3GPP TSG SA WG3 Security#33 **S3-040322**
10 – 14 May, 2004
Beijing, China

Agenda Item: **6.9.4 (GAA/HTTPS)**

Source: **Nokia, Siemens**

Title: **General Requirements and Principles for Access to NAF using HTTPS – Pseudo-CR**

Document for: **Discussion and decision**

Abstract

In the current version of the Access to NAF using HTTPS specification (TS 33.222 v100), the sections on overview and general requirements and principles are still empty. A proposal for adequate text is given.

1. Reason for proposed change to TS 33.222 v100

The sections of more general content need an overhaul. This applies to the following sections:

- *1. Scope:* Editor's note may be removed.
  The first statement of the editor's note is converted to a note, stating that this document is an umbrella specification for all HTTPS based use of Ua, and that application specific details are handled in separate documents, e.g. TS 33.141 for Presence.
  The second statement of the editor's note is removed completely, as TLS 1.1 is not expected to be stable and decided until freezing of Rel. 6.

- *4. Overview of the security architecture.* The editor's note was replaced by a cross-reference to TS 33.220, as the architecture is the same, and a link to section 6 concerning the details of AP solution (cf. the changes to that section given below).

- *5.2 General Requirements and Principles*. This section was missing text. Besides some minor editorial changes text for requirements on UE and Network elements (NAF, BSF) was added.
  The editor's note in section 5.2.1 could therefore be removed.
  The editor's note in section 5.2.2 could be removed as the relation to Presence document is cared about by the note in section 1 (cf. the text given above).

- 6. *Use of Authentication Proxy* (and subsections 6.1 through 6.3): Section 6 was missing a general introduction to the principle of authentication proxy.
  Sections 6.1 and 6.3 have a somewhat overlapping content. Therefore it is proposed to merge these sections in new section 6.1 and to remove section 6.3 completely. New text was added to section 6.1.
  In section 6.2 only minor changes for clarification were made.
  Please note: In the pseudo-CR below the text only moved from 6.3 to 6.1 is not highlighted with revision marks at the destination to show the editorial changes made to this text. At the source (place of deletion) the removed text is highlighted as deleted.

The next section contains a pseudo-CR to TS 33.222 v100, implementing the changes proposed in this section.

2. Pseudo-CR

********** begin change **********

1 Scope

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 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 requires 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 should be specified for use in this document.~~

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 change **********

********** begin change **********

4 Overview of the Security Architecture

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

The overall security architecture conforms to the architecture defined in TS 33.220 [3]. Details of the solution with authentication proxy are given in section 6.

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

********** begin change **********

5.2 General Requirements and Principles

This document is based on the architecture specified in TS 33.220 [3]. All notions not explained here can be found in TS 33.220 [3].

~~5.1.1~~5.2.1 Requirements on the UE

To utilise GBA as described in this document the UE shall be equipped with a HTTPS capable client (e.g. browser) implementing the particular features of GBA as specified in TS 33.220 [3].

~~Editor's note: requirements on the UE are FFS~~

5.~~1~~2.2 Requirements on the ~~Network~~NAF and BSF

To utilise GBA as described in this document the NAF and BSF shall support the features of GBA as specified in TS 33.220 [3].

Additionally in the scope of this specification, HTTP and TLS shall be supported by the NAF for UE-NAF interface (Ua).

~~Editor's note: care must be taken that this specification is in line with TS 33.141 on presence security.~~

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

********** begin change **********

6 Use of Authentication Proxy

An Authentication Proxy (AP) is an HTTP proxy which takes the role of a NAF for the UE. It handles the TLS security relation with the UE and relieves the application server (AS) of this task. Based on GBA the AP can assure the ASs that the request is coming from an authorized subscriber of the MNO.

6.1 Architectural view

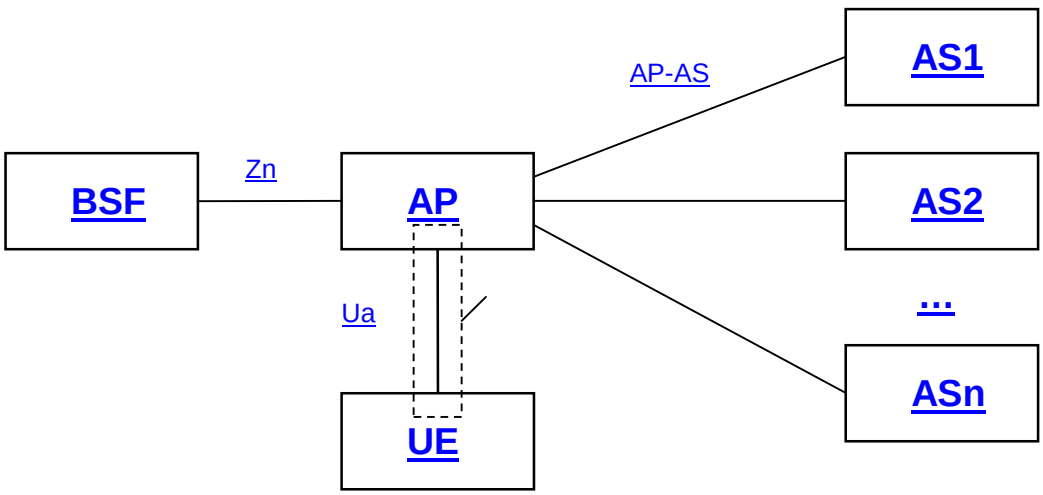

Figure 2: Environment and Interfaces of AP

The use of an authentication proxy (AP) is fully compatible with the architecture specified in TS 33.220 [3] and in section ~~4~~ 5 of this specification. ~~-~~When an AP is used in this architecture, the AP takes the role of a NAF. When an ~~https~~ HTTPS request is destined towards an application server (AS) behind an ~~authentication proxy (~~AP~~)~~, the AP terminates the TLS tunnel and performs UE authentication. The AP proxies the ~~http~~ HTTP requests received from UE to one or many~~the~~ application servers. The AP may add an assertion of identity of the subscriber for use by AS, when the AP forwards the request from the UE to the AS.

Figure ~~2~~ 3 presents an architectural view of using Authentication Proxy, for example, for IMS SIP based services. The UE shall manipulate own data such as groups, through the Ua/Ut interface. The interface Ut specified in TS 23.002 [1] shall be applicable to data manipulation of IMS based SIP services, such as Presence, Messaging and Conferencing services. The stage 1 requirements are specified in TS 22.250 [2].

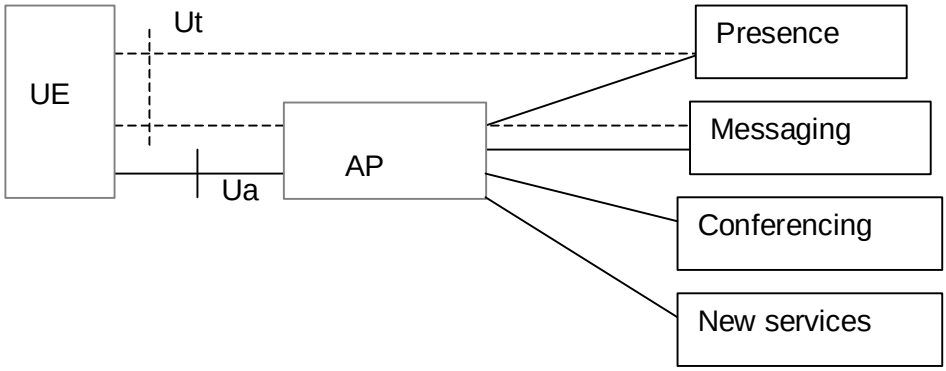

Figure ~~2~~3: The architectural view using Authentication Proxy for IMS SIP based services

Management of UE identities is described in clause 6.5.

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

6.2 Requirements and principles

The authentication proxy may reside between the UE and the NAF as depicted in Figure ~~y [tba to section 5.2~~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 a~~A~~uthentication proxy shall send ~~the~~it ~~authenticated identity of the UE~~ to the application server belonging to the trust domain with every HTTP request~~at the beginning of new HTTP session~~.
- 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.

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~~basis.

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 requirement~~s~~ may be revisited after the following issues are fully studied:

- feasibility of shared-key TLS~~;~~.

~~terminal configurability]~~

~~6.3 Authentication proxy architecture~~

~~<include figure y here>~~

~~The use of an authentication proxy (AP) is fully compatible with the architecture specified in [3] 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.~~

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