3GPP TSG SA WG3 Security#33 **S3-040325**
10 – 14 May, 2004
Beijing, China

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

Source: **Siemens**

Title: **Definition of Authentication Mechanisms in 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), there are three authentication mechanisms between UE and NAF mentioned. One of them is nearly completed in specification, while the other two only exist as headlines. A new structuring for this section is proposed together with the removal of the mechanisms unspecified until now.

1. Reason for proposed change to TS 33.222 v100

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

1.1 Restructuring of section 5

The structuring of section 5 "Authentication Schemes" is not satisfactory at the moment. Sub-sections 5.1 and 5.2 are reasonable, but the existing sub-sections 5.3 through 5.5 are a list of possible mechanisms, which should be collected in one section. It is proposed to replace the sub-sections 5.3 through 5.5 by one sub-section 5.3 "Authentication Mechanisms between UE and NAF". Each single mechanism is described in its own sub-clause, i.e. 5.3.1, 5.3.2, etc.

1.2 Selection of mechanisms to be standardised in Rel. 6

Up to now only the authentication mechanism "Shared key-based UE authentication with certificate-based NAF authentication" is elaborated and specified till near completion. The other two mechanisms are not yet specified except a placeholder header line. The proposal is to delete these placeholders for Rel. 6. The note introduced for the whole section explains, that further mechanisms may be specified in later releases. These may be introduced as sections 5.3.2 and following.

The following gives a more detailed reasoning for removal of the other mechanisms from Rel. 6:

It is proposed that, for Release 6, a workable solution is specified, which includes only the minimum required to secure Release 6 services, such as presence. Complexity not strictly needed should be avoided, and corresponding options should be postponed to Release 7. Only certificate-based server authentication is widely established in the web today, while shared-key TLS and certificate-based client authentication in TLS are non-existent or rare.

- *Shared key-based mutual authentication between UE and NAF:* The IETF drafts this mechanism builds on are not yet stable and finalised within IETF. It is doubtful if these drafts will become standards within Rel. 6 time frame.

- *Certificate based mutual authentication between UE and NAF:* Current http servers show intermittent failures with certain types of requests when client certificates are used. Furthermore, it is difficult to see that a PKI required for client certificates can be built before Release 7 specifications become available.

2. Pseudo-CR

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

5.3 Authentication Mechanisms between UE and NAF

NOTE: For Release 6 only one authentication mechanism is standardised. Further authentication mechanisms (e.g. shared key- based TLS or TLS with certificate based mutual authentication) may be added in later releases.

5.3.1 Shared key-based UE authentication with certificate-based NAF authentication

This section explains how the procedures specified in [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].

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. 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 [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 [3, 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 [3, Annex A and section 4.3.2].

7. 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 [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.

~~5.4 Shared key-based mutual authentication between UE and NAF~~

~~5.5 Certificate based mutual authentication between UE and NAF~~

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