3GPP TSG SA WG3 Security — S3#32 **S3-040070**
09 - 13 February 2004
Edinburgh, Scotland, UK

Title	**Psecudo-CR to TS 33.222 (HTTPS)**
Source:	**Nokia**
Document for:	**Approval**

Introduction

This contribution provides changes to the draft TS 33.222: Access to Network Application Functions using HTTPS. The changes are

- Add a specific section title for network reference model;
- Include the Ua/Ut interface requirement of supporting several IMS based SIP services, other than Presence that are part of REL-6, according to TS 22.250;
- Include the architecture view of using Authentication Proxy with IMS based SIP services.

Justifications

1. Stage 1 of Group managements (TS 22.250) for Presence, Chat/Conferencing and Mesaging were completed; stage 2 in SA2 has been done in TS 23.228; stage 3 is also progressing well (Conferencing TR 29.847 and TS 24.147, Messaging TS24.247). SA3 needs to investigate the solution for these services;
2. XCAP protocol in IETF is good progress. It specifies a way to refer to a service and the specific group in an unique format. For example,

https://example.com/XCAP/user_public1/APP_usage/presence_watcher_list.xml

3. TS 22.250 requires that the IMS group management is a generic capability that can be utilised together with several different services, such as Presence, Chat/Conferencing and Mesaging.
4. TS 23.228 section 4.10.1, specifies that “The capabilities required for IMS group management are defined in clause 5.4 of TS 22.250 [32]. The Ut reference point is used to manage groups from the UE.” And it also specifies that group lists can be accessed by different application servers. Those application servers sharing the data shall understand the data format. This enables sharing of common information between application servers, e.g. data managed via the Ut reference point. The statement suggests that the rational of data manipulation is the same for all SIP based services. It is carried over HTTP with different XML definition for each service, but the requirements of security are universal. Therefore it is a natural choice for SA3 to re-use the security solution for Presence over Ua/Ut interface, to other SIP based services, such as Messaging and Conferencing.

Below are the real changes:

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".

[x] 3GPP TS 22.250: “IP Multimedia Subsystem (IMS) group management”; Stage 1”.

--- NEXT CHANGE ---

4 ~~4~~ Authentication Schemes

4.1 Reference model:

Figure 1 shows a network model of the entities that utilize the bootstrapped secrets, and the interfaces used between them.

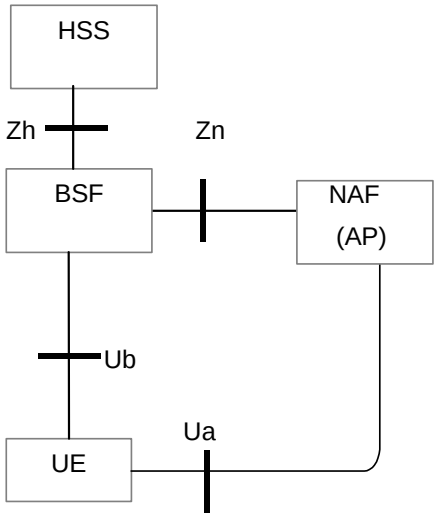

Figure 1: Simple network model for NAF using a bootstrapping service

~~4.2 Network entities~~

4.2 General 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].

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~~4.3 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].

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), 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~~4 Shared key-based mutual authentication between UE and NAF

4.~~4~~5 Certificate based mutual authentication between UE and NAF

5 ~~5~~ Use of ~~authentication~~ Authentication ~~p~~Proxy

5.1 Architectural view

Figure x presents an architectural view of using Authentication Proxy for IMS SIP based services. The UE shall manipulate own data such as groups, through the Ua/Ut interface. The interface name Ut is specific for Presence service, and ~~-~~the security solution specified in present specification shall be applicable to data manipulation of other IMS based SIP services, such as Presence service (Ut interface), Messaging and Conferencing services. The stage 1 requirements are specfied in [x].

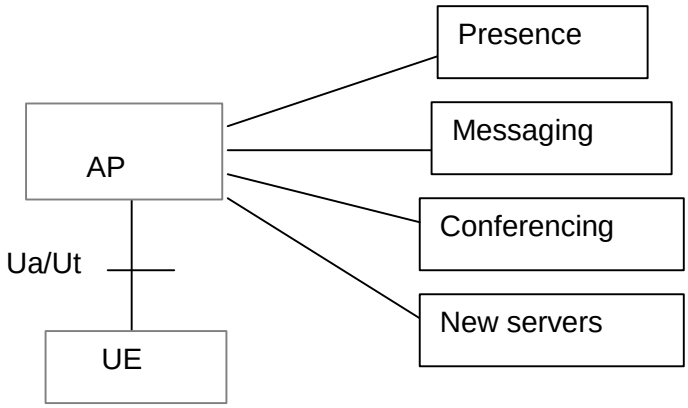

Figure x: The architectural view using Authentication Proxy for IMS SIP based services

~~5.1~~5.2 Requirements and principles

The authentication proxy may reside between the UE and the NAF as depicted in Figure y [tba to section 5.2]. 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.
- 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]