3GPP TSG SA WG3 Security — S3#32
Edinburgh, UK, 9-13 February 2004

Tdoc ⌘S3-040075

CR-Form-v7

Pseudo CHANGE REQUEST

⌘ **33.141** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **1.0.0** ⌘

*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:	⌘	GAA in Presence, general view
Source:	⌘	Nokia
Work item code:	⌘	GAA, Presence
Date:	⌘	30/1/2004
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 authentication of the subscriber and the network in Presence/Presence List Server as well as authentication proxy shall be based on GAA, i.e., shared secrets (e.g., TLS with HTTP Digest) and/or subscriber certifictes (TLS with certificate based client authentication) may be used in Ut interface. The editor's notes that are in clause 5 are removed, because they address the issues that are considered when using Ua interface. Also notice the difference when using terms GAA and GBA. GAA indicates the usage of subscriber certificates as well as shared secrets. GBA indicates the usage of shared secrets only.
Summary of change:	⌘	The authentication of the subscriber and the network in Presence/Presence List Server shall be based on GAA.
Consequences if not approved:	⌘	

Clauses affected:	⌘	4, 5			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	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 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: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service; Stage 1".

[3] 3GPP TS 23.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service; Architecture and functional description".

[4] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-based services".

[5] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".

[6] IETF RFC 2246 (1999): "The TLS Protocol Version 1".

[7] 3GPP TS 23.002: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture".

[8] IETF RFC 3268 (2002): "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)".

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

[10] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security".

[11] 3GPP TR 33.919: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); System Description".

[12] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[13] 3GPP TS 24.cde: "3rd Generation Partnership Project; Technical Specification Group Core Network; Bootstrapping interface (Ub) and Network application function interface (Ua); Protocol details".

[14] IETF RFC 2818 (2000): "HTTP over TLS".

******* END CHANGE *******

******* BEGIN 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 by sending a SIP SUBSCRIBE over IMS towards the network subscribe to or 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.

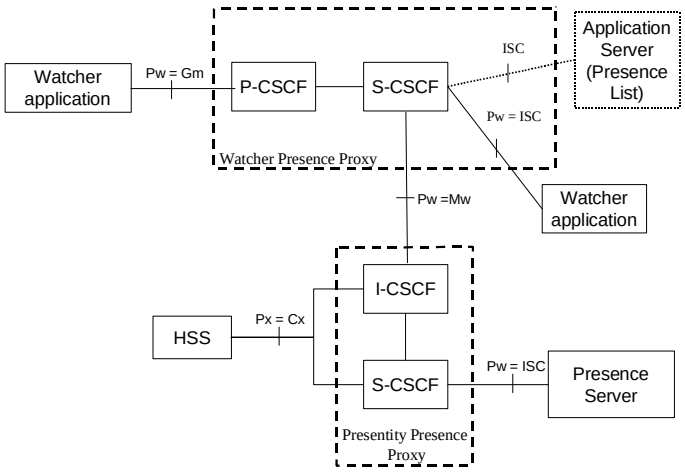

Figure 1: The Location of the Presence Server and the Presence List Server from an IMS point of view

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.

The Ut interface needs the following security features:

1. it shall be possible to provide with mutual authentication between the Server and the Watcher/Presentity;
2. a secure link and security association shall be established between the 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:

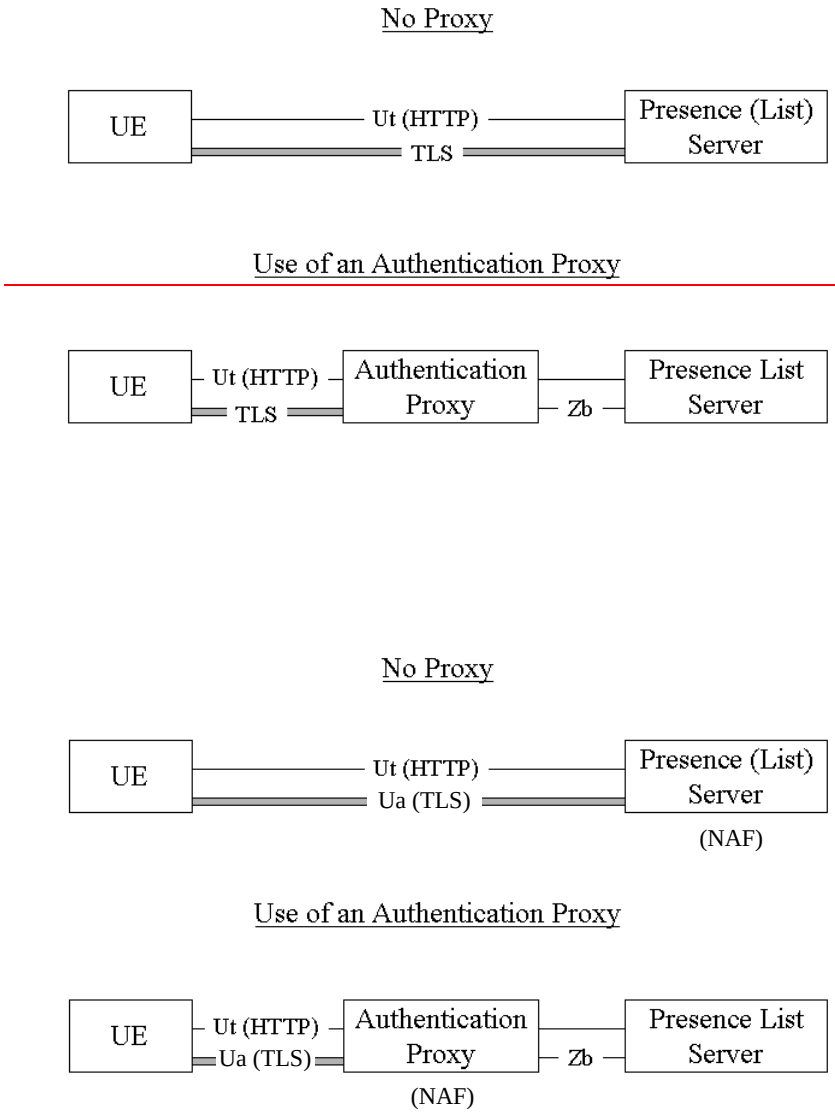

Figure 2: An overview of the Security architecture for the Ut interface including the support of an Authentication Proxy

5 Security features

5.1 Secure Access to the Presence Server/Presence List Server

5.1.1 Authentication of the subscriber and the network

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

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

[Editors Note: An Editors note will be included in TR33.919 clarifying that an AS or an AP should decide on what parts of GAA shall be used if any. This might need to be reflected in this TS which is left FFS, cf. S3-030722].

The authentication of the subscriber shall be based on the ISIM as defined in 3GPP TS 33.203 [4]. The authentication of the subscriber and the network shall be ~~HTTP~~ based on Generic Authentication Architecture as defined in 3GPP TR 33.919 [11] and 3GPP TS 33.220 [12]. 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. [13]).

The server certificate to be used for application server authentication shall be based on IETF RFC 2818 [14].

~~Editors Note: It is FFS what the detailed requirements are on profiling TLS. The following requirements are FFS: *The Server is authenticated by means of asymmetric cryptography using a Server Certificate. The authentication of the Server shall be based on strong security. The use of anonymous Diffie Hellman is not allowed.*~~

NOTE: The interleaving attack shall not be possible.

~~Editors Note: The exact details on Server Certificate are FFS cf. X509v3 certificate and PKIX~~

~~Editors Note: It is FFS how the user is authenticated the methods that are FFS are:~~
~~- A Presence Subscriber may be authenticated with the use of Subscriber Certificates~~
~~- The use of TLS and Shared keys i.e. the IETF draft on Shared Key TLS~~
~~- The use of Authentication Proxy is an option~~
~~- The user can also be authenticated through the use of the BSF and the creation of a shared secret~~
~~- etc.~~

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.

A UE may contact the Presence Server/Presence List 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.

5.1.2 Confidentiality protection

The Ut interface shall be confidentiality protected using TLS using effective key size of at least 128 bits. The terminal and the server shall be able to resume a previous session and to perform an abbreviated handshake.

5.1.3 Integrity protection

The Ut interface shall be integrity protected. The terminal and the server shall be able to resume a previous session and to perform an abbreviated handshake.

5.1.4 Authentication Proxy

The authentication proxy may reside between the UE and the Presence Server/Presence List 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 shall be able to 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 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 CHANGE *******