3GPP SA3 Meeting #26 **S3-020697**
Oxford, UK, 19-22 November 2002

Title:	**Presence Security Architecture**
Release:	6
Work Item:	PRESENCE
Source:	SA3
To:	CN1
Cc:	

Contact Person:
Name: Krister Boman
Tel. Number: +46313446055
E-mail Address: krister.boman@erv.ericsson.se

Attachments: S3-020620

---

1. Overall Description:

SA3 would like to thank CN1 for their LS on Verification of the identity of watchers S3-020598 (N1-022226). SA3 would also like to inform CN1 that SA3 is currently developing a TR for defining the security architecture as well as security requirements for Presence.

CN1 asked SA3 to review some proposed working assumptions. The review SA3 has performed suggests that CN1 should consider the following (please cf. also S3-020620 which is attached):

- If anonymity is allowed, the identity of those watchers that do not request anonymity should be verified.

  It is possible that the Presentity specifies a password utilising some out-of-band mechanism such that anonymous watchers can be authenticated i.e. that they know the correct password based on Digest. Furthermore if anonymity is allowed but privacy is not requested (i.e. the Privacy header has value 'none'), the identity of that user should be identified. In particular this means that CN1 should consider updating 7.2.2.1.1 reflecting this.

- Subscription Authorization Policy may define some additional access rules that must be verified before the subscription can be accepted.

  Examples of potential access rules are: required confidentiality protection for all notifications or authentication of anonymous watchers using presentity distributed HTTP Digest passwords.

- The semantics of missing access list should be clarified.

  If there is no access list, it is not clear if all watchers can access the presence information or if no watcher is allowed to access the presence information.

- Potential blocking lists should be checked before accepting the subscription.

  SA3 suggests that CN1 adds a functionality such that the Principal can add watchers that are not allowed to access presence information in blocking lists.

- CN1 should consider negative architectural consequences of situating the authentication of non-IMS watchers to the edge proxy.

  SA3 believes that such a requirement would complicate the design of presence service.

2. Actions:

To CN1 group.

ACTION: To review the feedback from SA3 and implement the security related recommendations in the CN1 TR for Presence

3. Date of Next SA3 Meetings:

SA3 Meeting #27	25-28 February 2003	Sophia Antipolis, France
SA3 Meeting #28	06-09 May 2003	Berlin, Germany

3GPP TSG SA WG3 Security — S3#26 **S3-020620**
19- 22 November 2002
Oxford, UK

Agenda Item: TBD

Source: Ericsson

Title: Watcher Authorization in Presence

Document for: Discussion/Decision

1. Introduction

CN1 has sent a LS [N1-022226] and accompanied document [N1-022225] to SA3 describing the watcher authorization and identity verification. CN1 requests SA3 to:

1) Verify the assumptions described in the documents.

2) Provide guidance, from the security point of view, as how to verify the identity of non-IMS watchers

This document analyses the CN1 documents and suggests a response to CN1.

2. Watcher Authorization in Presence

The access rules described in [N1-022225] are summarized in Table 1 below.

		Subscription request from the Watcher	
		Privacy Header included	No Privacy Header
List of users allowed to subscribe exists	Anonymity allowed	Decision 1: Access allowed, no identity verification	Decision 2: Access allowed, no identity verification
	Anonymity not allowed	Decision 3: No Access	Decision 4: Verify identity
List of users allowed to subscribe does not exist	-	Decision 5: N/A	Decision 6: N/A
Blocking lists	-	Decision 7: N/A	Decision 8: N/A

Table 1: Decision table describing the cases covered by [N1-022225].

It is suggested that the following details of [N1-022225] are commented by SA3 back to CN1:

- Verifying the identity of anonymous watchers: It is assumed that the identities of anonymous watchers are never verified (see Table 1, Decision 1). However, also anonymous watchers can be authenticated without revealing their identities using HTTP Digest. This feature could be useful when communicating with non-IMS subscriptions coming from open Internet. This is also related to an open issue in [TR 33.cde] on presence distributed Digest passwords. The passwords to be used in authentication could be distributed by the presentity using some 'out-of-band' channel, for example phone. Such mechanism could be useful with anonymous watchers. If the anonymous watcher does not have password, it can still use 'anonymous' username and empty password as specified in [RFC 3261]. In general, the authentication of anonymous watchers should be done only if the presentity has requested such service in the Subscription Authorization Policy.

- Anonymity allowed but no Privacy requested: It is assumed that when the Subscription Authorization Policy includes a private access list and, at the same time, anonymous subscriptions are allowed, the identity of watchers need not to be verified (see Table 1, Decision 2). In other words, the private access list does not have any functionality if anonymity is

allowed. This is seen here as a mistake. CN1 should add two sub cases to 7.2.2.1.1, 2a) describing the functionality if privacy was requested, and 2b) describing the functionality if privacy was not requested.

- Verifying other potential access rules: The presence information may be very sensitive in its nature, and consequently the end-user may want to set some additional access rules for subscriptions in the Subscription Authorization Policy. These additional access rules must be checked before the watcher is authorized. For example, the end-user may require that subscriptions are accepted only if confidentiality can be provided.

- Semantics of 'no access list': According to the current text in [N1-022225], the existence of private access list is not mandatory. It is not clear what happens if there is no such list. CN1 should specify if the semantics of 'no access list' is 'nobody allowed' or 'everybody allowed'.

- Blocking lists: The authorization rules include a list of users that are allowed, however, it does not include a list of users that are not allowed [cf. 23.141]. CN1 should consider adding such functionality. This may be needed in order to block out those watchers they request anonymity but are not allowed to access the presence information for that presentity, for example.

3. Authentication of non-IMS Watchers

CN1 has two alternative approaches where the authentication of the non-IMS watchers should take place: in the Presence Server or at the edge of the home network (e.g, I-CSCF). Both cases would probably use HTTP Digest for authentication because it is the common minimum denominator of authentication mechanisms in SIP. HTTP Digest is mandatory to implement in UA and proxies. It is also commonly used in web browsing.

Both solution are secure, however, the edge proxy approach clearly complicates the design, operation and maintenance of the presence service because:

- The edge proxy does not know whether the end application is interested in authenticating the user or not.
- The edge proxy would need to have a set of rules to decide when to authenticate users and when not, for example:
  - All SUBSCRIBE messages with Event=presence should be authenticated.
  - The edge proxy should have access to Subscriber Authorization Policy of the presentity.
- The edge proxy should have access to HTTP Digest passwords which may be specific only to Presence service.

4. Conclusions

It is suggested that SA3 sends a LS to CN1 verifying the security assumptions in document [N1-022225] but asking CN1 to consider and clarify the following details:

- If anonymity is allowed, the identity of those watchers that do not request anonymity should be verified.

- Subscription Authorization Policy may define some additional access rules that must be verified before the subscription can be accepted. Examples of potential access rules are required confidentiality protection for all notifications or authentication of anonymous watchers using presentity distributed HTTP Digest passwords.

- The semantics of missing access list should be clarified.

- Potential blocking lists should be checked before accepting the subscription.

It is also suggested that the LS should also guide the authentication of non-IMS watchers in the following way:

- CN1 should consider negative architectural consequences of situating the authentication of non-IMS watchers to the edge proxy.

5. References

[23.141] Presence service; Architecture and functional description; Stage 2; (Release 6).

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

[N1-022225] "Authorization of watchers", Ericsson, 3GPP TSG-CN1 Meeting #adhoc-Rel-6, Munich, Germany, 22 – 24 October 2002

[N1-022226] "LS on verification of the identity of watchers", 3GPP TSG-CN1 Meeting #adhoc-Rel-6, Munich, Germany, 22 – 24 October 2002

[RFC 3261] Session Initiation Protocol (SIP), IETF, RFC 3261.

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