3GPP TSG-SA WG3 Meeting #34
Acapulco, Mexico, 6 - 9 July 2004

Tdoc ⌘S3-040658

CR-Form-v7

CHANGE REQUEST

⌘ **33.222** **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⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Further modifications to TLS profile related text in 33.222
Source:	⌘	Ericsson, Siemens
Work item code:	⌘	SSC-GBA
Date:	⌘	09/06/2004
Category:	⌘	**F**
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:	⌘	SA3 has been aligning 33.141 and 33.222 on TLS profile related text. 33.141 has still some TLS related text that fits better to the scope of 33.222.
Summary of change:	⌘	Adding new clauses: - 5.3.1.3 Authentication of the AP/AS - 5.3.1.4 Authentication Failures - 5.3.1.5 Set-up of Security parameters - 5.3.1.6 Error cases Updating the references section Minor editorial in 5.3
Consequences if not approved:	⌘	Lack of clarity and concistency in the specifications

Clauses affected:	⌘	2, 5.3, 5.3.1

	Y	N			
Other specs affected:	X		Other core specifications	⌘	33.141
		X	Test specifications		
		X	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 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] IETF RFC 2616 (1999): "Hypertext Transfer Protocol (HTTP) – HTTP/1.1".

[13] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security".

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

[15] IETF Internet-Draft: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", February 6, 2004, URL: http://www.ietf.org/internet-drafts/draft-eronen-tls-psk-00.txt.

[16] 3GPP TS 33.221: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Support for subscriber certificates".

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

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

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

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

The authentication mechanism described in this section is mandatory to implement in UE and NAF.

This section explains how the procedures specified in TS 33.220 [3] have to be enhanced when HTTPS is used between a UE and a NAF. The following gives the complementary description with respect to the procedure specified in clause 4.5.3 of TS 33.220 [3]. This document specifies the logical information carried in some header fields. The exact definition of header fields is left to stage 3 specifications.

1) When the UE starts communication via Ua reference point with the NAF, it shall establish a TLS tunnel with the NAF. The NAF is authenticated to the UE by means of a public key certificate. The UE shall verify that the server certificate corresponds to the FQDN of the NAF it established the tunnel with. No client authentication is performed as part of TLS (no client certificate necessary).

2) In response to the HTTPS (HTTP over TLS) request received from UE over the Ua reference point, the NAF shall invoke HTTP digest as specified in RFC 2617 [10] with the UE in order to perform client authentication using the shared key as specified in section 4.5.3 of TS 33.220 [3]. The realm attribute of the WWW-Authenticate header field shall contain the constant string "3GPP-bootstrapping" and the FQDN of the NAF, to indicate the GBA as the required authentication method.

3) On receipt of the response from the NAF, the UE shall verify that the FQDN in the realm attribute corresponds to the FQDN of the NAF it established the TLS connection with. On failure the UE shall terminate the TLS connection with the NAF.

4) In the following request to NAF the UE sends a response with an Authorization header field where Digest is inserted using the B-TID as username and the session key Ks_NAF as password.

5) On receipt of this request the NAF shall verify the value of the password attribute by means of the Ks_NAF retrieved from BSF over Zn using the B-TID received as user name attribute in the query.

6) After the completion of step 5), UE and NAF are mutually authenticated as the TLS tunnel endpoints.

NOTE: RFC 2617 [10] mandates in section 3.3 that all further HTTP requests to the same realm must contain the Authorization request header field, otherwise the server has to send a new "401 Unauthorized" with a new WWW-Authenticate header. In principle it is not necessary to send an Authorization header in each new HTTP request for security reasons as long as the TLS tunnel exists, but this would not conform to RFC 2617 [10].

In addition, there may be problems with the lifetime of a TLS session, as the TLS session may time-out at unpredictable (at least for the UE) times, so any request sent by UE can be the first request inside a newly established TLS tunnel requiring the NAF to re-check user credentials.

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

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

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

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 [14] or higher. Earlier versions are not allowed.

NOTE: The management of Root Certificates is out of scope of 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 [7].

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

5.3.1.3 Authentication of the AP/AS

The AP/AS is authenticated by the Client as specified in WAP-219-TLS [14], which in turn is based on RFC 2246 [6].

The AP/AS certificate profile shall be based on WAP Certificate and CRL Profile as defined in WAP 211 WAPCert [17].

5.3.1.4 Authentication Failures

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

5.3.1.5 Set-up of Security parameters

The TLS Handshake Protocol negotiates a session, which is identified by a Session ID. The Client and the AP/AS 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.

5.3.1.6 Error cases

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

- if the received ciphersuites only includes all or some of the Ciphersuites in Clause 5.3.1.2;

- if the received ciphersuites do not include any integrity protection;

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