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

Tdoc ⌘S3-040657

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⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Further modifications to TLS profile related text in 33.141
Source:	⌘	Ericsson, Siemens
Work item code:	⌘	Presence Security
Date:	⌘	06/09/2004
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. The use of confidentiality protection is seen as application specific requirement, and error cases related to confidentiality protection are consequently left in clause 7.2 of 33.141.
Summary of change:	⌘	Text in sections 6.1.2, 6.1.4, 7.1 and 7.2 is moved to 33.222 and replaced with appropiate references. References are updated
Consequences if not approved:	⌘	Lack of clarity and concistency in the specifications

Clauses affected:	⌘	2, 6.1.2, 6.1.4, 7.1, 7.2

Other specs affected:	Y	N			
⌘	X		Other core specifications	⌘	33.222
		X	Test specifications		
		X	O&M Specifications		

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

***** 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] 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 24.109: "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] IETF RFC 3310 (2002); "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[19] 3GPP TS 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 of Change ****

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

6.1.2 Authentication of the AP/Presence Server

Authentication of the AP/Presence Server shall be performed according to clause 5.3.1.3 of TS 33.222 [19].~~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].~~

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

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

6.1.4 Authentication Failures

The handling of authentication failures shall be according to clause 5.3.1.4 of TS 33.222 [19].~~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.~~

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

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

7 Security parameters agreement

7.1 Set-up of Security parameters

Security parameters shall be set-up according to clause 5.3.15 of TS 33.222 [19].~~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.~~

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

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

7.2 Error cases

Error cases shall be handled as specified in clause 5.3.1.6 of TS 33.222 [19]. In addition, ~~T~~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 and the policy of the operator stipulates that encryption is required;
- if the policy of the operator stipulates that encryption is required and the common set of supported ciphersuites only include key material less than the number of bits required by the operator for confidentiality protection.~~128 bits for confidentiality protection.~~

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