3GPP TSG-SA3 Meeting #32
Edinburgh, Scotland, UK, 9-13 February 2004

Tdoc ⌘S3-040067

CR-Form-v7

CHANGE REQUEST

⌘ **33.222 CR CRNum** ⌘**rev** **-** ⌘ Current version: **0.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network □

Title:	⌘	Updates to draft HTTPS TS
Source:	⌘	Ericsson
Work item code:	⌘	GAA and support for subscriber certificates
Date:	⌘	02/02/2004
Category:	⌘	**B**
Release:	⌘	

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:	⌘	Progress draft HTTPS TS
Summary of change:	⌘	- Adding Introduction, scope, definitions, abbreviations - Updating references - Adding new chapter for describing overall security architecture - Adding new sub-chapters for requirements on the UE and the network in 4.1 - Adding editor's notes on open issues - Some editorial changes
Consequences if not approved:	⌘	

Clauses affected:	⌘	Introduction, 1, 2, 3, 4.1, 4.2, 5.1				
		Y	**N**			
Other specs affected:	⌘	□	□	Other core specifications	⌘	
		□	□	Test specifications		
		□	□	O&M Specifications		
Other comments:	⌘					

.

*** BEGIN SET OF CHANGES ***

Introduction

A number of services might be accessed over HTTP. For the Presence Service, it shall be possible to manage the data on the Presence Server over the Ut interface, which is based on HTTP. Services like conferencing, messages and push might be accessed using HTTP.

Access to services over HTTP can be done in a secure manner. The present document describes how the access over HTTP can be secured using TLS.

~~*This clause is optional. If it exists, it is always the second unnumbered clause.*~~

1 Scope

~~*This clause shall start on a new page.*~~

The present document ~~…~~specifies secure access methods to Network Application Functions (NAF) using HTTP over TLS, and provides Stage 2 security requirements and principles 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).

Editor's note: The present document provides a general description of HTTP over TLS for any service that require secure access over HTTP. For release 6, the Presence TS describes more specifically how access to the Presence server is secured. It is FFS if TLS 1.1 and TLS extension should be specified for use in this document.

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*.

~~[<seq>] <doctype> <#>[([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".~~

[1] 3GPP TR 41.001: "GSM Release specifications".

[2] 3GPP TR 21 912 (V3.1.0): "Example 2, using fixed text".

[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 2617 (1999): "HTTP Authentication: Basic and Digest Access Authentication"

[10] IETF RFC 3310 (2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)"

3 Definitions, symbols and abbreviations

~~*Delete from the above heading those words which are not applicable.*~~

~~Subclause numbering depends on applicability and should be renumbered accordingly.~~

3.1 Definitions

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] 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.

NAF: a Network Application Function is either an Authentication Proxy (AP) or an Application Server (AS) in the context of the present document.

~~Definition format~~

~~***<defined term>***~~*~~: <definition>.~~*

~~**example:** text used to clarify abstract rules by applying them literally.~~

~~3.2 Symbols~~

~~For the purposes of the present document, the following symbols apply:~~

~~Symbol format~~

~~<symbol> <Explanation>~~

3.2~~3~~ Abbreviations

For the purposes of the present document, the following abbreviations apply:

~~Abbreviation format~~

<ACRONYM>	<Explanation>
AP	Authentication Proxy
AS	Application Server
BSF	Bootstrapping Server Functionality
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over TLS
NAF	Operator-controlled network application function functionality
TLS	Transport Layer Security
UE	User Equipment

4 Overview of the Security Architecture

Editor's note: A picture explaining the overall architecture and text supporting the picture should be added.

5 Authentication Schemes

~~4.1~~5.1 Requirements and principles

This document is based on the architecture specified in [TS33.220]. All notions not explained here can be found in [TS33.220].

5.1.1 Requirements on the UE

Editor's note: requirements on the UE are FFS

5.1.2 Requirements on the Network

Editor's note: care must be taken that this specification is in line with TS 33.141 on presence security. ~~SA3 has yet to decide the split between the two documents.~~

~~4.2~~5.2 Shared key-based UE authentication with certificate-based NAF authentication

This section explains how the procedures specified in [TS33.220] have to be enhanced when HTTPS is used between a UE and a NAF. The only enhancement required is the need to specify how the set up of a TLS tunnel is included in the general procedures specified in [TS33.220].

Editor's note: The sequence of events needs to be updated to reflect the initiation of bootstrapping as described in TS 33.220, section 4.3.1.

When the UE accesses a NAF, with which it does not yet share a key, then the sequence of events is as follows:

1. the UE runs http digest aka [rfc3310] with the BSF over the Ub interface.

2. If the BSF has no authentication vectors for the UE it fetches authentication vectors from the HSS over the Zh interface.

After the completion of step 1), the UE and the BSF share a secret key. This shared key is identified by a transaction identifier supplied by the BSF to the UE over the Ub interface key, cf. [TS 33.220, section 4.3.1].

3. The UE establishes a TLS tunnel with the NAF. The NAF is authenticated to the UE by means of a public key certificate.

Editor's note: TLS needs to be profiled in an appropriate section of this specification.

4. The UE sends an http request to the NAF.

5. The NAF invokes http digest [rfc 2617] with the UE over the Ua interface in order to perform client authentication using the shared key agreed in step 1), as specified in [TS 33.220, Annex A].

Editor's note: bullet 5 references Annex A in TS 33.220, which is informative.

6. While executing step 5), the NAF fetches the shared key from the BSF over the Zn interface, as specified in [TS 33.220, Annex A and section 4.3.2].

6)After the completion of step 4), UE and NAF are mutually authenticated as the TLS tunnel endpoints.

The UE may now run an appropriate application protocol with the NAF through the authenticated tunnel.

When the UE accesses a NAF, with which it already shares a key, steps 1), 2), 5) and 6) may be omitted, as specified in [TS 33.220].

Editor's note: the above procedure is generally applicable and conforms to [TS 33.220]. For the case of a co-located BSF and NAF an optimisation is possible which is currently located in the informative Annex Z. SA3 still needs to decide whether the material in the annex should be moved to the main body, or remain in an informative or normative annex, or be deleted.

~~4.3~~5.3 Shared key-based mutual authentication between UE and NAF

~~4.4~~5.4 Certificate based mutual authentication between UE and NAF

~~5~~6 Use of authentication proxy

~~5.1~~6.1 Requirements and principles

The authentication proxy may reside between the UE and the NAF as depicted in Figure y [tba to section 5.2]. The usefulness of an Authentication Proxy may be to reduce the consumption of authentication vectors and/or to minimize SQN synchronization failures.

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 [Ts33.220].
- Authentication proxy shall send the authenticated identity of the UE to the application server belonging to the trust domain at the beginning of new HTTP session.
- If required, the ~~A~~authentication proxy may not reveal the authenticated identity of the UE to the application server not belonging to the trust domain ~~if required.~~
- 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.

NOTE1: 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 base.

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

NOTE2: 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 requirements may be revisited after the following issues are fully studied:

- feasibility of shared-key TLS;
- terminal configurability]

~~5.2~~6.2 Authentication proxy architecture

<include figure y here>

The use of an authentication proxy (AP) is fully compatible with the architecture specified in [TS33.220] and in section 4 of this specification. When an AP is used in this architecture, the AP takes the role of a NAF. When an https request is destined towards an application server behind an authentication proxy (AP), the AP terminates the TLS tunnel and performs UE authentication. The AP proxies the http request to the application server.

Annex A contains further guidance on technical solutions for authentication proxies.

~~5.3~~ 6.3 Interfaces

~~5.4~~ 6.4 Management of UE identity

*** END SET OF CHANGES ***