3GPP TSG SA WG3 Security — S3#30 **S3-030579**
6 - 10 October **2003**
Povoa de Varzim, Portugal

Title:	**The requirement and feasibility of IMS watcher authentication**
Release:	Rel-6
Work Item:	Presence
Source:	SA3
To:	SA1
Cc:	SA2, CN1
Attachment:	S3-030400

Contact Person:
Name: Tao Haukka
Mobile Number: +358 40 5170079
E-mail address: tao.haukka@nokia.com

1. Introduction

SA3 #29 plenary has investigated under the work item Presence, the authentication of IMS-capable watcher by the presence server to request password from watcher, where password is issued by presentity to watcher. The security concern of the function is analysed in the attached Tdoc (S3-030400), which shows feasibility flaws in below:

- Password delivery is an open issue
- Password storage in watcher equipment may be problemetic
- Password is weaker than IMS network security. In other words, if IMS authentication is broken, password request does not guarantee further secure

Moreover, it is questioned whether the requirement is needed at all to IMS watcher to be authenticated by password issued by presentity. SA3 bears the up-to-date understanding that IMS-capable watcher should be authenticated by security provided by IMS network, therefore the function mentioned above seems to be a new requirement.

2. Actions

To SA1: SA3 kindly asks SA1 to evaluate the need of the new requirement, whether IMS watcher should be authenticated by password

To SA1, SA2 and CN1: SA3 kindly ask comments from groups in question, whether password is a feasible requirement and solution for non-IMS watcher authentication

3. SA3 future meetings

SA3#31	18-21 Nov. 2003	London

3GPP TSG SA WG3 Security — S3#29 **S3-030400**

15 - 18 July 2003, San Francisco, USA

Agenda Item:	7.18 (Presence)
Source:	Nokia
Title:	IMS watcher authentication
Document for:	Discussion/Decision

1. Introduction

SA3 #28 in Berlin approved S3-030246 for watcher's authentication. It is not clear from the discussion paper whether the proposal is for watcher from IMS or non-IMS. Based on our later investigation this seems to a new requirement to IMS watcher, so the topic is raised here again for further clarification, discussion and decision.

In section 2 we quote the specifications from all related groups on the IMS watcher. Section 3 is security discussion around the requirement. Finally our proposal is in section 4.

2. Specification status

In stage 1 requirements, SA1 [22.141] reads:
"It shall be possible to authenticate at any time a watcher and/or a presentity requesting access to the presence service. Existing security mechanisms as well as mechanisms specific to presence service may be used."

In stage 2 architecture, SA2 specification [23.141] specifies

- in section 5.3.2 that watcher authentication is done by Watcher Presence Proxy,
- in section 5.3.3 that Presentity's Presence Proxy shall perform authentication of Watcher Presence Proxy;
- and in section 5.3.4 that "The functionalities of the Watcher Presence Proxy are then taken care of by the P-CSCF and the S-CSCF:
  - The S-CSCF is responsible for authentication according to procedures described in 3GPP TS 33.203 [5].
  - The security mechanisms between the Watcher and the Presentity Presence proxy are defined by 3GPP TS 33.210 [8].

  The functionality of the Presentity Presence Proxy is taken care of by the I-CSCF and the S-CSCF as defined in 3GPP TS 23.228 [9]."

In stage 3 detail, CN1 specification [24.841] gives the state machine in section 7.2.2.1.2 on Watcher identify verification at the PS. It reads: "

a) if a Privacy header is present in the SUBSCRIBE request and the Privacy header value is set to "id" or "user", then the watcher and the subscription are considered as anonymous, and no further actions are required. The PS shall continue with the subscription authorization procedures described in subclause 7.2.2.1.4;

b) if there is no Privacy header present in the SUBSCRIBE request, or if the Privacy header contains a value other than "id" or "user", then the PS shall check for the presence of a P-Asserted-Identity header in the SUBSCRIBE request. Two cases exists:

i) **the SUBSCRIBE request contains a P-Asserted-Identity header. This is typically the case when the watcher is located inside a trusted domain as defined by 3GPP TS 24.229** [5] **subclause 4.4. In this case, the PS is aware of the identity of the watcher and no extra actions are needed. The PS shall continue with the subscription authorization procedures described in subclause 7.2.2.1.4.**

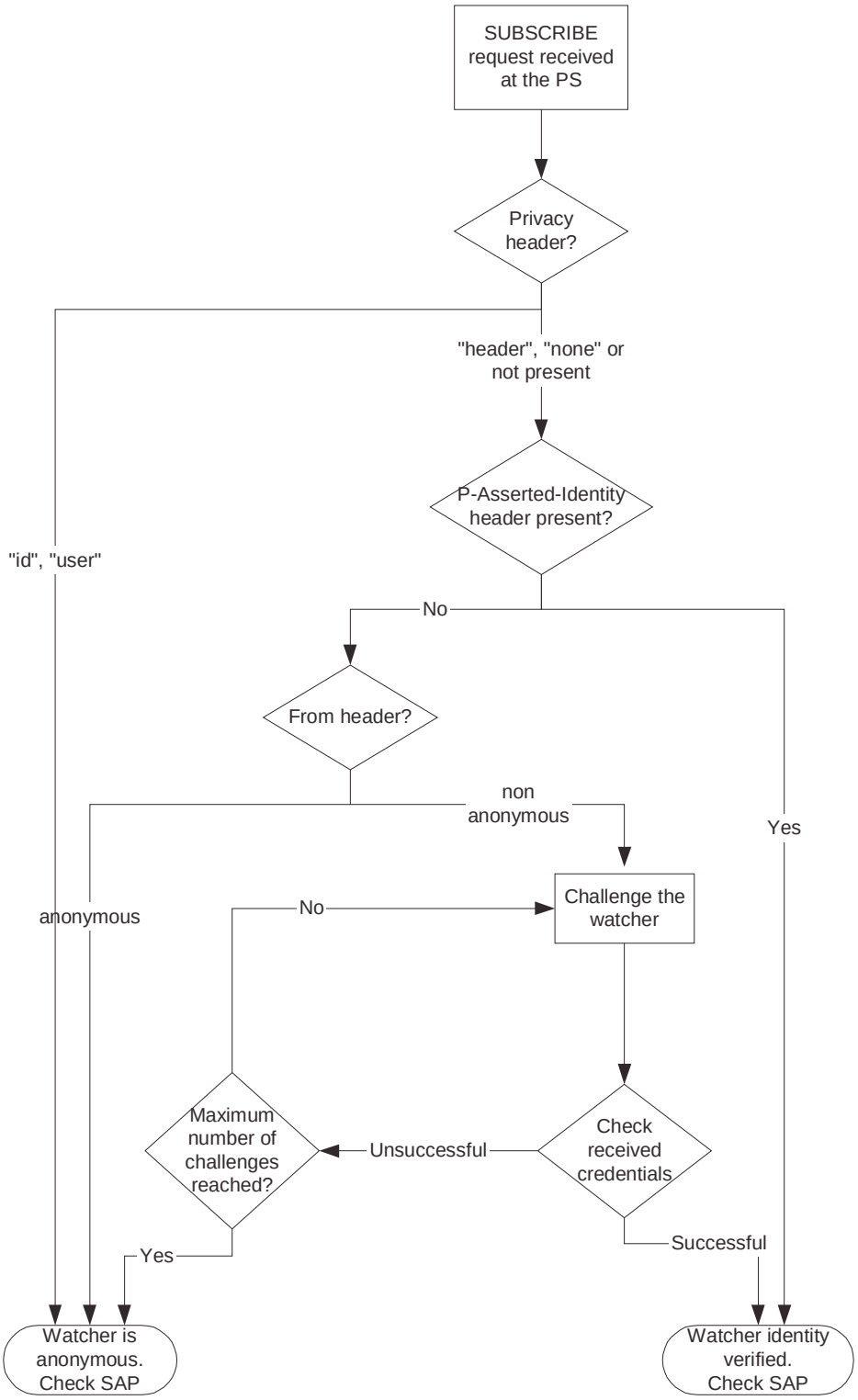
ii) the SUBSCRIBE request does not contain a P-Asserted-Identity header. This is typically the case when the watcher is located outside a trusted domain as defined by 3GPP TS 24.229 [5] subclause 4.4. In this case, the PS does not have a verified identity of the watcher. The PS shall check the From header of the SUBSCRIBE request. If the From header value in the SUBSCRIBE request is set to "Anonymous", then the watcher and the subscription are considered as anonymous and no further actions are required. If the From header value does not indicate anonymity, then the PS shall challenge the watcher by issuing a 401 (Unauthorized) response including a challenge as per procedures described in RFC 3261 [7.26]."

As we can see, once the IMS authentication is done and the P-asserted-identity header is present, the verification is complete. The other 2 related concepts here are

1) Anonymity of watcher. This means the watcher would like to keep anonymous to the subscription. Presence server does no further actions.
2) Check SAP means subscription authorization procedures. It means the Presence server shall check if the subscription authorization policy of the presentity allows that particular watcher. If policy allows anonymous watcher, then that type watcher will receive NOTIFY; or if only a list watchers are allowed, then Presence server must get and compare that particular watcher's identity against the list.

For non-IMS watcher, the mechanism is missing how to do the authentication, as suggested by an editor's notes:

" Editor's Note: it is not clear what are the mechanisms available to transport the credentials. These mechanisms can include, among others, P-Asserted-Identity, Authorization header, digital signatures, S/MIME body, etc." ([24.841])



3. Discussion

So this seems to be clear that IMS watcher authentication is based on IMS security in the specifications from all other group. The assumption is to simply trust other IMS networks that are interworking with the home IMS. Suppose this may be doubtful, we should still consier whether a password based authentication help to mitigate attack from other mis-behaved IMS network. Suppose a presentity has a higher trust in his home IMS, than other existing P-CSCFs, the Presence server would still need the P-CSCF to forward the challenge. As long as the correct watcher is on-line (P-CSCF has forwarded NOTIFY to that watcher), the P-CSCF can forward it to spoof the

expected Digest response, and hand it to an attacker. A more simplified way is even forward the NOTIFY containing someone's Presence Information to the correct watcher as well as another eavesdropper that could not be identified by Presentity nether watcher.

Next suppose the P-CSCF is trusted, but someone intruding IMS does the malicious insertion of the P-asserted-identity header. This could happen also with home IMS. So applying password based authentication to only external IMS does not seem to hold water completely.

Last but not least, we should think the feasibility of the solution. If a watcher checks his 50 buddies presence, it would not be a nice thing to remember all of theses, and input them one by one. Note it is required whenever watcher is registered to IMS again. If a presentity gives out his password to his 30 buddies (watchers), it is not clear who discloses it to another person, if the PI is disclosed. A requirement to that presentity to remember all different 50 passwords that s/he gives out to whom, seems to be also a user-unfriendly function.

In brief, we feel that password authentication is weaker than the mechanism provided by IMS identity verification, and does not improve IMS watcher authentication level. On the other hand, for non-IMS watcher this is better than trust on any identity provided by the end entity itself.

SA3 should also communicate with SA1 if the requirement is reasonable. In addition we should involve SA2 and CN1 what are their views on adding this new feature for IMS user since it will affect their specifications.

4. Proposal

Based on the discussion above, we would like to propose the presentity issued password based authentication as optional to the IMS, and maybe adopted for non-IMS watcher authentication.

Regardless of the decision, the communication to SA1should be generated on whether this new requirement makes sense to the IMS user, to SA2 and CN1 what are their views on adding this new feature for IMS user; and finally to all groups the solution for non-IMS watcher authentication.

5. Reference

[22.141] Presence Service, stage 1, V6.1.0, 3GPP. September, 2002.

[23.141] Presence Service: Architecture and Functional Description, V6.1.0, 3GPP. Dec. 2002.

[24.841] Presence service based on Session Initiation Protocol (SIP); Functional models, information flows and protocol details, 3GPP. May 2003.