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

Tdoc ⌘S3-040660

CR-Form-v7

CHANGE REQUEST

⌘ **33.222** **CR** **CRNum** ⌘ **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:	⌘	Ericsson, Nokia, Siemens
Work item code:	⌘	GBA-SSC
Date:	⌘	07/07/2004
Category:	⌘	**D**
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:	⌘	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 ****