

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.222 CR 015** ⌘ 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:	⌘ Keeping PSK TLS in 3GPP rel-6		
Source:	⌘ SA WG3		
Work item code:	⌘ SEC1-SC	Date:	⌘ 25/11/2004
Category:	⌘ F	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:	⌘ Keeping PSK TLS in 3GPP rel-6. PSK TLS is expected to reach RFC status soon.		
Summary of change:	⌘ - Update of references in subclause 2 ⌘ - Deleting of editoris notes in subclause 5.4 Note: SA3 has agreed earlier that PSK TLS is optional to implement in both the UE and in the NAF.		
Consequences if not approved:	⌘ Delay PSK TLS to Release 7		

Clauses affected:	⌘ 2, 5.4										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td style="width: 20px;">X</td> <td style="width: 20px;"></td> </tr> <tr> <td style="width: 20px;"></td> <td style="width: 20px;">X</td> </tr> <tr> <td style="width: 20px;"></td> <td style="width: 20px;">X</td> </tr> </table> Other core specifications Test specifications O&M Specifications	Y	N	X			X		X	⌘ 24.109	
Y	N										
X											
	X										
	X										
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) ñ 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)", May 24, 2004, URL: <http://www.ietf.org/internet-drafts/draft-ietf-tls-psk-0004.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 *****

5.4 Shared key-based mutual authentication between UE and NAF

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

~~Editor's note: If the "Pre-Shared Key Ciphersuites for TLS" Internet Draft [15] does not reach the RFC status by the time when Release 6 is frozen, this subclause shall be removed and the support for the Pre-Shared Key TLS is postponed to Release 7.~~

The HTTP client and server may authenticate each other based on the shared key generated during the bootstrapping procedure. The shared key shall be used as a master key to generate TLS session keys, and also be used as the proof of secret key possession as part of the authentication function. The exact procedure is specified in Pre-Shared Key Ciphersuites for Transport Layer Security (TLS) [15].

~~Editor's note: The exact procedure of "Pre-Shared Key Ciphersuites for TLS" is under inspection in IETF. When the procedure is ready in IETF, the description how it is used in GAA should be added to TS 24.109, and this subclause should refer to it. The following gives general guidelines for how the TLS handshake may be accomplished using a GBA-based shared secret. The exact definitions of the message fields are left to the stage 3 specifications.~~

This section explains how a GBA-based shared secret that is established between the UE and the BSF as specified in TS 33.220 [3] is used with Pre-Shared Key (PSK) Ciphersuites for TLS as specified in IETF Internet-Draft [15].

1. When an UE contacts a NAF, it may indicate to the NAF that it supports PSK-based TLS by adding one or more PSK-based ciphersuites to the ClientHello message. The UE shall include ciphersuites other than PSK-based ciphersuites in the ClientHello message. The UE shall send the hostname of the NAF using the server_name extension to the ClientHello message as specified in IETF RFC 3546 [8].

NOTE 1: The ability to send the hostname of the NAF is particularly necessary if a NAF can be addressed using different hostnames, and the NAF cannot otherwise discover what is the hostname that the UE used to contact the NAF. The hostname is needed by the BSF during key derivation.

NOTE 2: When the UE adds one or more PSK-based ciphersuites to the ClientHello message, this can be seen as an indication that the UE supports GBA-based authentication. If the UE supports PSK-based ciphersuites but not GBA-based authentication, the TLS handshake will fail if the NAF selected the PSK-based ciphersuite and suggested to use GBA (as described in step 2). In this case, the UE should attempt to establish the TLS tunnel with the NAF without including PSK-based ciphersuites to the ClientHello message, according to the procedure specified in clause 5.3. This note does not limit the use of PSK TLS to HTTP-based services.

2. If the NAF is willing to establish a TLS tunnel using a PSK-based ciphersuite, it shall select one of the PSK-based ciphersuites offered by the UE, and send the selected ciphersuite to the UE in the ServerHello message. The NAF shall send the ServerKeyExchange message with a PSK-identity that shall contain a constant string "3GPP-bootstrapping" to indicate the GBA as the required authentication method. The NAF finishes the reply to the UE by sending a ServerHelloDone message.

NOTE 3: If the NAF does not wish to establish a TLS tunnel using a PSK-based ciphersuite, it shall select a non-PSK-based ciphersuite and continue TLS tunnel establishment based on the procedure described either in clause 5.3 or clause 5.5.

3. The UE shall use a GBA-based shared secret for PSK TLS, if the NAF has sent a ServerHello message containing a PSK-based ciphersuite, and a ServerKeyExchange message containing a constant string "3GPP-bootstrapping" as the PSK identity hint. If the UE does not have a valid GBA-based shared secret it shall obtain one by running the bootstrapping procedure with the BSF over the Ub reference point as specified in TS 33.220 [3].

The UE derives the TLS premaster secret from the NAF specific key (Ks_NAF) as specified in IETF Internet Draft [15].

The UE shall send a ClientKeyExchange message with the B-TID as the PSK identity. The UE concludes the TLS handshake by sending the ChangeCipherSuite and Finished messages to the NAF.

4. When the NAF receives the B-TID in the ClientKeyExchange messages it fetches the NAF specific shared secret (Ks_NAF) from the BSF using the B-TID.

The NAF derives the TLS premaster secret from the NAF specific key (Ks_NAF) as specified in IETF Internet Draft [15].

The NAF concludes the TLS handshake by sending the ChangeCipherSuite and Finished messages to the UE.

The UE and the NAF have established a TLS tunnel using GBA-based shared secret, and then may start to use the application level communication through this tunnel.

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