3GPP TSG-SA WG3 Meeting #36 ***Tdoc ⌘S3-041096***
Shenzhen, China, November 23-26, 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.222 CR 013** ⌘**rev** **1** ⌘ 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:	⌘	TLS extensions support			
Source:	⌘	SA WG3			
Work item code:	⌘	SEC1-SC	***Date:***	⌘	16/11/2004
Category:	⌘	**C**	***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:

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:	⌘	TLS extension "server_name" support is mandated in the UE and in the NAF. This eases the handling of TLS server certificates in the case where the NAF is doing virtual name based hosting (e.g., in the authentication proxy case).
Summary of change:	⌘	- 5.3.1: The support for server_name extension of TLS extensions is mandated for both the UE and the NAF (corresponding editor's note in 5.3.1.1 is deleted). - Annex A: editor's notes are deleted and text is added to address the addition of server_name TLS extension. - Annex B: Editor's note is removed.
Consequences if not approved:	⌘	

Clauses affected:	⌘	5.3.1, 5.3.1.1, Annex A, Annex B				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	TS 24.109
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

==== BEGIN 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 1: The management of Root Certificates is out of scope of this Technical Specification.

The UE and the NAF shall support the server_name TLS extension. All other TLS extensions as specified in RFC 3546 [8] are optional for implementation.

NOTE 2: If the NAF is doing virtual name based hosting (e.g., in the case of authentication proxy, cf. Annex A), the NAF needs to either have a TLS server certificate that contains all the hostnames that the NAF can be addressed with (i.e., virtual hostnames), or have one TLS server certificate for each of the hostnames mentioned above. In the latter case, the server_name extension is needed because the NAF needs to be able to select the correct TLS server certificate.

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.~~

==== BEGIN NEXT 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 (cf., 5.3.1);

- 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].

Either approach may be chosen by the operator who operates the authentication proxy.

~~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.~~

==== BEGIN NEXT CHANGE ====

Annex B (informative): Guidance on Certificate-based mutual authentication between UE and application server

This section explains how subscriber certificates (see TS 33.221 [16]) are used in certificate-based mutual authentication between a UE and an application server. The certificate-based mutual authentication between a UE and an application server shall be based TLS as specified in IETF RFC 2246 [6] and IETF RFC 3546 [8].

When a UE and an application server (AS) want to mutually authenticate each other based on certificates, the UE has previously enrolled a subscriber certificate as specified in TS 33.221 [16]. After UE is in the possession of the subscriber certificate it may establish a TLS tunnel with the AS as specified in RFC 2246 [6] and RFC 3546 [8].

The AS may indicate to the UE, that it supports client certificate-based authentication by sending a CertificateRequest message as specified in section 7.4.4 of IETF RFC 2246 [6] during the TLS handshake. This message includes a list of certificate types and a list of acceptable certificate authorities. The AS may indicate to the UE that it supports subscriber certificate-based authentication if the list of acceptable certificate authorities includes the certification authority of the subscriber certificate (i.e. the operator's CA certificate).

The UE may continue with the subscriber certificate-based authentication if the list of acceptable certificate authorities includes the certification authority of the subscriber certificate. This is done by sending the subscriber certificate as the Certificate message as specified in sections 7.4.6 and 7.4.2 of IETF RFC 2246 [6] during the TLS handshake. If the list of acceptable certificate authorities does not include the certification authority of the subscriber certificate, then UE shall send a Certificate message that does not contain any certificates.

NOTE: Due to the short lifetime of the subscriber certificate, the usage of the subscriber certificate does not require on-line interaction between the AS and the PKI portal that issued the certificate.

If the AS receives a Certificate message that does not contain any certificates, it can continue the TLS handshake in two ways:

- if subscriber certificate-based authentication is mandatory according to the AS's security policy, it shall response with a fatal handshake failure alert as specified in IETF RFC 2246 [6], or

- if subscriber certificate-based authentication is optional according to AS's security policy, AS shall continue with TLS handshake as specified in IETF RFC 2246 [6].

In the latter case, if the AS has NAF functionality, the NAF may authenticate the UE as specified in clause 5.3 of the present specification, where after establishing the server-authenticated TLS tunnel, the procedure continues from step 4.

NOTE: In order to successfully establish a TLS tunnel between the UE and the AS using certificates for mutual authentication, the UE must have the root certificate of the AS's certificate in the UE's certificate store, and the AS must have the root certificate of the UE's subscriber certificate (i.e. operator's CA certificate) in the AS's certificate store. The root certificate is the root of the certification path, and should be marked trusted in the UE and the AS.

~~Editor's note: The support of accessing an AS in the visited network is FFS in future Release.~~

==== *END CHANGE* ====