for traffic between a client port at the UE and a server port at the P-CSCF and the other SA is for traffic between a client port at the P-CSCF and a server port at the UE. For a detailed description of the establishment of these security associations see section 7.

The encryption key CK_{ESP} is the same for the two pairs of simultaneously established SAs. The encryption key CK_{ESP} is obtained from the key CK_{IM} established as a result of the AKA procedure, specified in clause 6.1, using a suitable key expansion function.

[Editors Note: This key expansion function depends on the ESP encryption algorithm and should be specified in Annex I but is FFS.]

The encryption key expansion on the user side is done in the UE. The encryption 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.~~No confidentiality mechanism is provided in this specification, cf. clause 5.1.3.~~

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.~~procedure are:

- **Encryption algorithm**

  The encryption algorithm is DES-EDE3-CBC as specified in RFC 2541 [20].

  [Editors note: The encryption algorithm AES should be added as soon as it appears as an RFC in IETF.]

- **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.
- Key length: the length of the encryption key depends on the encryption algorithm. The entropy of the key shall at least be 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. 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 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 shall use a single protected port number for both TCP and UDP connections. The port number 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 port number and send it to the network. If the UE is not challenged by the network, the port number 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 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, 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, UE_protected_port), 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. 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 number for the protected port, as well as SPI number, do 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 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.

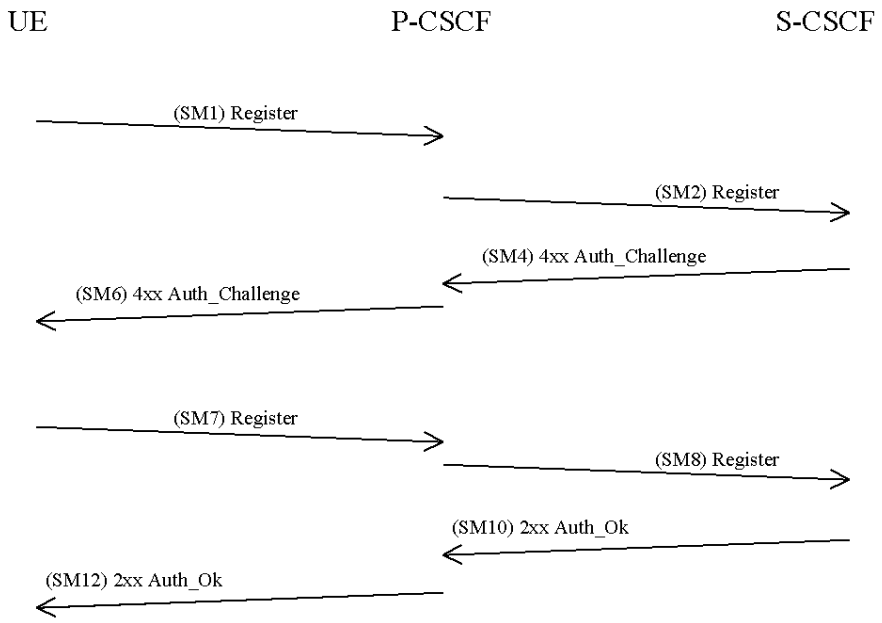
NOTE: If the integrity check of a received packet fails then IPsec will automatically discard the packet.

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

7.2 Set-up of security associations (successful case)

The set-up of security associations is based on [21]. Annex H of this specification shows how to use [21] 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. clause 6.1. In order to start the security mode set-up procedure, the UE shall include a *Security-setup*-line in this message.

The *Security-setup-line* in SM1 contains the Security Parameter Index values' and the protected ports selected by the UE. It also contains a list of identifiers for the integrity and encryption ~~algorithms which~~algorithms, which the UE supports.

SM1:
REGISTER(Security-setup = *SPI_U, Port_U, UE integrity and encryption algorithms list)*

~~SM1:~~
~~REGISTER(Security-setup = *SPI_U, Port_U, UE integrity algorithms list)*~~

SPI_U is the symbolic name of a pair of SPI values (cf. section 7.1) (*spi_uc*, *spi_us*) that the UE selects. *spi_uc* is the SPI of the inbound SA at UE's the protected client port, and *spi_us* is the SPI of the inbound SA at the UE's protected server port. The syntax of *spi_uc* and *spi_us* is defined in Annex H.

Port_U is the symbolic name of a pair of port numbers (*port_uc*, *port_us*) as defined in section 7.1. The syntax of *port_uc* and *port_us* is defined in Annex H.

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 keys IK_{IM} and CK_{IM} received from the S-CSCF to the temporarily stored parameters.

A Release 6 P-CSCF shall propose SA alternatives for Release 5 and Release 6 UE's since the UE may or may not support confidentiality protection. The P-CSCF selects the SPI for the inbound SA. The P-CSCF then selects the SPIs for the inbound SAs. The same SPI number shall be used for Release 5 and Release 6 options. The P-CSCF shall define the SPIs such that they are unique and different from any SPIs as received in the *Security-setup-line* from the UE.

NOTE: This rule is needed since the UE and the P-CSCF use the same key for inbound and outbound traffic.

In order to determine the integrity and encryption algorithm the P-~~CSCF proceeds~~CSCF proceeds as follows: the P-CSCF has a list of integrity and encryption algorithms it supports, ordered by priority. Release 6 algorithms must have higher priority than Release 5 algorithms. The P-CSCF selects the first ~~integrity~~ algorithm combination on its own list which is also supported by the UE.

The P-CSCF then establishes two new pairs of SAs in the local security association database.

The *Security-setup*-line in SM6 contains the SPIs and the ports assigned by the P-CSCF. It also contains a list of identifiers for the integrity and encryption ~~algorithms which~~algorithms, which the P-CSCF supports.

NOTE: P-CSCF may be configured to trust on the encryption provided by the underlying access network. In this case, the P-CSCF acts according to Release 5 specificatons, and does not include encryption algorithms to the *Security-setup*-line in SM6.

SM6:
4xx Auth_Challenge(Security-setup = *SPI_P, Port_P, P-CSCF integrity and encryption algorithms list)*

~~SM6:~~
~~4xx Auth_Challenge(Security-setup = *SPI_P, Port_P, P-CSCF integrity algorithms list)*~~

SPI_P is the symbolic name of the pair of SPI values (cf. section 7.1) (*spi_pc, spi_ps*) that the P-CSCF selects. *spi_pc* is the SPI of the inbound SA at the P-CSCF's protected client port, and *spi_ps* is the SPI of the inbound SA at the P-CSCF's protected server port. The syntax of *spi_pc* and *spi_ps* is defined in Annex H.

Port_P is the symbolic name of the port numbers (*port_pc, port_ps*) as defined in section 7.1. The syntax of Port_P is defined in Annex H.

Upon receipt of SM6, the UE determines the integrity and encryption algorithms as follows: the UE selects the first integrity and encryption algorithm combination on the list received from the P-CSCF in SM 6 which is also supported by the UE.

NOTE: Release 5 UE will not support any encryption algorithms, and will choose the first Release 5 integrity algorithm on the list received from the P-CSCF in SM6.

The UE then proceeds to establish two new pairs of SAs in the local SAD.

The UE shall integrity and confidentiality protect SM7 and all following SIP messages. Furthermore the integrity algorithms list, *SPI_P*, and *Port_P* received in SM6, and *SPI_U, Port_U sent in SM1* shall be included:

SM7:
REGISTER(Security-setup = *SPI_U, Port_U, SPI_P, Port_P, P-CSCF integrity and encryption algorithms list)*

After receiving SM7 from the UE, the P-CSCF shall check whether the integrity and encryption algorithms list, *SPI_P*, and *Port_P* received in SM7 is identical with the corresponding parameters sent in SM6. If this is not the case the registration procedure is aborted. The P-CSCF shall include in SM8 information to the S-CSCF that the received message from the UE was integrity protected as indicated in clause 6.1.5. The P-CSCF shall add this information to all

subsequent REGISTER messages received from the UE that have successfully passed the integrity and confidentiality check in the P-CSCF.

SM8:
REGISTER(Integrity-Protection = *Successful*, *Confidentiality-Protection =Successful*, IMPI)

The P-CSCF finally sends SM12 to the UE. SM12 does not contain information specific to security mode setup (i.e. a Security-setup line), but with sending SM12 not indicating an error the P-CSCF confirms that security mode setup has been successful. After receiving SM12 not indicating an error, the UE can assume the successful completion of the security-mode setup.

The use of the two pairs of unidirectional SAs is illustrated in the figure below with a set of example message exchanges protected by the respective IPsec SAs where the INVITE and following messages are assumed to be carried over TCP.

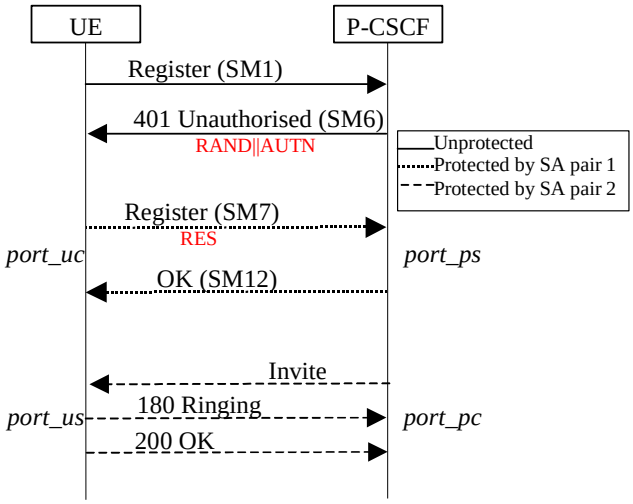


Figure 1