3GPP TSG SA WG3 Security — S3#33 **S3-040237**
10 - 14 May 2004
Beijing, China

Agenda Item: MBMS
Source: Ericsson

Title: Push versus pull based key management

Document for: Discussion /Decision

1. Introduction

In SA3#32 it was discussed whether MBMS key management for MSK delivery should be based on push or pull mechanism.

This contribution compares push and pull mechanisms and proposes that SA3 should adopt a pull mechanism.

2. Discussion

2.1 Pull is needed anyway

Even though push mechanism would be used for normal key deliveries, pull is required for mismatch situations where UE has missed a key update and detects from the received MBMS data that is has not got the current key. This requirement is reflected in requirement 5f in [2] and has been admitted also in [1] (which otherwise promoted push based model):

From [2]:

> *R5f: All keys used for the MBMS service shall be uniquely identifiable. The identity may be used by the UE to retrieve the actual key (based on identity match, and mismatch recognition) when an update was missed or was erroneous/incomplete.*

From [1]:

> *The decision to ask for a new key should not be terminal originated in the general case. However a mechanism to ask for keys (e.g. when subscriber loses a rekeying procedure) is to be defined.*

Therefore, if a pull mechanism is used key delivery, only one mechanism needs to be standardized and implemented for MBMS key management. If push mechanism is used, then two mechanisms need to be standardized and implemented.

2.2 Network control versus UE control

It was stated during the discussion in SA3#32 meeting that in a pull mechanism the UE controls the initiative to start the re-keying procedure and this could lead to uplink congestion when many users try to request the key simultaneously whereas in a push mechanism this problem would not exist.

A way to mitigate this problem could be that UEs would randomly request for a new key before the current key expires. However, if this is deemed not to be sufficient, the network could control the initiation of key request by setting a time to the UE when it should request for the next key. This key request time can be different to each UE and it is not the same as the key expiration time since the key expiration time is the same for all UEs in the service. Therefore also the pull mechanism can be network controlled.

2.3 Some use cases require pull

Some presented use cases seem to require pull mechanism. E.g. the following case has been in SA3 mailing list regarding MBMS download services:

Overnight Download News Service: An operator download using MBMS an audio/video news summary to many customers in the night. If a customer wants to listen to /watch the news summary, they need to fetch the MSK needed to decrypt the data from the BM-SC. Only when the customer downloads the MSK are they charged.

This kind of services cannot be implemented with push.

2.4 Deleting a user before planned key update

If a user needs to be removed from the service before the next planned key update, push mechanism seems to be the only way to do this, since the network cannot initiate a pull.

3. Conclusion

Ericsson proposes that SA3 endorses a pull mechanism for MBMS key management since:

- A pull mechanism is needed anyway
- The network can control key deliveries also in pull
- Some use cases require pull

4. References

[1] TD S3-040051, Discussion paper on MBMS key management, SA2#32, Axalto et al

[2] TS 33.246, Security of Multimedia Broadcast/Multicast Service, v 1.1.0