**3GPP TSG SA WG3 Security** **S3-030247**

**6th – 9th May, 2003**

**Berlin, Germany**

**Agenda Item:** 7.19 Presence

**Source:** Ericsson

**Title:** Presence / IMS Confidentiality

**Document for:** Discussion/Decision

# 1. Introduction

Ericsson presented a discussion paper and a Pseudo-CR related to the confidentiality protection solution in the Peu and Pw interfaces in SA3#27 [S3-030070]. Alternative solutions were described for further study.

This document describes Ericsson's preferred solution. SA3 is asked to make a decision on the issue, and accept the accompanied pseudo-CR to [Presence-Security] as the working assumption.

# 2. Summary of alternative solutions

The current confidentiality mechanism in [Presence-Security] does not fulfil the confidentiality requirement in Peu and Pw interfaces between the UE and P-CSCF. In particular, it is not possible to use IPsec encryption between Release-6 UE and Release-5 P-CSCF.

Six alternative solutions have been documented in [Presence-Security] for this backwards compatibility problem. However, all of them include some known shortcomings (see Table 1).

| **Alternative** | **Shortcomings** |
|---|---|
| Loose the requirement and leave the responsibility to the end-user. | No standard solution in SIP for S-CSCF to inform Presence Server about the confidentiality mechanism.<br>End-users may not understand what really happens. |
| The use of Presence via Release 5 proxy is not allowed. | Restricts the use of Presence to Release 6 proxies only |
| The use of Presence via Release 5 proxy is allowed only when the underlying access network provides confidentiality protection. | Restricts the use of Presence to access networks that provide encryption in the underlying network.<br>SIP application is not aware if confidentiality is provided or not. |
| End-to-end protection using S/MIME. | Limited to Presence: the body of the SIP message (e.g. SDP) cannot be encrypted in IMS.<br>SIP headers not encrypted.<br>Mandatory use of subscriber certificates.<br>UEs overloaded by different security mechanisms, e.g. IPsec, TLS and S/MIME. |
| IPsec replaced by TLS in Release 6. | TLS cannot be used with UDP. |
| The support of IPsec confidentiality is mandated for Release 5 P-CSCF. | Too big change to Release 5 specifications at this phase. |

Table 1: Alternative solutions to the confidentiality protection backwards compatibility problem.

Seventh solution to the problem would be to remove the LCS interface from IMS/Presence until end-to-end confidentiality protection can be provided for location data only. However, this would limit the type of presence data that can be distributed in IMS/Presence and cannot be recommended from business point of view. Furthermore, there can still be some sensitive end-user data that should be confidentiality protected.

# 3. Proposal

None of the analyzed solutions are technically satisfactory for solving the backwards compatibility problem related to confidentiality. For this reason, it is proposed that other than technical means are used to solve the problem.

Firstly, it is assumed that the case when Release 5 P-CSCF is used over an RAN/GERAN access network that does not provide confidentiality protection is rare. From this perspective, the problem of distributing Presence information over the air-interface in clear-text would also be rare or even theoretical.

Secondly, all Mobile Operators providing services in some country are under the local privacy legislation. If the local privacy legislation requires confidentiality protection for user data delivered in Presence/IMS, then the Mobile Operators shall take care that the needed protection is provided. IMS Release 6 should be enhanced by mechanisms for confidentiality protection using IPsec, however, at the end it is a deployment issue whether this protection is provided using IPsec or if the encryption of the underlying network layer is used instead.

This solution assumes that Mobile Operators are able to resolve the backwards compatibility issue when making roaming agreements with other Operators. If the Visited Network does not provide confidentiality protection using IMS IPsec encryption or using the underlying network security, the Home Network should not use such access network for Presence if the local legislation mandates confidentiality protection. It is believed that such Visited Networks are rare and the decision of not using Presence via such networks is also in the interests of the subscriber as well.

Even though the underlying network security can be trusted, it is still believed that IMS Release-6 needs to be enhanced by IPsec encryption. This will increase the flexibility of future network security design, e.g. in WLAN context. Also, there are potential future scenarios where the underlying network is not operated by the same entity than the P-CSCF. In these cases, it is beneficial for the P-CSCF to request IPsec encryption from the UE.

Ericsson proposes the following solution for the backward compatibility problem in IMS confidentiality between UE and P-CSCF in Release 6:

- IMS specific confidentiality protection between UE and P-CSCF is made mandatory to implement but optional for use. The Mobile Operator may configure the P-CSCF to use IPsec encryption or to trust on the underlying network confidentiality protection. It shall be in the responsibility of the Mobile Operator to configure their IMS access network in the way that the requirements of the local privacy legislation are fulfilled.

- If the Mobile Operators provide IMS/Presence services for their subscribers, they shall agree in the roaming agreements on the level of confidentiality protection provided for roaming IMS subscribers. Mobile Operator that need to provide confidentiality for its subscribers based on the local privacy legislation, cannot allow the use of IMS/Presence with a roaming access network that does not provide confidentiality protection using IPsec encryption or confidentiality protection of the underlying network.

Accompanied Pseudo-CR to [Presence-Security] demonstrate the changes in more detail.

# 4. Conclusions

Ericsson proposes that the principles presented in this document are accepted as a working assumption for SA3. SA3 should also accept the accompanied Pseudo-CR to [Presence-Security].

# 5. References

[S3-030070] Ericsson (2003) Confidentiality in Presence, SA3#27, 25th – 28th February, Sophia-Antipolis, France.

[Presence-Security] 3GPP (2003) Presence service; Security (Release 6), TR 33.cde v0.3.0.

**3GPP TSG-SA3 Meeting #27**
**Berlin, Germany, 6th-9th May, 2003**

***Tdoc ⌘DocNumber***

*CR-Form-v7*

# CHANGE REQUEST

⌘ **33.cde** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **0.3.0** ⌘

*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:*** | ⌘ | Presence confidentiality |
| ***Source:*** | ⌘ | Ericsson |
| ***Work item code:*** | ⌘ | PRESNC |
| ***Date:*** | ⌘ | 01/05/2003 |
| ***Category:*** | ⌘ | |
| ***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 backwards compatibility problem in IMS/Presence confidentiality is currently open in Presence Security TR. The problem can be solved local deployment policies and roaming agreements by Mobile Operators. There is no need for solving the problem by technical means. |
| ***Summary of change:*** | ⌘ | - IMS confidentiality between UE and P-CSCF is changed mandatory to implement but optional to use.<br>- The local deployment policies and roaming agreements of Mobile Operators shall take care that local privacy legislation is fulfilled.<br>- Alternative solutions presented in the editors notes are removed. |
| ***Consequences if not approved:*** | ⌘ | All known technical solutions increases the complexity of the system or restricts the usability of IMS/Presence in the way that is not acceptable from business point of view. |

| | | | | | |
|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | | | | |
| ***Other specs affected:*** | ⌘ | **Y** | **N** | | ⌘ |
| | | [ ] | [ ] | Other core specifications | |
| | | [ ] | [ ] | Test specifications | |
| | | [ ] | [ ] | O&M Specifications | |
| ***Other comments:*** | ⌘ | | | | |

**How to create CRs using this form:**
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

### 4.5.2 IMS related

The following working assumptions related to Presence have been defined:

1) Peu: Existing IMS security architecture fulfils the security requirements related to 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 confidentiality protection mechanism is mandatory to implement in UE and P-CSCF. P-CSCF shall decide whether the IPsec encryption or the underlying network layer encryption is used based on the local network security policy.
10) Pw: IMS is enhanced by a security mechanism for the Watcher to request anonymity.

~~*[Editors Note: The solution must be able to guarantee that confidentiality can be provided also for the case in which Release 6 UE is communicating with Release 5 P-CSCF. Alternatively, the presentity must be able to decide whether the notifications can be sent to a wathcer that does not have confidentiality protection. This is FFS.]*~~

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: The degree of anonymity provided by 'anonymous IMPU' should be further studied.
4) Peu & Pw: Ability of non-IMS accesses (e.g. WAP/SMS/WV) to fulfil the security requirements should be further studied.
5) Pw: The Presence Server may need additional mechanism for authenticating the Watchers. For example, the Presentity may provide passwords for Watcher authentication.
6) Pw: The Presentity may need additional mechanism for authenticating the Watchers. For example, the Watcher may provide a token or electronic signature for authentication.
7) Pw: IMS may need to be enhanced by a security mechanism for the Watcher to request anonymity.
8) Pw: IMS may need to be enhanced by an authentication mechanism between the Watcher and the Presence Server

---

## 6.1 IMS related security features

### 6.1.1 Confidentiality protection

Possibility for IMS specific c~~C~~onfidentiality 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 when IMS is used for Presence. The following mechanisms are provided at SIP layer.

1. The UE shall always offer encryption algorithms for ~~and the~~ P-CSCF ~~shall negotiate the encryption algorithm that shall~~ to be used for the session, as specified in chapter ~~7~~8.

2. The P-CSCF shall decide whether the IMS specific encryption mechanism is used. If used, ~~The~~ 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].~~

~~*[Editors Note: The current text above assumes IPsec. However, the suitability of other solutions is FFS. The following solutions are known to fulfil the confidentiality and backwards compatibility requirements:*~~

~~*1)The SIP messages are protected end-to-end between the Presence Server and the UE using S/MIME. However, the protection of SIP headers, which also includes privacy intensive information, may be problematic. Furthermore, the use of S/MIME would most probably require the use of subscriber certificates. Also, the UEs may be overloaded by different security mechanisms, e.g. IPsec, TLS and S/MIME.*~~

~~*Note that S/MIME cannot be used to protect the confidentiality of the messages between UE and P-CSCF because Session Initiation Protocol (SIP) and SIP Security Agreement Mechanism do not allow the use of S/MIME for hop-by-hop protection.*~~

~~*IPsec used between UE and P-CSCF is replaced by TLS in Release 6. From the Rel-5 P-CSCF point of view, the use of TLS is possible because all SIP proxies support TLS. Furthermore, TLS may need to be implemented in UEs in order to allow the protection of HTTP in Presence. However, TLS cannot be used with UDP.]*~~

---

# 8.1 IMS related security mechanisms

## 8.1.1 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 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.

### 8.1.2.1 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.]*

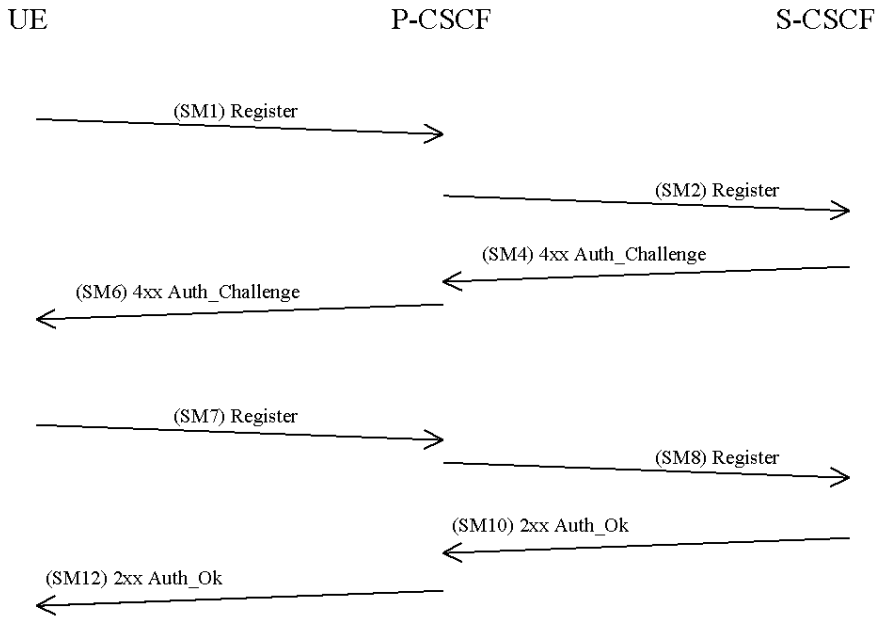
NOTE: This, in particular, excludes the use of the NULL enryption algorithm.

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

### 8.1.2.2 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.

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)*

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.

~~*[Editors Note: There is a backward compatibility problem related to the proposed mechanism on to handle Release 5 P-CSCF and Release 6 UEs. In particular, the confidentiality protection can not be guaranteed in this case. The following solutions are FFS:*~~

~~*1)The use of Presence via Release 5 proxy is not allowed. However, this is restricting the use of Presence (and most probably SIP based Instant Messaging also) to Release 6 proxies only.*~~

~~*2)The use of Presence via Release 5 proxy is allowed only when the underlying access network (e.g. GPRS/UMTS) provides confidentiality protection. However, this is restricting the use of Presence (and most probably SIP based Instant Messaging also) to IMS access networks that use the encryption in the underlying network. Also, the use Presence in other access network, such as WLAN, that has Release 5 proxy would not be possible.*~~

~~*The support of IPsec confidentiality is mandated for Release 5 P-CSCF. However, it may be difficult to introduce such a big changes to Release 5 specifications at this phase.]*~~