3GPP TSG SA WG3 Security — S3#32 **S3-040096**
9-13 February 2004
Edinburgh, UK

Source: **Siemens**

Title: **MBMS: Key Replay Protection**

Document for: **Discussion and decision**

Agenda Item: **6.20 (MBMS)**

1 Introduction

SA3#31 did agree on the requirement to find a solution to guarantee session key freshness. The requirements as agreed by SA3 currently read (SP-030586):

R5h: A UICC, realizing the function of providing session keys for decrypting the streaming data at the UE, shall only give session keys back to the UE if the input values used for obtaining the session keys were fresh (have not been replayed) and came from a trusted source.

Based on the proposal contained within S3-030701 (Siemens, SA3#31), this contribution further details the solution for the above requirement and proposes some Pseudo-CR text to be incorporated into the TS 33.246.

2Requirement, Solutions and evaluation

2.1Requirement

Following changes to the requirement is proposed:

R5h: ~~A UICC, realizing~~ T~~t~~he function of providing MSKs to the ME~~session keys for decrypting the streaming data at the UE~~, shall only deliver a MSK~~give session keys back~~ to the M~~U~~E if the input values used for obtaining the MSK,~~session keys~~ were fresh (have not been replayed) and came from a trusted source.

The reason for the requirement change[1] is two-fold:

A) It was agreed at SA3#31 that the MBMS data stream structure shall be the same of ME and UICC based Key management solutions. Therefore the requirement shall be made independent on the availability of a UICC.

B) The UE has to be replaced by ME.

2.2 Solutions and Evaluation

A solution to realize the above requirement basically functions as follows (based on the initial description of S3-030701 and described under the assumption that the freshness checking function is realized in a secure environment. ***This secure environment may be the UICC or a specific trusted execution environment within the ME).***

[1] See other Siemens contribution to SA3#32 for proposed MBMS keying names (introduction of MSK).

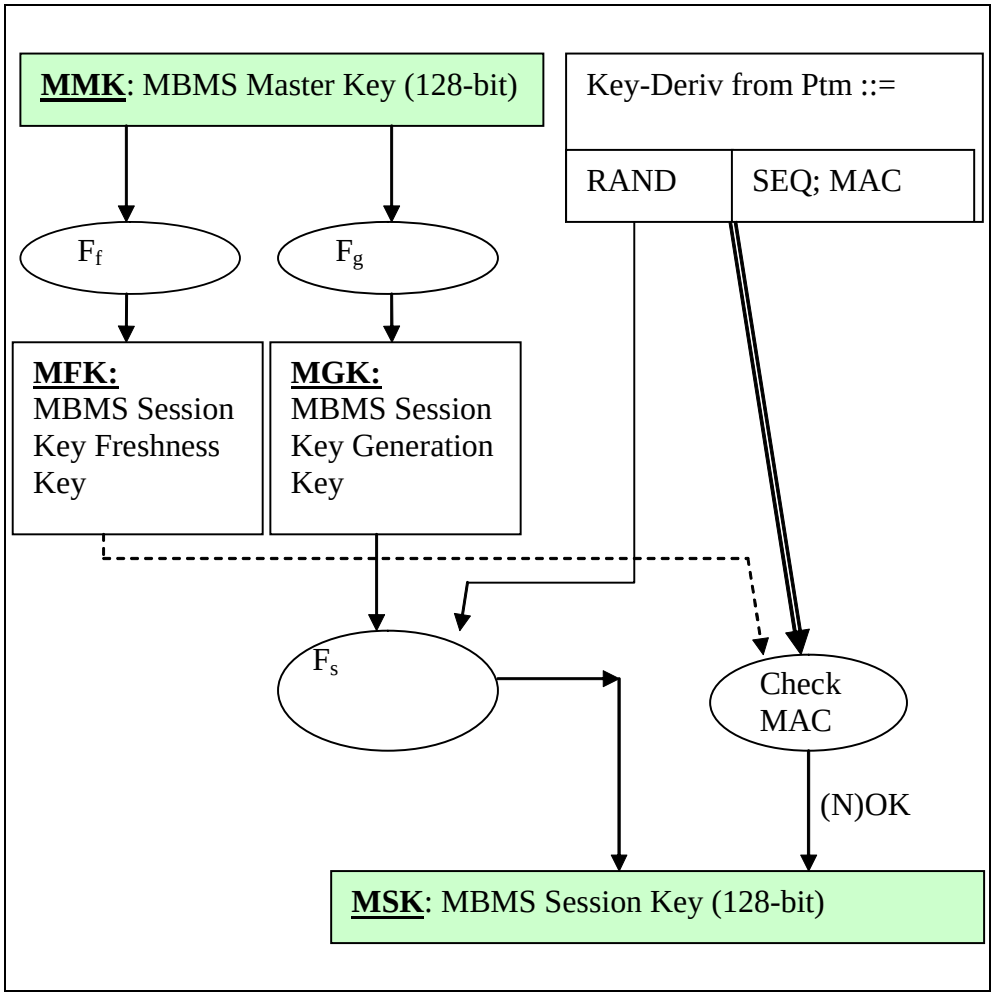

Figure 1: MSK Validation and Generation Function.

Whereas the description within S3-030701 assumed UICC storage of the MBMS Master keys, the description below introduces a '*MSK Generation and Validation Function (MGV-F)*'. This MGV-F may be realized both on the UICC and on the ME. It is assumed that this MGV-F stores the MMKs and is called MGV-S (*MGV-Storage*) further on.

The MGV-F shall only deliver the MBMS Session Keys (MSK) to the ME if the RAND [2]is deemed to be fresh. An MBMS Freshness Key (MFK) could be maintained and updated to the MGV-S similar as the MBMS Master Key (MMK). In that case both keys have to be transferred to the MGV-S during the ptp delivery to the UE. It is therefore proposed (for reasons of efficiency), that the MFK shall be derived from the MMK as well as the MBMS Session Key Generation Key (MGK). Both keys MFK and MGK will not be visible outside of the MSK validation and generation function. How the MGK and MFK shall be derived from the MMK could be asked to SAGE.

In principle the key derivation functions (F_f, F_g and F_s) may be decided by the MBMS service provider, but it is proposed to standardize these functions to avoid extra complexity, storage and signaling at the receiver[3].

---

[2] If the Nokia's combined delivery method would be chosen then RAND shall be replaced by an encrypted MSK. The key MGK would then be used to encrypt MSK and the function Fs will be realised by an encryption/decryption algorithm. This choice can be taken independent from the details of the key replay protection.

[3] Otherwise one receiver may have to download/install many key derivation functions as it may interconnect with many MBMS service providers.

The purpose of the MFK is to protect a sequence number SEQ and number RAND from tampering during transport. A keyed-hash function (F_m) with as input the MFK and SEQ/RAND shall produce a MAC value. The MBMS receiver will obtain {MMK Key-ID, SEQ, RAND, MAC} and pass all this data to the MSK Validation and Generation Function (MGV-F). The MGV-F will check the MAC validity, as well as check if SEQ is not old (has been incremented) and will only give back an MSK to the ME if the MAC and SEQ were valid.

The requirements on the SEQ-freshness check within the MGV-F are:

REQ-1. Arbitrary increments in SEQ shall be allowed

To allow the possibility that the receiver misses certain parts of the MBMS data stream and so has missed key data parts that were send along with the MBMS stream.

REQ-2. The SEQ reference value needs to be stored in loss-less memory.

Otherwise the freshness check cannot be performed reliably.

REQ-3. The MGV-S shall contain an initial value or receive an initial SEQ value when the MMK is delivered.

Otherwise the freshness check cannot be performed.

REQ-4. The SEQ reference value shall not decrement (no roll-over shall be allowed).

Otherwise the freshness check cannot be performed reliably.

Consequence of the freshness check mechanism:

CON-1.*Repetition of the same data stream cannot be done by repeating the same encrypted stream*[4].

Receivers having received a part of the data stream with a high SEQ will not be able to receive the older data (with a lower SEQ) again. The BM-SC shall take this property into account. An efficient repetition of the same data stream may be performed on the following manner: The BM-SC takes the same (stored) encrypted content by keeping the same RANDs, but using higher SEQs then used already for that MMK.

CON-2.*The ME shall be able to recognize the repetition of {MMK Key-ID,SEQ,RAND,MAC} within the MBMS ptm stream.*

Otherwise the ME will ask MSK generation for an already generated MSK, which will fail. The ME needs to store temporarily the last validated SEQ to assure an optimal handling.

CON-3. *The BM-SC needs to store and handle SEQ in a reliable way.*

The same is true for the MMK.

[4] With encrypted stream it is meant: the encrypted data including the keying data.

3 Calculation on the required length of SEQ

Each MSK-generation will use 1-bit of SEQ.

Assumed that the lifetime of one MSK will be 1 Minute[5], then for an MMK lifetime of 1 day of continuous RTP traffic, 1440 MSK generations will take place. A SEQ of 16-bit will allow 65536 MSK generations.

MSK generation Frequency and SEQ-length → Max MMK lifetime	8-bit SEQ (256 MMKs)	16-bit SEQ (65536 MMKs)
10 seconds	42 minutes	7,5 days
1 Minute	4 hours	45 days
10 Minutes	40 Hours	15 months

It is proposed that a SEQ length of 16-bit shall be adopted.

Total length calculation for {MMK Key-ID, SEQ, RAND, MAC}

- MMK KEY-ID: Minimum 2-Bit
- SEQ: 16-bit
- RAND[6]: 32-bit.
- MAC: 32-bit.

A total of 84-bit is needed for the ptm multipoint rekeying messages!

As was suggested in the discussions of previous SA3-meeting, as an optimization both SEQ and RAND may be used as input to the MSK-generation function (Fs). As indicated by the analysis in CON-1 this will create inflexibility at the BM-SC. The BM-SC will not be able to take the stored encrypted content generated[7] at the first streaming with a certain RAND and stream it a second time with modifying only the SEQ. The optimization in amount of bits would be only 32-bits per MSK rekeying period [8]. It is therefore proposed not to use the SEQ as additional input to the MSK generation function.

[5] The assumption made in S3-030580 (Overhead of re-keying (Nokia), Povoa) was 10 minutes

[6] When using MGK[MSK] then 128-64 extra bit will be required.

[7] With the combined keying method proposed by Nokia the MGK[MSK] could be stored and need only be protected again using Integrity protected SEQs.

[8] Possibly multiplied by a repetition rate to assure reliable Keying input

4 Pseudo-CR text for session key freshness

4.1 Pseudo-CR text in case the SK_RAND model is chosen

New section 6.3: Key generation and validation at the UE

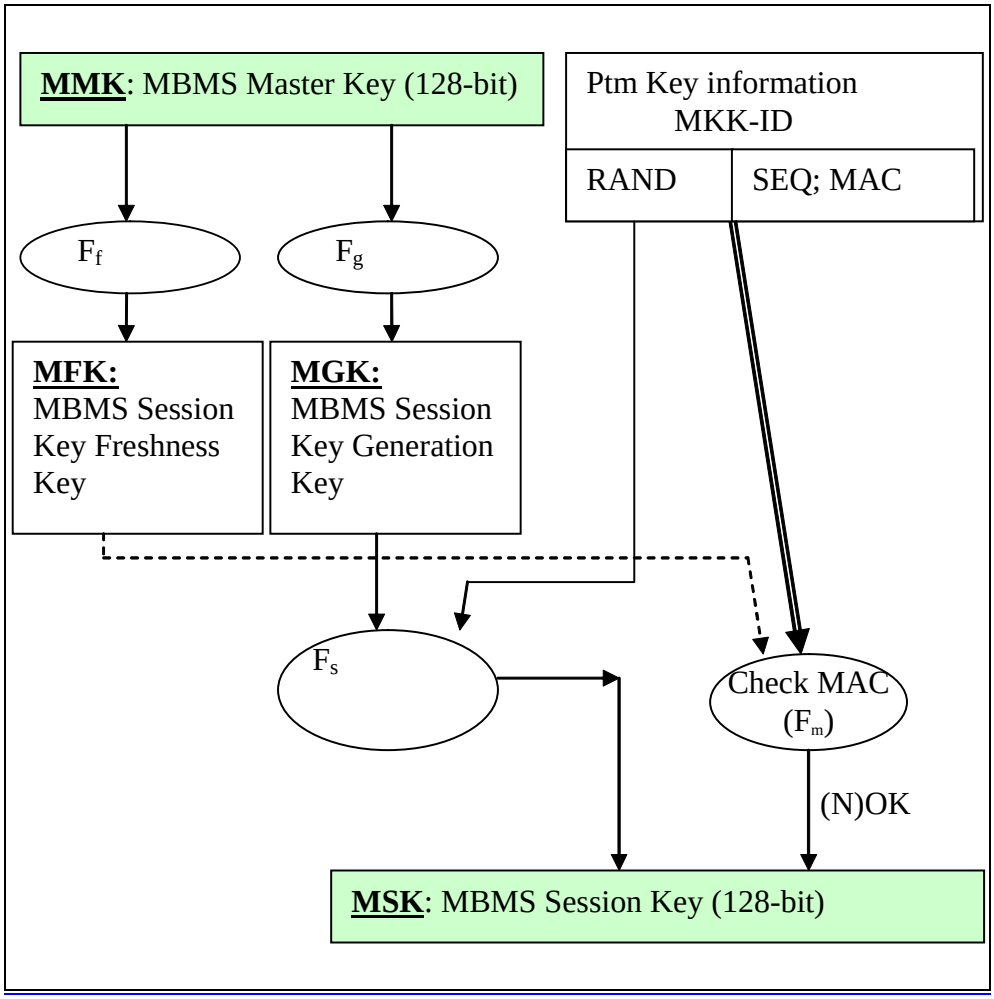

Figure 2: MSK Validation and Generation Function.

The ME will call the (*MSK Generation and Validation Function)* MGV-F that is realized as part of the ME or as part of the UICC. It is assumed that the MBMS service specific data, MKK and the sequence number SEQs, have been stored within a secure storage (MGV-S). This MGV-S may be realized on the ME or on the UICC but for certain type of MBMS services the UICC shall be used as determined by the service provider. Both MKK and SEQs were transferred to the MGV-S with the execution of the key update procedures as described in section 6.1. The initial value of SEQs is determined by the service provider.

When the ME receives {MMK Key-ID, SEQp, RAND, MAC} from the ptm data stream, it shall give that information to the MGV-F. The MGV-F shall only deliver the MBMS Session Keys (MSK) to the ME if the ptm-key information is deemed to be fresh. How this shall be done is described below:

The MGV-F shall derive a key MFK (MBMS session key Freshness Key) from the MKK using a key derivation function F_f, and shall derive a key MGK (MBMS session key Generation Key) from the MKK using a key derivation function F_g.

The session key generation shall be performed in the following way:

The session key generation function F_s uses RAND and the key MGK as input to produce MBMS Session key MSK.

The freshness check shall be performed in the following way:

Using a keyed MAC function f_m with the inputs SEQ, RAND and the key MGK, a MAC is calculated. This MAC is compared with the one received from the ptm key information. If the MAC defers then the MGV-F will indicate a failure to the ME. If the MAC is equal then the MGV-F shall compare the received SEQp from the ptm key information with the stored SEQs. If SEQp is greater than SEQs than the MGV-F shall update SEQs with SEQp value and start with the generation of MSK. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME.

4.2 Pseudo-CR text in case the combined model is chosen

New section 6.3: Key generation and validation at the UE

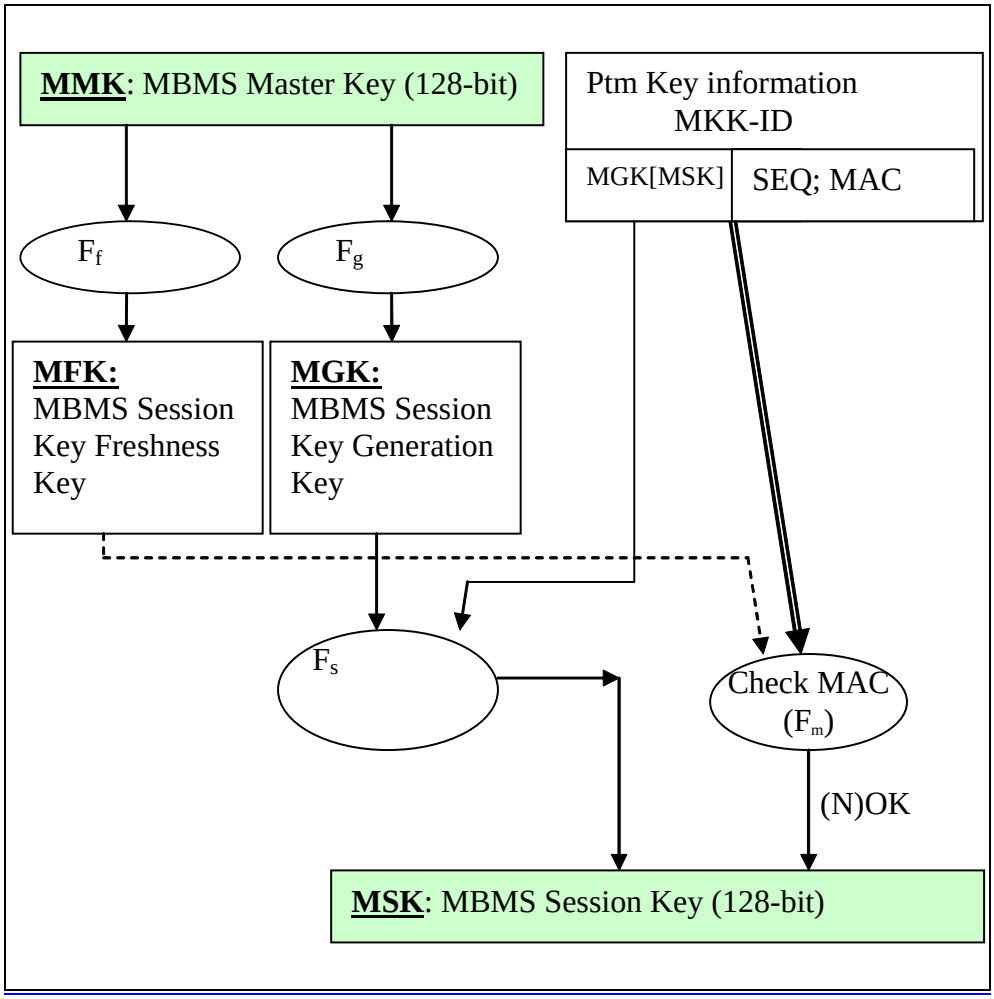

Figure 3: MSK Validation and Generation Function.

The ME will call the *(MSK Generation and Validation Function)* MGV-F that is realized as part of the ME or as part of the UICC. It is assumed that the MBMS service specific data, MKK and the sequence number SEQs, have been stored within a secure storage (MGV-S). This MGV-S may be realized on the ME or on the UICC but for certain type of MBMS services the UICC shall be used as determined by the service provider. Both MKK and SEQs were transferred to the MGV-S with the execution of the key update procedures as described in section 6.1. The initial value of SEQs is determined by the service provider.

When the ME receives {MMK Key-ID, SEQp, MGK[MSK], MAC} from the ptm data stream, it shall give that information to the MGV-F. The MGV-F shall only deliver the MBMS Session Keys (MSK) to the ME if the ptm-key information is deemed to be fresh. How this shall be done is described below:

The MGV-F shall derive a key MFK (MBMS session key Freshness Key) from the MKK using a key derivation function F_f, and shall derive a key MGK (MBMS session key Generation Key) from the MKK using a key derivation function F_g.

The session key generation shall be performed in the following way:

The session key decrypt function F_s decrypts the received MGK[MSK] to obtain MSK.

The freshness check shall be performed in the following way:

Using a keyed MAC function f_m with the inputs SEQ, RAND and the key MGK, a MAC is calculated. This MAC is compared with the one received from the ptm key information. If the MAC defers then the MGV-F will indicate a failure to the ME. If the MAC is equal then the MGV-F shall compare the received SEQp from the ptm key information with the stored SEQs. If SEQp is greater than SEQs than the MGV-F shall update SEQs with SEQp value and start with the generation of MSK. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME.

5 Conclusion

Siemens proposes

A) to accept the modifications to requirement R5h, as listed in Section 2.1 of this contribution.

B) to adopt one of the Pseudo-CR's as listed in section 4.1 respectively section 4.2, depending on the two-tiered model that is chosen by SA3#32. If SA3#32 does not take a decision on the two-tiered model, then it is proposed to add both alternatives to the MBMS security specification and add an editors note to describe the outstanding decision.

C) to adopt the working assumption NOT to use both SEQ and RAND as a seed for the MSK generation but only to use RAND, if the SK_RAND model would be chosen by SA3 (relates to section 4.1)

D) to decide on how to realize functions Ff, Fg, Fs, F_m. A possibility could be to ask ETSI SAGE to take on the work to specify these functions. In principle, the key derivation functions (F_f, F_g, F_s, F_m) may be decided by the MBMS service provider, but it is proposed to standardize these functions.