3GPP TSG SA WG3 Security – SA3#32 **S3-030045**

9-13, February, 2004

Edinburgh, Scotland

Agenda Item: Presence

Source: Ericsson

Title: TLS profile for Presence Security

Document for: Discussion/Decision

1. Introduction

In this paper Ericsson discusses the status of TLS and what different TLS extensions and TLS profiles that are available.

Ericsson suggests that 3GPP should as a working assumption implement the TLS profile developed in WAP, cf. [WAP-219-TLS] as well as [WAPCert] for certificate profiles. The rationale behind this recommendation is that Ericsson believes that the most efficient and effective way forward is to re-use existing profiles for a wireless environment.

Furthermore Ericsson also suggests that SA3 as a working assumption for Presence security implements also future OMA defined TLS profiles that should consider the existing IETF TLS extensions like AES cipher suites and TLSv1.1

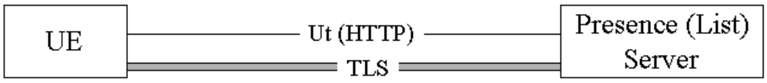
Ericsson proposes that SA3 sends an LS to OMA to ask them to report on the time schedule for implementation of these extensions for enhancing the OMA TLS profile since e.g. the implementation of an AES cipher suite should be essential for Presence Security.

Ericsson also asks SA3 to endorse the attached Pseudo CR.

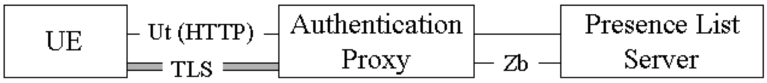
2. Presence Security Requirements

The current architecture for the use of Presence Ut interface is depicted in the figure below, where the case of the use of a reverse proxy is included:

No Proxy



Use of an Authentication Proxy



It is currently assumed in TS33.141 that TLS shall be used but there is an editor's note in the TS that highlights that several TLS standards document are available. This contribution aims to define what TLS specifications that the TS shall make references to.

3. TLS profiling

3.1 TLS profile status in standards

There are several different standards document that are TLS related available i.e. RFCs, Profiles and IETF drafts e.g.

- RFC 2246 The TLS Protocol Version 1.0, cf. [RFC 2246]
- RFC 3546 TLS Extensions, cf. [RFC 3546]
- IETF Draft TLSv1.1 Draft v5.0, cf. [Draft-TLSv1.1]
- RFC 3268 AES Ciphersuites, [RFC 3268]
- WAP-219-TLS TLS Profile and Tunneling which is a profile of RFC 2246 TLSv1.0, cf. [WAP-219-TLS]
- IETF Draft Shared Key TLS

On the IETF draft for Shared Key TLS Ericsson already identified several open issues, cf. [S3-030721] at SA3#31, which need to be clarified. Therefore Ericsson leaves that draft out from the discussion in this paper.

3.2 Profiling Discussion

When WAP Forum launched WAP2.0 it was a step to bring the wireless environment closer to the Internet Protocols like TCP, HTTP and TLS. For TLS a wireless profile was defined in [WAP-219-TLS] which requires that client and server implementations are compliant with TLSv1.0 [RFC 2246]. The WAP2.0 profile requires that a server support both cipher suites in the list below whereas the client shall support at least one of them:

1. TLS_RSA_WITH_RC4_128_SHA
2. TLS_RSA_WITH_3DES_EDE_CBC_SHA

From a confidentiality protection point of view cipher suite 2 is related to the encryption of IMS signalling where it is specified in TS33.203 that IPsec ESP implementation should use DES-EDE3-CBC. Hence this TLS cipher suite should take precedence over 1 since it facilitates the possibility to re-use existing implementations in the terminal.

In order to minimise the need to perform a full TLS handshake too often a session resume shall be used. The TLSv1.0 stipulates that a key shall not have a longer lifetime than 24 hours. This is also reflected in the [WAP-219-TLS]. Hence also Presence TS should respect this guideline.

For Presence TLS shall not be used for Client Authentication instead it is up to the Authentication Proxy or the Server to decide what part of [GAA] shall be used if any e.g. the use of GBA where HTTP Digest is used as the protocol for client authentication. For Server Authentication it is recommended that the WAP profiled X.509 Server Certificates as defined in [WAPCert] are utilised however it is not forbidden to use [X.509] Server Certificates.

A final note on the TLS tunnelling part as specified in [WAP-219-TLS] is that if the Client is aware of a Proxy between the Client and an Application Server the Client shall use the HTTP Connect method for setting up an end to end protected session. However if an operator implements a Reverse Proxy as specified in TS33.141 then the client is not aware of such a proxy and hence the TLS tunnelling is not used.

The RFC 3268, cf. [RFC 3268] defines a number of suites with AES support all in Cipher Block Chaining Mode with 128- or 256- bit keys e.g. TLS_RSA_WITH_AES_128_CBC_SHA. Ericsson suggests to add an Editors Note on AES in the Presence TS on AES since it is desirable that the Presence Security includes at least one mandatory AES cipher suite.

In IETF there is ongoing work to further enhance TLSv1.0 to TLSv1.1 [Draft-TLSv1.1]. The list below highlights some of the enhancements that have been made in the draft:

- RSA/3DES is the mandatory cipher suite
- Removal of the requirement that the Server Random has to be different from the Client Random
- Editorial changes like removal of RSA patent statement
- Prevention of certain CBC attacks

Ericsson assumes that when the TLSv1.1 is available that the TLS profile in OMA should be updated accordingly. From a security point of view it is natural that TLSv1.1. would take precedence over TLS1.0 when it is available as an RFC since it prevents some certain known TLSv1.0 CBC attacks.

The TLS-Extensions [RFC 3546], defines extensions to TLS that may be used for added functionality in particular in wireless environments like:

- Negotiation of Client Certificate URLs
- Negotiation of Maximum Fragment Length
- TLS Clients enabled to communicate which CA Root Keys it supports
- Negotiation of the use of Truncated MACs (80 bit MAC)
- Mechanism that avoids that a full CRL is sent

Ericsson recognises that the RFC 3546 have identified several relevant requirements for constrained environments and constrained clients like bandwidth limitations, computational power limitations and battery life limitations to name a few.

Therefore it seems attractive that 3GPP considers to implement these extensions e.g. to Presence Security. However it could be discussed whether this RFC could then be for post Release 6 and included in the HTTP TS.

3.3 Recommended way forward

Considering that OMA is now responsible for WAP protocols like WTLS and the wireless profile of TLSv1.0 [RFC 2246] Ericsson recommends that 3GPP SA3 adopts the working assumption that Presence Security is based on [WAP-219-TLS] for Server Authentication, Confidentiality Protection and Integrity Protection and [WAPCert] for Certificate profiles. However the Tunneling part in [WAP-219-TLS] is not required for Presence since the UE is not aware of the Reverse Proxy.

Ericsson believes that this recommended way forward should be chosen since it minimises the risk that both 3GPP and OMA would start to work on wireless TLS profiles and perhaps increase the risk that the groups identify even conflicting requirements. It seems that such an approach would also decrease the workload e.g. minimising the number of LSs that need to be sent between the groups. This proposal also re-uses the existing work already done on TLS profiles in OMA and it is the belief of Ericsson that it is better to evolve future extensions to TLS and related profiles based on an existing specifications like [WAP-219-TLS], which is owned by OMA.

4. Conclusions

In this document several different TLS standards documents were discussed. It was concluded that the Presence TS should base the TLS profile on OMA specifications. It was also recommended that the most efficient and effective way forward is that OMA based on the existing specifications under their ownership evolve and profile based on the ongoing work on TLS in IETF e.g. the inclusion of a mandatory AES based cipher suite.

Ericsson suggests that 3GPP SA3 sends an LS to OMA to highlight the ongoing work on Presence Security and ask OMA to report the status on evolving the TLS profile [WAP-219-TLS] to include e.g. AES Cipher suites [RFC 3268], TLSv1.1 [Draft-TLSv1.1] and TLS Extensions [RFC 3546] and what the time schedule for this is.

5. References

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

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

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

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

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

[Draft-TLSv1.1] IETF Draft (2003): “The TLS Protocol Version 1.1”, draft-ietf-tls-rfc2246-bis-05.txt

[S3-030721] Ericsson 2003, “Challenges in using shared-secret TLS with NAFs”, S3030721, Munich

3GPP TSG SA WG3 Security — S3#31 **S3-030xxx**
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”

***** 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.

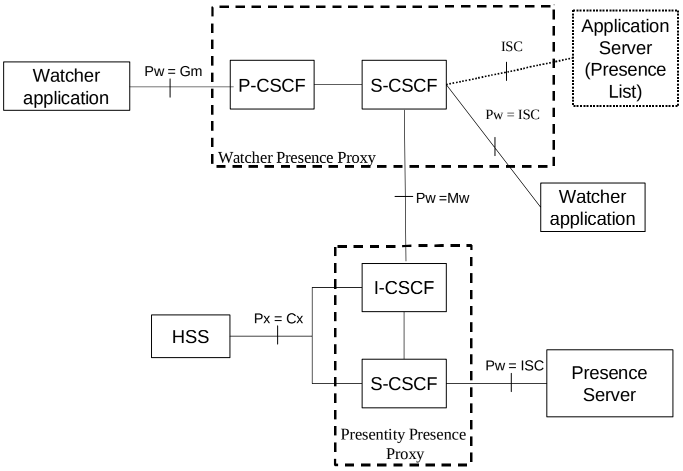


Figure 1: The Location of the Presence Server and the Presence List Server from an IMS point of view

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:

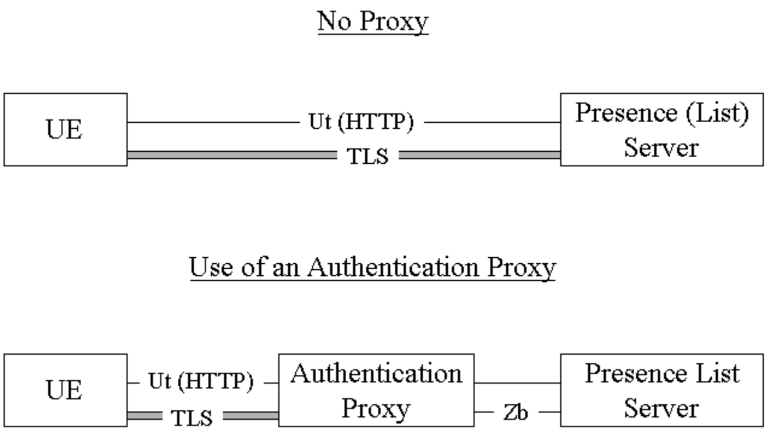


Figure 2: An overview of the Security architecture for the Ut interface including the support of an Authentication Proxy

***** 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.

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 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 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.

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 ****