3GPP TSG SA WG3 Security **S3-030539**

6th – 10th October, 2003

Povoa de Varzim, Portugal

Agenda Item: 7.20

Source: Ericsson

Title: Key management considerations for MBMS

Document for: Discussion/Decision

1. Introduction

This document discusses different key management methods that are non-UICC based and UICC based. Ericsson concludes that the UICC based solutions need further studies.

Several key management methods were discussed at the SA3 Ad hoc meeting in Antwerp. Three methods received enough support to be considered further: The Simple point-to-point method proposed by Ericsson and described in [1], Combined method proposed by Nokia in [2] and the method (also called BAK method) proposed by Qualcomm in [3]. The Combined method has two variants in order to provide with a migration path: one UICC based and one non-UICC based. This paper discusses the non-UICC based methods and identifies issues on UICC based methods.

2. Discussion

2.1 Non-UICC based methods

Two methods can be used with current UICC: Simple method and non-UICC variant of the Combined method. These are described in figures 1 and 2, which are copied from the Nokia paper presented at SA3#29bis, cf. [2].

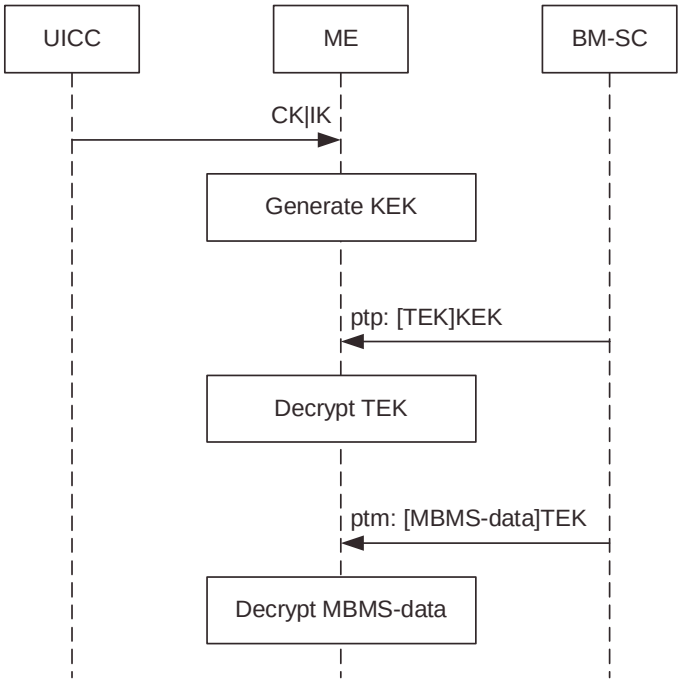

Figure 1 – Simple model sequence diagram, cf. [2]

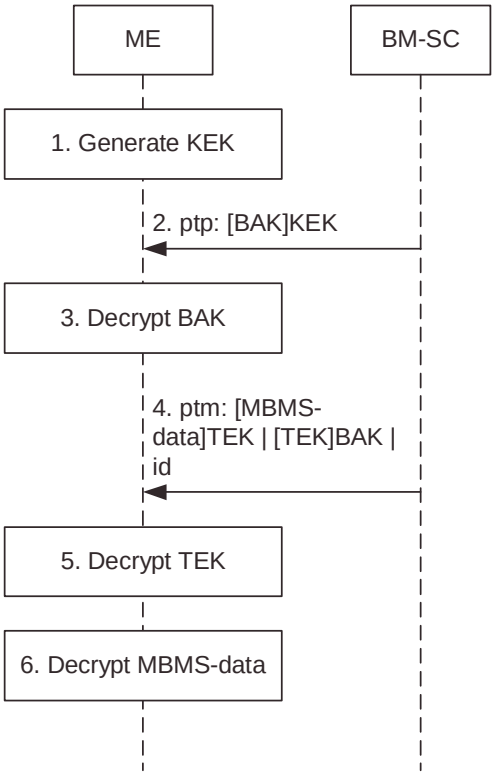

Figure 2 – The combined model with an old UICC, cf. [2]

2.1.1 Security level and point-to-point re-keying signalling load

Due to the nature of MBMS, re-keying is presumably not done when a user leaves the service. Two reasons for re-keying are:

1. Prevent or limit malicious users from leaking the keys to unauthorised users
2. Handle the subscription management in a controllable way

In the combined method proposed by Nokia the BAK is encrypted by a KEK and the encrypted BAK is transferred to the UE in a ptp fashion. The traffic encryption key TEK is encrypted by the BAK and included together with a key indicator in the traffic. Hence if the BAK is leaked to the open Internet then it means that an attacker can decrypt the traffic.

In the MIKEY based solution proposed by Ericsson then the TEK is encrypted from the network towards the mobile in a ptp fashion. Hence if the TEK is leaked to the open Internet it is possible for an attacker to listen to the content without paying anything to the operator.

Let the TEK in the combined method be denoted TEK-C and the TEK used in the MIKEY be denoted TEK-M. The frequency of changing the TEK-C is determined by the BM-SC and as long as the UE has the correct BAK it can derive the correct TEK-C. Hence the frequency of updating the TEK-C and TEK-M may vary. In particular the TEK-C will be updated more frequently. However the change of BAK is probably done with the same frequency as the TEK-M. Note that both TEK-M and BAK resides on the ME. An attacker to the Combined method would prefer to publish the BAK rather than the TEK-C.

Hence the security of point-to-point transmitted key in Combined method (BAK) and the MIKEY based scheme proposed by Ericsson is the same, since both are protected with KEK , which is stored in the ME. Hence should the ME be broken, the keys can be leaked equally easily in both solutions i.e. the *risk for key leakage* and hence the security level is equal.

Thus it can be stated that the *severity of key leakage* in Simple method and Combined method is equal i.e. if an attacker gets the TEK (Simple method) or BAK (Combined method), security is compromised and the attacker gets access to MBMS data with the same effort as a normal user.

The recovery effort from the attack is the same: a new point-to-point re-keying is required when a TEK (Simple method) or BAK (Combined method) is leaked. Note that it is equally difficult (if possible at all) in both methods to trace which user is leaking the key material. Thus *the frequency of point-to-point re-keying is assumed to be the same.*

If the KEK is leaked and the leak is traceable then a new AKA authentication needs to be run in both methods.

From a signalling point of view the Simple Method and the Combined method are equal since they require an equal amount of point-to-point signalling for updating the TEK-M and the BAK respectively.

2.1.2 Bandwidth overhead

The encrypted TEK-C needs some key identification information, probably TEK-C_id and BAK_id ([2] does not specify exactly). The exact size of this overhead in bits is FFS, but for example one recommended value for TEK in MIKEY draft is 128 bits, which is what 3GPP requires for applications that need strong security.

Hence the Combined method needs extra bandwidth overhead since the encrypted TEK together with key id's are transmitted with each MBMS data packet i.e. the overhead is bigger than in Simple method.

2.1.3 Protocol support

The MIKEY scheme proposed by Ericsson has been designed to work with SRTP for traffic encryption. It is not yet clear how the management of the TEK-C can be designed from a protocol point of view. Should SRTP be chosen as protocol for MBMS protection it could be argued that SRTP could carry the required keying information, e.g. in the MKI field.

However, SRTP does not only specify what is carried in the protocol fields, but it also specifies how to process those fields. Hence should an encrypted key be transported in the MKI field it is not what an IETF compliant SRTP receiver is expecting to receive. Thus supporting the Combined method would require either updates to SRTP or a completely new protocol should SRTP be chosen as security protocol for MBMS. Ericsson acknowledges though that no decision has yet been taken in 3GPP what protocol to use.

Should a new profile of the SRTP be necessary in order to support the Combined method, this would require a standardisation effort either in 3GPP or in IETF. It is assumed that the standardisation work in IETF would take longer time than doing it in 3GPP.

2.2 UICC based methods

Two UICC based methods have been proposed: The BAK method proposed by Qualcomm [3] and a UICC based variant of the Combined method [2].

The UICC based methods aim to have higher security since they use UICC frequently in key management of the TEK. It seems that the implications of using the UICC in the described ways are not clear and there are issues that need more studies. Ericsson highlights some open issues below that need clarification regarding UICC based key management methods. The list is not exhaustive.

- **Trust model**

UICC based solutions refer to a trust model where the ME is not trusted. Before making decisions on key management schemes the used trust model should be clarified.

- **Relation to DRM**

UICC based solutions could be suitable for high value services. At the same time OMA is defining DRM framework for protecting digital content and high value services. The relation of MBMS to DRM should be clarified.

- **Updates to UICC**

UICC based solutions seem to require extensive modifications to UICC, cf. [4]. It should be clarified whether the modifications can be done to the existing UICC e.g. by using OTA or if a new UICC is required, cf. [5].

- **Access to UICC**

UICC based solutions require frequent access to the UICC in key management. It should be clarified what are the implications of this to power consumption and other use of the USIM. The user has no control of when a MBMS service is multi-cast to the mobile. If the user is involved in other ongoing services that requires USIM usage/access, then the user experience of the services in the terminal might be suffered. It's unclear though how often re-keying would be required with the different UICC-based methods to solve potential attacks.

- **Storage of KEK**

The storage of KEK should be clarified in UICC based solutions. The BAK method uses permanently stored RK as KEK for key encryption in UICC. The vulnerability of not being able to block a leaking USIM was highlighted in Antwerp SA3 Ad hoc. The Combined method aims to use AKA to derive the KEK in the UICC. However, it is an open issue how this is done since AKA as it is currently specified does not have a key generation function for this.

- **Migration**

Backwards compatible migration path from non-UICC based solution to UICC-based solution needs to be further clarified.

3. Conclusions

The analysis in section 2.1 in this paper has shown that non-UICC based variant of the Combined method has the same security level as the Simple method. The point-to-point signalling load of the methods is also equal. However, the Combined method has more bandwidth overhead. Also protocols don't exist to support the Combined method.

A number of concerns were raised regarding to UICC based key management solutions. It is proposed that concerns raised in section 2.2 are clarified before making a decision on key management method.

4. References

[1] TD S3-030368 Introducing SRTP and MIKEY in TS 33.246, Ericsson

[2] TD S3z030020, MBMS Combined re-keying method, Nokia

[3] TD S3-030360, Levels of key hierarchy for MBMS, Qualcomm

[4] TD T3-030599, USIM enhancements for MBMS support, Schlumberger

[5] TD S3-030xxx, Draft report from SA WG3 ad hoc meeting, 3-4 September