3GPP TSG SA WG3 Security — S3#32 **S3-040033**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda item: **6.9.2 GBA**

Title: **Validity of the TID and key material**

Source: **Huawei Technologies Co., Ltd**

Document for: **Discussion and Decision**

1 Introduction

In bootstrapping procedure, after the HTTP Digest AKA succeeds, the BSF supplies a transaction identifier(TID) to the UE and generates the corresponding key materials. The NAF uses the Bootstrapped Security Association and shares the key material to protect the Ua interface with the UE. The TID and corresponding key materials(shared in NAF and UE) should not remain valid forever. The NAF should check the validity of key materials , and if it's invalid , the NAF sends a suitable key update request to UE in line with the current TS.

2 Discussion

"The BSF can restrict the applicability of the key material to a defined set of NAFs by using a suitable key derivation procedure"(r.f.33.220 clause 4.2.2.1). If it is needed, the BSF will generate the Ks-NAF to a special NAF and supply this key material to the NAF to protect the Ua interface. If the parameter n in the bootstrapping procedure equal 0, then the Ks-NAF= Ks. From that we can see the BSF controls the key material, so it is easy to ensure the BSF controls the validity of key material.

the validity can be decided by some different conditions.

1 The lifetime

2 The valid times

BSF set the lifetime/valid times of key material, when the NAF requests the key material by TID , it gets the key material to protect the Ua interface. At the same time the NAF get the lifetime/valid times of that key material. Subsequently, the UE uses same TID to connect to the NAF , and the NAF finds it had share the key material with that UE , then it can check the validity of the key material(e.g. check the lifetime/valid times of the key material).Base on result of this check , the NAF sends the key update request to UE and terminates the protocol over the Ua interface , or continues the protocol.

The lifetime/valid times of the key material setting by BSF is the limit at the latest. If the special NAF need update the key more frequently than the setting by BSF, it can implement by it's rule. But the NAF checks the validity basing on the minimal condition between the it's rule and the setting rules by BSF.

The length of lifetime/ the number of valid times may be set according the security level of a specific NAF or a defined set NAFs. The defined set of NAFs may be the set when determining the parameter n in bootstrapping procedure. The lifetime/valid times also may be selected flexibly. Using the valid times is more accurate. E.g. for a NAF with high security, the number of the valid times may set to 1, then the key material can be used only once. But in this example , it will need require more HTTP-Digest AKA requests.

3 Proposal

The BSF may manage the validity of key material and when NAF shares the key material with UE, the NAF may check the validity of key material.

Include the following changes in the TS

**********Begin of change**********

4.3.3 Procedures using bootstrapped Security Association

After UE is authenticated with the BSF, every time the UE wants to interact with an NAF the following steps are executed as depicted in **Error! Reference source not found.**

UE starts communication over Ua interface with the NAF

- In general, UE and NAF will not yet share the key(s) required to protect Ua interface. If they already do, there is no need for NAF to retrieve the key(s) over Zn interface.

- If the NAF shares a key with the UE, and~~but~~ the NAF checks the validity of the key and finds it is invalid e.g. out of the lifetime/valid times, an update of that key should then be initiated~~it~~ by sending~~s~~ a suitable key update request to the UE and terminates the protocol used over Ua interface. The form of this indication may depend on the particular protocol used over Ua interface and is ffs.

- It is assumed that UE supplies sufficient information to NAF, e.g. a transaction identifier, to allow the NAF to retrieve specific key material from BSF.

- The UE derives the keys required to protect the protocol used over Ua interface from the key material, as specified in clause 4.3.2.

NOTE: The UE may adapt the key material Ks_NAF to the specific needs of the Ua interface. This adaptation is outside the scope of this specification.

NAF starts communication over Zn interface with BSF

- The NAF requests key material corresponding to the information supplied by the UE to the NAF (e.g. a transaction identifier) in the start of the protocol used over Ua interface.

- The BSF derives the keys required to protect the protocol used over Ua interface from the key material and the key derivation parameters, as specified in clause 4.3.2, and sets the validityon condition of the key according to a defined set of NAFs or the requested NAF, then~~and~~ supplies to NAF the requested key material and the corresponding valid condition. The validity condition may be lifetime or valid times. If the key identified by the transaction identifier supplied by the NAF is not available at the BSF, the BSF shall indicate this in the reply to the NAF. The NAF then indicates a key update request to the UE.

NOTE: The NAF may adapt the key material Ks_NAF to the specific needs of the Ua interface in the same way as the UE did. This adaptation is outside the scope of this specification.

NAF continues with the protocol used over Ua interface with UE

Once the run of the protocol used over Ua interface is completed the purpose of bootstrapping is fulfilled as it enabled UE and NAF to use Ua interface in a secure way.

Editor's note: Message sequence diagram presentation and its details will be finalized later.

**********End of change**********