3GPP TSG SA WG3 Security **S3-030246**

6th – 9th May, 2003

Berlin, Germany

Agenda Item: 7.19 Presence

Source: Ericsson

Title: Watcher Authentication

Document for: Discussion/Decision

1. Introduction

This document discusses the issue related to Watcher authentication in Presence introduced in [S3-030068]. Different alternative solutions are further analyzed.

Ericsson's preferred solution is based on HTTP Digest. This proposal explicitly excludes the use of S/MIME and Enhanced Identity Management, but may still include features from solutions that use HTTP Digest AKA.

2. Alternative solutions

[S3-030068] described a potential security problem related to Watcher authentication in Presence. In general, security provided by the existing IMS trust management mechanism (i.e. P-Asserted-Identity header) was questioned to protect the end-user privacy in sufficient manner. Since Presence may carry privacy sensitive information, such as geographic location, the use of more advanced security measures than just P-Asserted-Identity header may be appropriate.

This document further analyses solutions related to Watcher authentication. All presented scenarios assume that the watcher belongs to different home network than the presentity. All SIP elements in the figures may include additional Proxy Servers between them.

2.1 Solutions based on transitive trust

Re-use of HTTP Digest AKA

It is possible to re-use HTTP Digest AKA if all SUBSCRIBE messages are authenticated by some entity in the home network, and the rest of the path to the Presence Server is protected using some underlying security mechanism, for example TLS. The Presence Server must not accept any SUBSCRIBE request that is not protected with TLS, and which is not coming from trusted source. Figure 1 demonstrates the principles of the architecture.

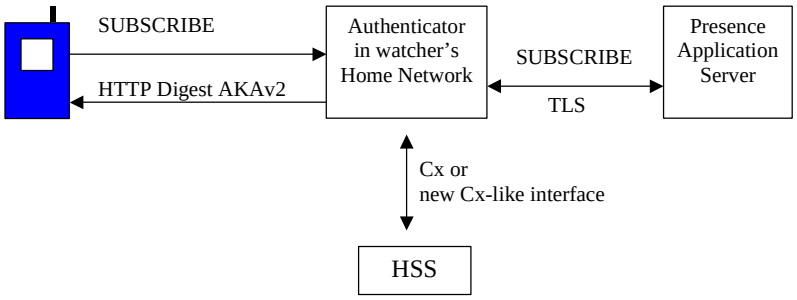

Figure 1: Architecture based on HTTP Digest AKA. Note that the figure does not include all possible proxies.

- If the authenticator is not S-CSCF, then new Cx-like interface would be needed.

SIPS

If the presentity had a SIPS URI as an identity, the use of TLS in every hop between the Watcher application and the home domain of the Presence Server would be required. In this way, the Presence Server would be able to trust that the Presence subscriptions originate from authorized source.

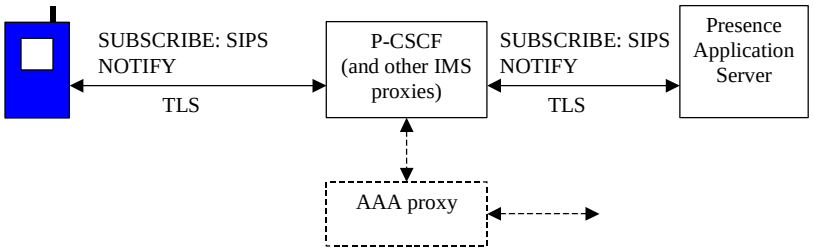

Figure 2: Architecture based on SIPS. Note that the figure does not include all possible proxies.

- The use of SIPS would require parallel use of TLS and IPsec towards IMS capable watcher application. It is not clear if IPsec could be used with SIPS in the first hop, or if the IPsec could be replaced by TLS in IMS Release 6. Note that TLS may need to be implemented in the UE for the Mt interface.

- If IPsec was replaced by TLS, and the watcher did not have certificate, it would still need to be authenticated using HTTP Digest AKA. According to IETF SIP model, P-CSCF should perform the authentication in the visited network using, e.g. some new AAA infrastructure to derive the AKA authentication credentials from the home network. Alternatively, the TLS based solution could re-use the Release 5 variant where the REGISTER messages are forwarded to the home without authentication, and leave the TLS connection open for subsequent SIP requests.

Enhanced identity management

IETF is currently working on enhancements for authenticated identity management, and there exists plans to introduce cryptographic tokens to secure the distribution of authenticated identities [draft-sip-identity].

There are two alternative architectures where different entities in the IMS network act as the Authenticator who could verify the identity information: one based on P-CSCF, and another based on home network. In both cases, the Authenticator may need to act as “back-to-back-user-agent” (B2BUA) in order to minimize the number of roundtrips.

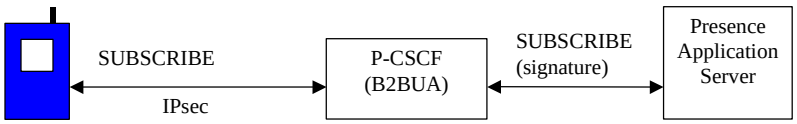

Figure 3a: Enhanced identity management in P-CSCF. Note that the figure does not include all possible proxies.

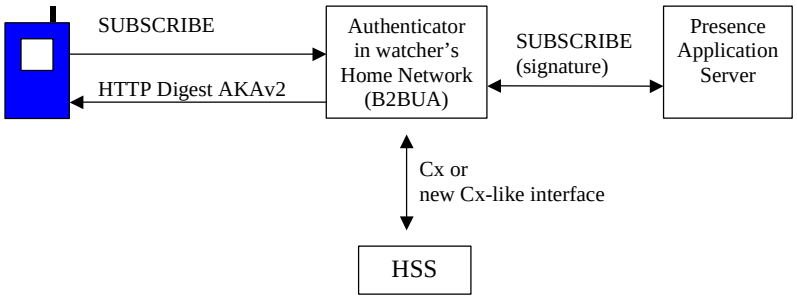

Figure 3b: Enhanced identity management in the home network. Note that the figure does not include all possible proxies.

- The standards in IETF are not mature yet.

- Would require IMS-domain specific PKI. In particular, the Presence Server should be able to verify digital signatures created by the authenticator in some other network. Similar work is currently defined for NDS/Authentication Framework work item.
- If the Authenticator was located in the home network, then would need to use HTTP Digest AKA, and solve the problem related to Cx-like interface.

2.2 End-to-end authentication solutions

HTTP Digest

HTTP Digest is the only authentication mechanism that is mandatory to implement in all SIP User Agents and Proxies. Even though HTTP Digest includes a password distribution problem, it can be used to fulfil the requirement. In those cases in which the watcher does not belong to the same network as the presentity, the presentity may be able to distribute the passwords. Furthermore, anonymous watchers may use “anonymous” usernames and “empty” passwords as defined in [RFC3261]. It is also possible that Watchers outside the home network of the presentity could register to the Presence Server via some HTTP related procedure, for example. Also, the use of some HTTP compliant Single-Sign-On solution may be appropriate.

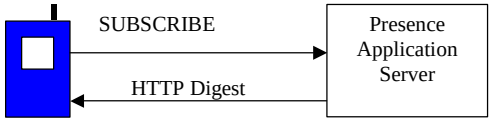

Figure 4: Solution based on HTTP Digest. Note that the figure does not include all possible proxies.

- Distribution of HTTP Digest passwords may include scalability problems.

S/MIME

The use of S/MIME for authentication is possible if the terminal has subscriber certificate. The use of symmetric keys is not appropriate with S/MIME since HTTP Digest is already implemented in every UE (see solution above).

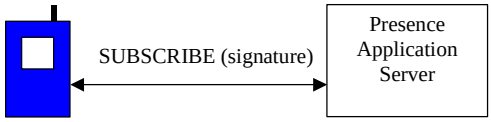

Figure 5: S/MIME based solution. Note that the figure does not include all possible proxies.

- Requires IMS specific PKI. In minimum, the Presence Server should be able to verify digital signatures created by the watcher, and vice versa. Note that even though Subscriber Certificate work item may cover the certificate part of this solution, it does not cover the PKI part.
- S/MIME would create an interrelationship with subscriber certificate WID. This may not be appropriate within Release 6 time scale.
- The UE already includes quite many security mechanisms (IPsec, TLS for Mt-interface, HTTP Digest, HTTP Digest AKA). For this reason, the use of S/MIME may not be appropriate if some of the existing ones is not removed at the same time.

3. Conclusions

At least the following issues should be taken into account before the final decision on the issue is taken:

- Existing IMS trust model is based on the use of P-Asserted-Identity header and underlying network security. The Watcher authentication problem could be solved by changing the existing IMS trust model to fit the IETF trust model by adding TLS between every proxy in the network. Changing this fundamental assumption is probably too big step between Release 5 and 6.
- Security mechanisms in UE: UE already includes IPsec, HTTP Digest and HTTP Digest AKA implementations. The Mt interface may require the implementation of TLS for the UE. The number of security mechanisms should not be increased from this unless some existing ones are removed at the same time.
- The use of S/MIME or Enhanced Identity Management requires PKI, which seems to create unnecessary complexity.

Ericsson proposes that SA3 chooses the use of HTTP Digest as the solution for the Watcher authentication problem. The requirement of authenticating every subscription request could be lowered from mandatory to optional; however, all Presence Servers should be able to authenticate the watcher if required by the presentity via the Authorization policy.

Distribution of HTTP Digest passwords is seen as an implementation problem. The use of HTTP Digest AKA would be possible if the Watcher belong to the same home network than the presentity. However, this would require a new Cx-like interface between Presence Server and HSS. If the presentity and the watcher belong to different networks, the distribution could be done by the presentity. Alternatively, watchers outside the home network of the presentity may need to register to the Presence Server via some HTTP procedure.

4. References

[draft-sip-identity] J. Peterson (2003) Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), IETF, Work in progress, draft-ietf-sip-identity-01.

[RFC3261] J. Rosenberg et. al. (2002) SIP: Session Initiation Protocol, IETF. RFC 3261.

[S3-030068] Ericsson (2003) End-to-end authentication of Presence subscriptions in Pw, 3GPP, S3#26, 25 - 28 February, Sophia Antipolis, France.

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 ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Authentication of subscriptions in Presence
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 current trust management mechanisms in IMS need to be enhanced in the way that end-user privacy can be sufficiently protected.
Summary of change:	⌘	Based on subscription authorization policy, the Presence Server may authenticate the watcher using HTTP Digest. The use of HTTP Digest AKA and LCS specific security are for further study.
Consequences if not approved:	⌘	The end-user privacy may not be sufficiently protected.

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.

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.

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

---

6.1.3 Subscription authentication

~~*[Editors Note: This is a placeholder for IMS related Watcher authentication requirement.]*~~

The Presence Server shall authenticate the subscription requests originated from Watchers if required in the Subscription Authorization Policy. The Subscription Authorization Policy shall indicate the method and credentials used in authentication.

8.1.4 Subscription authentication mechanism

Subscription Authorization Policy may require that the Presence Server must authenticate the Watchers during the subscription phase. The Subscription Authorization Policy shall define which authentication method and credentials are used in the authentication. The following mechanisms shall be supported:

- HTTP Digest

NOTE: Distribution of HTTP Digest passwords is outside the scope of this specification. There are many known solutions, e.g. the presentity can take responsibility of the key distribution, or the watchers may need to register to Presence Servers via HTTP.

[Editors Note: ~~This is a placeholder for end-to-end Watcher authentication solution. At least the following solutions may be considered~~ The use of HTTP Digest AKA is FFS:

- *HTTP Digest AKA: If the watcher belongs to the same home network than the presentity, HTTP Digest AKA could be used for authentication. In this case, the related session keys IK and CK would also be available for end-to-end integrity and confidentiality protection if needed. Note that it is also possible to change the IMS/Presence security architecture in the way that all subscriptions are always routed via the Presence Server, and that the communication between the IMS sub-domains is done only between the Presence Servers.*

~~- *HTTP Digest: HTTP Digest is the only authentication mechanism that is mandatory to implement in all SIP User Agents and Proxies. Even though HTTP Digest includes a password distribution problem, it can be used to fulfil the requirement. In those cases in which the watcher does not belong to the same network as the presentity, the presentity may be able to distribute the passwords. Furthermore, anonymous watchers may use "anonymous" usernames and "empty" passwords as defined in [RFC3261]. Also, enhancement of HTTP authentication framework with SIP compatible Single Sign On solution should be further studied.*~~

~~- *SIPS: If the presentity has a SIPS URI as an identity, the use of TLS in every hop between the Watcher application and the home domain of the Presence Server is required.*~~

~~- *S/MIME: The use of S/MIME for authentication is possible if the terminal has subscriber certificate.*~~

~~IETF is currently working on enhancements for authenticated identity management, and there exists plans to introduce cryptographic tokens to secure the distribution of authenticated identities [draft-sip-identity-enhancement].~~]