**Source:** **SA WG3**

**Title:** **8 CRs to 33.222: (Rel-6)**

**Document for:** **Approval**

**Agenda Item:** **7.3.3**

The following CRs have been agreed by SA WG3 and are presented to TSG SA for approval.

| TSG SA Doc number | Spec | CR | Rev | Phase | Subject | Cat | Version-Current | SA WG3 Doc number | Work item |
|---|---|---|---|---|---|---|---|---|---|
| SP-040857 | 33.222 | 005 | - | Rel-6 | GBA supported indication in PSK TLS | C | 6.1.0 | S3-040731 | GBA-SSC |
| SP-040857 | 33.222 | 007 | 1 | Rel-6 | Adding Support for AES in the TLS Profile | C | 6.1.0 | S3-041092 | GBA-SSC |
| SP-040857 | 33.222 | 008 | - | Rel-6 | Removing PSK TLS from 3GPP rel-6 | F | 6.1.0 | S3-040965 | GBA-SSC |
| SP-040857 | 33.222 | 010 | 1 | Rel-6 | Authorization flag transfer between AP and AS | C | 6.1.0 | S3-041093 | GBA-SSC |
| SP-040857 | 33.222 | 012 | - | Rel-6 | Correction of inconsistencies within AP specification | F | 6.1.0 | S3-040985 | GBA-SSC |
| SP-040857 | 33.222 | 013 | 1 | Rel-6 | TLS extensions support | C | 6.1.0 | S3-041096 | SEC1-SC |
| SP-040857 | 33.222 | 014 | - | Rel-6 | Visited AS using subscriber certificates | C | 6.1.0 | S3-041026 | SEC1-SC |
| SP-040857 | 33.222 | 015 | 1 | Rel-6 | Keeping PSK TLS in 3GPP rel-6 | F | 6.1.0 | S3-041142 | SEC1-SC |

**3GPP TSG-SA WG3 Meeting S3#35**
**St Paul's Bay, Malta, October 5-8, 2004**

***Tdoc ⌘S3-040731***

*CR-Form-v7*

# CHANGE REQUEST

⌘ **33.222** **CR** **005** ⌘ **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 [X] Radio Access Network ☐ Core Network [X]

| | | |
|---|---|---|
| ***Title:*** | ⌘ | GBA supported indication in PSK TLS |
| ***Source:*** | ⌘ | SA WG3 |
| ***Work item code:*** | ⌘ | GBA-SSC |
| ***Date:*** | ⌘ | 21/09/2004 |
| ***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:*

| | |
|---|---|
| *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:*** | ⌘ | GBA indication with Pre-Shared Key TLS (PSK-TLS) currently limits the use of the ciphersuites to GBA. Other key generation mechanisms can not be used. The general design principle of GBA has been that NAF holds control of the used authentication mechanism (i.e. the use of GBA or non-GBA originated credentials). |
| ***Summary of change:*** | ⌘ | In order to keep the option of having non-GBA originated credentials with PSK-TLS, the NAF should be able to indicate to UE that it supports non-GBA based credentials. Also, UE must indicate which credentials are used. |
| ***Consequences if not approved:*** | ⌘ | PSK-TLS can only be used with one set of credentials. NAF is not able to use PSK-TLS with GBA and non-GBA method at the same time. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 2, 5.4 |

***Other specs affected:*** ⌘

| Y | N | | |
|---|---|---|---|
| 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) 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)", August 18, ~~May 24,~~ 2004, URL: http://www.ietf.org/internet-drafts/draft-ietf-tls-psk-01~~0~~.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 PSK~~KS~~-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 the appropriate stage 3 specification [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.

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

**3GPP TSG-SA WG3 Meeting #36**
**Shenzhen, China, 23 ñ 26 November 2004**

***Tdoc ⌘S3-041092***

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **33.222** **CR** **007** ⌘**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 [X] Radio Access Network ☐ Core Network [X]

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Adding Support for AES in the TLS Profile |
| ***Source:*** | ⌘ | SA WG3 |
| ***Work item code:*** | ⌘ | GBA-SSC |
| ***Date:*** | ⌘ | 22/11/2004 |
| ***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:*** | ⌘ | Currently, only ìTLS_RSA_ WITH_3DES_EDE_CBC_SHAî shall be supported both in the UE and the NAF. It is considered general security practice to support several algorithms for confidentiality and integrity protection |
| ***Summary of change:*** | ⌘ | Adding support for the ìTLS_RSA_WITH_AES_128_CBC_SHAî cipher suite. |
| ***Consequences if not approved:*** | ⌘ | The general security practice of supporting several algorithms is not implemented in TS 33.222 |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 5.3.1 |

| ***Other specs affected:*** ⌘ | Y | N | | ⌘ |
|---|---|---|---|---|
| | | X | Other core specifications | |
| | | X | Test specifications | |
| | | X | O&M Specifications | |

***Other comments:*** ⌘

# ***** Begin of 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: The management of Root Certificates is out of scope of this Technical Specification.

### 5.3.1.1 Protection mechanisms

The UE shall support the CipherSuite TLS_RSA_ WITH_3DES_EDE_CBC_SHA and the CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA. All other Cipher Suites as defined in RFC 2246 [6] and RFC 3268 [7] 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 and the CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA.. All other Cipher Suites as defined in RFC 2246 [6] and RFC 3268 [7] 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 *****

**3GPP TSG-SA WG3 Meeting #36**
**Shenzhen, China, 23 ñ 26 November 2004**

***Tdoc ⌘S3-040965***

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **33.222** **CR** **008** ⌘ **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:*** | ⌘ | Removing PSK TLS from 3GPP rel-6 |
| ***Source:*** | ⌘ | SA WG3 |
| ***Work item code:*** | ⌘ | GBA-SSC |
| ***Date:*** | ⌘ | 22/11/2004 |
| ***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:*

| | |
|---|---|
| *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:*** | ⌘ | The PSK TLS Internet Draft is unlikely to reach RFC status before rel-6 is frozen. Thus, PSK TLS should be postponed to rel-7 according to earlier agreements in SA3. |
| ***Summary of change:*** | ⌘ | Removing PSK TLS from TS 33.222 for rel-6 |
| ***Consequences if not approved:*** | ⌘ | TS 33.222 will use and reference technology that is not mature. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 2, 5.4, Annex A |

| ***Other specs affected:*** | ⌘ | Y | N | | | |
|---|---|---|---|---|---|---|
| | | X | | Other core specifications | ⌘ | 24.109 |
| | | | X | Test specifications | | |
| | | | X | O&M Specifications | | |

| | | |
|---|---|---|
| ***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-00.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 PKS-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 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 *****

***** 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 *****

**3GPP TSG-SA WG3 Meeting S3#36**
**Shenzen, PRC, November 23-26, 2004**

***Tdoc ⌘S3-041093***

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **33.222** **CR** **010** ⌘ **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 **X**

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Authorization flag transfer between AP and AS |
| ***Source:*** | ⌘ | SA WG3 |
| ***Work item code:*** | ⌘ | GBA-SSC |
| ***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:*** | ⌘ | Editorís note on transfer of user profile from AP to AS is no longer needed, since the identities of the user are transferred in the HTTP header from the AP to the AS. In case the AS resides behind the AP, the AS would need to obtain the authorization flags to make a decision on the user authorization (based on the flags). |
| ***Summary of change:*** | ⌘ | 1. Removal of editorís note in 6.4.2 and correcting wrong reference number<br>2. Removal of editorís note in 6.5.2<br>3. Addition in 6.5.2.3 to transfer the authorization profile flags in the HTTP header of message from AP to AS. |
| ***Consequences if not approved:*** | ⌘ | The editorís notes will indicate open issues and the AS that resides behind the AP will not be able to make an authorization decision that is based on authorization flags. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 6.4.2, 6.5.2, 6.5.2.3 |

| | | Y | N | | | |
|---|---|---|---|---|---|---|
| ***Other specs affected:*** | ⌘ | X | | Other core specifications | ⌘ | TS 24.109 CR009R1 |
| | | | X | Test specifications | | |
| | | | X | O&M Specifications | | |

| | | |
|---|---|---|
| ***Other comments:*** | ⌘ | |

**===== BEGIN 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~~13]. 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.~~

**===== BEGIN NEXT 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.~~

**===== BEGIN NEXT CHANGE =====**

### 6.5.2.3 Authorised User of Application with Transferred Identity asserted to AS

The AP checks that the UE is an authorised user of the application. The user identity (or user identities) received from the BSF shall be transferred to AS. Based on AS-specific configuration of the AP, any authorization flags existing in application-specfic user security settings shall also be transferred to AS.

Depending on the application specific user security setting and the AS-specific configuration of the AP, the transferred user identity (or identities) may be the private user identity (IMPI), or may be taken from the application specific user security setting (e.g. an IMPU), or may be a pseudonym chosen by AP (e.g. Random, B-TID).

This case may be supported by AP.

NOTE 1: If the AP is configured to transfer a pseudonym to AS, any binding of this pseudonym to the user identity (e.g. for charging purposes by AS) is out of scope of this specification.

NOTE 2: If the AP is configured not to request an application specific user security setting from BSF, only the private user identity (IMPI) or a pseudonym may be transferred to AS. In this case any authorised participant of GBA is supposed to be an authorised user of the application.

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

**3GPP TSG SA WG3 Security ó S3#36** **S3-040985**
**November 23-26, 2004, Shenzhen, China**

CR-Form-v7

# CHANGE REQUEST

⌘ **33.222** **CR** **012** ⌘ **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 **X**

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Correction of inconsistencies within AP specification |
| ***Source:*** | ⌘ | SA WG3 |
| ***Work item code:*** | ⌘ | GBA-SSC |
| ***Date:*** | ⌘ | 12/11/2004 |
| ***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:*** | ⌘ | Subclauses 6.4 and 6.5 were changed in S3-040319 at SA3#33. At that time two inconsistencies slipped in:<br>- Subclause 6.5.2.3 and stage 3 TS 24.109 specify the transfer of asserted identity to AS as optional to implement (ìmayî). Subclause 6.4.2 is corrected accordingly.<br>- Subclause 6.5.1.2 specifies access control based on user security settings as mandatory to implement. Subclause 6.5.2.2 is a consequence of 6.5.1.2 and therefore also (automatically) implemented. |
| ***Summary of change:*** | ⌘ | Alignment of subclause 6.4.2 with 6.5.2.3 and stage 3 spec.<br>Alignment of subclause 6.5.2.2 with 6.5.1.2. |
| ***Consequences if not approved:*** | ⌘ | Inconsistency between mentioned subclauses and between stage 2 and 3 specs. |

| | | | | | |
|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 6.4.2, 6.5.2.2 | | | |
| ***Other specs affected:*** | ⌘ | **Y** / **N** | Other core specifications | ⌘ | TS 24.109 |
| | | **X** / | Other core specifications | | |
| | | / **X** | Test specifications | | |
| | | / **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | - | | | |

**********  begin 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~~ may 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.

**********  begin next change  **********

### 6.5.2.2 Authorised User of Application Anonymous to AS

The AP checks that the UE is an authorised user of the application according to application specific user security setting received from BSF. No user identity shall be transferred to AS.

This case ~~may~~ shall be supported by AP.

**********  end change  **********

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

***Tdoc ⌘S3-041096***

*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 [X] Radio Access Network ☐ Core Network [X]

| | | |
|---|---|---|
| ***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).<br>- Annex A: editor's notes are deleted and text is added to address the addition of server_name TLS extension.<br>- Annex B: Editor's note is removed. |
| ***Consequences if not approved:*** | ⌘ | |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 5.3.1, 5.3.1.1, Annex A, Annex B |

| ***Other specs affected:*** | Y | N | | | |
|---|---|---|---|---|---|
| ⌘ | 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* ====**

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

***Tdoc ⌘S3-041026***

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **33.222** **CR** **014** ⌘ **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:*** | ⌘ | Visited AS using subscriber certificates |
| ***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:*** | ⌘ | Clarification is added how a visited AS can use subscriber certificates to authenticate the subscriber. |
| ***Summary of change:*** | ⌘ | When the AS resides in the visited network, the visited network can decide to trust the home operatorís CA certificate as trusted root certificate. Therfore, the editorís note is not needed. |
| ***Consequences if not approved:*** | ⌘ | |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | Annex B |

| | | Y | N | | |
|---|---|---|---|---|---|
| ***Other specs affected:*** | ⌘ | | X | Other core specifications | ⌘ |
| | | | X | Test specifications | |
| | | | X | O&M Specifications | |

| | | |
|---|---|---|
| ***Other comments:*** | ⌘ | |

==== ***BEGIN 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 1: 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 2: 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.~~

NOTE 3: In order to enable access to an AS in a visited network with subscriber certificates requires that the AS has the CA certificate of subscriber's home operator and it is marked trusted in the visited AS. The procedure to do this is outside the scope of this specification.

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

**3GPP TSG-SA WG3 Meeting #36**
**Shenzhen, China, 23 ñ 26 November 2004**

***Tdoc ⌘S3-041142***

*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 [X] Radio Access Network ☐ Core Network [X]

| | | |
|---|---|---|
| ***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 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:*** | ⌘ | 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<br>- Deleting of editorís notes in subclause 5.4<br>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 |

| | Y | N | | | |
|---|---|---|---|---|---|
| ***Other specs affected:*** | X | | Other core specifications | ⌘ | 24.109 |
| | | X | Test specifications | | |
| | | X | O&M Specifications | | |

| | | |
|---|---|---|
| ***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-~~00~~04.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 PKS-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 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 *****