**3GPP TSG SA WG3 Security — S3#36** **S3-040924**
**23 - 26 November 2004**
**Shenzhen, China**

**Source:** CCSA/ZTE Cooperation

**Title:** key lifetime of GBA

**Document for:** Discussion and decision

**Agenda Item:** GBA

# 1. Introduction

In GBA procedure, BSF and UE mutually authenticate and negotiate session key that is afterwards applied between UE and NAF using HTTP Digest AKA protocol. BSF shall be able to indicate to UE the lifetime of the key material Ks in 200 OK message. UE shall use the Ks to derive the key material Ks_NAF, and compute lifetime of Ks_NAF. The lifetime of the Ks_NAF may be the same as lifetime of Ks, or it may not be the same as lifetime of Ks. That is based on UE's local policy. When NAF requests key from BSF, BSF also indicates to NAF the lifetime of key material Ks_NAF that shall be identical to the key lifetime sent to UE.

The present version of TS 33.220 mentions "if the NAF shares a key with the UE, but the NAF requires an update of that key, e.g. because the key's lifetime has expired, it shall send a suitable bootstrapping renegotiation request to the UE and terminates the protocol used over reference point Ua, see figure 4.5. The form of this indication depends on the particular protocol used over reference point Ua." in section 4.5.3.

Otherwise, the specification also mentions "This does not preclude a UE to refresh the key before the expiry time according to the UE's local policy."and "This does not preclude a NAF to refresh the key before the expiry time according to the NAF's local policy."

# 2. Problem description

According to the specification, the key renegotiation process is triggered at NAF when key expired. Because NAF can't use the key any more, application traffic over interface Ua shall be terminated. By this means, the current method of key renegotiation affects continuity of communication between UE and NAF.

Although UE and NAF can refresh the key before it has expired, it is not mandatory in present specification. Moreover, there is no detail of renegotiation process.

# 3. Proposed solution

In section 4.5.3, NAF terminates the protocol used over reference point Ua when it find key has expired. We suggest to modify the process as follow: Before the key has expired, NAF must refresh the key. The purpose of

the suggestion is to ensure the continuity of communication.

Base on the above suggestion, we also propose a method of key renegotiation in this proposal.
When UE or NAF receives key lifetime from BSF, the lifetime is regarded as hard lifetime, which means that when the hard lifetime has expired, the corresponding key should not be used any more. Beside the hard lifetime, we suggest to add soft lifetime, which is smaller than the hard lifetime. The soft lifetime is calculated by UE and NAF respectively. The calculation of soft lifetime may be various, but we suggest that the interval between the soft lifetime and hard lifetime should be enough to complete a successful AKA procedure.

UE and NAF should check the key status continually. When the soft lifetime has expired, they will initiate key renegotiation. During renegotiation, the current key can be used continually. If renegotiation is successful, UE and NAF can use new key to protect application traffic immediately, or use new key after the old one expired. If renegotiation failed, the old key can be used until the end of hard lifetime. In this case, whether UE and NAF initiate another renegotiation depends on their local policy before the old key is expired.

Both UE and NAF can initiate key renegotiation, but there is some difference in procedure. When UE requires the update of key, it will first send a notification message to NAF. Then, NAF replies a bootstrapping renegotiation request message to UE. After that, UE can start a run of AKA protocol with BSF (see figure 1). Another method of UE initiating renegotiation is that UE run AKA protocol with BSF straightly, no need of sending message to NAF. Once UE sends new B-TID to NAF, NAF know that new key has been negotiated. But if NAF first finds key has expired, it only sends a bootstrapping renegotiation request message to UE for triggering renegotiation (see figure 2).

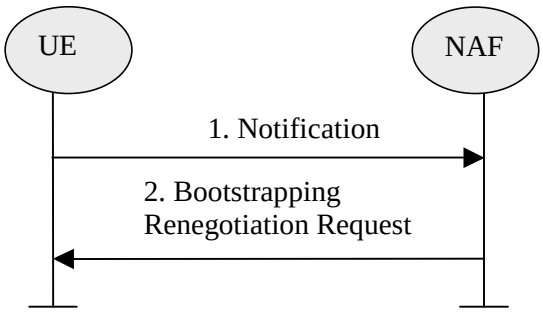


Figure1: UE initiate key renegotiation

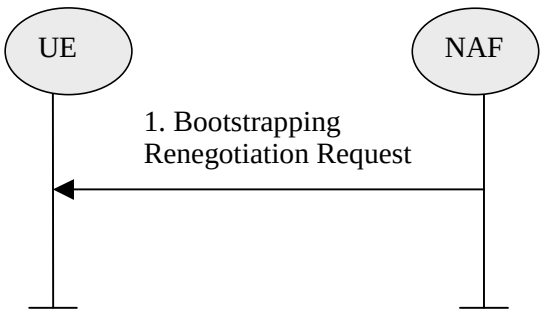


Figure2: NAF initiate key renegotiation

## 4. Conclusion

The present proposal suggests that renegotiation should start, to get a new key before the original key that is shared by UE and NAF has expired, This can ensure communication not to be terminated. Based on it , we also specify a particular method in this proposal. We kindly ask SA3 to comment on the document and if SA3 decides to accept the suggestion we will gladly prepare the CR.