**3GPP TSG SA WG3 Security#33** **S3-040320**
**10 – 14 May, 2004**
**Beijing, China**

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

**Source:** **Nokia, Siemens**

**Title:** **New text for section 5.3 "Shared key-based UE authentication with certificate-based NAF authentication "of TS 33.222 – 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 section 5.3 on "Shared key-based UE authentication with certificate-based NAF authentication" is not clear enough and partly outdated. This proposal gives new text for this section.*

# 1. Reason for proposed change to TS 33.222 v100

The existing text for this section is mostly copied from TS 33.220 with some enhancements specific to this specification. Additionally it referenced the informative annex A of TS 33.220, which is not allowed for a normative section.

In the new text duplications of the normative text of TS 33.220 were removed as much as possible. Some text from annex A of TS 33.220 was taken to this section, as that annex dealt in particular with HTTP. Some clarifications which evolved during the progress of standardisation in SA3 were included.

(Note: The editor's note referring to profiling of TLS is left in this text, but it is cared for in an accompanying Tdoc with pseudo-CR. Note also that another Pseudo-CR to this meeting proposed to remove Annex A of TS 33.220.)

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

# 2. Pseudo-CR

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

## 3.2 Abbreviations

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

| | |
|---|---|
| AP | Authentication Proxy |
| AS | Application Server |
| BSF | Bootstrapping Server Functionality |
| FQDN | Fully Qualified Domain Name |
| 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

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

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

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

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 ~~only enhancement required is the need to specify how the set up of a TLS tunnel is included in the general procedures specified in [3].~~ 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.

~~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 [11] 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. [3, section 4.3.1].~~

~~3~~1. When the UE starts communication via Ua interface with the NAF, it shall ~~The UE~~ establish~~es~~ 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).

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~~2. In response to the HTTPS (HTTP over TLS) request received from UE over the Ua interface, t~~T~~he NAF shall invoke~~s~~ ~~http~~ HTTP digest as specified in RFC 2617 [10] with the UE ~~over the Ua interface~~ in order to perform client authentication using the shared key ~~agreed in step 1),~~ as specified in section 4.5.3 of TS 33.220 [3~~, Annex A~~]. 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.

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

3 On receipt of the response from 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 an response with 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. While executing step 5), the NAF fetches the shared key from the BSF over the Zn interface, as specified in [3, Annex A and section 4.3.2].~~

~~7~~6. After the completion of step ~~4~~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. 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.

~~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 [3].~~

~~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.~~

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