3GPP TSG SA WG3 Security — S3#34 **S3-040513**
6 - 9 July 2004
Acapulco, Mexico

Agenda item: 7.9.1 GAA

Title: key safety with usage

Source: Huawei

Document for: Discussion and Decision

1 Introduction

Generic Bootstrapping Architecture (GBA) include two parts, one is ME keep the Ks(GBA-ME) , another is UICC keep Ks(GBA-U). Most of the service will use GBA-ME model. This paper discuss the key safety in ME and intend to identify an issue that should be considered in GAA application.

2 Discussion

According to the GBA-ME model, after the AKA procedure, the Ks by concatenating CK and IK will be kept in ME and used to key derivation. The Ks-NAF derived from Ks will secure the Ua reference point. If the Ks-NAF or Ks is leaked out, the Ua reference point will be broken.

From the view of algorithm, we can assume the algorithms for key derivation or secure communication are full strong, and the attacker can’t get any key information from algorithms.

From the view of ME, TS 33.220 state: when the UE is powered down, or when the UICC is removed, any keys Ks and Ks_NAF shall be deleted from storage, so the attacker can’t get any key from thus ME.

From the view of service, the local connection to ME will be allowed e.g. Bluetooth. There is no relation with GAA, but it present a slot that attacker may steal the key information from an active ME. Although the local connection specifications have their secure mechanism, the GAA as a whole security architecture should have mechanism detect and mitigate such security threat as much as possible, especially when the Application use the shared secret generated in GBA, the NAF should be able to detect abnormal using of the shared secret and take action to deal with it.

3 Conclusion

The key leaking out is an inevitable security threaten during the service, e.g. not well safed local connections. From the whole architecture consideration, GAA and the corresponding Application(NAF) should be able to detect the abnormal using of the shared secret and take action to mitigate it as much as possible.

4 Proposal

Add the follow text to TR 33.919:

“7.1 Use of shared secrets and GBA

When the Application use the shared secret generated in GBA, the NAF should be able to detect abnormal using the shared secrets and initiate the bootstrapping renegotiation described in TS 33.220 to get new shared secrets.

”