3GPP TSG SA WG3 Security#33 **S3-040323**
10 – 14 May, 2004
Beijing, China

Agenda Item: **6.9.4 (GAA/HTTPS) and 6.18 (Presence)**

Source: **Nokia, Siemens**

Title: **Definition of TLS profile for shared key based UE authentication according to clause 5.3 of TS 33.222 – Pseudo-CRs to 33.222 and 33.141**

Document for: **Discussion and decision**

Abstract

In the current version of the Access to NAF using HTTPS specification (TS 33.222 v100), section 5.3 "Shared key based UE authentication with certificate based NAF authentication" an editor's note still requires profiling of TLS. This profile is given here. It is the same profile as currently specified in TS 33.141 on Presence.

It is proposed to add this profile to TS 33.222. Additionally it is proposed, to remove this profile from TS 33.141, and only to include a reference to TS 33.222 in specification TS 33.141 instead.

1. Reason for proposed change to TS 33.222 v100 and TS 33.141 v111

In particular for use in low-performance UEs a restricted profile for mandatory features of TLS is advisable. This profile should be the same for all applications using "Shared key based UE authentication with certificate based NAF authentication" according to clause 5.3 of TS 33.222. Therefore it is proposed to shift this profile definition from TS 33.141 to TS 33.222, and to include a reference to TS 33.222 in TS 33.141 (and in any future document specifying application specific extensions or profiles to TS 33.222). The profile definition taken from 33.141 and introduced into 33.222 was adapted only editorially, i.e. references to AP/Presence server were replaced by NAF.

For TS 33.141 on Presence this means, that section 6 has a changed text giving the reference, and sections 6.2 and 6.3 are removed. (Note to the editor of TS 33.141: There is another pseudo-CR proposing a renumbering of clauses in TS 33.222. This would mean that the reference to clause 5.3 must be changed to 5.3.1 – depending on acceptance of this other pseudo-CR).

The next sections contain pseudo-CRs to TS 33.222 v100 and TS 33.141 v111, implementing the changes proposed in this section.

2. Pseudo-CR to TS 33.222 v100

********** 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 TS 23.002: “Network architecture”.

[2] 3GPP TS 22.250: “IP Multimedia Subsystem (IMS) group management”; Stage 1”.

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

[4] 3GPP TR 33.919: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); System description".

[5] 3GPP TS 33.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service; Security"

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

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

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

[9] IETF RFC 2818 (2000): “HTTP Over TLS ”.

[10] IETF RFC 2617 (1999): "HTTP Authentication: Basic and Digest Access Authentication"

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

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

********** end change **********

********** begin change **********

5.3 Shared key-based UE authentication with certificate-based NAF authentication

This section explains how the procedures specified in [3] have to be enhanced when HTTPS is used between a UE and a NAF. The only enhancement required is the need to specify how the set up of a TLS tunnel is included in the general procedures specified in [3].

Editor’s note: The sequence of events needs to be updated to reflect the initiation of bootstrapping as described in TS 33.220, section 4.3.1.

When the UE accesses a NAF, with which it does not yet share a key, then the sequence of events is as follows:

1. the UE runs http digest aka [11] with the BSF over the Ub interface.

2. If the BSF has no authentication vectors for the UE it fetches authentication vectors from the HSS over the Zh interface.

After the completion of step 1), the UE and the BSF share a secret key. This shared key is identified by a transaction identifier supplied by the BSF to the UE over the Ub interface key, cf. [3, section 4.3.1].

3. The UE establishes a TLS tunnel with the NAF. The NAF is authenticated to the UE by means of a public key certificate.

~~Editor's note: TLS needs to be profiled in an appropriate section of this specification.~~

4. The UE sends an http request to the NAF.

5. The NAF invokes http digest [10] with the UE over the Ua interface in order to perform client authentication using the shared key agreed in step 1), as specified in [3, Annex A].

Editor's note: bullet 5 references Annex A in TS 33.220, which is informative.

6. While executing step 5), the NAF fetches the shared key from the BSF over the Zn interface, as specified in [3, Annex A and section 4.3.2].

7. After the completion of step 4), UE and NAF are mutually authenticated as the TLS tunnel endpoints.

The UE may now run an appropriate application protocol with the NAF through the authenticated tunnel.

When the UE accesses a NAF, with which it already shares a key, steps 1), 2), 5) and 6) may be omitted, as specified in [3].

Editor's note: the above procedure is generally applicable and conforms to [TS 33.220]. For the case of a co-located BSF and NAF an optimisation is possible which is currently located in the informative Annex Z. SA3 still needs to decide whether the material in the annex should be moved to the main body, or remain in an informative or normative annex, or be deleted.

5.3.1 TLS Profile

The UE and the NAF shall support the TLS version as specified in RFC 2246 [6] and WAP-219-TLS [12] or higher. Earlier versions are not allowed.

NOTE: The management of Root Certificates is out of scope for this Technical Specification.

5.3.1.1 Protection Mechanisms

The UE 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 NAF 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 NAF.

Editors Note: It is FFS if 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 [8] shall be implemented in this TS.

5.3.1.2 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:

- 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 change **********

3. Pseudo-CR to TS 33.141 v111

**********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 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] 3GPP TR 33.222: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Access to Network Application Functions using HTTPS".

**********end change **********

********** begin change **********

6 Security Mechanisms

The UE and the AP/Presence Server shall support the TLS version and profile as specified in ~~RFC 2246 [6] and WAP-219-TLS [13] or higher. Earlier versions are not allowed.~~section 5.3 "Shared key based UE authentication with certificate based NAF authentication " of TS 33.222 [18].

~~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 change **********

**********begin change **********

~~6.2Protection mechanisms~~

~~The UE 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/Presence 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/Presence 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 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 change **********