Technical Specification Group Services and System Aspects
Meeting #25, Palm Springs, USA

TSGS#25(04)0621

Source: **SA WG3**

Title: **4 CRs to 33.222: GBA: Various changes to Subscriber Certificates (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CRs were 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
	33.222	001	-	Rel-6	GBA User Security Settings	D	6.0.0	S3-040503	SEC1-SC
	33.222	002	-	Rel-6	GBA supported indication and NAF hostname transfer in HTTP and in PSK TLS	C	6.0.0	S3-040656	SEC1-SC
	33.222	003	-	Rel-6	Editorial clean-up of TS 33.222	D	6.0.0	S3-040660	SEC1-SC
	33.222	004	-	Rel-6	Further modifications to TLS profile related text in 33.222	F	6.0.0	S3-040658	SEC1-SC

CR-Form-v7

CHANGE REQUEST

⌘ 33.222 CR 001 ⌘ rev - ⌘ Current version: 6.0.0 ⌘

*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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	GBA User Security Settings
Source:	⌘	SA WG3
Work item code:	⌘	SEC1-SC
Date:	⌘	29/06/2004
Category:	⌘	D
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:	⌘	The use of the term GBA User Security Settings (previously termed GAA user profiles) is aligned with TS 33.220.
Summary of change:	⌘	Alignment with TS 33.220.
Consequences if not approved:	⌘	Mismatch of specifications.

Clauses affected:	⌘	6.5

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	TS 29.109
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	-

6.5 Management of UE identity

~~Editor's Note: The changes made to handling of application specific user profiles in TS 33.220 may affect this clause.~~

Different ASs need different kinds of authentication information. To support the requirements of different servers, the AP needs to perform authentication with varying granularity and with varying degree of assertion to the AS. The authentication and the corresponding assertion is therefore AS specific and has to be configured in the AP per AS.

6.5.1 Granularity of Authentication and Access Control by AP

The AP is configured per AS if the particular application or applications served by the AS is in need of an application specific user security setting, cf. TS 33.220 (Definitions)~~profile~~. This user security setting ~~profile~~ may contain the public user identities in the authentication part of the USS. The authorisation part of the USS may contain indications, which of the applications residing on the AP, and the Application Servers behind the AP, a user is allowed to access.

6.5.1.1 Authorised Participant of GBA

The AP checks that the UE is an authorised participant of GBA. Access is granted on success of the basic GBA mechanism, i.e. the UE sends a valid B-TID and performs digest authentication with the Ks_NAF received from BSF.

The AP is configured not to request an application specific user ~~profile~~ security setting from BSF for the AS named in the request. Depending on configuration of BSF the AP may receives the private user identity (IMPI) from BSF.

This case shall be supported by AP.

NOTE: This case may apply when all subscribers of an operator, but no other users, are allowed access to operator defined services. The BSF may not send the IMPI out of privacy considerations or because the AP does not need it. If the BSF does not send the IMPI to the AP, the user remains anonymous towards the AP; or more precisely, the B-TID functions as a temporary user pseudonym.

6.5.1.2 Authorised User of Application

The AP is configured to request an application specific user security setting ~~profile~~ from the BSF. Depending on the policy of the BSF, the AP receives the application specific user security setting ~~profile~~ and the private user identity (IMPI) from the BSF. Access is granted if allowed according to the application specific user security setting ~~profile~~ received from BSF.

The AP may do further checks on user inserted identities in the HTTP request if required according to clause 6.5.2.4.

This case shall be supported by AP.

NOTE: If there is no application specific user security setting ~~profile~~ configured for an application, this case reduces to authentication according to clause 6.5.1.1.

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.

6.5.2.1 Authorised Participant of GBA

The AP checks that the UE is an authorised participant of GBA. If the authentication of the UE by the AP fails, the AP does not forward the request of the UE to the AS.

This case shall be supported by AP.

NOTE: This case simply implies that the NAF checks that the user is known to, and has established a valid key, with the BSF, according to the GBA procedures described in TS 33.220 [3].

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 ~~profile~~ received from BSF. No user identity shall be transferred to AS.

This case may be supported by AP.

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.

Depending on the application specific user security setting ~~profile~~ 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 ~~profile~~ (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: 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: If the AP is configured not to request an application specific user security setting ~~profile~~ 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.

6.5.2.4 Authorised User of Application with Transferred Identity asserted to AS and Check of User Inserted Identity

This case resembles clause 6.5.2.3 with the following extension:

Based on the user identity received from BSF, the AP authenticates user related identity information elements as sent from UE. These "user inserted identities" may occur within header fields or within the body of the HTTP request.

Depending on application specific user security setting ~~profile~~ and AS-specific configuration of AP, all user-inserted identities (or a subset thereof) are authenticated by checking against the private user identity (IMPI) or the application specific user security setting~~profile~~.

Depending on the application specific user security setting ~~profile~~ and the AS-specific configuration of AP, the transferred user identity (or identities) may also be selected from the authenticated user inserted identities.

This case may be supported by AP.

NOTE: If AP authenticates certain or all user related identity information elements of a request, and the AS shall rely on the check of these elements, then a corresponding policy between the AP and the AS needs to be in place between the AP and the AS.

NOTE: Any application specific details are beyond the scope of this document and may be specified within the application, e.g. for Presence in TS 33.141 [5]. This specification does not preclude that any other application specific specifications (e.g. Presence) declare this feature as mandatory in their scope.

3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040656

CR-Form-v7

CHANGE REQUEST

⌘ **33.222** **CR** **002** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	GBA supported indication and NAF hostname transfer in HTTP and in PSK TLS
Source:	⌘	SA WG3
Work item code:	⌘	SEC1-SC
Date:	⌘	29/06/2004
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:	⌘	The UE should be able to indicate to the NAF that it supports GBA based authentication. Also, the UE should be able to send NAF's hostname to the NAF.
Summary of change:	⌘	In order to ease the authentication method decision, the UE should be able to indicate to the NAF that it supports GBA based authentication. Also, in certain cases (e.g., virtual name based hosting) the hostname used by the UE when accessing the NAF is not unique, thus a method to transfer the hostname of the NAF used by the UE is needed. In HTTP case (subclause 5.3) these requirements are fulfilled by using HTTP headers "Host" and "User-Agent". In PSK TLS case (subclause 5.4) there requirements are fullfilled by using PSK-based ciphersuites, and the server_name TLS extension. The PSK TLS is now IETF TLS WG draft, thus the corresponding reference is updated.
Consequences if not approved:	⌘	The UE is not able to indicate to the NAF that is supports GBA-based authentication in HTTP and in PSK TLS. The UE is not required to send the hostname of the NAF to the NAF.

Clauses affected:	⌘	2, 5.3, 5.4

Other specs affected: ⌘

Y	N	
	X	Other core specifications
	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)”, ~~February 6~~ May 24, 2004, URL: http://www.ietf.org/internet-drafts/draft-~~eronen~~ietf-tls-psk-00.txt

[16] 3GPP TS 33.221: “Generic Authentication Architecture (GAA); Support for subscriber certificates”.

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

5.3 Shared key-based UE authentication with certificate-based NAF authentication

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

This section explains how the procedures specified in TS 33.220 [3] have to be enhanced when HTTPS is used between a UE and a NAF. The following gives the complementary description with respect to the procedure specified in section 4.5.3 of TS 33.220 [3], This document specifies the logical information carried in some header fields. The exact definition of header fields is left to stage 3 specifications.

1. When the UE starts communication via Ua reference point with the NAF, it shall establish a TLS tunnel with the NAF. The NAF is authenticated to the UE by means of a public key certificate. The UE shall verify that the server certificate corresponds to the FQDN of the NAF it established the tunnel with. No client authentication is performed as part of TLS (no client certificate necessary).

2. The UE sends an HTTP request to the NAF inside the TLS tunnel (HTTPS, i.e., HTTP over TLS). The UE shall indicate to the NAF that GBA-based authentication is supported by adding a constant string "3gpp-gba" to the "User-Agent" HTTP header as a product token as specified in IETF RFC 2616 [12]. The UE shall send the hostname of the NAF in "Host" HTTP header.

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.

~~2~~3. In response to the ~~-~~HTTP~~S (HTTP over TLS)~~ request received from UE over the Ua reference point, the NAF shall invoke HTTP digest as specified in RFC 2617 [10] with the UE in order to perform client authentication using the shared key as specified in section 4.5.3 of TS 33.220 [3]. The realm attribute of the WWW-Authenticate header field shall contain the constant string "3GPP-bootstrapping" and the FQDN of the NAF, to indicate the GBA as the required authentication method.

~~3~~4. On receipt of the response from the NAF, the UE shall verify that the FQDN in the realm attribute corresponds to the FQDN of the NAF it established the TLS connection with. On failure the UE shall terminate the TLS connection with the NAF.

~~4~~5. In the following request to NAF the UE sends a response with an Authorization header field where Digest is inserted using the B-TID as username and the session key Ks_NAF as password.

~~5~~6. On receipt of this request the NAF shall verify the value of the password attribute by means of the Ks_NAF retrieved from BSF over Zn using the B-TID received as user name attribute in the query.

~~6~~7. After the completion of step ~~5~~6~~)~~, UE and NAF are mutually authenticated as the TLS tunnel endpoints.

NOTE 2: RFC 2617 [10] mandates in section 3.3 that all further HTTP requests to the same realm must contain the Authorization request header field, otherwise the server has to send a new "401 Unauthorized" with a new WWW-Authenticate header. In principle it is not necessary to send an Authorization header in each new HTTP request for security reasons as long as the TLS tunnel exists, but this would not conform to RFC 2617.

In addition, there may be problems with the lifetime of a TLS session, as the TLS session may time-out at unpredictable (at least for the UE) times, any request sent by UE can be the first request inside a newly established TLS tunnel requiring the NAF to re-check user credentials.

===== 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 3GPP 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 subclause 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 subclause 5.3 or subclause 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 3GPP 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 CHANGE =====

3GPP TSG-SA WG3 Meeting #34
Acapulco, Mexico, 6 - 9 July 2004

Tdoc ⌘S3-040660

CR-Form-v7

CHANGE REQUEST

⌘ **33.222** **CR** **003** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	Editorial clean-up of TS 33.222
Source:	⌘	SA WG3
Work item code:	⌘	SEC1-SC
Date:	⌘	07/07/2004
Category:	⌘	**D**
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:	⌘	As a result of the clean-up of the overlaps between 33.141 and 33.222, some editorial modifications are also needed in 33.222. In addition, the scope section is updated to contain normative text.
Summary of change:	⌘	Editor's note in scope changed to normative text Definitions for reverse proxy and session management mechanism are added Removing obsolete editor's note in 6.2
Consequences if not approved:	⌘	The scope will not contain normative text, some definitions will be missing and an obsolete editor's note remains.

Clauses affected:	⌘	1, 3.1, 6.2

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

⌘

Other comments: ⌘

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

1 Scope

~~Editor's Note:~~ The present document specifies secure access methods to Network Application Functions (NAF) using HTTP over TLS in the Generic Authentication Architecture (GAA), and provides Stage 2 security requirements~~,~~ ~~and~~ principles and procedures for the access. The document describes both direct access to an Application Server (AS) and access to an Application Server through an Authentication Proxy (AP).

NOTE: Any application specific details for access to Applications Servers are not in scope of this specification and are covered in separate documents. An example of such a document is TS 33.141 [5], which specifies the security for presence services.

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

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

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

HTTPS: For the purpose of this document, HTTPS refers to the general concept securing the HTTP protocol using TLS. In some contexts, like in the IETF, the term HTTPS is used to refer to the reserved port number (443) for HTTP/TLS traffic.

Reverse Proxy: A reverse proxy is a web server system that is capable of serving web pages sourced from other web servers (AS), making these pages look like they originated at the reverse proxy.

Session management mechanism: A mechanism for creating stateful sessions when using the HTTP protocol.

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

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

6.2 Requirements and principles

The authentication proxy may reside between the UE and the NAF as depicted in figure 2. The usefulness of an Authentication Proxy may be to reduce the consumption of authentication vectors and/or to minimize SQN synchronization failures. Also the AP relieves the AS of security tasks.

The following requirements apply for the use of an Authentication Proxy:

- authentication proxy shall be able to authenticate the UE using the means of Generic Bootstrapping Architecture, as specified in TS 33.220 [3];
- if the application server requires an authenticated identity of the UE the authentication proxy shall send it to the application server belonging to the trust domain with every HTTP request;
- if required, the authentication proxy may not reveal the authenticated identity of the UE to the application server not belonging to the trust domain;
- the authenticated identity management mechanism shall not prevent the application server to use an appropriate session management mechanisms with the client;
- the UE shall be able to create multiple parallel HTTP sessions via the authentication proxy towards different application servers;

NOTE 1: The used session management mechanism is out of the scope of 3GPP specifications.

- implementation of check of asserted user identity in the AS is optional;
- activation of transfer of asserted user identity shall be configurable in the AP on a per AS basis.

The use of an authentication proxy should be such that there is no need to manage the authentication proxy configuration in the UE.

NOTE 2: This requirement implies that the authentication proxy should be a reverse proxy in the following sense: A reverse proxy is a web server system that is capable of serving web pages sourced from other web servers - in addition to web pages on disk or generated dynamically by CGI - making these pages look like they originated at the reverse proxy.

~~Editors' note: The above requirement may be revisited after the following issues are fully studied:~~

~~feasibility of shared key TLS~~

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

3GPP TSG-SA WG3 Meeting #34
Acapulco, Mexico, 6 - 9 July 2004

Tdoc ⌘S3-040658

CR-Form-v7

CHANGE REQUEST

⌘ **33.222** **CR** **004** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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:	⌘	Further modifications to TLS profile related text in 33.222
Source:	⌘	SA WG3
Work item code:	⌘	SEC1-SC
Date:	⌘	09/06/2004
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:	⌘	SA3 has been aligning 33.141 and 33.222 on TLS profile related text. 33.141 has still some TLS related text that fits better to the scope of 33.222.
Summary of change:	⌘	Adding new clauses: - 5.3.1.3 Authentication of the AP/AS - 5.3.1.4 Authentication Failures - 5.3.1.5 Set-up of Security parameters - 5.3.1.6 Error cases Updating the references section Minor editorial in 5.3
Consequences if not approved:	⌘	Lack of clarity and concistency in the specifications

Clauses affected:	⌘	2, 5.3, 5.3.1

	Y	N			
Other specs affected:	X		Other core specifications	⌘	33.141
		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) – 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)", February 6, 2004, URL: http://www.ietf.org/internet-drafts/draft-eronen-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 ****

5.3 Shared key-based UE authentication with certificate-based NAF authentication

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

This section explains how the procedures specified in TS 33.220 [3] have to be enhanced when HTTPS is used between a UE and a NAF. The following gives the complementary description with respect to the procedure specified in clause 4.5.3 of TS 33.220 [3]. This document specifies the logical information carried in some header fields. The exact definition of header fields is left to stage 3 specifications.

1) When the UE starts communication via Ua reference point with the NAF, it shall establish a TLS tunnel with the NAF. The NAF is authenticated to the UE by means of a public key certificate. The UE shall verify that the server certificate corresponds to the FQDN of the NAF it established the tunnel with. No client authentication is performed as part of TLS (no client certificate necessary).

2) In response to the HTTPS (HTTP over TLS) request received from UE over the Ua reference point, the NAF shall invoke HTTP digest as specified in RFC 2617 [10] with the UE in order to perform client authentication using the shared key as specified in section 4.5.3 of TS 33.220 [3]. The realm attribute of the WWW-Authenticate header field shall contain the constant string "3GPP-bootstrapping" and the FQDN of the NAF, to indicate the GBA as the required authentication method.

3) On receipt of the response from the NAF, the UE shall verify that the FQDN in the realm attribute corresponds to the FQDN of the NAF it established the TLS connection with. On failure the UE shall terminate the TLS connection with the NAF.

4) In the following request to NAF the UE sends a response with an Authorization header field where Digest is inserted using the B-TID as username and the session key Ks_NAF as password.

5) On receipt of this request the NAF shall verify the value of the password attribute by means of the Ks_NAF retrieved from BSF over Zn using the B-TID received as user name attribute in the query.

6) After the completion of step 5), UE and NAF are mutually authenticated as the TLS tunnel endpoints.

NOTE: RFC 2617 [10] mandates in section 3.3 that all further HTTP requests to the same realm must contain the Authorization request header field, otherwise the server has to send a new "401 Unauthorized" with a new WWW-Authenticate header. In principle it is not necessary to send an Authorization header in each new HTTP request for security reasons as long as the TLS tunnel exists, but this would not conform to RFC 2617 [10].

In addition, there may be problems with the lifetime of a TLS session, as the TLS session may time-out at unpredictable (at least for the UE) times, so any request sent by UE can be the first request inside a newly established TLS tunnel requiring the NAF to re-check user credentials.

It shall be possible for the AP/AS to request a re-authentication of an active UE, see TS 33.220 [11], clause 4.5.3.

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

***** 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. 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.

Editors 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.

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

5.3.1.2 Key Agreement

The Key exchange method shall not be anonymous. Hence the following cipher suites as defined in RFC 2246 [6] are not allowed for protection of a session:

- CipherSuite TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
- CipherSuite TLS_DH_anon_WITH_RC4_128_MD5
- CipherSuite TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
- CipherSuite TLS_DH_anon_WITH_DES_CBC_SHA
- CipherSuite TLS_DH_anon_WITH_3DES_EDE_CBC_SHA

5.3.1.3 Authentication of the AP/AS

The AP/AS is authenticated by the Client as specified in WAP-219-TLS [14], which in turn is based on RFC 2246 [6].

The AP/AS certificate profile shall be based on WAP Certificate and CRL Profile as defined in WAP 211 WAPCert [17].

5.3.1.4 Authentication Failures

If the UE receives a Server Hello Message from the AP/AS that requests a Certificate then the UE shall respond with a Certificate Message containing no Certificate if it does not have a certificate. The AP/AS upon receiving this message may respond with a failure alert, however if the AP/AS shall authenticate the UE as configured by the policy of the operator the AP/AS should continue the dialogue and assume that the UE will be authenticated as specified in TS 33.220 [11].

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.

5.3.1.5 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 maximum 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.

5.3.1.6 Error cases

The AP/AS shall consider the following cases as a fatal error:

- if the received ciphersuites only includes all or some of the Ciphersuites in Clause 5.3.1.2;

- if the received ciphersuites do not include any integrity protection;

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