3GPP TSG SA WG3 Security — S3#33 **S3-040257**
10 - 14 May 2004
Beijing, China

Agenda Item: MBMS
Source: Ericsson

Title: Comments to 232, 243 and 249

Document for: Discussion /Decision

1. Introduction

Some contributions [232, 243] have raised concerns that MIKEY solution with GBA is a pull method. Discussion on SA3 list regarding document 249 raised the issue if the overhead of GBA-MIKEY solution could be enhanced by using UDP to transport MIKEY.

This is a comment contribution to the raised issues. This contribution illustrates that MIKEY can be used also for push based key management and it can be carried over UDP in the GBA architecture.

DiscussionThe following illustrates how MIKEY can be used for push and pull key management. It is assumed that the UE has authenticated with BM-SC, e.g. using GBA and both have a shared key (i.e. MUK) to protect the messages.

2.1 Push

It should be noted that MIKEY [] is designed originally for push cases, so it does not necessarily require a pull message from the UE. The push MSK management may be implemented as follows:

1. The BM-SC pushes MIKEY message to the UE over UDP.
2. If the BM-SC has requested it, the UE may send a MIKEY acknowledgement message over UDP. MIKEY has a defined acknowledgement message that can be used to this purpose.

This solution requires that a UDP port is defined for MIKEY.

2.2 Pull

It has been widely acknowledged in SA3 that it is inevitable to support pull in MBMS, e.g. due to cases when the UE detects a key-id mismatch in the multicast traffic. The pull may also be a stand-alone solution without push. The pull MSK management may be implemented as follows. The request message is authenticated with a key derived from GBA keys:

1. The UE requests MSK from the BM-SC with HTTP GET message.
2. The BM-SC sends the MIKEY message encapsulated in HTTP 200 OK to the UE.
3. If the BM-SC has requested it, the UE may send a MIKEY acknowledgement message over HTTP.

This case may have some variations: it would be possible that message 3 or messages 2 and 3 are carried over UDP. Carrying the messages over HTTP may however provide more reliable transport.

2.3 Push initiated pull

A special case of pull is a push initiated pull. In this case the BM-SC solicits the UE to pull the key with a certain key availability message. The push initiated pull MSK management may be implemented as follows:

1. The BM-SC solicits the UE to request for a key.
2. The next messages are the same as in pull case in 2.2.

2.4 Overhead

It can be seen that the overhead of MIKEY transport is at its smallest when MIKEY is transported over UDP, i.e. it can be as low as 60 (approximate value) bytes if optional acknowledgement message is ignored (compared to 98 bytes of OTA model in document 249).

2. Conclusion

This contribution has shown that MIKEY can be used with push method and it can be carried over UDP.

When SA3 takes the decision on the MBMS key management, it is proposed that SA3 takes these properties into account.

3. References

[232] TD S3-040232, OTA versus GBA key management

[243] TD S3-040232, MBMS UICC based solution

[249] TD S3-040249, MBMS key Management comparison