3GPP TSG SA WG3 Security — S3#32 **S3-040065**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda Item: 6.9.2
Source: Ericsson
Title: Requirements for Transaction Identifier in GBA
Document for: Discussion/Decision

1. Introduction

Generic Bootstrapping Architecture (GBA) uses Transaction Identifier (TID) as a binding element that helps UE, BSF and NAFs to agree on the UE identity and related keying material. This document intends to identify requirements and open issues related to TID in order to make it useful and secure in GBA.

2. Transaction Identifier

Transaction Identifier (TID) is used as a binding element between BSF, UE, and NAFs to agree on a common key. The generic bootstrapping server function (BSF) and the UE mutually authenticates each other by using the AKA protocol. At this phase, BSF also generated TID that will uniquely identify the created keying material. UE uses TID when it contacts network application function (NAF) as an identifier. Based on TID, NAF can request corresponding keying material from BSF.

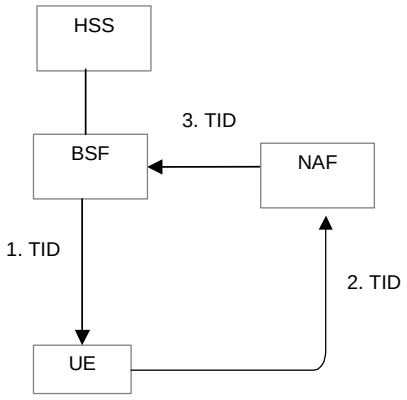

Figure 1: TID circulation in GBA

3. Requirements for TID

3.1 Global uniqueness

UE may use TID with any NAF, in any protocol, and in any network (in R6 only in home, but in future releases also in visited network).

BSF, who generates the TID, does not know the identity of NAF at the time of creation. Also, BSF does not know which protocol will use the key identifier. Neither will BSF know which network (home or visited) will use TID.

This suggests that TID must be globally unique for all Operators, all UEs, all NAFs and all protocols.

Suggested requirement for 33.220:

TID shall be globally unique.

3.2 Suitability for different using protocols

One of the requirements for GBA is that the keying material must be usable with several using protocols. TID will be used as a key identifier, e.g.

- If the using protocol were HTTP Digest, TID would be placed in the “username” field.
- If the using protocol were shared-key TLS as specified in [shared-key-tls], TID would be placed as a session identifier.
- Other potential using protocol, such as IPsec/IKE with shared keys.

The maximum length of the key identifier fields may vary between different protocols.

Suggested requirement for 33.220:

TID shall be usable as a key identifier in protocols used in the Ua interface.

3.3 Co-existence of GBA and non-GBA infrastructures

There are use cases when NAF may want to use GBA and non-GBA based infrastructures at the same time. For example, a NAF may want to authenticate subscribers both by using normal HTTP Digest authentication (where the usernames and passwords are distributed using some other mechanism than GBA), and by using GBA based HTTP Digest. However, it seems that in most telecommunication protocols, the server side (i.e. NAF) controls the name space related to key identifiers (cf. TID). For example, in HTTP authentication, the server issues the usernames, and does not allow the re-use of already existing usernames. The parallel use of GBA and non-GBA based infrastructures may cause conflicts on TID namespace. In particular, BSF may assign TID values that NAFs are already using with non-GBA UEs.

There are at least three ways to solve the problem:

1. The name space in the Ua interface should be divided between GBA and non-GBA clients. NAF should not be allowed to use the GBA part of the name space with non-GBA clients in the Ua interface.
2. Ua interface should be restricted for GBA clients only. Co-existence of GBA and non-GBA security should not be allowed.
3. Develop a recovery mechanism for the cases when the name spaces overlap. For example, the UE could be able to figure out if some TID value is already in use in the Ua interface. In this case, the UE could re-try a new TID value. (Note that NAF is not typically able to indicate to the UE that the TID is already in use because NAF sees such UE as an attacker!)

Suggested changes to 33.220:

Add an Editors note stating that the TID name space control problem in the Ua interface should be further studied in the case when both GBA and non-GBA based security is used at the same time.

3.4 Subscriber identity

When GBA is used with ISIM, it is not necessarily clear which subscriber identity is related to TID.

In the case of Presence Ut interface, there are several potential identities, i.e. IMPI and IMPUs. The subscriber may have several Presence accounts related to same IMPI. TID does not carry enough information on which IMPU the end-user is trying to use.

There are at least two solutions to the problem:

1. Assuming that the protocol in the Ua interface is able to carry IMPU information to NAF (e.g. in the XML/XCAP body in the case of Presence Ut interface), it is enough if NAF gets all IMPUs from BSF.

2. If the protocol in the Ua interface is not able to carry IMPU (e.g. because TID is already carried in the identity field, and there is no room for the other identity, i.e. IMPU, in the protocol), TID should be designed in the way that it uniquely identifies the subscriber identity that the end-user intends to use with NAF.

Suggested change to 33.220:

Add an Editors note stating that GBA must further specify on how TID is related to different identities of the subscriber (e.g. IMPI, or IMPUs), and how the NAF knows which identity has been authenticated.

3.5 Removing and/or updating security associations

GBA can be used to set-up new "security associations" between UE and NAF. GBA does not currently specify how security associations are removed, and/or updated.

Each bootstrapping procedure creates a new TID value even when the same UE is communicating with the same NAF. If the intend is just to update the password in HTTP Digest to a fresh one, for example, this would also mean that the identity of the end-user would need to be changed. It is not currently clear what happens to the old username and password in NAF. The same potential problem is also related to the use of GBA with other protocols, such as "shared-secret-TLS" as specified in [shared-key-tls]. The use of TID as a TLS session identifier is not possible unless the TLS implementation would be able to remove the old sessions from session cache.

There are at least two solutions to the problem:

1. NAF must be able to distinguish that different TID values are actually related to the same security association. In this way, NAF can remove old security associations (or update old ones) when new security associations are created.

2. Each bootstrapping procedure creates new security association. NAF removes security associations only when the key lifetime (specified by BSF) expires.

   Note that this solution has a general problem for letting the UE create new states in NAF (DoS attack). Also, the control of security association removal is outside NAF, in BSF. This may be a problem if both NAF and BSF are located in different networks.

Suggested changes to 33.220:

Add an Editors note stating that GBA must further specify on how security associations are removed and/or updated in NAF.

3.6 Routability

If the NAF is located in the visited network, TID is most likely the only available identifier that can be used to find the right BSF. This suggests that TID should be routable in AAA infrastructure, i.e. include the domain name of the subscriber.

Suggested requirement for 33.220:

NAF shall be able to detect the home network of the UE from the Transaction identifier. Home network information may be used to locate BSF.

3.7 Infeasibility to guess unused TID values

In the current form, BSF does not know if the NAF is really talking to the UE. The system is based on the assumption that if the TID is valid, then keying material is returned to NAF. If badly behaving NAF is able to guess an unused (but generated) TID value, it is able to request related keys from BSF. As a result, the UE is not able to use the next TID and related key because BSF thinks they are already in use.

Suggested requirement for 33.220:

It should be infeasible to guess the next value of TID for specific UE.

4. Conclusion

TID is a core element of GBA. It is important that TID is designed in the way that it is both secure, and useful with several protocols in the Ua interface.

It is proposed that SA3 considers adding the following requirement for [33.220]:

- TID shall be globally unique. Different BSFs must not use the same TID values.
- TID shall be usable as a key identifier in protocols used in the Ua interface.
- NAF shall be able to detect the home network of the UE from the Transaction identifier. Home network information may be used to locate BSF.
- It should be infeasible to guess the next value of TID for specific UE.

It is also proposed that SA3 considers adding the following Editors notes to [33.220]:

- Add an Editors note stating that GBA must further specify on how TID is related to different identities of the subscriber (e.g. IMPI, or IMPUs), and how the NAF knows which identity has been authenticated.
- Add an Editors note stating that the TID name space control problem in the Ua interface should be further studied in the case when both GBA and non-GBA based security is used at the same time.
- Add an Editors note stating that GBA must further specify on how security associations are removed and/or updated in NAF.

5. References

[33.220] 3GPP, Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture, Release 6, version 0.2.0, 11/2003.

[shared-key-tls] P.Gutmann: Use of Shared Keys in the TLS Protocol, IETF, work in progress, draft-ietf-tls-sharedkeys-02.

CR-Form-v7

Pseudo - CHANGE REQUEST

⌘ **33.220** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: 1.0.0 ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	GBA Transaction Identifier (TID) requirements
Source:	⌘	Ericsson
Work item code:	⌘	***Date:*** ⌘ 26 January 2004
Category:	⌘	***Release:*** ⌘ Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	GBA does not currently specify any requirements for TID. TID is a core element of GBA. It is important that TID is designed in the way that it is both secure, and useful with several using protocols in the Ua interface.
Summary of change:	⌘	Introduce requirements. See related discussion paper on the background of proposed requirements.
Consequences if not approved:	⌘	TID may not be secure, or it may not serve all potential using protocols in the Ua interface.

Clauses affected:	⌘	

		Y	N		
Other specs affected:	⌘	Y		Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	

Other comments:	⌘	

***** Begin of Change ****

4.1.7 Requirements on transaction identifier

Transaction identifier shall be used to bind the subscriber identity to the keying material in Ua, Ub and Zn interfaces.

Requirements for transaction identifier are:

- Transaction identifier shall be globally unique.
- Transaction identifier shall be usable as a key identifier in protocols used in the Ua interface.
- NAF shall be able to detect the home network of the UE from the Transaction identifier. Home network information may be used to locate BSF.
- It should be infeasible to guess the next value of transaction identifier for specific UE.

Editor's note: Relationship between TID and subscriber identity is ffs.

In the case of Presence Ut interface, there are several potential identities that are related to TID, i.e. IMPI and IMPUs. The subscriber may have several Presence accounts related to same IMPI. TID does not carry enough information on which IMPU the end-user is trying to use.

Editor's note: Parallel use of GBA and non-GBA infrastructure is ffs.

There are use cases when NAF may want to use GBA and non-GBA based infrastructures at the same time. For example, a NAF may want to authenticate subscribers both by using normal HTTP Digest authentication (where the usernames and passwords are distributed using some other mechanism than GBA), and by using GBA based HTTP Digest. However, it seems that in most telecommunication protocols, the server side (i.e. NAF) controls the name space related to key identifiers (cf. TID). For example, in HTTP authentication, the server issues the usernames, and does not allow the re-use of already existing usernames. The parallel use of GBA and non-GBA based infrastructures may cause conflicts on TID namespace. In particular, BSF may assign TID values that NAFs are already using with non-GBA UEs.

Editor's note:

GBA must further specify on how security associations are removed and/or updated in NAF. Each bootstrapping procedure creates a new TID value even when the same UE is communicating with the same NAF. If the intend is just to update the password in HTTP Digest to a fresh one, for example, this would also mean that the identity of the end-user would need to be changed. It is not currently clear what happens to the old username and password in NAF.

***** End of Change ****