3GPP TSG SA WG3 Security — S3#32 **S3-040169**
9 – 13 February, 2004, Edinburgh, Scotland

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:	⌘	Security Mechanisms for Presence		
Source:	⌘	Ericsson		
Work item code:	⌘		***Date:*** ⌘	26 January 2004
Category:	⌘	**B**	***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:	⌘	Currently clause 6 and 7 are empty
Summary of change:	⌘	Adding requirements for the security mechanisms
Consequences if not approved:	⌘	Some clauses will remain empty

Clauses affected:	⌘	Clause 6 and 7				
		Y	**N**			
Other specs affected:	⌘	**Y**		Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

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

[13] 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”.

***** 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 ~~by~~ be sending a SIP SUBSCRIBE over IMS towards the network to subscribe ~~to~~ 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.

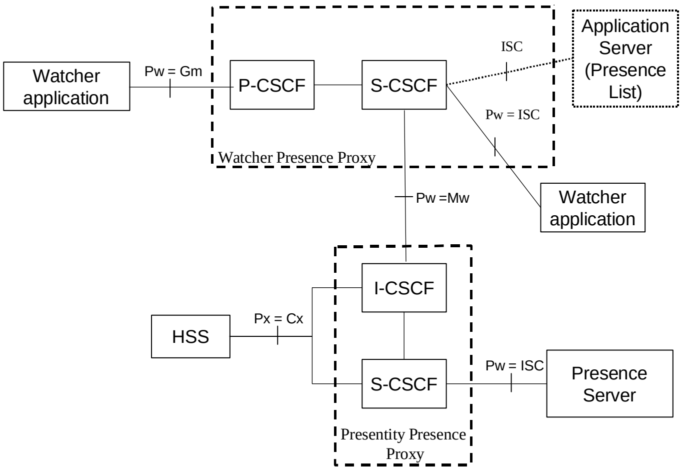


Figure 1: The Location of the Presence Server and the Presence List Server from an IMS point of view

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.

The Ut interface needs the following security features:

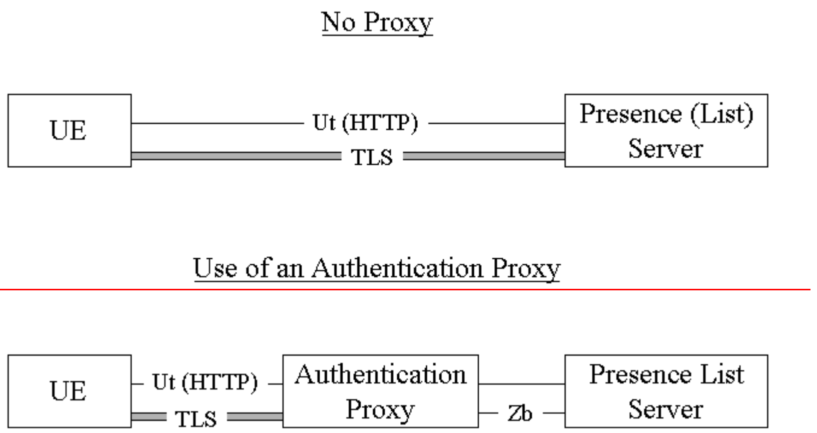
1. it shall be possible to provide with mutual authentication between the Server and the Watcher/Presentity;

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:



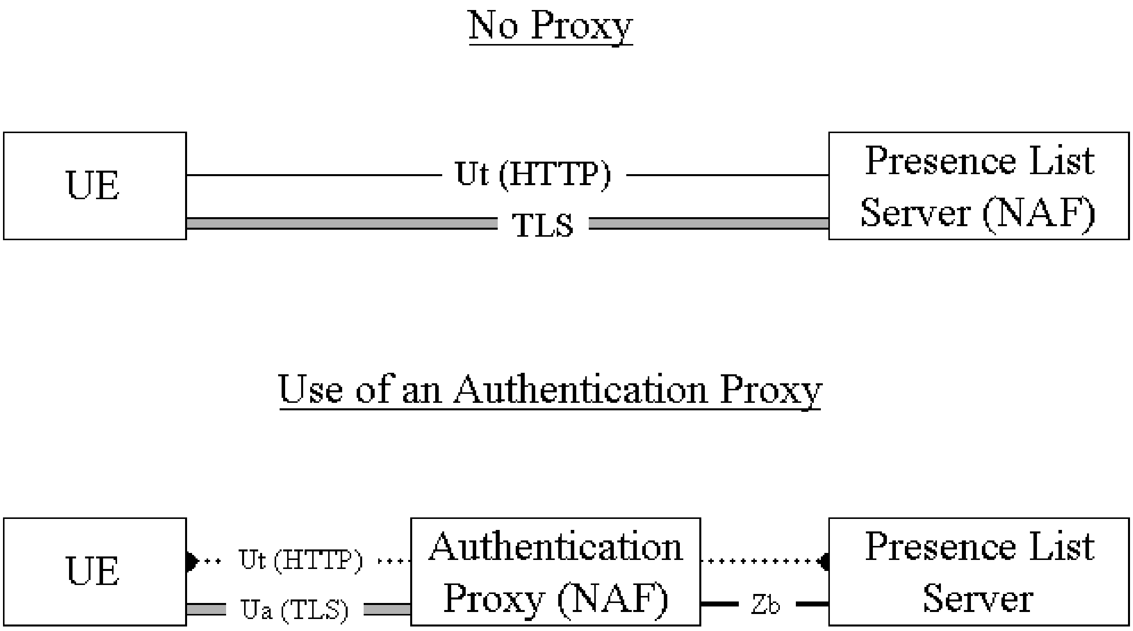

No Proxy
UE
Ut (HTTP)
TLS
Presence List Server (NAF)
Use of an Authentication Proxy
UE
Ut (HTTP)
Ua (TLS)
Authentication Proxy (NAF)
Zb
Presence List Server

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 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].~~

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].

~~The authentication of the subscriber shall be based on the ISIM as defined in 3GPP TS 33.203 [4]. The authentication of the subscriber shall be HTTP based.~~

~~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.

***** End of Change ****

***** Begin of Change ****

5.1.2 Confidentiality protection

It shall be possible to apply ~~The Ut interface shall be~~ confidentiality ~~protected~~ protection over the Ut interface using TLS ~~using~~ 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.

***** End of Change ****

***** Begin of Change ****

6 Security Mechanisms

~~Editors Note: This should be a profiling of [6] and [8]~~

~~Editors Note: The clause 6 and 7 do not include much text. During the work with the security for Presence a TR was developed from which much of the content was moved to TS 33.203 Access Security for IMS Release 6. SA3 has an agreed working assumption on the use of TLS (some version of it). When the decision is taken there are no known issues available that should make it technically difficult to stabilise these clauses . The basis for this work is already outlined in S3-030749, which is approved in SA3 for inclusion in TS 33.222.~~

The UE and the AP/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

6.1 Authentication and key agreement

6.1.1 Authentication of the ~~user~~UE

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

The authentication of the UE may take place in either the Authentication Proxy or the Server. However the AP or the Server may given the policy of the operator conclude that the AP/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.

Otherwise if the AP/Server concludes that the authentication shall take place in the AP/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/Server). ~~The AP/Server shall not require that the UE is authenticated through the use of UE Certificates, cf. RFC 2246 [6].~~

It shall be possible for the operator at any time to request a re-authentication of an active~~the~~ UE.

6.1.2 Authentication of the AP/Server

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

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

6.1.3 Authentication Failures

If the UE receives a Server Hello Message from the AP/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/Server upon receiving this message may respond with a failure alert, however if the AP/Server shall authenticate the UE as configured by the policy of the operator the AP/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 initated 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/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/Server shall re-authenticate the UE and not give access to the AP/Server unless the authentication was successful.

6.2 ~~Confidentiality~~ Protection mechanisms

~~Both t~~The UE ~~and the AP/Server~~ 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/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/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

~~6.3 Integrity mechanisms~~

6.4 Key Agreement

The Key exchange method shall not be anonymous. Hence the following cipher suites as defined in RFC 2246 [6] are not allowed for protection of a session for Presence Services:

- CipherSuite TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
- CipherSuite TLS_DH_anon_WITH_RC4_128_MD5
- CipherSuite TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
- CipherSuite TLS_DH_anon_WITH_DES_CBC_SHA
- CipherSuite TLS_DH_anon_WITH_3DES_EDE_CBC_SHA

***** End of Change ****

***** Begin of Change ****

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/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/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

***** End of Change ****