3GPP TSG SA WG3 Security — S3#26 **S3-020598**
19- 22 November 2002
Oxford, UK

3GPP TSG-CN1 Meeting #adhoc-Rel-6 ***Tdoc N1-022226***
Munich, Germany, 22 – 24 October 2002

Title: LS on verification of the identity of watchers
Release: 6
Work Item: PRESENCE

Source: CN1
To: SA2, SA3

Contact Person:
Name: Miguel A. Garcia
Tel. Number: +358 9299 3553
E-mail Address: Miguel.A.Garcia@Ericsson.com

Attachments: N1-022225

---

1. Overall Description:

CN1 is developing the stage 3 specifications for the Presence service. CN1 has created the Technical Report 24.841 as placeholder for the Release 6 documentation, with the idea of moving the agreed text to the Release 6 version of the specifications under CN1 control.

During the discussion of tdoc N1-022225 (attached), some concerns were raised as with respect authentication of non IMS watchers. CN1 is seeking for guidance from SA2 and SA3.

2. Problem Description:

According to the stage 2 documentation for the Presence service, TS 23.141, the Presence Server (PS) is an application server, which is located in the presentity's home network.

The PS will receive SUBSCRIBE request coming from watchers who are interested on receiving the presentity's presence information. When the PS receives one of this requests, the PS has to verify the identity of the watcher and, and if Subscription Authorization Policy allows it, authorize the subscription.

Since it is required to provide access to the presentity's presence information to both IMS and non-IMS watchers, it is necessary to verify the identity of non-IMS watchers.

When the watcher is located in a trusted domain, such as the 3GPP IMS, the authentication is done according to the regular IMS procedures, that is, the P-CSCF inserts a P-Asserted-Identity with a valid identity of the watcher. The Presence Server trusts the contents of the P-Asserted-Identity.

However, based on the current security mechanisms for Release 5, when the watcher is located outside the trusted domain, e.g., an Internet watcher, there is not P-Asserted-Identity in the SIP request, and therefore, the Presence Server cannot verify its identity. If these mechanisms continue to be the same in Release 6, the presence server needs to verify the identity of the watcher.

In this case, an entity inside the home network needs to verify the identity the watcher. It is believed that the watcher may be provided with a username/password combination to access the presentity's presence information.

One possible solution is that the Presence Server answers a SUBSCRIBE request with a 401 (Unauthorized) response, giving the opportunity to the watcher to authenticate himself, with a general authentication mechanism, such as Digest (mandatory in RFC 3261 to all User Agents and Proxies)

Another possible solution is to provide some other means to verify the identity of the watcher at the edge of the network, e.g., at the I-CSCF. The I-CSCF could insert a P-Asserted-Identity if it gets valid credentials.

CN1 has not taken a determination yet, and is investigating all the possible solutions to the described problem.

Additionally, CN1 believes that verifying the identity of SIP requests coming from non IMS networks is a general problem that may affect not only subscriptions, but also other types of SIP requests.

3. Actions:

To SA2 group.

ACTION: CN1 asks SA2 to verify the assumptions described in this LS and the companion document, and provide guidance, from the architectural point of view, as for how to verify the identity non-IMS watchers subscription attempts

To SA3 group.

ACTION: CN1 asksSA3 to verify the assumptions described in this LS and the companion document, and provide guidance, from the security point of view, as for how to verify the identity non-IMS watchers subscription attempts

4. Date of Next TSG-CN1 Meetings:

CN1_27	11th – 15th November 2002	Bangkok, Thailand
CN1_28	10th – 14th February 2003	Dublin, Irland
CN1_29	07th – 11th April 2003	?, ?

3GPP TSG-CN1 Meeting #adhoc-Rel-6 ***Tdoc N1-022225***
Munich, Germany, 22 – 24 October 2002

Source: Ericsson

Title: Authorization of watchers

Agenda item: 8.1

Document for: Approval

Introduction

This document proposes the addition of two new subclauses under subclause 7.2.2.1 to the Application Server procedures in TR 24.841.

The new subclauses detail the procedures related to the authorization and verification of the identity of watchers and presentities.

Proposal

It is proposed to add some definitions to the definitions subclause and add new subclauses dealing with watcher identity verification and authorization.

First proposed change

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: "3G Vocabulary".

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

[3] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model; Stage 2".

[4] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

[5] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[6] 3GPP TS 23.141: "Presence Service; Architecture and Functional Description".

[7] RFC 2778: "A Model for Presence and Instant Messaging"

Next proposed change

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions defined in 3GPP TS 21.905 [1], ~~and~~ 3GPP TS 22.141 [2], RFC 2778 [7] and the following apply:

Presence network agent: a network located element that collects and sends network related presence information on behalf of the presentity to a presence server.

Presence server: a network entity responsible for managing presence information on behalf of a presence entity.

Presence user agent: a terminal or network located element that collects and sends user related presence information to a presence server on behalf of a Principal.

Subscription Authorization Policy: a policy that determines which Watchers are allowed to subscribe to a Presentity's Presence information. The Subscription Authorization Policy also determines which tuples of the Presentity's Presence information the watcher has access.

Next proposed change. New subclauses

7.2.2.1 Application Server (AS) acting as terminating UA, or redirect server

7.2.2.1.1 Watcher authorization at the Presence Server (PS)

When the PS receives a SUBSCRIBE request from a watcher who is subscribing to the presence information for a determined presentity, several cases exist:

1) If the Subscription Authorization Policy for the presentity contains a closed list of users who can access to the presentity information and the Subscription Authorization Policy indicates that anonymous access is not granted, the PS shall first check if the Privacy header indicates if privacy was requested.

   a) If Privacy was requested, then the PS shall not authorize the subscription.

   b) If Privacy was not requested then the PS shall verify the identity of the watcher according to the procedures described in subclause 7.2.2.12. Once the identity of the watcher is verified, then PS shall check if any of the URIs included in the P-Asserted-Identity header or supplied in the authentication procedure are allowed to subscribe to the presence information. If none of these URIs are listed in the Subscription Authorization Policy for the presentity, then if the Presentity has subscribed to it's own watcher information then the PS shall notify the presentity of the pending subscription by sending a NOTIFY request with a partial state update containing the public user identity of the unauthorized watcher. Otherwise the PS shall not authorize the subscription.

Editor's Note: The exact mechanism for the presentity to provide authorization is FFS.

2) If the Subscription Authorization Policy for the presentity indicates that anonymous subscriber access is granted, then the PS shall authorize the subscription.

The procedures by which the PS does not authorize a subscription are any of the following:

- the PS rejects the subscription; or

- the PS does a polite blocking

7.2.2.1.2 Watcher identify verification at the Presence Server (PS)

When the PS receives a SUBSCRIBE request from a watcher who is subscribing to the presence information for a determined presentity, the PS, depending on the Subscription Authorization Policy, may need to verify the identity of the watcher prior to authorize the subscription.

If the PS needs to verify the identity of the watcher, when the PS receives a SUBSCRIBE request that does not contain credentials, two cases exist:

a) 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 24.229 subclause 4.4. In this case, the PS is aware of the identity of the watcher and no extra actions are needed.

b) 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 subclause 4.4. In this case, the PS does not have a verified identity of the watcher. The PS, depending on the Subscription Authorization Policy may need to verify the identity of the watcher.

Editor's Note: The exact mechanism to verify the identity of the user is FFS. One possible mechanism to verify the identity of the watcher is that the PS challenges the watcher by issuing a 401 (Unauthorized) response including a challenge (as per normal procedures described in RFC 3261). Later, when the PS receives a SUBSCRIBE request that contains credentials but it does not contain a P-Asserted-Identity, the PS will check the credentials to verify the identity of the watcher.

Editor's Note: Another possible mechanism is that an edge proxy, such as the I-CSCF verifies the identity of the user and inserts a P-Asserted-Identity. In this case, the paragraph b above becomes an error case.