3GPP TSG SA WG3 Security — S3#37 **S3-050020**
21 - 25 February 2004
Sophia Antipolis, France

Source: ZTE Corporation

Title: Security capability negotiation in GBA

Document for: Discussion and decision

Agenda Item:

1. Introduction

GBA specification is applied to other specifications, such as MBMS security (33.246), Presence service security (33.141) etc. UE and NAF should use identical security algorithm that is decided by two entities before communication, because there is no security capability negotiation between them in current version. UE can't normally communicate with NAF if they have different security feature. So specification's flexibility and extension ability is not so good in this aspect. In this discussion document, we suggest that add security capability negotiation procedure, and specify the details.

2. Problem description

The purpose of GBA is which design general authentication architecture for user equipment accessing application server, and generate a shared key. The cases that using the shared key include:

- protect application traffic between UE and NAF;
- send other keys safely, for example sending session key in MBMS security;
- entity authentication between UE and NAF, for example NAF authenticate UE when UE access NAF by using HTTPS.

There is no security capability, include security algorithm, encryption mode, key length parameters negotiation between UE and NAF in current version. Although GBA is authentication architecture based on shared key, but if security capability on UE and NAF are different, the above first and second case shall be affected. That implies UE and NAF must use same security algorithm before application or other traffic is sent. It isn't easy to extend GBA to various situations. In addition, some countries have special demand on security algorithm, so their user equipment have different security feature. When UE is roaming to other country, and wants to access a visited NAF, generally need to negotiate security capability with NAF. So it is necessary to add the procedure in GBA specification.

To general users, they don't have lots of information security knowledge, and don't familiar with security function configuration on mobile equipment. It affects that take all advantage of security function. If we can define some security grades based on equipment's capability, and tell users the function and primary use situation of each grade. User may configures security function by simply choose security grade, it is convenient to general user or senior user.

ITU-T WG 17 is working out a draft **MSEC3** "**General security policy for secure mobile end-to-end data communication**", the document mentions that mobile equipment's security functions is transformed to security grades or levels by combining and classifying them. Mobile equipment should negotiate security grade with application server. The idea and method can also be used in GBA.

3. Proposed solution

We suggest that combine and classify security algorithm supported by UE, and transform them to several security grades. User sets grade depending on application he wants to use. In original GBA procedure, we advise to add security capability negotiation (security grade negotiation to UE), in order to improve flexibility of specification. The negotiation details are as follows:

1. Operator classifies and combines security algorithms supported by almost all UE and application server, defines security grades based on need of application. Each grade may include an authentication algorithm, an encryption algorithm, and other parameters, it is suitable to protecting certain application. Operator may advises user how to use these grades;
2. There are also security grades on UE, the method of definition is the same as operator's. The grade list on UE is a subset of grades of operator's, and can be stored in USS of user;
3. User configures security grade based on his application need, the grade could be a single value, or a range;
4. When UE wants to interact with NAF, and NAF requires the use of shared keys obtained by GBA, the NAF replies with a bootstrapping initiation message. NAF can include its security algorithm list in the initiation message;
5. When UE receives the message, UE can processes it in one of following way:
   - Compare NAF's security algorithm list with its corresponding algorithms to the grade setting, chooses the first match algorithms. Then, UE sends the result in first request packet (or second, the second packet may be better, because UE has already authenticated BSF) to BSF, let BSF knows the algorithms that will be used by UE and NAF later;
   - UE sends its security grade and NAF's algorithm list to BSF, BSF can find out the algorithms configured by UE, because BSF can gets USS of user from HSS, and USS includes the relation table between grade and algorithms. So BSF can compares, and chooses the first match ones. BSF could sends the result in 200 OK message to UE;
6. The AKA procedure between UE and BSF is successful;
7. When NAF requests ks_NAF to BSF, BSF replies the key and the algorithm that be negotiated as above;
8. Then UE and NAF can use the negotiated algorithms protecting traffic.

Figure 1 and Figure 2 show the process described above.

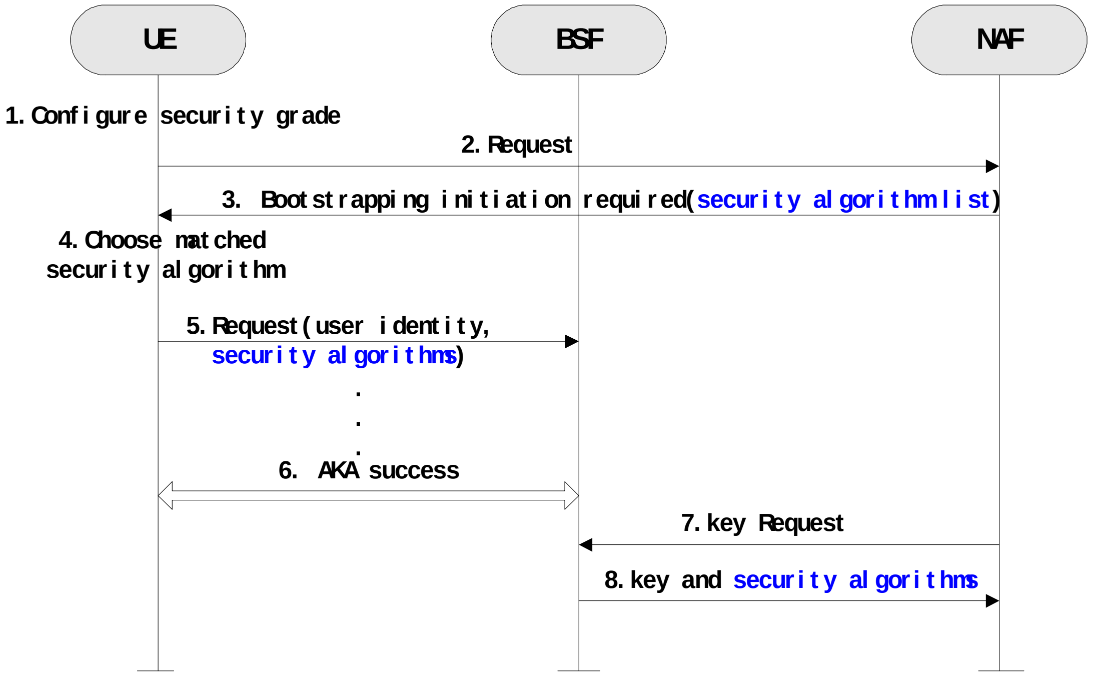
UE
BSF
NAF
1. Configure security grade
2. Request
3. Bootstrapping initiation required(security algorithm list)
4. Choose matched security algorithm
5. Request(user identity, security algorithms)
6. AKA success
7. key Request
8. key and security algorithms

Figure 1. UE compares and chooses security algorithm

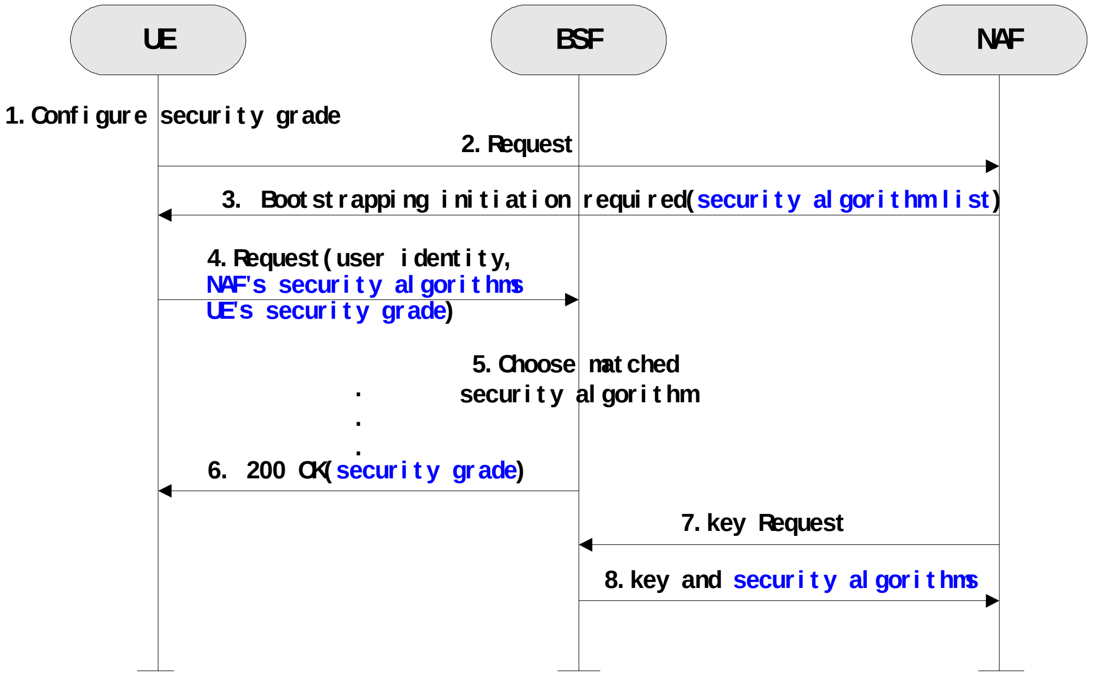
UE
BSF
NAF
1. Configure security grade
2. Request
3. Bootstrapping initiation required(security algorithm list)
4. Request(user identity, NAF's security algorithms UE's security grade)
5. Choose matched security algorithm
6. 200 OK(security grade)
7. key Request
8. key and security algorithms

Figure 2. BSF compares and chooses security algorithm

There are few difference between two methods of negotiation. If UE has the relation information about grade and algorithms, it can compare algorithms directly. However, if UE just stores the security grade, the particular information can be acquired from HSS, the second method is better. Another advantage of second method is operator can adjust the grade list in time according to external situation, for example certain algorithm is broken down, operator can replace it with stronger algorithm in grade list, it doesn't need to change the value of grade on UE.

We can know from above, UE and NAF could negotiate security capability by adding parameters in AKA message, consequently improve flexibility and extension ability. On the other hand, user could configure security function conveniently by introducing the conception of security grade. And storing grade information can save memory on UE. To operators, they can change the definition method of security grade in time according to application’s need, to improve network security. It is helpful to both sides.

4. Conclusion

We suggest that add security capability negotiation procedure in GBA, and specify the detail. Besides, we also introduce the idea and method of security grade. We hope SA3 consider and comment on our document.