3GPP TSG SA WG3 Security — SA3#37 **S3-050053**
February 21-25, 2005
Sophia Antipolis, France

Source: Nokia

Title: Introducing 2G GBA

Agenda item: 6.9.1 (GAA)

Document for: Discussion/Decision

1 Introduction

GBA is currently based on 3G USIMs and ISIMs, i.e., 3G GBA [1]. On the one hand, as is well known, the 3G Authentication and Key Agreement is more secure than the 2G SIM authentication. On the other hand, there are more than one billion people with SIMs in their phones and it will take long time to provision UICCs capable of 3G authentication to such a large population. In the meanwhile there should be a way to offer services whose authentication is based on GAA also to 2G subscribers. Essentially, this requires having an option to bootstrap based on SIM authentication in the Ub interface. However, if it is possible to choose between 2G and 3G authentication procedures between a particular UE and the BSF, then it should be ensured that the 3G authentication procedure is chosen, because it is more secure. Moreover, the support for 2G GBA should be completely under MNO control, i.e., the BSF would be configurable either allow or disallow 2G GBA. This document introduces the concept and needed changes to GAA related specifications. Also, it should be noted that the approach taken in this contribution is meant for existing SIMs, i.e., it does not cause any change needs to the existing SIM specifications, in particular GBA_U as in 3G will not be included in 2G GBA.

2 2G GBA

2.1 Differences between 3G and 2G GBA

Reference points: Several changes are needed on the GBA related reference points and they are listed below:

- **Zh reference point** (HSS - BSF): The Zh reference point needs to be able transfer 2G authentication vectors. No other changes are necessary.
- **Zn reference point** (BSF - NAF): The Zn reference point does not need to be changed. The length of the Ks_NAF can be the same as in 3G GBA as padding and/or hashing as needed can be used.
- **Ua reference point** (UE - NAF): The Ua reference point does not need to be changed.
- **Ub reference point** (UE - BSF): 2G GBA will potentially impact Ub and Zh reference points depending on how 2G issues are taken into account. The Ub reference point can be used two ways:

  a) HTTP Digest SIM would be used instead of HTTP Digest AKA, or

  b) HTTP Digest AKA is used with conversion functions, which adapt the SIM authentication parameters to those needed by HTTP Digest AKA

  But, since HTTP Digest SIM has not been specified in IETF, the conversion function approach is considered further. An advantage of using HTTP Digest AKA with conversion functions is that the Ub reference point does not need to be changed (or the change would be minimal).

2.2 Bootstrapping procedure

Several issues have to be solved in the bootstrapping procedure with 2G authentication vectors:

- what conversion functions to use with HTTP Digest AKA, and

- is there a need to authenticate the network, and if so how is it done.

As indicated in section 2.1, in 2G GBA the bootstrapping procedure should be based on HTTP Digest AKA and conversion functions. A set of possible conversion functions are described and discussed in Annex A.

If there is a need to authenticate the network, the bootstrapping procedure (i.e., HTTP Digest AKA with conversion functions) may be conducted inside a TLS connection where the network is authenticated using a server certificate. The server certificate must contain the FQDN of the BSF server as specified in RFC 2818 ("HTTP over TLS").

2.3 Key derivation

Several issues have to be solved in the key derivation procedure that uses 2G authentication vectors:

- how many authentication vectors should be used per bootstrapping, and
- how to derive the bootstrapping shared key Ks.

As the length of the Ki key of the SIM is 128 bits the strength of all keys derived from the Ki is effectively 128bits, regardless of how many authentication vectors would be used. This suggests that with two authentication vectors where Kc is 64 bits, would be sufficient. However, as the Kc may contain leading zero bits in which case it may be beneficial to use an additional authentication vector. Therefore, we recommend that three authentication vectors are used during bootstrapping. However, this effects the selected conversion functions in Annex: the server specific data field in the nonce field of HTTP Digest AKA needs to be used. If this not desired, we can use only one authentication vector in which case there is no need to use the "server specific data" field.

As the selected conversion functions in the Annex A, for the CK_{UMTS} and IK_{UMTS} to be exactly 128 bits in length, the Ks can be formed the same as the Ks in the 3G GBA, i.e., by concatenating them to form a Ks that is 256 bits in length. This key can be used in further key derivations that are required when the NAF specific keys Ks_NAFs are derived.

2.4 Interoperability

2.4.1 Discovery of UICC type

The BSF needs to be able to discover what type of UICC the UE is equipped with. Several methods can be identified:

1. The UE may indicate to the BSF the type of the UICC;
2. The BSF may discover the type of the UICC by examining the IMPI given by the UE;
3. The BSF may blindly request authentication vectors from the HSS, and the HSS would return either 2G or 3G authentication vectors to the BSF. The BSF may discover the type of the UICC by examining the authentication vector returned by the BSF.
4. Same as 3, but the BSF may discover the UICC type of examining the uiccType parameter in subscriber's GUSS returnred by the HSS.

Option 1 requires additional changes to Ub reference point thus it is not considered further. If the BSF needs request authentication vectors from different servers depending on the UICC type then option 2 should be used. Option 2 is also the only alternative if the HSS is not able to handle with both 2G and 3G authentication vector requests. If the HSS is able to handle both 2G and 3G authentication vector requests, then either option 3 or 4 should be selected as with those options the BSF is less complex that with option 2 where the BSF needs to be able to decided by examining the IMPI whether the corresponding xSIM application in the UICC is 2G or 3G.

Suggestion: Option 4.

2.4.2 UE equipped with both 2G SIM and 3G xSIM

It the UE is equipped with both 2G SIM or 3G USIM or ISIM, the UE should always use 3G GBA as it is more secure. The BSF shall get the uiccType indication "2G SIM" (cf., 2.4.1) in subscriber's GUSS only when the UE is indeed equipped with only 2G SIM. This disables the possibility that an attacker downgrades the 2G GBA when also 3G GBA is available.

Suggestion: All MEs supporting 2G GBA shall support also 3G GBA.

2.4.3 NAF requires 3G GBA

The NAF may require to know whether 2G GBA or 3G GBA was used to authenticate the UE. A NAF may have a policty that it requires the bootstrapping to be based on 3G GBA in which case it should reject such an UE that used 2G GBA for bootstrapping. Thus, it may be required that the type of bootstrapping method needs to be communicated to the NAF. This would require an additional parameter to be added to the Zn reference point indicating this method.

2.4.4 Migration from 2G GBA to 3G GBA

If the BSF is able to reliably discover the supported authentication methods (i.e., 2G or 3G GBA) of the UE, the migration from 2G GBA to 3G GBA is pretty straightforward.

In the beginning, the operator may have only 2G GBA enabled terminals with 2G SIMs. In this case, the BSF supporting both 2G and 3G GBA can be used as it is. As the operator starts to roll out 3G USIMs and/or ISIM, the BSF that supports both 3G and 3G GBA can still handle this situation. Finally, when the operator wants to use only 3G GBA, it can disable the support for 2G GBA in its BSF, use only 3G GBA. In all these scenarios, the BSF (supporting both 2G and 3G GBA), the HSS (supporting both 2G and 3G authentication vectors), and the NAFs can functions as they have been specified. There is no need to update any of the servers.

The support for 2G GBA may also be an upgrade to the BSF in which case only the BSF (and possibly the HSS) needs to upgraded if the operator whiches to use 2G GBA. In any case, the support for 2G GBA is decided by the operator. In order to have operator in full control of the migration, then all ME supporting 2G GBA should also support 3G GBA (see also 2.4.2).

Suggestion: All MEs supporting 2G GBA shall support 3G GBA.

2.5 Security analysis

As the changes in 2G GBA compared to 3G GBA affects mostly the Ub reference point the security analysis concentrates on that reference point. The security aspects in the other reference points are the same than in 3G GBA, except that the key strength used in the Ua reference point is weaker but still sufficient (i.e., 128 bits[1]).

As 2G authentication vector does not provide network authentication nor replay protection, the following counter measures can be taken in the ME using 2G GBA:

2.5.1 Network authentication

Option 1: Network authentication may be provided by using TLS with server certificates. The URL used to address the BSF, may be mandated to use "https://" scheme, i.e., the ME mandates that the 2G GBA bootstrapping must be conducted through a TLS tunnel. The ME can further check that the "realm" attribute contains the same FQDN of the BSF that was present in the server certificate offered by the BSF.

NOTE: Whether there are valid attacks in GBA prevented by network authentication needs to be studied further. One possible attack is a combination of a false BSF and a false NAF in which case the UE may be fooled to reveal confidential information to the false NAF.

However, the assumption is that network authentication is not really needed between the UE and the BSF, and thus TLS would not be needed which means that the problem with issuing TLS certificates to the BSFs goes away.

Option 2: Network authentication may also be provided by using conversion functions (see section 2.2 and Annex A). Instead of having an empty AUTN (see Annex A), an AUTN can be generated by using a key derivation function with

---

1 Strictly speaking, key entropy is not increased by using multiple vectors. If the attacker can send a RAND to an ME and convince it to encrypt some known text using the resulting Kc. He can then brute-force Kc in at most 2^64 steps. Sending n RANDs would only slow him down to n*2^64 steps (not 2^(n*64)). So the real entropy is only 65 bits. However, if the special RAND scheme is used to provide cryptographic separation between 2G GAA and GSM (special 2G GAA RANDs that have some bits set to reserve it for 2G GAA only), then the attacker cannot attack against individual Kc keys, and it is possible to get 128 bit key strength.

generated IK and RAND (as depicted in Annex A). The BSF will generate the AUTN and send it to the UE. The UE will then verify that the AUTN is correct - thus authenticating the network.

Option 3: It may be possible to use a variation of EAP/SIM and network certificate as specified in TS33.234 WLAN interworking. This options would require further studies.

Suggestion: Use AUTN to authenticate the network (option 2).

2.5.2 Replay protection

The lack of replay protection causes problems when 2G authentication vectors are used in different security contexts. The 2G GBA can mitigate this problem by mandating a 2G GBA enabled ME to remember the RANDs that were used during bootstrapping procedure during the key lifetime set by the BSF. This enables the ME to protect against an active attack where an attacker tries to discover the three Kc keys that were used to derive the Ks_SIM key during the lifetime of that key, thus preventing the attacker to discover the keys through re-running SIM authentication in other security context than 2G GBA. After the key lifetime has expired the corresponding RANDs can be deleted from ME's memory, the key is not usable in active attacks any more. However, an attacker may re-run the corresponding RANDs after the key lifetime has expired and compromise the transactions between the UE and a NAF afterwards. It should be noted however that the TLS + HTTP Digest (see [2], subclause 5.3) approach is not affected by this attack as the compromised NAF specific key is used only in HTTP Digest, and the messaging itself is protected by TLS that has nothing to do with the NAF specific key. The same applies for subscriber certificates (see [2], subclause 5.5) as the NAF specific key is not directly used. However, TLS PSK (see [2], subclause 5.4) has a problem because the NAF specific key is directly used when the TLS tunnel is established, and thus the attacker can discover the message flows after the key lifetime has expired, and therefore the confidentiality is broken. It should be noted that in all of these cases an active attack is not possible if the ME does prevent the usage of the RANDs in other security contexts when they are used in 2G GBA security context.

3 Conclusion & Proposal

This paper discussed the possibilities to include optional support for 2G GBA to current GBA framework. We ask SA3 to comment on this issue. We also provide an example annex how 2G GBA could be incorporated to the GAA specifications (see Annex B of this contribution). For the case that SA3 would like to study the details of 2G GBA further, a work item description is attached that covers the work on 2G GBA.

References

[1] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[2] 3GPP TS 33.222: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

Annex A: Conversion functions for 2G GBA

A.1 Proposal

We propose the use the following conversion functions with *n* triplets in 2G GBA:

1. Derive a key from *n* triplets by concatenting Kc values from the triplets. If the concatenated key is less than 256 bits then pad it with alternative Kc values as many times as needed to form 256 bits long key as follows:

   n=1: key = Kc || Kc || Kc || Kc
   n=2: key = Kc_1 || Kc_2 || Kc_1 || Kc_2
   n=3: key = Kc_1 || Kc_2 || Kc_3 || Kc_1
   n>3: key = Kc_1 || Kc_2 || ... || Kc_n

2. Derive the pseudo UMTS quintet using the key derived in step one and the GBA key derivation function (KDF) defined in Annex B of TS 33.220 as follows:

   $RAND_{UMTS}$ = $RAND_1$
   RES_{UMTS} = KDF (key, "3gpp-gba-res" || $SRES_1$ || $SRES_2$ || ... || $SRES_n$), truncated to 128 bits
   $AUTN_{UMTS}$ = KDF (key, "3gpp-gba-autn" || $RAND_1$ || $RAND_2$ || ... || $RAND_n$), truncated to 128 bits
   CK_{UMTS} = KDF (key, "3gpp-gba-ck" || $SRES_1$ || $SRES_2$ || ... || $SRES_n$), truncated to 128 bits
   IK_{UMTS} = KDF (key, "3gpp-gba-ik" || $SRES_1$ || $SRES_2$ || ... || $SRES_n$) , truncated to 128 bits
   server specific data = $RAND_2$ || $RAND_3$ || ... || $RAND_n$ || other server specific data

   NOTE: The KDF is implemented in both the BSF and the UE as it is used to derive the NAF specific keys according to the existing specifications (see [1]).

   || marks concatenation

   truncation to 128 bits is always performaed such a way that 128 most significant bits are preserved.

We propose that the conversion function described above is used with three triplets (n=3). This requires that server specific data field is taken into use in HTTP Digest AKA. If this is not desired then limiting the number of triplets can be set to one (n=1) in which case the server specific data is not to be needed.

A.2 History

T-Mobile suggested to use the following conversion functions in S3-020602:

Conversion functions:

- $RAND_{UMTS}$ = $RAND_{GSM}$
- RES_{UMTS} = $SRES_{GSM}$
- $AUTN_{UMTS}$ = 0
- CK_{UMTS} = Kc || Kc
- IK_{UMTS} = (Kc[0..31] XOR Kc[32..63]) || Kc || (Kc[0..31] XOR Kc[32..63])

Conversion functions with *n* triplets:

- $RAND_{UMTS}$ = $RAND_1$
- RES_{UMTS} = $SRES_1$ || $SRES_2$ || ... || $SRES_n$
- $AUTN_{UMTS}$ = 0
- CK_{UMTS} = SHA1(Kc_1 || Kc_2 || ... || Kc_n), truncated to 128 bits
- IK_{UMTS} = SHA1(Kc_n || Kc_{n-1} || ... || Kc_1), truncated to 128 bits
- server specific data = $RAND_2$ || $RAND_3$ || ... || $RAND\_GSM_n$

Annex B: Example annex to TS 33.220

Editor's note: This annex contains an example annex that specifies the 2G GBA functionality. This is not be taken as an official CR proposal.

===== BEGIN CHANGE ====

Annex G (normative):
2G GBA: Bootstrapping procedure using 2G SIM

It is assumed that the UE, the BSF, and the HSS involved in the procedures specified in this annex are capable of handling the 2G GBA specific enhancements.

G.1 Introduction

<TODO>

G.2 Architecture and reference points

The architecture and reference points used in 2G GBA are the same as specified in clause 4 of this specification with the additions and exceptions specified in clause G.3.

G.3 Requirements and principles for 2G bootstrapping

In addition to the requirements and principles specified in clause 4 of this specification, the following requirements and principles are application to 2G-based bootstrapping (2G GBA) procedure. The BSF supporting 2G GBA shall also support 3G GBA. The UE supporting 2G GBA shall also support 3G GBA.

Requirements related to the 2G bootstrapping are:

- 2G GBA shall use the existing SIM application functionality and SIM related UICC-ME interface;
- Mobile network operator shall be able to decide whether 2G SIM based authentication procedures are allowed for its subscribers;
- BSF and UE supporting 2G GBA shall be able to authenticate each other using 2G SIM authentication procedures over Ub reference point;
- 2G GBA shall use Ub reference point as specified in clause 4 (i.e., HTTP Digest AKA) with 2G-to-3G authentication vector conversion functions;
- UE supporting 2G GBA shall prevent the usage of the RANDs that were used in 2G GBA in other security contexts during the lifetime of the bootstrapped security association;

NOTE: The UE must have RANDs that have been used in 2G GBA on a list as long as the corresponding key lifetime is valid, and prevent the listed RANDs being used in any other security context. Especially, if the UE re-bootstraps using new set of RANDs this will not cause the UE to delete the older RANDs from the list. Only when the key lifetime has expired the corresponding RANDs can be deleted from the list.

- if UE supporting 2G GBA is equipped with both a 2G GBA capable and a 3G GBA capable UICC application, the UE shall use the 3G GBA capable UICC application;

- BSF supporting 2G GBA shall be able to request 2G authentication vectors from the HSS over Zh reference point;
- 2G GBA shall use three authentication vector triplets per one bootstrapping run;
- 2G GBA shall not require additional functionality from 2G SIM application on the UICC;

G.4 Procedures for 2G bootstrapping

G.4.1 Initiation of bootstrapping

The text from clause 4.5.1 of this specification shall also apply here.

G.4.2 Bootstrapping procedure

The procedure specified in this clause differs from the procedure specified in 4.5.2 in that 2G authentication vector is used in the bootstrapping procedure instead of 3G authentication vectors. The UE and the BSF shall use a conversion function to convert the 2G authentication vector to 3G authentication vector and wise versa. The messages exchanged over the Ub reference point are identical for both procedures.

When a UE wants to interact with a NAF, and it knows that the bootstrapping procedure is needed, it shall first perform a bootstrapping authentication (see figure G.1). Otherwise, the UE shall perform a bootstrapping authentication only when it has received bootstrapping initiation required message or a bootstrapping renegotiation indication from the NAF, or when the lifetime of the key in UE has expired (see clause G.4.3).

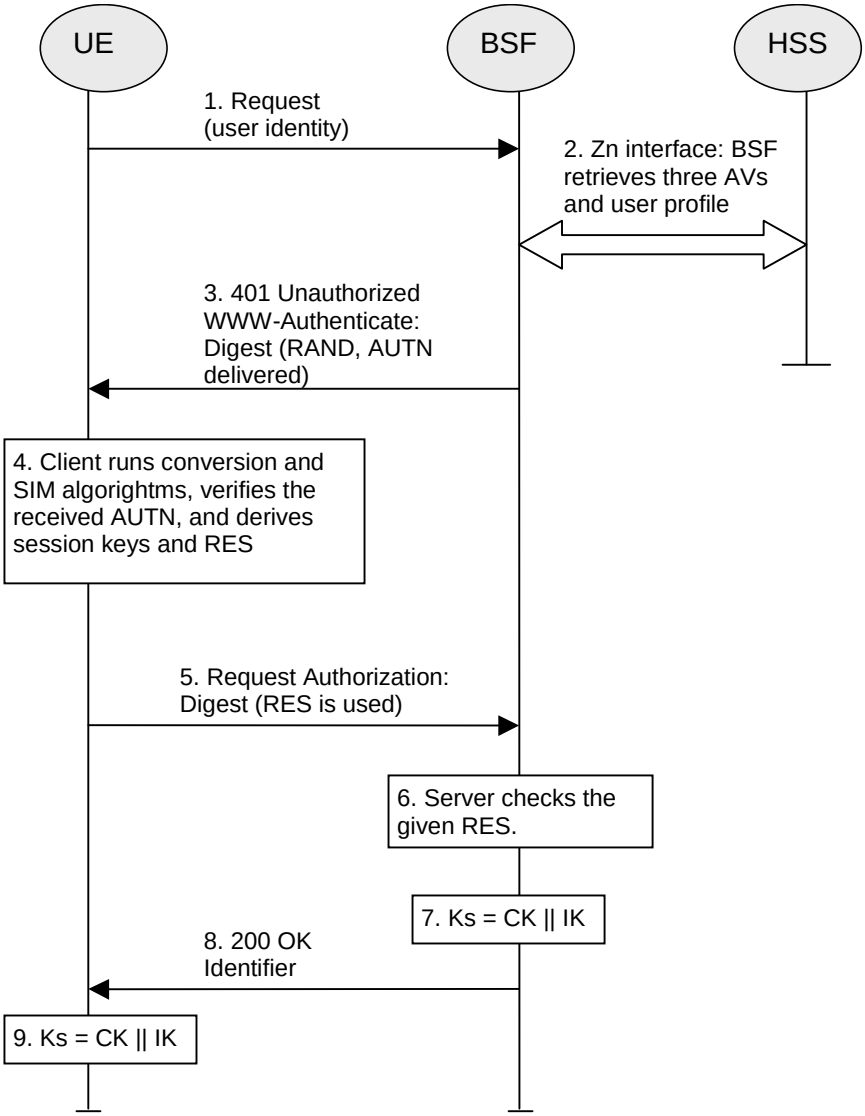

Figure G.1: The bootstrapping procedure with 2G authentication vectors

1. The ME sends an HTTP request towards the BSF.

2. The BSF retrieves the complete set of GBA user security settings and three 2G authentication vectors (AVs, AV = RAND, SRES, Kc) over the Zh reference point from the HSS. The BSF discovers that the UE is equipped with 2G SIM both by looking at the AV type, i.e., triplet, and the contents of the GUSS where the UICC type is marked to be 2G SIM.

   The BSF converts the three 2G authentication vector triplets to a single pseudo 3G authentication vector quintet:

   - $RAND_{UMTS} = RAND_1$
   - RES_{UMTS} = KDF (conv-key, "3gpp-gba-res" || $SRES_1$ || $SRES_2$ || $SRES_3$), truncated to 128 bits
   - $AUTN_{UMTS}$ = KDF (conv-key, "3gpp-gba-autn" || $RAND_1$ || $RAND_2$ || $RAND_3$), truncated to 128 bits
   - CK_{UMTS} = KDF (conv-key, "3gpp-gba-ck" || $SRES_1$ || $SRES_2$ || $SRES_3$), truncated to 128 bits
   - IK_{UMTS} = KDF (conv-key, "3gpp-gba-ik" || $SRES_1$ || $SRES_2$ || $SRES_3$) , truncated to 128 bits
   - server specific data = $RAND_2$ || $RAND_3$ || other server specific data

   where conv-key is Kc_1 || Kc_2 || Kc_3 || Kc_1.

NOTE 1: The subscript in the triplet parameters (i.e., RAND, SRES/RES, and Kc) marks the different set of triplets received from the HSS.

NOTE 2: "Truncated to 128 bits" means that from the 256 bits output of KDF, the 128 bits numbered as [0] to [127] are used.

$RAND_2$ and $RAND_3$ are sent to the UE in HTTP Digest AKA as server specific data as specified in IETF RFC 3310 [xx].

3. The BSF forwards to $RAND_{UMTS}$, $AUTN_{UMTS}$, and server specific data (i.e. $RAND_2$ and $RAND_3$) in the 401 message (without CK_{UMTS}, IK_{UMTS}, RES_{UMTS}). This is to demand the UE to authenticate itself.

4. The UE extracts $RAND_1$, $RAND_2$, and $RAND_3$ from the message and calculates the corresponding Kc and RES values. It then calculates the pseudo 3G authentication vector quintet from these values as specified in step 2. The UE then verifies the $AUTN_{UMTS}$ using the calculated the pseudo 3G authentication vector values to authenticate the network.

5. The UE sends another HTTP request, containing the Digest AKA response (calculated using RES_{UMTS}) to the BSF.

6. The BSF authenticates the UE by verifying the Digest AKA response.

7. The BSF generates key material Ks by concatenating CK_{UMTS} and IK_{UMTS} (calculated in step 2). The B-TID value shall be also generated in format of NAI by taking the base64 encoded [12] $RAND_{UMTS}$ value from step 3, and the BSF server name, i.e. base64encode($RAND_{UMTS}$)@BSF_servers_domain_name.

8. The BSF shall send a 200 OK message, including a B-TID, to the UE to indicate the success of the authentication. In addition, in the 200 OK message, the BSF shall supply the lifetime of the key Ks. The key material Ks is generated in UE by concatenating CK_{UMTS} and IK_{UMTS}.

9. Both the UE and the BSF shall use the Ks to derive the key material Ks_NAF during the procedures as specified in clause G.4.3. Ks_NAF shall be used for securing the reference point Ua.

   Ks_NAF is computed as Ks_NAF = KDF (Ks, key derivation parameters), where KDF is the key derivation function as specified in Annex B, and the key derivation parameters consist of the user's IMPI, the NAF_Id and RAND_UMTS. The NAF_Id consists of the full DNS name of the NAF. KDF shall be implemented in the ME.

NOTE 3: To allow consistent key derivation based on NAF name in UE and BSF, at least one of the three following prerequisites shall be fulfilled:

(1) The NAF is known in DNS under one domain name (FQDN) only, i.e. no two different domain names point to the IP address of the NAF. This has to be achieved by administrative means.
This prerequisite is not specific to 3GPP, as it is necessary also under other circumstances, e.g. for TLS V1.0 without use of wildcard or multiple-name certificates.

(2) Each DNS entry of the NAF points to a different IP address. The NAF responds to all these IP addresses. Each IP address is tied to the corresponding FQDN by NAF configuration. The NAF can see from the IP address, which FQDN to use for key derivation.

(3) Ua uses a protocol which transfers the host name (FQDN of NAF as used by UE) to NAF (e.g. HTTP/1.1 with mandatory Host request header field). This requires the NAF to check the validity of the host name, to use this name in all communication with UE where appropriate, and to transfer this name to BSF to allow for correct derivation of Ks_NAF.
In case of a TLS tunnel this requires either multiple-identities certificates or the deployment of RFC 3546 [9] or other protocol means with similar purpose.

The UE and the BSF shall store the key Ks with the associated B-TID for further use, until the lifetime of Ks has expired, or until the key Ks is updated.

G.4.3 Procedures using bootstrapped Security Association

The text from clause 4.5.3 of this specification shall also apply here.

G.4.4 Procedure related to service discovery

The text from clause 4.5.4 of this specification shall also apply here.

===== END CHANGE =====

Work Item Description

Title

2G GBA: 2G SIM usage in 3GPP GAA framework

1 3GPP Work Area

	Radio Access
	Core Network
	Services

2 Linked work items

GAA and Support for subscriber certificates (SEC1-SC)

3 Justification

GBA is currently based on 3G USIMs and ISIMs, i.e., 3G GBA [TS33.220]. The security level of 3G Authentication and Key Agreement is higher than the 2G SIM authentication. On the other hand, there are more than one billion people with SIMs in their phones and it will take long time to provision UICCs capable of 3G authentication to such a large population. In the meanwhile there should be a way to offer services whose authentication is based on GAA also to 2G subscribers. However, if it is possible to choose between 2G and 3G authentication procedures between a particular UE and the BSF, then it should be ensured that the 3G authentication procedure is chosen, because it is more secure. Moreover, the support for 2G GBA should be completely under MNO control. We suggest studying and outlining possible 2G GBA approaches. It should be noted that the work outlined in this WID **does not cause any change needs to the existing SIM specifications**, in particular GBA_U as in 3G will not be included in 2G GBA.

4 Objective

This work item will specify how 2G SIMs can be used in 3GPP GBA framework securely. The support for 2G GBA is completely under MNO control, i.e., the BSF would be configurable either allow or disallow 2G GBA.

5 Service Aspects

None identified

6 MMI-Aspects

None identified

7 Charging Aspects

None

8 Security Aspects

This is a security work item.

9 Impacts

Affects:	UICC apps	ME	AN	CN	Others
Yes		X		X	
No	X		X		
Don't know					X

10 Expected Output and Time scale (to be updated at each plenary)

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments

11 Work item rapporteur(s)

Silke Holtmanns (Nokia)

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Nokia (at least 4 Individual Members)

14 Classification of the WI (if known)

	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

SEC1-SC (GAA and support for subscriber certificates)

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)