3GPP TSG-SA WG3 Meeting #37
Sophia Antipolis, France, February 21-25, 2005

Tdoc ⌘S3-050145

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.222**	**CR**	**015**	⌘ **rev**	**3**	⌘	Current version:	**6.2.0** ⌘

*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:	⌘	Nokia		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	02/02/2005
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:* *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:	⌘	- PSK TLS is kept in Release-6 as it as proceeded well in IETF. - TLS profile for PSK TLS is added - the approved CR005 (S3-040731 list of PSK identity hints) is reimplemented in this CR as V6.2.0 does not include it
Summary of change:	⌘	Editor's notes are removed, CR005 is reimplemented, and TLS profile section added.
Consequences if not approved:	⌘	- Uncertaintity of PSK TLS in Rel-6 remains in the specification - Interoperability between different PSK TLS implementations is not ensured

Clauses affected:	⌘	2, 5.4, 5.4.1 (new)				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	TS 24.109
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

===== BEGIN 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)", ~~November~~December 2004, URL: http://www.ietf.org/internet-drafts/draft-ietf-tls-psk-0~~4~~5.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.

[18] 3GPP TS 24.109: "3rd Generation Partnership Project; Technical Specification Group Core Network; Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

===== BEGIN NEXT 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 PSK-based TLS~~GBA-based authentication~~. If the UE supports ~~PKS~~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 CientHello 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 list of PSK-identity hints.~~that shall contain a~~ A constant string "3GPP-bootstrapping" ~~to~~shall indicate the GBA as the required authentication method. Also other PSK-identity hints may be supported, however, they are out of the scope of this specification. 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 PSK identity in the ClientKeyExchange message shall include a prefix indicating the PSK-identity name space that was selected, and the B-TID. The prefix must match one of the PSK-identity hints that NAF offered in ServerKeyExchange message. The precise format of the PSK identity is specified in 3GPP TS 24.109 [18]. The UE concludes the TLS handshake by sending the ChangeCipherSuite and Finished messages to the NAF.

4. When the NAF receives the "3GPP-bootstrapping" prefix and 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.

5.4.1 TLS Profile

If the PSK TLS based authentication mechanism is supported, the UE or the NAF shall support the TLS version as specified in RFC 2246 [6], WAP-219-TLS [14], PSK TLS [15], or higher. Earlier versions are not allowed.

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, see Annex A), the NAF needs to be able to discover the correct server name to indicate the correct NAF_ID to the BSF. Otherwise the BSF is not able derive the correct Ks_NAF.

5.4.1.1 Protection mechanisms

The UE shall support the CipherSuite TLS_PSK_WITH_AES_128_CBC_SHA. All other Cipher Suites as defined in PSK TLS [15] are optional for implementation for the UE.

The NAF shall support the CipherSuite TLS_PSK_WITH_AES_128_CBC_SHA. All other Cipher Suites as defined in PSK TLS [15] are optional for implementation for the NAF.

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.

5.4.1.2 Authentication of the AP/AS

The AP/AS is authenticated by the Client as specified in PSK TLS [15].

5.4.1.3 Authentication Failures

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.

5.4.1.4 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 the lifetime of the GAA shared secret or maximum of 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 CHANGE =====