3GPP TSG SA WG3 Security — SA3#34 **S3-040563**
6-9 July 2004
Acapulco, Mexico

Source: **3**

Title: **Handling MSKs and decrypting download data in MBMS**

Document for: **Discussion/Decision**

Agenda Item: **MBMS**

1 Introduction

An operator will have a range of services that they will deliver over MBMS bearers. Over multicast there is the ability to protect this data. Much of the work in SA3 so far has considered streaming type services. This papers considers the protection applied to download type service. It then proposes a format for MSK identifier and how this can be used to handle MSKs in streaming and some download services. Finally it considers the shortcomings of this method in relation to other download services and proposes some possible method to solve this. The choice between these methods requires further study.

2 Protection of download data

Much of the discussion in SA3 has focussed on the issue of protecting streaming. This contribution tries to highlight the differences and draw some high level conclusions.

With streaming the encrypted data arrives on the UE and is immediately decrypted and consumed by the UE. This is very different to download when the user may consume the data more than once and not only as the data arrives on the UE. This opens up the question about whether the data from a download service should be stored on the ME encrypted after it is decrypted for the first time. There seems little value in storing the data encrypted, as the aim of MBMS security is to replace the air interface security that is applied on PTP bearers and not to produce a full DRM mechanism. If an operator wishes to control the consumption of content on a terminal, the operator should apply DRM techniques to the content. **Hence it is proposed that download data is stored decrypted on UE once it has been decrypted.**

A second difference with download is that there is no requirement for the required MSK to already be on the UE when the data arrives. This leads onto the question, when should downloaded data be decrypted. It could be decrypted either as soon as it is available for decryption assuming the relevant MSK is already on the UE or when the user wishes to consume the data. If the relevant MSK is already on the UE, it seems sensible to decrypt the data immediately, as this minimises the time that a particular MSK will need to be stored on the UE. **Hence it is proposed that download data is decrypted as soon as possible, if the relevant MSK is on the UE.**

Finally, streaming and download differ in the number of MTKs that can be usefully used to protect either a piece of content or a single download of data. For a stream there is value in changing the MTK that is used to protect a stream, particularly for long stream, as anyone trying to get free access to the stream will need to keep getting MTKs in real time. The frequency of those changes would be a balance between making it harder for an attacker and the load on the UE to change the key. For a downloaded file that is stored on a UE, there seems little value having more than one MTK to protect different parts of the file, as an attacker does not need to get the MTKs in real time. **It is proposed to take these comments into account when choosing a protection methods for download and streaming and also remove the below editor's note from clause 5.2.**

Editor's note: It needs to be decided if there is to be a minimum amount of traffic that is to be protected with one key, as this puts a lower limit on the frequency of key changes, e.g. one continuous transmission of data. It could also be possible for several of these minimum amounts to be transmitted with changing the key. It is ffs what this minimum amount should be and whether several of these minimum amounts can be transmitted without changing the key.

3 Handling of MSKs

To create services over MBMS, an operator will group data together that will be protected by one MSK (note: the protection is actually achieved by protecting an MTK with an MSK and then using the MTK to protect the traffic). This MSK will be shared with the UEs that wish to access the service. Over time, the MSK will become redundant and be replaced by a new MSK. The section proposes a method for achieving this replacement for streaming service and many types of download services. The shortcomings of the proposed method for other kinds of download service are also discussed.

3.1 Format of MSK Identifier

There are several properties needed for an MSK identifier. Firstly the identifier should be globally unique, in order to ensure that a UE does not use the incorrect MSK. Secondly the issuer of an MSK needs a way of linking several MSKs together in a kind of “service” to allow old MSKs to be replaced by new ones. This leads onto the following proposal for the format of an MSK Identifier

MSK ID = Network ID || Key service ID || Key ID

where || is the concatenation of string and each part is the following

Network ID = MCC + MNC and is 3 bytes long

Key service ID is 2 bytes long

Key ID is 2 bytes long.

Key service ID is used to group MSKs together to allow removal by the UE of an MSK that has become redundant, while Key ID is used to distinguish the different keys that belong to a Key service.

Note: Key service is introduced, as it is clear from TS 22.246 that each MBMS User service may require more than one MSK simultaneously and each MSK may be used to “protect” data belonging to more than MBMS User service.

3.2 Handling of MSKs

A UE receiving MBMS services will receive many MSKs. In order to make efficient use of the storage on the UE, there should be a way to remove MSKs that are no longer useful. From the MSK handling purpose there seem to be two types of service, firstly a service where the MSKs are already in the UE before the data arrives and secondly services where the MSK can be fetched after the data has arrived (at the point that the user wants to view the data). Clearly the second type of service is only possible for download MBMS User services. The following sections will look at the key management for service that require the MSKs to be there when the data arrives and then service which does not require the key to be there when the data arrives.

3.2.1 Services with MSK present when data arrives

This sort of service includes all streamed data and could also include a download services. For this types of service the data protected by a particular MSK (via a MTK) and is decrypted on arrival at the UE (this may be after any repair service has done its work) before being consumed by the user either immediately in the case of streaming or when required later in the case of download. Over a period of time, a particular service will change the MSK it is using to protect the data. Once the new MSK has been taken into use, the old MSK should no longer be used as this means that any user wishing to start accessing the service would then need to be download two MSKs to be able to receive the service. If they only get one MSK, then they could receive data that they can not decrypt without the other MSK.

From this analysis it seems that it is enough to have two MSK with the same Network ID and Key Service ID stored. If a third MSK is received then the key received first of the other two keys received should be deleted.

3.2.2 Service with MSK downloaded after the data arrives

For this type of service the data is downloaded to the user and at some later time the user request the key to decrypt this data. This causes problem if the MSK management proposals from the last sections are used because there is no control over the order the data is decrypted. This causes problems with both the replay protection of MTKs and the storage of

only two MSKs. These problems would not exist, if in a service where the MSK can be fetched after the data arrives, each MSK is only used to protect only one piece of data.

A possible solution would be to download the MSK which would allow all new data to be decrypted, while any old data could be decrypted by requesting the MTK directly from the BM-SC (the feasibility of this would need study). A second solution would be to remove the replay protection for particular services if it could be removed without affecting the other services. Finally a different management of MSKs could be used for these types of download services. The best alternative for this needs further study.

3.3 Proposals for MBMS TS

It is proposed that the suggested format of an MSK identifier is accepted and included in TS along with the proposed method of handling MSKs for services that require the MSK to be on the UE when the data arrives. For other types of services, an editor's note could be added describing the problems and possible solutions. This could replace the editor's note in clause 3.1.

Editors Note: How the MSK is used for download is still under study.

4 Conclusion

This contribution proposes several changes to the MBMS TS. The exact changes are given in a pseudo CR in an accompanying document.