3GPP TSG-SA3 Meeting #26 ***Tdoc ⌘S3-020621***
Oxford, England 19th – 22nd November, 2002

CR-Form-v7

CHANGE REQUEST

⌘ **33.cde** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **0.2.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Confidentiality protection between UE and P-CSCF in IMS/Presence
Source:	⌘	Ericsson
Work item code:	⌘	Presence
Date:	⌘	14/11/2002
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:	⌘	The use of Presence services requires confidentiality protection from IMS.
Summary of change:	⌘	Confidentiality protection has been made mandatory for Release 6.
Consequences if not approved:	⌘	Sensitive presence information about the end-user may be revealed to unauthorized parties.

Clauses affected:	⌘	

		Y	N		
Other specs affected:	⌘			Other core specifications	⌘
				Test specifications	
				O&M Specifications	

Other comments:	⌘	

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.141: "Presence service; Stage 1".

[3] 3GPP TS 23.141: "Presence service; Stage 2".

[4] Common Presence and Instant Messaging (CPIM) Presence Information Data Format, Internet Draft http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-pidf-05.txt, May 2002

Editor's note: The above document is not yet published as an RFC, where possible the reference should be converted to an RFC prior to approval should this document be converted to a Technical Specification.

[5] Session Initiation Protocol (SIP) Extensions for Presence, Internet-Draft http://www.ietf.org/internet-drafts/draft-ietf-simple-presence-07.txt, May 2002

Editor's note: The above document is not yet published as an RFC, where possible the reference should be converted to an RFC prior to approval should this document be converted to a Technical Specification.

[6] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[7] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[8] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[9] IETF RFC 3265: "Session Initiation Protocol (SIP) Event Notification"

[10] A SIP Event Package for List Presence, Internet-Draft, http://search.ietf.org/internet-drafts/draft-ietf-simple-presencelist-package-00.txt, June 2002

Editor's note: The above document is not yet published as an RFC, where possible the reference should be converted to an RFC prior to approval should this document be converted to a Technical Specification.

[11] IETF RFC 2778: "A Model for Presence and Instant Messaging".

[12] IETF RFC 2779: "Instant Messaging / Presence Protocol Requirements".

[13] IETF RFC 2406 (1998) "IP Encapsulating Security Payload (ESP)".

[14] IETF RFC 2401 (1998) "Security Architecture for the Internet Protocol".

[15] RFC 2451 (1998): "The ESP CBC-Mode Cipher Algorithms".

[16] Draft-ietf-sip-sec-agree-05: " Security Mechanism Agreement for the Session Initiation Protocol ". October, 2002.

4.4.2 IMS related

It is suggested that SA3 adopts the following working assumptions related to Presence:

1) Peu: Existing IMS security architecture fulfils the security requirements related to authentication, integrity protection, replay protection and anonymity.
2) Ph: No additional security requirements.
3) Pi: No additional security requirements.
4) Pc: No additional security requirements.
5) Pg: No additional security requirements.
6) Pk: No additional security requirements.
7) Pl: No additional security requirements.
8) Pw: Existing IMS security architecture fulfils the security requirements related to authentication, integrity protection and replay protection.
9) Peu & Pw: IMS needs to be enhanced by IPsec encryption between UE and P-CSCF in order to fulfil the confidentiality requirement.

The following interfaces are left FFS:

1) Pex: Security between PEA and external information source should be further studied.
2) Pex, Peu & Pen: Threats and potential solutions for false presence information inside the network should be further studied.
3) ~~Peu & Pw: IMS may need to be enhanced by IPsec encryption between UE and P-CSCF in order to fulfil the confidentiality requirement.~~
4) Peu & Pw: The degree of anonymity provided by 'anonymous IMPU' should be further studied.
5) Peu & Pw: Ability of non-IMS accesses (e.g. WAP/SMS/WV) to fulfil the security requirements should be further studied.
6) Pw: The Presence Server may need additional mechanism for authenticating the Watchers. For example, the Presentity may provide passwords for Watcher authentication.
7) Pw: The Presentity may need additional mechanism for authenticating the Watchers. For example, the Watcher may provide a token or electronic signature for authentication.
8) Pw: IMS may need to be enhanced by a security mechanism for the Watcher to request anonymity.

It is suggested that LSs related to the following issues are sent to other 3GPP working groups:

[Editors note: Peu: It is not clear yet which protocols will be used in Peu interface. Peu may include protocols for web access (e.g. HTTP for access list manipulation and registrations), and consequently there may be a need for additional security.]

6 Security features

6.1 IMS related security features

6.1.1 Confidentiality protection

Confidentiality protection shall be provided to SIP signalling messages between the UE and the P-CSCF. The following mechanisms are provided.

1. The UE and the P-CSCF shall negotiate the encryption algorithm that shall be used for the session, as specified in chapter 7.

2. 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 of [6].

Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [7].

8 Security mechanisms

8.1 IMS related security mechanisms

8.1.1 Confidentiality mechanisms

IPsec ESP as specified in reference [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 of [6]. As a result of the registration procedure, a pair of unidirectional SAs between the UE and the P-CSCF shall be established. The pair consists of an SA for traffic from the UE to the P-CSCF (inbound SA at the P-CSCF) and an SA for traffic from the P-CSCF to the UE (outbound SA at the P-CSCF).

The encryption key CK_{ESP} is the same for the two 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 of [6], using a suitable key expansion function. This key expansion function depends on the ESP encryption algorithm and is specified in Annex I.

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.

8.1.2 Security association set-up procedure

The security association set-up procedure is necessary in order to decide what security services to apply and when the security services start. In the IMS authentication of users is performed during registration as specified in clause 6.1 of [6]. Subsequent signaling communications in this session will be integrity and confidentiality protected based on the keys derived during the authentication process.

8.1.1.1 New security association parameters

- **Enryption algorithm**

The enryption algorithm is DES-EDE3-CBC [15].

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

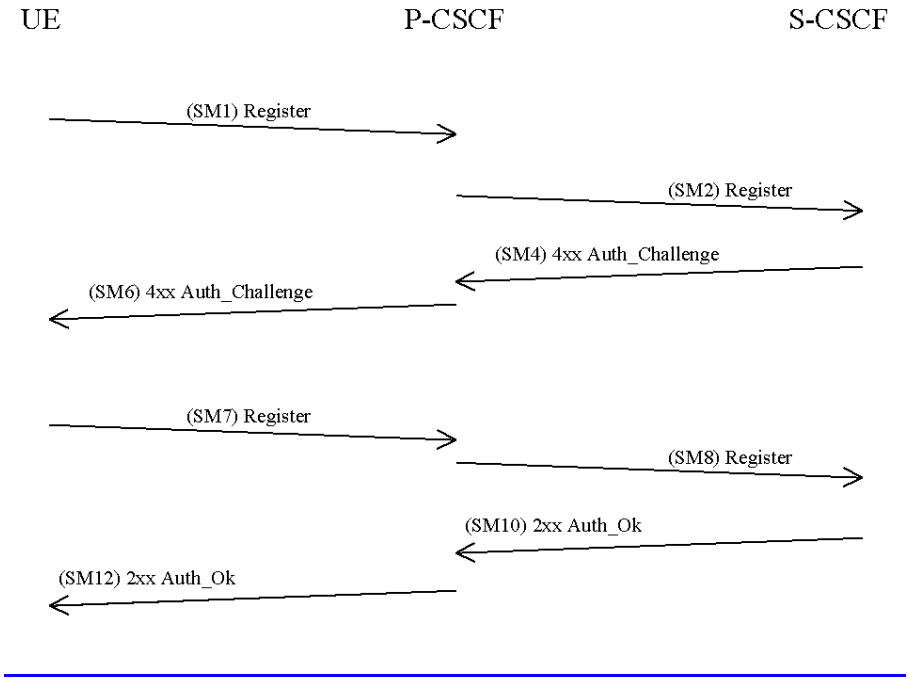
NOTE: This, in particular, excludes the use of the NULL enryption algorithm.

[Editors note: The key expansion function is FFS.]

8.1.1.2 Set-up of security associations (successful case)

The set-up of security associations is based on [16]. Annex H of [6] shows how to use [16] 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 of [6]. 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 SPI numbers and the protected port selected by the UE. It also contains a list of identifiers for the integrity and encryption algorithms, which the UE supports.

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

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.

Release 6 P-CSCF must propose SA alternatives both for Release 5 and Release 6 UE's. The P-CSCF selects the SPI for the inbound SA. 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 keys for inbound and outbound traffic.

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

The P-CSCF then establishes corresponding pair of SAs in the local security association database.

The *Security-setup*-line in SM6 contains the SPI assigned by the P-CSCF and the fixed number of the protected port at the P-CSCF. It also contains a list of identifiers for the integrity and encryption algorithms which the P-CSCF supports.

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

Upon receipt of SM6, the UE determines the integrity and encryption algorithm as follows: the UE selects the first integrity and encryption algorithm combination on the list received from the P-CSCF in SM6 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 another pair of SAs in the local SAD.

The UE shall integrity and confidentiality protect SM7 and all following SIP messages. Furthermore the integrity and encryption algorithms list received in SM6 shall be included:

SM7:
REGISTER(Security-setup = *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 received in SM7 is identical with the list 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 and confidentiality protected. 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.