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

Tdoc ⌘S3-040347

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:	⌘	Editorial Updates to draft TS 33.141
Source:	⌘	Ericsson
Work item code:	⌘	Presence
Date:	⌘	03/05/2004
Category:	⌘	**D**
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:	⌘	Clarifications in TS 33.141
Summary of change:	⌘	- clarifications about presentity - adding RFC 3310 to references - adding definitions for reverse proxy and session management mechanism - update of figure 2 (Presence List Server changed to Presence Server) - clarification of note and minor editorials in 5.1.1 - key size requirement for integrity protection - editorials in 6, 6.1.3 and Annex A
Consequences if not approved:	⌘	

Clauses affected:	⌘	Introduction, 2, 3.1, 4, 5.1.1, 5.1.3, 6, 6.1.3, Annex A

Other specs affected:	⌘	Y	N		⌘
		☐	☐	Other core specifications	
		☐	☐	Test specifications	
		☐	☐	O&M Specifications	

Other comments:	⌘	

*** BEGIN OF CHANGE ***

Introduction

This technical specification defines the security architecture and requirements for the presence services. Presence services enable the spreading of presence information of a user to users or services. A presence entity or presentity comprises the user, users devices, services and services components. It is the intention that this platform will enable new services like e.g. enhancement to chat, multimedia messaging, cinema ticket information, the score of a football game and so on.

A user has the possibility to control if her or his information shall be available to other users or services. This control is possible to achieve with high granularity e.g. explicitly define which user or users and services that shall have access to presence information.

A presentity is an uniquely identifiable entity with the capability to provide with presence information and it has only one principal associated with it. Hence a principal is distinct from all other principals and can be e.g. a human, organisation, program or even a collection thereof. One example of such a relation is when the presentity is a terminal and the principal of the terminal is the subscriber. However, the presence service is based on Public Identities, and consequently it is possible to have several terminals related to the same presentity. A watcher is also a~~n~~ uniquely identifiable entity but with the aim to fetch or request information about a presentity. There are access rules that set the rules for the presence service how presence information gets available to watchers.

Presence information consists of a number of elements or presence tuples as defined in 3GPP TS 23.141 [3].

*** END OF CHANGE ***

*** BEGIN OF 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 TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[12] OMA WAP-211-WAPCert, 22.5.2001: http://www.openmobilealliance.org/tech/affiliates/wap/wap-211-wapcert-20010522-a.pdf

[13] OMA WAP-219-TLS, 4.11.2001: http://www.openmobilealliance.org/tech/affiliates/wap/wap-219-tls-20010411-a.pdf

[14] IETF draft-ietf-tls-rfc2246-bis-05 (2003): "The TLS Protocol Version 1.1"

[15] 3GPP TR 33.919: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); System Description".

[16] 3GPP TS 24.cde: "3rd Generation Partnership Project; Technical Specification Group Core Network; Bootstrapping interface (Ub) and Network application function interface (Ua); Protocol details".

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

[18] IETF RFC 3310 (2002); "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)"

*** END OF CHANGE ***

*** BEGIN OF CHANGE ***

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

Reverse Proxy: A reverse proxy is a web server system that is capable of serving web pages sourced from other web servers (AS), making these pages look like they originated at the reverse proxy.

Session management mechanism: A mechanism for creating stateful sessions when using the stateless HTTP protocol.

*** END OF CHANGE ***

*** 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.

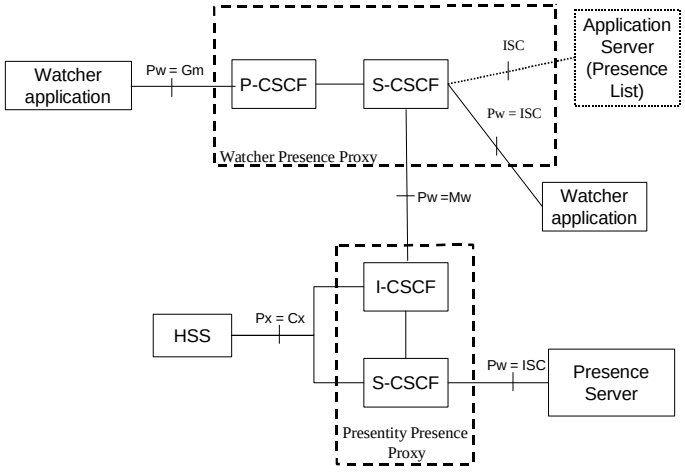

Figure 1: The Location of the Presence Server and the Presence List Server from an IMS point of view

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:

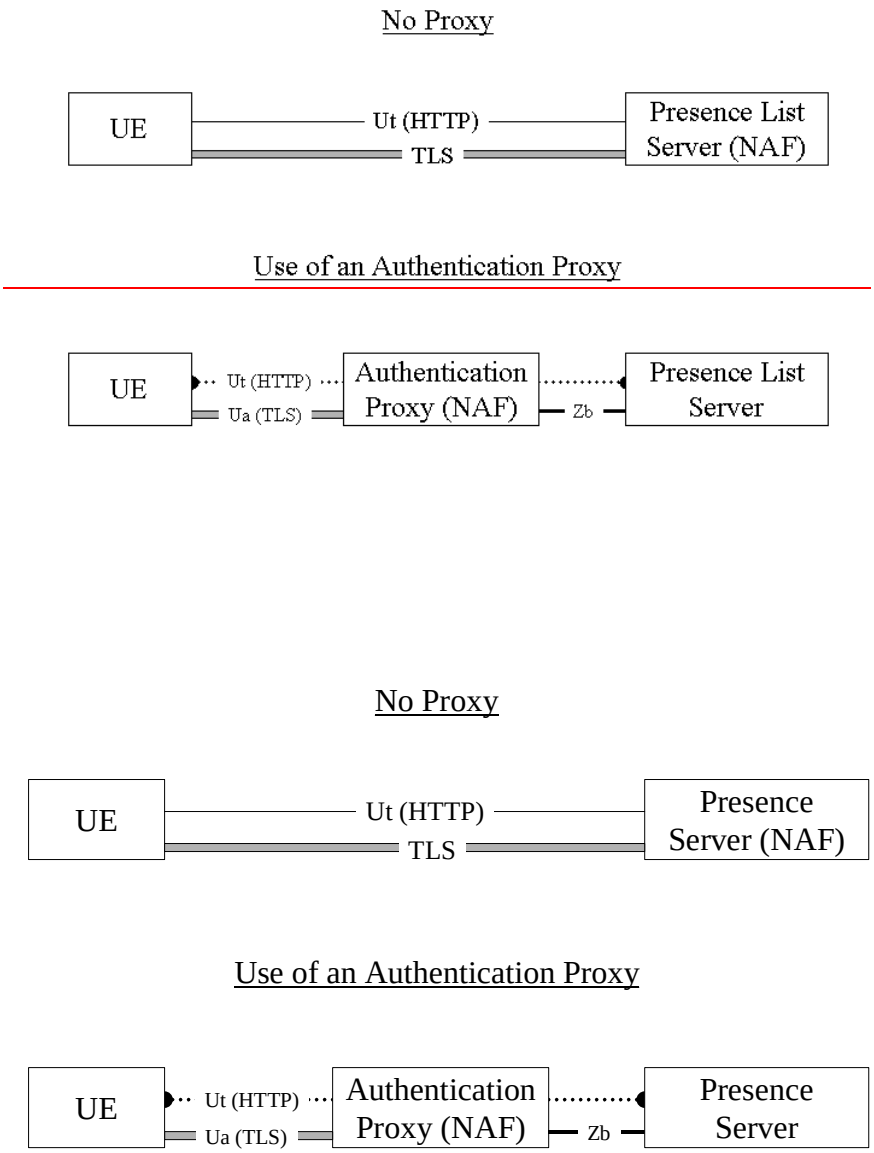

Figure 2: An overview of the Security architecture for the Ut interface including the support of an Authentication Proxy

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 subscriber 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. This essentially means that the use of HTTP Digest AKAv1 [18] is not recommended unless the related session keys (IK/CK) are somehow tied to the communication session.

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~~AP for further instructions on authentication procedures.

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

*** END OF CHANGE ***

*** BEGIN OF CHANGE ***

5.1.3 Integrity protection

The Ut interface shall be integrity protected using TLS and with 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.

*** 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 ***

6.1.3 Authentication Failures

If the UE receives a Server Hello Message from the AP/Presence Server that requests a Certificate then the UE shall respond with a Certificate Message containing no Certificate if it does not have a certificate. The AP/Presence Server upon receiving this message may respond with a failure alert, however if the AP/Presence Server shall authenticate the UE as configured by the policy of the operator the AP/Presence Server should continue the dialogue and assume that the UE will be authenticated as specified in TS 33.220 [11].

If there is no response within a given time limit from a network initiated re-authentication request an authentication failure has occurred after that the request has been attempted for a limited number of times. This failure can be due to several reasons e.g. that the UE has powered off or due to that the message was lost due to a bad radio channel. The AP/Presence Server shall then still assume that if a TLS session is still valid that it can be re-used by the UE at a later time. Should then the UE re-use an existing session then the AP/Presence Server shall re-authenticate the UE and not give access to the AP/Presence Server unless the authentication was successful.

*** 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 ***