CR-Form-v7

CHANGE REQUEST

⌘ **33.141** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Editorial cleanup of TS 33.141
Source:	⌘	Siemens
Work item code:	⌘	SSC-GBA
Date:	⌘	29/06/2004
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:	⌘	TS 33.141 and TS 33.222 were created in parallel, as it was uncertain for some time whether all of TS 33.222 would become ready for Release 6. But since TS 33.222 was put under change control at the last SA plenary meeting, it can now be referenced in TS 33.141, therefore all text overlapping with TS 33.222 is removed from TS 33.141. In addition, some adjustment of the section structure and the scope was done.
Summary of change:	⌘	Clean-up, remove overlap with other specifications
Consequences if not approved:	⌘	Untidy specification

Clauses affected:	⌘	all

Other specs affected: ⌘	Y	N		⌘	
	X		Other core specifications	⌘	TS 24.109
		X	Test specifications		
		X	O&M Specifications		

Other comments:	⌘	-

Introduction

This technical specification ~~defines~~ gives an overview of the security architecture, and defines the security features and security mechanisms ~~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 a 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 an 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 TS 23.141 [3]

1 Scope

The present document ~~describes~~ is the Stage 2 specification for the security requirements, security architecture, security features and security mechanisms ~~security requirements~~ for the Presence Service, which includes the elements necessary to realise the requirements in TS 22.141 [2] and TS 23.141 [3]. As far as SIP-based procedures are concerned, this specification refers to TS 33.203. The main content of this specification is the security for the Ut reference point, which is HTTP–based, as applied in presence services.

The present document includes information applicable to network operators, service providers and manufacturers.

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: "Vocabulary for 3GPP Specifications".

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

[3] 3GPP TS 23.141: "Presence service; Architecture and functional description".

[4] 3GPP TS 33.203: "3G Security; Access security for IP-based services".

[5] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

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

[7] 3GPP TS 23.002: "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: "3G Security; Network Domain Security; IP network layer security".

[11] 3GPP TS 33.220: "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: "Generic Authentication Architecture (GAA); System description".

[16] 3GPP TS 24.109: "Bootstrapping ~~interface~~reference point (Ub) and Network application function ~~interface~~reference point (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)".

[19] 3GPP TS 33.222: " Generic Authentication Architecture (GAA); Access to network application functions using secure hypertext transfer protocol (HTTPS)".

3 Definitions and abbreviations

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 HTTP protocol.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply, TR 21.905 [1] contains additional applicable abbreviations:

AKA	Authentication and key agreement
CSCF	Call Session Control Function
HSS	Home Subscriber Server
IM	IP Multimedia
IMPI	IM Private Identity
IMPU	IM Public Identity
IMS	IP Multimedia Core Network Subsystem
ISIM	IM Services Identity Module
MAC	Message Authentication Code
ME	Mobile Equipment
SA	Security Association
SEG	Security Gateway
SDP	Session Description Protocol
SIP	Session Initiation Protocol
UA	User Agent

4 ~~Overview of the s~~Security architecture

4.1 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, see TS 22.141 [2]. The access security for IMS is specified in 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 TS 33.210 [10] with the access security provided in 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, see figure 1.

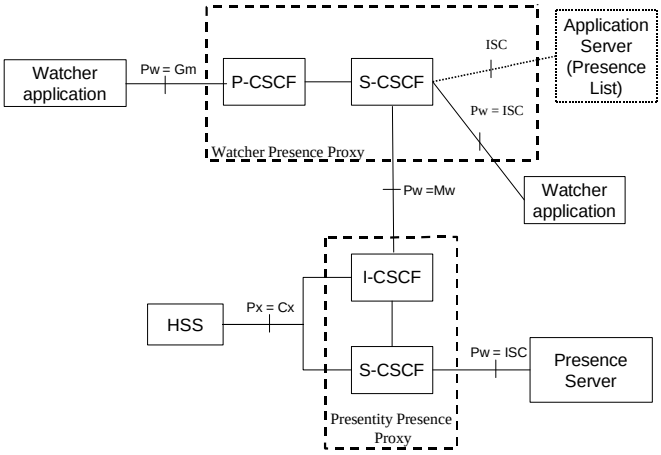

Figure 1: The Location of the Presence Server and the Presence List Server from an IMS point of view

4.2 The Ut reference point

A Presence User Agent shall be able to manage the data on the AS over the Ut ~~interface~~reference point, see TS 23.002 [7], which is based on HTTP. This ~~interface~~reference point is not covered in TS 33.203 [4] and it is mainly this ~~interface~~reference point 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 see 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.~~

~~Editor's 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~~reference point is depicted in figure 2:

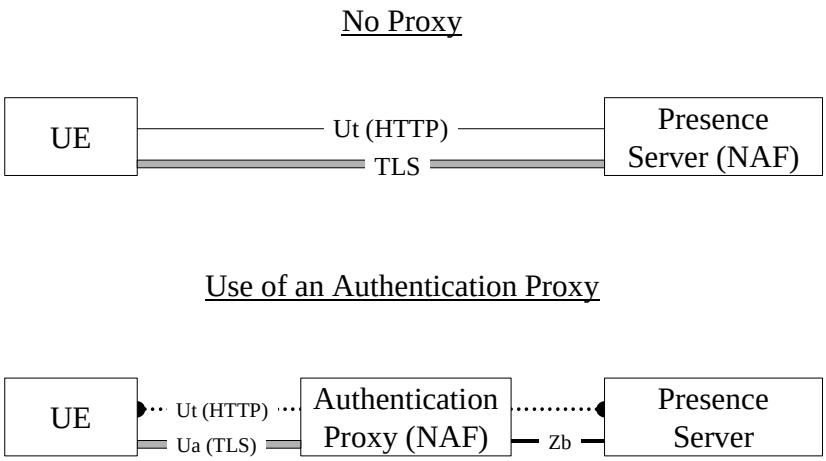

Figure 2: An overview of the Security architecture for the Ut ~~interface~~reference point including the support of an Authentication Proxy

~~Editor's Note: The Authentication Proxy and the Presence Server shall utilize the security protection specified in TS 33.210 [10] to protect the data carried between them. This is compliant with the mechanism specified in TS 33.222 [19].~~

5 Security features

5.1 Secure Access to the Presence Server over the Ut reference point

5.1.1 Authentication of the subscriber and the ~~network~~presence server

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. A subscriber shall authenticate the presence server.

~~Editor's 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~~ presence server 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 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, see RFC 2246 [6], RFC 3268 [8] and , RFC 3546 [9]); or~~

~~shared secrets (e.g. TLS with HTTP Digest, see RFC 2818 [17]).~~

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

~~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/AP for further instructions on authentication procedures.~~

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

5.1.2 Confidentiality protection

It shall be possible to apply confidentiality protection over the Ut ~~interface~~reference point. ~~using TLS and with effective key size of at least 128 bits. The terminal shall in the negotiation phase include protection alternatives that include at least one alternative with encryption algorithm support. 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~~reference point 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~~.

5.1.4 Authentication Proxy

The Authentication Proxy may reside between the UE and the Presence Server as depicted in Figure 2. Its use is specified in TS 33.222 [19]. ~~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 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.~~

~~Confidentiality and integrity protection may be provided for the interface between the AP and the AS, using the Zb interface of NDS/IP as specified in TS 33.210 [10].~~

6 Security Mechanisms for the Ut reference point

The UE and the AP/Presence Server shall support the TLS version and profile as specified in clause 5.3 of TS 33.222 [19].

6.1 Authentication and key agreement

6.1.1 Authentication of the subscriber

~~From a TLS point of view the UE shall be considered as un-authenticated, see RFC 2246 [6].~~

The authentication of the UE may take place in either the Authentication Proxy, cf. TS 33.222 [19] or the Presence server.

Subscriber authentication can be also performed by the operator using proprietary or non-3G standardized methods. A UE may contact the Presence Server/AP for further instructions on authentication procedures, see initiation of bootstrapping in TS 33.220 [11], clause 4.5.1.

In case 3GPP authentication mechanisms are used, the authentication of the subscriber shall be based on the Generic Authentication Architecture as defined in 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 or
- shared secrets

For both cases, the authentication of the subscriber shall conform to the use of the Generic Authentication Architecture [15] for access to network application functions using HTTPS, as specified in TS 33.222 [19].

~~However the AP or the Presence server may, depending on given the policy of the operator conclude that the AP/Presence Server shall not authenticate the UE using GBA i.e. the UE is considered as authenticated already or the UE is authenticated by other means, see initiation of bootstrapping in TS 33.220 [11], clause 4.5.1.~~

~~Otherwise if the AP/Presence Server concludes that the authentication shall take place in the AP/Presence Server then the UE may be authenticated as specified in TS 33.220 [11] (where the Ua interface is between the UE and the AP/Presence Server).~~

~~It shall be possible for the AP/Presence Server at any time to request a re-authentication of an active UE, see TS 33.220 [11], clause 4.5.3.~~

6.1.2 Authentication of the AP/Presence Server

The AP/Presence Server is authenticated by the Client as specified in WAP-219-TLS [13], which in turn is based on RFC 2246 [6].

The AP/Presence Server certificate profile shall be based on WAP Certificate and CRL Profile as defined in WAP-211-WAPCert [12].

6.1.3 Management of public user identities

~~The general concept of Ua interface is specified in TS 33.222 [19], clause 6. This section specifies how TS 33.222 [19] is applied to the case of Presence services. The AP or Presence server shall authenticate the subscriber as specified in TS 33.222 [19], clause 5. In particular, the~~ The presence server, acting as a NAF in the sense of TS 33.220, may obtain identities related to the subscriber over the Zn reference point, as part of the GBA user security setting for presence, according to the policies of the BSF, cf. TS. 33.220, section 4.5.3 [11]. These identities may include the IMPI and several IMPUs.~~AP or presence server can associate an authenticated HTTP request with a transaction identifier and one or several public user identities (IMPUs). The IMPUs form part of a GAA specific user profile for presence~~. The UE shall send its preferred public user identity in each HTTP request. The Presence server (or AP) shall then verify that the preferred identity inserted in the HTTP request by the UE is one of the IMPUs, associated with the HTTP request, according to TS 33.222, section 6.5.2.4 [19].

If the presence server sits behind an AP and the verification of the preferred identity, which was inserted by the UE in the HTTP request, was successful, then the AP shall verify the value of the preferred identity of the user in the HTTP request before forwarding it to the presence server. How the asserted user identity is carried in each HTTP request is specified in the relevant stage 3 specification.

If there is no preferred identity inserted in the HTTP request, the AP shall insert a default IMPU from the user profile in the HTTP request, before forwarding it to the Presence server. If the validation of the UE inserted preferred identity fails in the AP the HTTP request shall be dropped.

6.1.4 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.

6.2 Confidentiality protection

If confidentiality protection is provided over the Ut interface, then it shall be provided using TLS and with effective encryption key size of at least 128 bits. The terminal shall in the negotiation phase include protection alternatives that include at least one alternative with encryption algorithm support. The terminal and the server shall be able to resume a previous session and to perform an abbreviated handshake.

6.3 Integrity protection

Integrity protection over the Ut reference point shall be provided 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.

7 Security parameters agreement

7.1 Set-up of Security parameters

The TLS Handshake Protocol negotiates a session, which is identified by a Session ID. The Client and the AP/Presence Server shall allow for resuming a session. This facilitates that a Client and Server may resume a previous session or duplicate an existing session. The lifetime of a Session ID is maximum 24 hours. The Session ID shall only be used under its lifetime and shall be considered by both the Client and the Server as obsolete when the Lifetime has expired.

7.2 Error cases

The AP/Presence Server shall consider the following cases as a fatal error:

- if the received ciphersuites only includes all or some of the Ciphersuites in Clause 6.4;
- if the received ciphersuites do not include any integrity protection;
- if none of the received ciphersuites include encryption;
- if the policy of the operator stipulates that encryption is required and the common set of supported ciphersuites only include key material less than 128 bits for confidentiality protection.

~~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].~~