3GPP TSG SA WG3 Security **S3-020622**

19th – 22nd November, 2002

Oxford, England

Agenda Item: TBD

Source: Ericsson

Title: IMS based anonymity in Presence

Document for: Discussion/Decision

1. Introduction

This document discusses anonymity in Presence. Accompanied pseudo-CR suggests some new text on anonymity to be added to [33.cde]. These requirements and mechanisms should later be included in [33.203] because all privacy requirements and mechanisms discussed in this and accompanied documents apply to Presence and all other SIP based services.

2. Anonymity in Presence

2.1 Status in IETF

In IETF, SIP WG is currently developing mechanisms for end-user privacy and anonymity [draft-ietf-sip-privacy-general-01, draft-ietf-sip-asserted-identity-02]. These IETF documents include several alternatives to provide anonymity for subscribers. The type of anonymity depends on the ‘priv-value’ field in the Privacy header. The current values are as follows:

- none: “The user requests that a privacy service apply no privacy functions to this message, regardless of any pre-provisioned profile for the user or default behavior of the service. User agents can specify this option when they are forced to route a message through a privacy service which will, if no Privacy header is present, apply some privacy functions which the user does not desire for this message.” [draft-ietf-sip-privacy-general-01]

- user: “This privacy level is set only by intermediaries, in order to communicate that user level privacy functions … must be provided by the network, presumably because the user agent is unable to provide them.” [draft-ietf-sip-privacy-general-01]

- session: “The user requests that a privacy service provide anonymization for the session(s) (described, for example, in a Session Description Protocol …) initiated by this message. This will mask the IP address from which the session traffic would ordinarily appear to originate.” [draft-ietf-sip-privacy-general-01]

- header: “The user requests that a privacy service obscure those headers which cannot be completely expunged of identifying information without the assistance of intermediaries (such as Via and Contact). Also, no unnecessary headers should be added by the service that might reveal personal information about the originator of the request.” [draft-ietf-sip-privacy-general-01]

- critical: “The user asserts that the privacy services requested for this message are critical, and that therefore, if these privacy services cannot be provided by the network, this request should be rejected.” [draft-ietf-sip-privacy-general-01]

- id: “The presence of this privacy type in a Privacy header field indicates that the user would like the Network Asserted Identity to be kept private with respect to SIP entities outside the Trust Domain with which the user authenticated.” [draft-ietf-sip-asserted-identity-02]

In addition to these privacy mechanisms, IETF has defined two headers related to IMS identities: P-Preferred-Identity and P-Asserted-Identity headers [draft-ietf-sip-asserted-identity-02]. These headers can be used by the UE to 'hint' about the preferred identity to the network, and by the network to assert the identity of authenticated users within a trust domain.

2.2 Status in IMS Release 5

In release 5, IMS uses P-Preferred-Identity and P-Asserted-Identity headers [draft-ietf-sip-asserted-identity-02] to cope with multiple IMPUs. All the SIP proxies in IMS (CSCFs, Application Servers, BGCF) and the MRFC and MGCF are part of the 3GPP trust domain. All these elements assumes that the content of P-Asserted-Identity header includes a trustworthy and verified identity of the subscriber. If an IMS entity receives a SIP message from a non-trusted source, it will discard the P-Asserted-Identity header field, if present. If an IMS entity is forwarding a SIP message to a non-trusted source, it will remove the P-Asserted-Identity header.

The ME uses the Privacy header [draft-ietf-sip-privacy-general-01] to request that the subscriber identity of the message originator is hidden from the recipient.

The following rules on anonymity applies on IMS Release 5:

- The UE may request anonymity for the subscriber by using the Privacy header as defined in [draft-ietf-sip-privacy-general-01].
- The last hop P-CSCF will remove the identity information from the SIP message before forwarding the message to the receiver [cf. 23.228, section 5.11.4].
- The Lawful Interception functions need to have access to the identity information of SIP messages [33.106, 33.107, 33.108], and consequently, the identity of the message originator cannot be hidden from any intermediary element (proxy) within the IMS network.

The exact procedure for hiding the subscriber identity within IMS is as follows:

- The originating UE adds a Privacy header with value 'id' to the SIP request. The UE also populates the From header value (and other relevant SIP headers) with an anonymous SIP URI (e.g. "Anonymous" <sip:anonymous@anonymous.invalid>), as defined in [draft-ietf-sip-privacy-general-01]. The P-Preferred-Identity header is only used from the UE to the P-CSCF (the P-CSCF removes it).
- The first hop P-CSCF validates the subscriber identity, and replaces the P-Preferred-Identity header field with P-Asserted-Identity header field.
- IMS network delivers the SIP message to the last hop P-CSCF.
- The last hop P-CSCF hides the identity of the message originator by removing the P-Asserted-Identity header field.

Interoperation with open Internet set some additional requirements for IMS entities. The following rules on anonymity applies to this case:

- If any IMS or Presence subscriber has requested anonymity, all messages must not contain a P-Asserted-Identity header before sending them out of the IMS trust domain. In other words, the edge proxy to the open Internet (e.g. I-CSCF) must check every outgoing message, and if requested, remove the P-Asserted-Identity header. It is assumed that the UE has populated the From header value (and other relevant SIP headers) with an anonymous SIP URI (e.g. "Anonymous" <sip:anonymous@anonymous.invalid>), as defined in [draft-ietf-sip-privacy-general-01].
- Requests coming from open Internet may also include P-Asserted-Identity header. The edge proxy, according to the procedures defined in [draft-ietf-sip-asserted-identity-02], must remove that header.
- The Lawful Interception function is not able to identify the identity of anonymous requests coming from the open Internet, if the message does not include P-Asserted-Identity header. Allowing anonymous requests without identity information to access the IMS trust domain should be up to the local legislation and policy. If such requests are not allowed, and the network still receives such request inside IMS trust domain, the network should reject the request with appropriate error code.

Note that previous anonymity mechanisms can be used only for the subscriber who originates the SIP dialog. The identity of the message receiver cannot be hidden using this mechanism. The only way to hide the identity of the receiver of the SIP dialog request is to use pseudonym IMPUs, or some more advanced anonymity service. The use of pseudonym IMPUs has currently a shortcoming related unprotected REGISTER messages: someone may monitor the registration traffic in the air-interface in order to link pseudonym IMPUs and 'normal' IMPUs via the common IMPI.

Anonymity in Presence does not differ anything from the IMS procedures. The watcher requesting for anonymous subscription within IMS will do exactly same as the originating UE in the previous example, however, the identity is not hidden from the Presence Server. Even the notification sent towards the presentity (in the case in which the presentity is subscribed to the watcher-info) should include the identity information in the P-Asserted-Identity header field in order to make Lawful Interception possible. The identity information is finally removed by the last hop P-CSCF.

The IMS-Internet inter-working with Presence follows the basic IMS rules described above.

3. Conclusions

Currently SA3 documents does not set requirements, or describe mechanisms for IMS subscriber anonymity. It is suggested that these requirements and mechanisms are defined in IMS Release 6. These requirements and mechanisms shall apply to all IMS-based services, such as Presence.

The following privacy mechanisms are suggested for IMS Release 6:

- The UA may use the following priv-value types for the Privacy header: 'none', 'id', 'critical', 'user'.
- The home network (e.g. S-CSCF or an Application Server) may provide the anonymity on behalf of the UA using the following priv-value type in the Privacy header: 'user'.
- P-CSCF and the edge proxy (e.g. I-CSCF) must implement the following priv-value types of the Privacy header: 'none', 'id', 'critical', 'user'.

The privacy type 'session' should be left open for implementations.

The need of 'header' privacy type is for further study.

SA3 should include new sections on anonymity requirements and mechanisms to [33.cde]. Accompanied pseudo-CR suggests one alternative text. These requirements and mechanisms should later be added to [33.203].

4. References

[23.228] IP Multimedia Subsystem (IMS); Stage 2; (Release 5).

[33.106] 3G Security; Lawful Interception Requirements; (Release 5).

[33.107] 3G Security; Lawful Interception Architecture and Functions; (Release 5).

[33.108] 3G Security; Handover Interface for Lawful Interception; (Release 5).

[33.203] 3G Security; Access security for IP-based services; (Release 6).

[33.cde] Presence Service; Security; (Release 6).

[draft-ietf-sip-privacy-general-01] IETF, A Privacy Mechanism for the Session Initiation Protocol (SIP); June 6, 2002.

[draft-ietf-sip-asserted-identity-02] IETF, Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Newtworks; June 21, 2002.

3GPP TSG-SA3 Meeting #26 **Tdoc ⌘DocNumber**
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 ☒ Radio Access Network □ Core Network ☒

Title: ⌘	Anonymity in Presence		
Source: ⌘	Ericsson		
Work item code: ⌘	Presence	***Date:*** ⌘	14/11/2002
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: ⌘	IMS Release 5 already includes some degree of privacy. However, these requirements are not currenty described in any SA3 document. Furthermore, IMS Release 6 needs to supplemented with greater degree of subscriber anonymity in order to fulfill the privacy needs of Presence subsystem.
Summary of change: ⌘	Two sections describing subscriber anonymity requirements, and mechanisms has been added.
Consequences if not approved: ⌘	Implementations may use different approach, and the anonymity of the subscriber may be jeopardised.

Clauses affected: ⌘				
	Y	**N**		
Other specs affected: ⌘			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.

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".

[17] Draft-ietf-sip-privacy-general-01: A Privacy Mechanism for the Session Initiation Protocol (SIP), June 6, 2002.

[18] Draft-ietf-sip-asserted-identity-02: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Network, June 21, 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) Pw: IMS is enhanced by a security mechanism for the Watcher to request anonymity.

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)~~4) Peu & Pw: Ability of non-IMS accesses (e.g. WAP/SMS/WV) to fulfil the security requirements should be further studied.

~~6)~~5) Pw: The Presence Server may need additional mechanism for authenticating the Watchers. For example, the Presentity may provide passwords for Watcher authentication.

~~7)~~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.

~~8)Pw: IMS may need to be enhanced by a security mechanism for the Watcher to request anonymity.~~

[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

6.1.2 Subscriber anonymity

6.1.2.1 Initiator of a SIP dialog

The network shall hide the identity of the initiator of a SIP dialog in the following cases:

- The initiator has requested from the network that her identity is hidden from the receiver of the request.

- The initiator has agreed with the home network that the home network takes care of the identity blocking for certain messages on behalf of the initiator.

Anonymity shall be provided if the subscriber requests it. The network shall not deliver the message to the receiver if the initiator has set the anonymity request as ‘critical’, and the network is not able to provide the requested anonymity. The same anonymity rules shall apply to all messages within a SIP dialog.

Anonymity shall be provided by the last-hop P-CSCF. If the IMS originated messages are sent outside the IMS trust domain (e.g. to the open Internet), the edge proxy (e.g. I-CSCF) shall provide the anonymity.

Anonymity may be requested with multimedia sessions, or with any other services that will use IMS, such as Presence or Instant Messaging.

Even when the anonymity is provided, the Lawful Interception function may need to be able to monitor the SIP identities of the originator. It is up to the local legislation if the messages without identity information coming from open Internet are allowed to access the IMS trust domain without authentication. If such messages are not allowed within some sub-network, the edge proxy (e.g. I-CSCF) shall reject the message with appropriate error code.

6.1.2.2 Receiver of a SIP dialog initiation request

The receiver of a SIP dialog initiation request is able to have some degree of anonymity if she registers a pseudonym as IMPU. In this case, the subscriber shall be responsible for not revealing the relationship between the pseudonym IMPU and her real identity to unauthorized parties. If she releaves her real identity, there is no anonymity.

8 Security mechanisms

8.1 IMS related security mechanisms

8.1.2 Subscriber anonymity mechanisms

8.1.2.1 Anonymity of SIP dialog initiator

The anonymity mechanism is optional for implementation in UA. The UA may provide anonymity for the subscriber following the privacy mechanisms described in [17, and 18]. This includes populating the SIP headers with values that reflect the privacy requirements of the subscriber, as well as requesting further privacy from the network.

The UA may use the following priv-value types of the Privacy header in [17, and 18]:

- ‘none’
- ‘id’
- ‘critical’
- ‘user’

[Editors note:priv-value types ‘header’ and ‘session’ are FFS.]

The home network (e.g. S-CSCF or an Application Server) may provide the anonymity on behalf of the UA using the following priv-value type [17]:

- ‘user’

P-CSCF and the edge proxy (e.g. I-CSCF) must implement the following priv-value types of the Privacy header in [17, and 18]:

- ‘none’
- ‘id’
- ‘critical’
- ‘user’

[Editors note:priv-value types ‘header’ and ‘session’ are FFS.]

P-CSCF and the edge proxy shall monitor the privacy requests in all terminating SIP requests, and provide the requested privacy (e.g. hide the identity of the subscriber). P-CSCF and the edge proxy shall not provide privacy for originating SIP requests.

P-CSCF, edge proxy, S-CSCF, or an Application Server may reject all anonymous SIP requests without subscriber identity information if required in the local Lawful Interception policy.

8.1.2.2 Pseudonym IMPU

Subscriber may use pseudonym IMPU to obtain some degree of anonymity. From system point of view, the pseudonym IMPU is like any other IMPU. All existing rules related IMPUs shall apply.

> Note: Unprotected SIP REGISTER messages include identity information that may be intercepted by unauthorized parties when sent over the air-interface. These messages may be used to combine the IMPU and IMPI information, and consequently this information may reveal the parallel IMPUs related to the pseudonym IMPU.

[Editors note: There may be a need for additional rules related to the registration of pseudonym IMPUs.]