Source: **Nokia**

Title: **GAA-Application-Profiles definition**

Document for: **Discussion**

Agenda Item: **7.9 GAA and Support for subscriber certificates**

---

1. INTRODUCTION

This contribution gives a description how requirements in SA3 TS [S3-030488] chapter A.2.4 (home operator control) could be implemented.

Some GAA applications (e.g., Subscriber Certificate) need user specific profile information to be stored in HSS. This GAA application profile information is downloaded from HSS to BSF during bootstrapping procedure (over C/Zh interface), and the GAA application specific part of the profile information is downloaded from BSF to NAF during GAA application usage (over D/Zn interface). SA3 needs to define this HSS profile content at least in minimum level. Currently, a definition is needed for GAA Subscriber Certificate Application for updating the 3GPP subscriber data specifications [TS 23.008], and for continuing the specification of the stage 3 specification work for C/Zh and D/Zn interfaces.

2. STRUCTURE OF GAA-PROFILES

User's GAA profile information element is called **GAA-Application-Profiles**. Inside the GAA-Application-Profiles is an information element for each GAA application that is defined for the user. All GAA applications may not need profile information. The profile of the Subscriber Certificate (SSC) application is called **SSC-Profile**. The following picture gives an outline of the UML model of user's GAA-profiles:

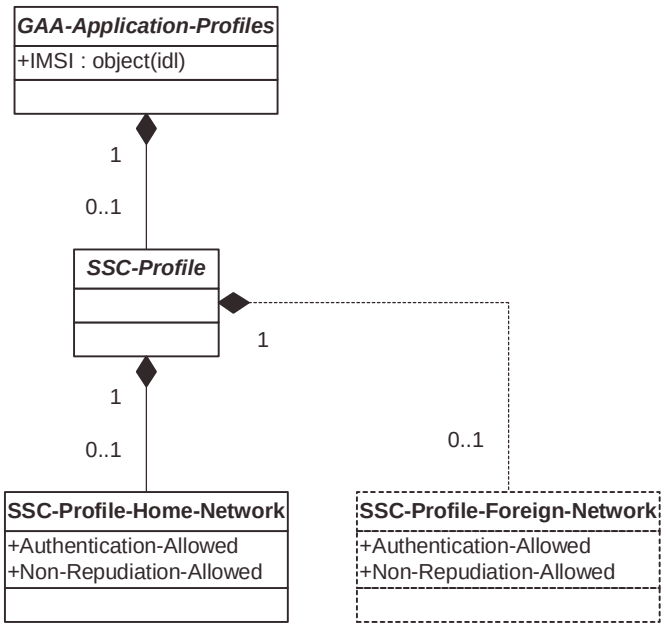

Figure 1: The structure of the GAA application profiles

The SSC Profile definition for home network is called **SSC-Profile-Home-Network**, and for foreign network **SSC-Profile-Foreign-Network**. Since it may be possible in later releases, that the PKI Portal (NAF) is located in non-home network, it is reasonable to define own profiles for both home and foreign network cases. However, only support for home network PKI Portal (NAF) is required in release 6.

The following pseudo-code outlines the same hierarchy than the previous UML class diagram:

```
GAA-Application-Profiles
    SSC-Profile
        SSC-Profile-Home-Network
            Authentication-Allowed
            Non-Repudiation-Allowed
```

2.1 Subscriber Certificate profile

At least the following items are needed for the home operator to control the issuance of the subscriber certificate. The PKI Portal (NAF) shall make the certificate issuing decision based on this information.

2.1.1 Authentication-Allowed

Using the “Authentication-Allowed” control item the home operator can allow or deny the issuance of subscribe certificate for “Authentication” purposes (see keyUsage and extKeyUsage parameters in [WAPprof]) to the cellular subscriber.

2.1.2 Non-Repudiation-Allowed

Using the “Non-Reputation-Allowed” control item the home operator can allow or deny the issuance subscribe certificate for “Non-Reputation” purposes (see keyUsage parameter in [WAPprof]) to the cellular subscriber.

3. CONCLUSION

This contribution presented further information about requirements in the chapter A.2.4 of TS SSC [S3-030488]. We recommend to send this contribution to CN4 as an LS to guide CN4 on their stage 3 specification work for the C/Zh and D/Zn interfaces.

4. REFERENCES

[TS 23.008] 3GPP TS 23.008: “Organization of subscriber data”;

[WAPprof] WAP Forum, “WAP Certificate and CRL Profiles”, WAP-211-WAPCert, May 2001.

[S3-030488] Draft 3GPP TS 33.109 v0.3.0 “Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description (Release 6)”.