3GPP TSG SA WG3 Security — SA3#33 **S3-040349**
10-14 May 2004
Beijing, China

Source: **Ericsson**

Title: **Presence Security Updates**

Document for: **Discussion and decision**

Agenda Item: **Presence**

1 Introduction

The target for freezing release 6 specifications is set to September 2004. Decisions on open issues need to be taken at SA3 #33 to complete the Presence Security TS for release 6. Some issues - like the transfer of user identities - need to be resolved, but except for that we think that the current TS 33.141 v 1.1.1 meets the need for Presence Security for release 6.

We propose not to specify TLS v1.1, TLS extensions and shared key TLS for release 6. We also propose to choose the reverse proxy as the Authentication Proxy solution.

2 Discussion

2.1 TLS v1.1 and TLS extensions

TS 33.141 v 1.1.1 [1] contains the following editor's notes:

> Editors Note The specification need to consider [6], [8] and [9] and make appropriate profiling of these TLS protocols and the TLS version 1.1. need to be considered also. [TS 33.141, Section 4]
>
> Editors Note: It is FFS if it is possible to base the Presence Security on TLSv1.1 [14], which is currently in draft status in IETF. [TS 33.141, section 6]
>
> Editors Note: It is FFS what parts (if any) of the TLS extensions as specified in RFC 3546 [9] that shall be implemented in this TS [TS 33.141, section 6.2]

TLS v 1.1 [2] is still in draft status in IETF. Transport Layer Security (TLS) Extensions [3] has been published as RFC 3546.

An appropriate profiling of TLS for version 1 was agreed at SA3 #32 [4]. Currently no compelling arguments are seen for specifying TLS v1.1 and TLS extensions in release 6. Thus, we think that the editor's notes above can be removed from the draft Presence Security TS, and that TLS v1.1 and TLS extensions can be considered for use in later releases.

Proposal 1: TLS v1.1 and TLS extensions are not specified for Presence Security in release 6. The feasibility of TLS v1.1 and TLS extensions are to be reconsidered in later releases.

2.2 Shared Key TLS

Two proposals for shared key TLS are under consideration in the IETF TLS working group: "Use of Shared Keys in the TLS Protocol" [5] and "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)" [6]. No decisions have been made thus far on which proposal should be chosen. The "Use of Shared Keys in the TLS Protocol" Internet Draft expired in April 2004 and the "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)" (draft-eronen-tls-psk-00.txt) Internet Draft is not adopted as an IETF TLS WG working document yet.

We see it as unlikely that work on shared key TLS will be ready in release 6 timeframe. Therefore, we think that SA3 should endorse the following proposal:

Proposal 2: Shared key TLS needs to be more mature before being considered for Presence Security, and thus shared key TLS should not be specified for Presence Security in release 6. The feasibility of shared key TLS can be reconsidered in later releases.

2.3 Authentication Proxy

TS 33.141 v1.1.1 [1] section 4 contains the following text:

> "The use of an Authentication Proxy should be such that there is no need to manage the Authentication Proxy configuration in the UE.
>
> NOTE 2: This requirement implies that the Authentication Proxy should should be a reverse proxy in the following sense: A reverse proxy is a web server system that is capable of serving web pages sourced from other web servers - in addition to web pages on disk or generated dynamically by CGI - making these pages look like they originated at the reverse proxy
>
> [Editors Note: The above requirement may be revisited after the following issues are fully studied:
>
> - Feasibility of shared-key TLS
> - Terminal Configurability]"

TS 33.141 Annex A contains the following editor's notes:

> Editor's Note: The shared-key TLS based authentication does not require server's certificate, but the possession of the key for authentication. The procedure is FFS.
>
> Editors Note: The text in this informative annex may need to be revisited if changes in the main body of the text are made and when a final solution have been chosen.

As mentioned in section 2.2, shared key TLS is experiencing slow progress in IETF and cannot be considered mature. There has been no input in SA3 on terminal configurability so far. In order to progress Presence Security for release 6 in a timely manner, we therefore think that these editor's notes should be removed and that SA3 decides that the Authentication Proxy should be a reverse proxy.

Proposal 3: The Authentication Proxy shall be a reverse proxy.

3 Proposal

We propose that SA3 endorses Proposals 1-3:

> Proposal 1: TLS v1.1 and TLS extensions are not specified for Presence Security in release 6. The feasibility of TLS v1.1 and TLS extensions are to be reconsidered in later releases.
>
> Proposal 2: Shared key TLS needs to be more mature before being considered for Presence Security, and thus shared key TLS should not be specified for Presence Security in release 6. The feasibility of shared key TLS can be reconsidered in later releases.
>
> Proposal 3: The Authentication Proxy shall be a reverse proxy.

The attached pseudo-CR implements the relevant changes to TS 33.141. We propose that SA3 endorses these changes.

4 References

[1] 3GPP TS 33.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service; Security"

[2] P.Gutmann, Use of Shared Keys in the TLS Protocol, draft-ietf-tls-sharedkeys-02 (expired), October 2003

[3] P. Eronen, H. Tschofenig, Pre-Shared Key Ciphersuites for Transport Layer Security (TLS), draft-eronen-tls-psk-00.txt (work in progress), February 6, 2004

[4] 3GPP TSG SA WG3, S3-040169, Security Mechanisms for Presence

[5] IETF draft-ietf-tls-rfc2246-bis-05 (2004): “The TLS Protocol Version 1.1”

[6] IETF RFC 3546 (2003): "Transport Layer Security (TLS) Extensions".

3GPP TSG-SA WG3 Meeting #33
Beijing, China, 10 - 14 May 2004

Tdoc ⌘DocNumber

CR-Form-v7

CHANGE REQUEST

⌘	**33.141**	**CR**	**CRNum**	⌘ **rev**	**-**	⌘	Current version:	**1.1.1** ⌘

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:	⌘	Presence Security Updates		
Source:	⌘	Ericsson		
Work item code:	⌘	Presence	***Date:*** ⌘	03/05/2004
Category:	⌘	**C**	***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:	⌘	Progress Presence Security for release 6
Summary of change:	⌘	- TLS v1.1 and TLS extensions are not specified for Presence Security in release 6. - Shared key TLS needs to be more mature before being considered for Presence Security, and thus shared key TLS should not specified for Presence Security in release 6. - The authentication Proxy shall be a reverse proxy.
Consequences if not approved:	⌘	

Clauses affected:	⌘	4, 5.1.1, 5.1.4, 6, 6.2, Annex A				
		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.

*** BEGIN OF CHANGE ***

4 Overview of the security architecture

An IMS operator using the CSCFs as Watcher Presence proxies and Presentity Presence proxies may offer the Presence services on top of the IMS network, cf. 3GPP TS 22.141 [2]. The access security for IMS is specified in 3GPP TS 33.203 [4] ensuring that SIP signalling is integrity protected and that IMS subscribers are authenticated through the use of IMS AKA. The security termination point from the UE towards the network is in the P-CSCF utilising IPsec ESP.

A watcher can be sending a SIP SUBSCRIBE over IMS towards the network to subscribe or to fetch presence information, i.e. the Presence Service supports SIP-based communications for publishing presence information. The presence information is provided by the Presence Server to the Watcher Application using SIP NOTIFY along the dialogue setup by SUBSCRIBE. This traffic is protected in a hop-by-hop fashion using a combination of SEGs as specified in 3GPP TS 33.210 [10] with the access security provided in 3GPP TS 33.203 [4].

The Presence Server is responsible for managing presence information on behalf of the presence entity and it resides in the presentity's home network. Furthermore the Presence Server provides with a subscription authorization policy that is used to determine which watchers are allowed to subscribe to certain presence information. Also the Presence Server shall before subscription is accepted try to verify the identity of the watcher before the watcher subscribes to presence information. Optionally, depending on the implementation, the Presence Server may authenticate an anonymous watcher depending on the Subscription Authorization Policy.

A Presence List Server is responsible of storing grouped lists of watched presentities and enable a Watcher Application to subscribe to the presence of multiple presentities using a single SIP SUBSCRIBE transaction. The Presence List Server also stores and enables management of filters in the presence list, cf. Figure 1.

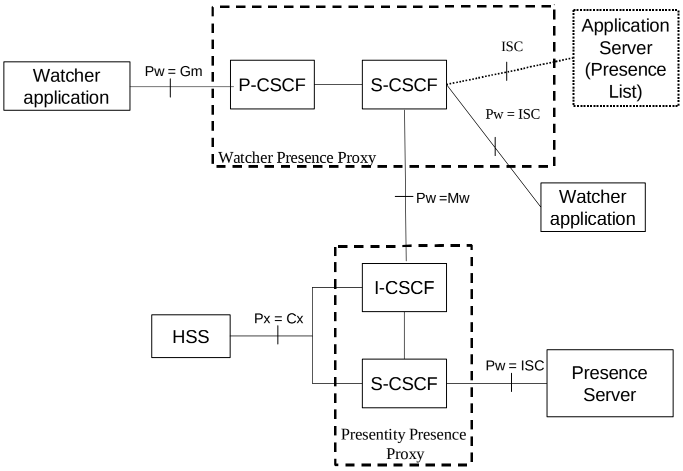

Figure 1: The Location of the Presence Server and the Presence List Server from an IMS point of view

A Presence User Agent shall be able to manage the data on the AS over the Ut interface, cf. 3GPP TS 23.002 [7], which is based on HTTP. This interface is not covered in 3GPP TS 33.203 [4] and it is mainly this interface for Presence use, which is covered in this specification. Before manipulation is allowed the user needs to be authenticated.

Note: In the text below the term Presence Server refers to both the Presence Server and the Presence List Server as depicted in Figure 1 above. For definitions of the Application Servers for Presence services the reader should consult 3GPP TS 23.141 [3]

The Ut interface needs the following security features:

1. it shall be possible to provide with mutual authentication between the Presence Server and the Watcher/Presentity;
2. a secure link and security association shall be established between the Presence Server and the Watcher/Presentity. Data origin authentication shall be provided as well as confidentiality protection.

~~Editors Note The specification need to consider [6], [8] and [9] and make appropriate profiling of these TLS protocols and the TLS version 1.1. need to be considered also.~~

Editors Note: The exact details of the security architecture is FFS and dependant on decisions related with the ongoing work on GBA (Generic Bootstrapping Architecture).

An overview of the security architecture for Presence Ut Interface is depicted in figure 2:

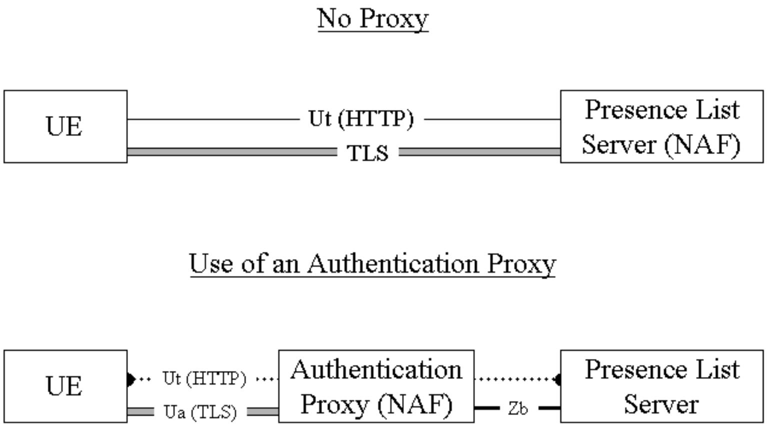
No Proxy
UE
Ut (HTTP)
TLS
Presence List Server (NAF)
Use of an Authentication Proxy
UE
Ut (HTTP)
Ua (TLS)
Authentication Proxy (NAF)
Zb
Presence List Server

Figure 2: An overview of the Security architecture for the Ut interface including the support of an Authentication Proxy

Editors Note: The exact requirements on the Zb interface the use of NDS/IP for Presence Security are FFS.

*** END OF CHANGE ***

*** BEGIN OF CHANGE ***

5.1.1 Authentication of the subscriber and the network

A subscriber shall be authenticated before accessing user data in a server. The subscriber shall only be able to manipulate data that is associated with that particular subscriber.

Editors note: Relationship between Transaction Identifier and subscriber identity is ffs. In the case of Presence Ut interface, there are several potential identities that are related to the Transaction Identifier, i.e. IMPI and IMPUs. The subscriber may have several Presence accounts related to same IMPI. Transaction Identifier does not carry enough information on which IMPU the end-user is trying to use.

Authentication between the subscriber and the network shall be performed as specified in clause 6.1.

Subscriber authentication can be made by the operator using proprietary or non-3G standardized methods. In case 3GPP authentication mechanisms are used, the authentication of the subscriber shall be based on the USIM. The authentication of the subscriber and the network shall be based on Generic Authentication Architecture as defined in 3GPP TR 33.919 [15]. Generic Authentication Architecture enables the use of different authentication methods to be used for the authentication of the subcriber by using:

- subscriber certificates (e.g., TLS, cf. [6,8,9]), or
- shared secrets (e.g., TLS with HTTP Digest, cf. [17]).

The server certificate to be used for application server authentication shall be based on WAPCert [12].

NOTE: The interleaving attack shall not be possible.

~~Editors Note: It is agreed that the shared key TLS draft need to be more mature in IETF before being considered for Presence. It is FFS and a decision is expected at SA3#32, cf. also S3-030721 and S3-030732.~~

Editors Note: If 3GPP decides that ISIM-only UICCs are allowed then it needs to be studied further if also the ISIM may be used in the Generic Authentication Architecture

A UE may contact the Presence Server/Presence Server for further instructions on authentication procedures.

The consumption of Authentication Vectors should be minimized. The architecture shall ensure that SQN synchronization failures is minimized.

*** END OF CHANGE ***

*** BEGIN OF CHANGE ***

5.1.4 Authentication Proxy

The Authentication Proxy may reside between the UE and the Presence Server as depicted in Figure 2. The usefulness of an Authentication Proxy may be to reduce the consumption of authentication vectors and/or to minimize SQN synchronization failures.

The following requirements apply for the use of an Authentication Proxy:

- Authentication Proxy may authenticate the UE using the means of Generic Bootstrapping Architecture.
- Authentication Proxy shall send the authenticated identity of the UE to the application server belonging to the trust domain at the beginning of new HTTP session.
- Authentication Proxy may not reveal the authenticated identity of the UE to the application server not belonging to the trust domain if required.
- The authenticated identity management mechanism shall not prevent the application server to use an appropriate session management mechanisms with the client.
- The UE shall be able to create multiple parallel HTTP sessions via the Authentication Proxy towards different application servers.
- Activation of transfer of asserted user identity shall be configurable in the Authentication Proxy on a per AS base.
- Implementation of check of asserted user identity in the AS is optional.

NOTE 1: The used session management mechanism is out of the scope of 3GPP specifications.

The use of an Authentication Proxy should be such that there is no need to manage the Authentication Proxy configuration in the UE.

NOTE 2: This requirement implies that the Authentication Proxy ~~should be~~is a reverse proxy in the following sense: A reverse proxy is a web server system that is capable of serving web pages sourced from other web servers - in addition to web pages on disk or generated dynamically by CGI - making these pages look like they originated at the reverse proxy

~~[Editors Note: The above requirement may be revisited after the following issues are fully studied:~~

- ~~Feasibility of shared key TLS~~
- ~~Terminal Configurability]~~

*** END OF CHANGE ***

*** BEGIN OF CHANGE ***

6 Security Mechanisms

The UE and the AP/Presence Server shall support the TLS version as specified in RFC 2246 [6] and WAP-219-TLS [13] or higher. Earlier versions are not allowed.

~~Editors Note: It is FFS if it is possible to base the Presence Security on TLSv1.1 [14], which is currently in draft status in IETF~~.

Note 1: The management of Root Certificates is out of scope for this Technical Specification

*** END OF CHANGE ***

*** BEGIN OF CHANGE ***

6.2 Protection mechanisms

The UE shall support the CipherSuite TLS_RSA_ WITH_3DES_EDE_CBC_SHA. All other Cipher Suites as defined in RFC 2246 [6] are optional for implementation for the UE.

The AP/Presence Server shall support the CipherSuite TLS_RSA_ WITH_3DES_EDE_CBC_SHA and the CipherSuite TLS_RSA_WITH_RC4_128_SHA. All other Cipher Suites as defined in RFC 2246 [6] are optional for implementation for the AP/Presence Server.

Editors Note: It is FFS is this specification should mandate any of the AES cipher suites as specified in RFC 3268.

Cipher Suites with NULL encryption may be used. The UE shall always include at least one cipher suite that supports encryption during the handshake phase.

Cipher Suites with NULL integrity protection (or HASH) are not allowed.

~~Editors Note: It is FFS what parts (if any) of the TLS extensions as specified in RFC 3546 [9] that shall be implemented in this TS~~

*** END OF CHANGE ***

*** BEGIN OF CHANGE ***

Annex A (informative): Technical solutions for access to application servers via Authentication Proxy and HTTPS

This annex gives some guidance on the technical solution for authentication proxies so as to help avoid misconfigurations. An Authentication Proxy acts as reverse proxy which serves web pages (and other content) sourced from other web servers (AS) making these pages look like they originated at the proxy.

To access different hosts with different DNS names on one server (in this case the proxy) the concept of virtual hosts was created.

One solution when running HTTPS is to associate each host name with a different IP address (IP based virtual hosts). This can be achieved by the machine having several physical network connections, or by use of virtual interfaces which are supported by most modern operating systems (frequently called "ip aliases"). This solution uses up one IP address per AS and it does not allow the notion of "one TLS tunnel from UE to AP-NAF" for all applications behind a NAF together.

If it is desired to use one IP address only or if "one TLS tunnel for all" is required, only the concept of name-based virtual hosts is applicable. Together with HTTPS, however, this creates problems, necessitating workarounds which may deviate from standard behaviour of proxies and/or browsers. Workarounds, which affect the UE and are not generally supported by browsers, may cause interoperability problems. Other workarounds may impose restrictions on the attached application servers."

To access virtual hosts where different servers with different DNS names are co-located with an AP, the following two solutions could also be used to identify the host during the TLS handshaking phase:

1. Extension of TLS is specified in RFC 3546 [9]. This RFC supports the UE to indicate a virtual host that it intends to connect in the very initial TLS handshaking message;

2. The other alternative is to issue a multiple-identities certificate for the AP. The certificate will contain identities of AP as well as each server that rely on AP's proxy function. The verification of this type of certificate is specified in RFC 2818 [17].

~~Editor's Note: The shared-key TLS based authentication does not require server's certificate, but the possession of the key for authentication. The procedure is FFS.~~

~~Editors Note: The text in this informative annex may need to be revisited if changes in the main body of the text are made and when a final solution have been chosen.~~

*** END OF CHANGE ***