3GPP TSG SA WG3 Security — S3#34 **S3-040475**
6 - 9 July 2004
Acapulco, Mexico

Source: **AXALTO**

Title: **Alternative to Special Random or AMF indication for GBA_U:**

MAC indication

Document for: **Discussion and decision**

Agenda Item: **GBA**

1 INTRODUCTION

At SA3#33 the concept of GBA_U was introduced in TS 33.220 [TD S3-040413]. However, the usage of Special-RAND mechanism to identify GBA_U specific Authentication Vectors was not agreed and further proposals were expected in SA#34. (From comments on **TD S3-040216** in SA#33 draft meeting report: *Due to the comments received in discussion of related documents on the use of Special-RAND it was decided to allow until the next meeting for alternative proposals to be presented. This is intended to be finalised and agreed at the next SA WG3 meeting)*

This contribution proposes an alternative to the solution in **TD S3-040216** (which was based on Special-RAND indication) and to the proposal using AMF indication (which was also suggested during SA#33)

2 PROBLEM STATEMENT

The following section describes why a special indication for GBA_U authentication vectors is needed.

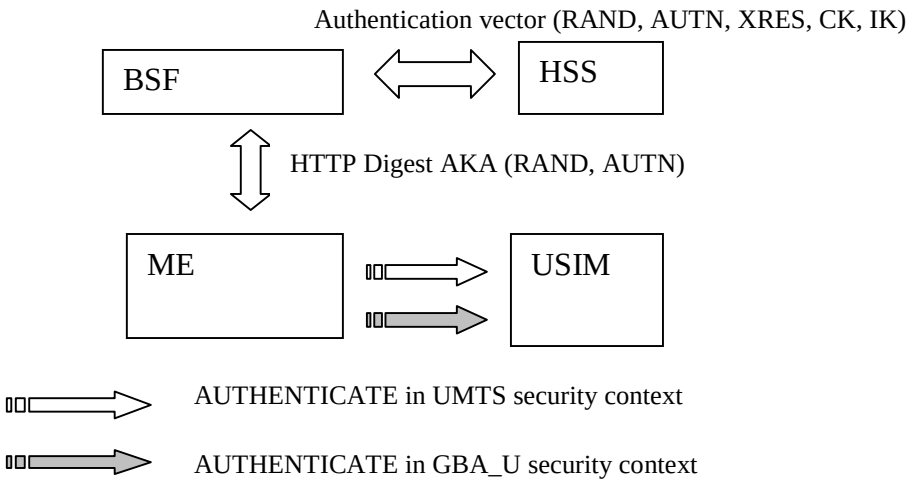
Authentication vectors to be used for GBA_U need to be invalid authentication vectors in UMTS security context. In other words, a ME receiving (RAND, AUTN) from a BSF wanting to perform a GBA_U procedure shall not be able to use this (RAND, AUTN) as a valid input argument for the USIM AUTHENTICATE command in UMTS security context. Then, an ME receiving GBA_U (RAND, AUTN) shall not be able to obtain CK/IK from them. In other words, the USIM shall recognize that this (RAND, AUTN) is for usage in GBA_U security context and shall never reveal CK/IK in that case.

The following requirements shall be respected:

1) The USIM shall recognize that a (RAND, AUTN) pair is for usage in GBA_U context.

2) The ME shall not be able to convert a GBA_U (RAND, AUTN) pair into a standard (RAND, AUTN) pair valid in UMTS security context.

A basic architecture, including a possible ME-UICC interface is depicted below. When a non GBA_U capable UICC is inserted, ME uses the AUTHENTICATE in UMTS security context. Otherwise the ME uses AUTHENTICATE in GBA_U context.



2.1 REQUIREMENTS & GOALS for designing a solution.

The following requirements shall be met when defining a satisfactory solution:

1- Fulfilment of the two specific requirements of GBA_U

2-No impact on AKA security (nor HTTP Digest AKA).

Additionally, the following desirable goals should be achieved:

3-Minimise impact in non-GBA entities. It seems suitable that GBA_U enhancements do not impact network entities outside those defined for GBA/GBA_U. In other words, impacts to HSS are considered as not suitable and should be minimised. A BSF should be able to perform either GBA or GBA_U without requiring AUC upgrades.

4-The solution should be properly standardised even if both USIM and BSF are in the Home Network domain to assure interoperability between different vendors.

2.2 Proposal: MAC* indication

When the BSF is bootstrapping secrets to a GBA-U aware UE, it may decide to use a GBA_U (RAND , AUTN) pair (e.g. on subscription basis).

-In this case, the BSF proceeds as follows:

1-Take a standard authentication vector (retrieved by existing procedures) from the HSS:

AV= RAND, AUTN (:= SQN ⊕ AK || AMF || MAC) , XRES, CK, IK

2-Modify the value of MAC in the following way:

MA C* = MAC ⊕ CK_1 (where CK= CK_1|| CK_2 as described in 33.102)

-When performing GBA_U bootstrapping, the ME then will perform AUTHENTICATE command in GBA_U security context using the modified (RAND, AUTN*= SQN ⊕ AK || AMF || MAC*) values.

-In this context, the order of the AKA function in the USIM is modified as follows:

1-The USIM first computes the cipher key CK = $f3_K$ (RAND)

2-The USIM retrieves MAC = MAC* ⊕ CK_1

3-The USIM continues AKA procedure as described in 33.102 (i.e anonymity key AK computation, MAC verification, SQN verification and RES/IK calculation)

4-The USIM will then produce specific GBA_U key derivation (i.e. Ks_int and Ks_ext) and send back RES as already described in TS 33.220.

-It is also possible (unless it is maybe non suitable regarding other considerations) that the same ME -UICC command may be able to carry both GBA_ME and GBA_U authentication challenges. In that case the USIM needs to proceed as follows:

The USIM tests if the received MAC is a correct MAC. If that is the case, standard AKA procedure for GBA_ME is run.

Else, the USIM will proceed as in the previous steps (1-4) for GBA_U run.

2.3 Security analysis: Fulfilment of security requirements

A malicious ME wanting to use this (RAND, AUTN*) in other context (i.e. and obtain CK/IK values) will fail, since the MAC verification will not succeed.

This GBA_U indication is protected by MAC. The ME will not be able to derive MAC from MAC* since it is not able to obtain CK_1. It assures a security of 64 bits for GBA_U indication.

Note: The method could be extensible to other applications in the future by choosing another MAC modification value (CK_1) (e.g. It could be possible to use CK_2, IK_1, IK_2 , (or any combination of them), for other security context in the future). In all cases, the main property of this indication is assured: The corresponding AV will not be valid in other, previous or future, different security context.

Additionally, there are no impacts in AKA security.

From the security perspective it assures all the requirements given in section 2.1.

2.4 BENEFITS

The following additional benefits of the solution are identified:

-Negotiation of GBA_U corresponds exclusively to the BSF. No impacts in HSS are needed for retrieving GBA_U AV. Operators shall not be required to upgrade existing HLR/AUCs before providing GBA_U security functions.

Note: GBA subscriber profile in the HSS will likely need to be taken into account in the HSS. This is not taken into account.

-No impacts in Zh interface is then required.

-The solution does not preclude any further signalling (AMF/ Special RAND) between HSS and USIM (e.g. for usage in GBA_U algorithm selection, sequence number management or other cases depicted in 33.102).

-In the USIM side, no modifications to existing UMTS security context is needed. GBA_U AV will not be valid authentication vectors except in GBA_U context.

From the deployment/migration perspective it assures all the requirements given in section 2.1.

2.5 COMPARISION with other indications

This section compares briefly MAC* indication with the other methods proposed in SA3#33 (i.e. Special RAND and AMF)

Both Special RAND and AMF provide also comfortable protection to GBA_U indication. However, both require specific modifications in AUC and HLR.

Additionally, up to now, the usage of these methods has never been standardised. For instance, 33.102 ANNEX F illustrates some usages of AMF indication (multiple authentication algorithms, SQN management,…). In some cases these mechanisms could have already been put in place. This could cause major problems since requiring a specific AMF indication for GBA_U may conflict with these existing procedures.

2.6 PROPOSAL

The following two bullets are proposed:

1) **It is proposed that SA3 agrees on the proposed solution for usage in GBA_U. An attached CR [S3-040476] is presented for approval.**

2) **Additionally, since the BSF enhancements needed for GBA_U support are minimum (MAC modification and h1 derivation function) and in order to minimise complicated deployment/migration/interoperation scenarios, it is proposed to adopt the following working assumption:**

    - **A Rel 6 BSF shall be able to perform both GBA/GBA_U bootstrapping. The choice on either GBA or GBA_U will be performed exclusively based in subscription information (i.e. USIM capabilities)**