

CR-Form-v7.1

CHANGE REQUEST

33.222 CR 009 rev - Current version: **6.1.0**

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:	Clean-up of TS 33.222		
Source:	Ericsson		
Work item code:	GBA-SSC	Date:	22/11/2004
Category:	D	Release:	Rel-6
	Use <u>one</u> 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 <u>one</u> of the following releases: Ph2 (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) Rel-7 (Release 7)

Reason for change:	Cleaning up TS 33.222 for rel-6		
Summary of change:	Removing editor's notes from the TS for rel-6, as work on the issues has not been progressed within rel-6.		
Consequences if not approved:	Unnecessary editor's notes remain in the specification		

Clauses affected:	5.3.1.1, 6.4.2, 6.5.2, Annex A										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">X</td> <td style="text-align: center;"></td> </tr> <tr> <td style="text-align: center;"></td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"></td> <td style="text-align: center;">X</td> </tr> </table> Other core specifications	Y	N	X			X		X	24.109 may be affected?	
Y	N										
X											
	X										
	X										
Other comments:											

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

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.

Editor's 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.

~~Editor's Note: It is FFS what parts (if any) of the TLS extensions as specified in RFC 3546 [8] shall be implemented in this TS.~~

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

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

6.4.2 AP-AS reference point

The HTTP protocol is run over the AP-AS reference point.

Confidentiality and integrity protection can be provided for the reference point between the AP and the AS using NDS/IP mechanisms as specified in TS 33.210 [12]. For traffic between different security domains, the Za reference point shall be operated. For traffic inside a security domain, it is up to the operator to decide whether to deploy the Zb reference point. As AP terminates the TLS tunnel from UE, also a TLS tunnel is possible.

The AP shall support the transfer of an identity of the UE authenticated by the AP from AP to AS in a standardised format. The format of this information element in the HTTP request header is left to stage 3 specifications.

~~Editor's Note: If further information elements from the application specific user profile are transferred in standardised format to AS is ffs.~~

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

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

6.5.2 Transfer of Asserted Identity from AP to AS

The AP is configured per AS to perform authentication and access control according to one of the following subclauses: if required in the subclause, the user identity is transferred to AS in every HTTP request proxied to AS.

~~Editor's Note:— It is ffs if further information elements from application specific user profile may be transferred to AS.~~

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

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

Annex A (informative): Technical Solutions for Access to Application Servers via Authentication Proxy and HTTPS

~~Editors' note: The text in this informative annex may need to be revisited if changes in the main body of the text are made.~~

This annex gives some guidance on the technical solution for authentication proxies so as to help avoid misconfigurations. An authentication proxy acts as reverse proxy which serves web pages (and other content) sourced from other web servers (AS) making these pages look like they originated at the proxy.

To access different hosts with different DNS names on one server (in this case the proxy) the concept of virtual hosts was created.

One solution when running HTTPS is to associate each host name with a different IP address (IP based virtual hosts). This can be achieved by the machine having several physical network connections, or by use of virtual interfaces which are supported by most modern operating systems (frequently called "*ip aliases*"). This solution uses up one IP address per AS and it does not allow the notion of "one TLS tunnel from UE to AP-NAF" for all applications behind a NAF together.

If it is desired to use one IP address only or if "one TLS tunnel for all" is required, only the concept of name-based virtual hosts is applicable. Together with HTTPS, however, this creates problems, necessitating workarounds which may deviate from standard behaviour of proxies and/or browsers. Workarounds, which affect the UE and are not generally supported by browsers, may cause interoperability problems. Other workarounds may impose restrictions on the attached application servers.

To access virtual hosts where different servers with different DNS names are co-located on AP, either of the solutions could be used to identify the host during the handshaking phase:

- Extension of TLS is specified in RFC 3546 [8]. This RFC supports the UE to indicate a virtual host that it intends to connect in the very initial TLS handshaking message;
- The other alternative is to issue a multiple-identities certificate for the AP. The certificate will contain identities of AP as well as each server that rely on AP's proxy function. The verification of this type of certificate is specified in RFC 2818 [9].

~~Editor's note: The shared-key TLS based authentication does not require server's certificate, but the possession of the key for authentication. The procedure is ffs.~~

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