3GPP TSG SA WG3 Security — SA3#34
6-9 July, 2004
Acapulco, Mexico

S3-040591
revised S3-040517

Source: Nokia, Gemplus, Alcatel, Motorola

Title: ISIM usage in GAA

Agenda item: GBA

Document for: Discussion/Approval

1 Introduction

In the last SA3 meeting, S3-040340 [1] introduced the necessary changes to TS 33.220 [2] in order to support ~~all~~ smart card cases to access GBA, including USIM and distinct ISIM. It was agreed that further discussion is needed regarding the procedures and the handling of the identities in GBA when both a USIM and an ISIM are present (as distinct applications in a UICC). This contribution clarifies these issues.

The handling of identities regarding both USIM and distinct ISIM in GAA presents two issues that needs to be clarified:

- selection of which identity should be used with GAA: USIM or distinct ISIM, and
- mapping of GAA profile data[1] and subscriber's identity (i.e., IMPI)distinct in HSS.

These issues are discussed in the following chapter.

2 Discussion

2.1 Selection in UE

Figure 1 depicts the relation~~-~~ships between different components in the UE. The GBA application together with a USIM application or a distinct ISIM application on the UICC handle the bootstrapping procedure and the key derivation. The SSC client handles the subscriber certificate enrolment~~,~~ and the presence client handles the presence list admin procedures. The UE may contains other client applications (NAF client) that use GBA, for example, a web browser.

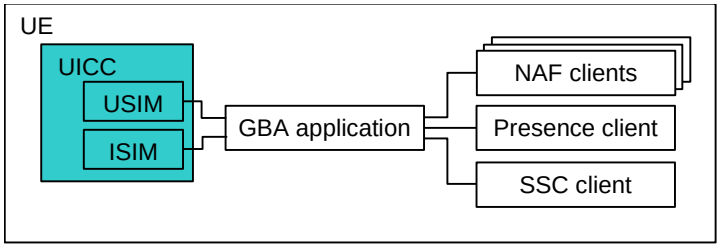

Figure 1. UE equipped with both USIM and distinct ISIM.

The selection problem is for the ME. ~~The~~ There are possible solutions for selecting the identity to be used.~~include that t~~the specification ~~itself w~~should clearly state the logic for selecting an identity.

1. It could be a static selection logic in the GBA application in the ME, for example: "a distinct ISIM application is selected if it is present in the UICC, otherwise a USIM application is selected". This is similar as the rule for IMS, cf. TS 33.203, section 8.

If the selection logic is static as above, this causes GBA always to use the distinct ISIM application when it is present. However, there may be cases where a USIM application should be used regardless of the fact whether there is a distinct

[1] The name and the content of the GAA user settings data in the HSS are under discussion in SA3. The possibilities for the GAA user settings data content include a subscriber pseudonym and application specific user security settings (USS).

ISIM application present on the UICC. Hence, a dynamic decision logic may be needed. Two ways to do the selection dynamically can be identified:

2a. The GBA application in the ME could be configured to select either one of them. This configuration in the ME would be made for example by sending an OTA configuration message or the subscriber could set the preference.

2b. The applications using GBA (e.g., SSC client or Presence list client) in the ME could have a role in deciding which one should be used. For example, by default the distinct ISIM is used (as described in option 1), but if preferred the application can indicate which identity should be used. This could be a configuration option in the application.

The first option (2a) would just change the default behaviour, e.g., a USIM is always used, and thus does not introduce a real dynamic selection logic behaviour. The second option (2b) would introduce ~~a~~ dynamic selection logic. For example, the Presence list client in the ME could always use the default selection, i.e., the distinct ISIM application would be used if it present, otherwise a USIM application would be used. The SSC client could be configured to always use ~~always~~ the USIM application, i.e., when the subscriber certificate enrolment procedure is running, the SSC application would request bootstrapping data from the GBA client and indicate that the USIM application should be used.

It should be noted that allowing ~~to have~~ GBA with a USIM for some applications and GBA with an ISIM for others leads to a need to manage more than one (in this cases 2 and 3) different keys Ks (Ks_USIM and Ks_ISIM) in the BSF and the UE. These parallel bootstrapping sessions cause minor complexity in the UE but not in the BSF. In the UE, the bootstrapping session must be also addressable using the IMPI that was used to obtain them. When an application in the UE selects a particular IMPI to be used with GBA, the UE can discover whether a bootstrapping session for that IMPI already exists in the UE. The BSF will consider separate IMPIs as different subscribers and will function as before.

It should be also noted that a problem arises if distinct ISIM's IMPI and the generated IMPI format from USIM's IMSI are the same. In this case, both IMPIs are identical but corresponding authentication vectors would be different. This problems is valid only~~,~~ if the above scenario is possible and if the ME can select either a distinct ISIM or a USIM to be used with GBA. If the selection method is synchronized, there is no problem, e.g., by default the distinct ISIM is always selected if it is present. This problem can be avoided if one of the following actions is taken:

- only allow the default selection logic (option 1), i.e., no dynamic selection;
- let the UE signal to the BSF which one was used: USIM application or distinct ISIM application;
- avoid the possibility that IMPI generated from USIM coincides with IMPI from distinct ISIM.

Since clear requirements and use cases for having a dynamic selection method on the UE have not been identified, and in order to keep GBA simple and avoid complexity in the UE (as well as in the BSF and in the HSS), we propose that the selection method between an ISIM or a USIM application is static only in Release-6. If there is need for a dynamic selection method in later releases, it can be added to that release.

We propose that the identity selection logic is the following: "By default, an ISIM is used if it is present on the UICC, otherwise a USIM is used in GBA.", and that this selection logic is added to TS 33.220.

2.2 Mapping in HSS

The second problem is for the HSS. If the subscriber has several identities (i.e., a USIM and a distinct ISIM), the subscriber's GAA profile data entry in the HSS must be referable with the particular IMPI that is used over Ub and Zh interfaces. The solution for this would be to add the possibility that subscriber's GAA profile data entry is referable with multiple IMPIs instead of just one. When the operator provisions a new USIM and distinct ISIM applications, then the corresponding IMPI should also be added to the IMPI list of the subscriber's GAA profile data entry.

It should be noted that the mapping problem ,i.e., mapping of GAA profile data to a particular IMPI exists for GBA in general, and not just for this case.

We propose to add an requirement to TS 33.220 that it shall be possible to refer to subscriber's GAA profile data in the HSS using multiple identities.

2.3 Migration issues

Similar issues arise when an operator migrates from a USIM only solution to a USIM/ISIM solution, or to a USIM and a distinct ISIM solution. An identity selection method must be in place in the ME, and the HSS must be able to map the new IMPI to the GAA subscriber profile entry in the HSS. Whether the HSS contains one combined GAA subscriber profile entry for all IMPIs or multiple entries for IMPIs is decided by the operator. ~~Same~~Similar solutions apply here as in the previous section: a consistent method to select the identity in the UE must be possible~~,~~ and the HSS should be able to map the selected identity to the correct subscriber profile in the HSS.

3 Conclusion & proposals

If bootstrapping in GBA can also be done using a distinct ISIM, two issues must be addressed in TS 33.220:

- selection logic in the UE as to what identity to use: a USIM or a distinct ISIM, and
- the HSS must be able to map multiple identities (IMPIs) belonging to single subscriber to the subscriber's GAA profile data entry in the HSS.

Otherwise there are no problems foreseen when using a distinct ISIM instead of a USIM within GAA.

Thus, we propose to add the following to TS 33.220:

- the USIM/ISIM selection logic on the ME ~~to be~~is the following: By default, an ISIM shall be used in GBA if it is present on the UICC, otherwise a USIM shall be used in GBA.
- add a the requirement to TS 33.220 that it shall be possible to refer to subscriber's GAA profile data in the HSS using multiple identities.

References

[1] S3-040340: "Private identity for GBA procedure", S3#33, Nokia, Motorola, Gemplus, Alcatel.

[2] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

Annex A: USIM and distinct ISIM usage in GAA

The usage of either USIM or distinct ISIM has no other effects on different entities of GAA than described in the main body of this contribution. As can be seen from the list below, USIM and distinct ISIM can be used in GAA:

- IMPI is used as the username in HTTP Digest AKA. If USIM is used, IMPI is generated from IMSI according to TS 23.003 [3].
- HTTP Digest AKA is run between the UE and the BSF. Since the AKA procedure is the same for both USIM and ISIM, they both can be used over Ub reference point.
- In the Diameter request over Zh reference point, the subscriber is identified by the IMPI given by the UE over Ub reference point.
- The HSS generates the authentication vector for the subscriber identified by the IMPI.
- The BSF and the UE generate either the GBA_ME or the GBA_U key material as specified in TS 33.220 [2]. IMPI may be used in the key derivation.
- The NAF fetches the NAF specific key material from the BSF based on the B-TID.
- The UE and the NAF use the NAF specific key material to secure Ua reference point.