3GPP TSG SA WG3 Security — adhoc **S3z030020**

3-4 September 2003

Antwerp, Belgium

Source: **Nokia**

Title: **MBMS – Combined Re-keying Method**

Document for: **Discussion**

Agenda Item: **6.3**

1. INTRODUCTION

This discussion paper compares different re-keying methods: two-tiered [1], simple point-to-point model [2], LKH [3] and hybrid MBMS key management scheme [4]. A combined re-keying method is also presented, which tries to combine good aspects of two-tiered and simple point-to-point methods.

2. COMPARISON

2.1 Two-Tiered Method

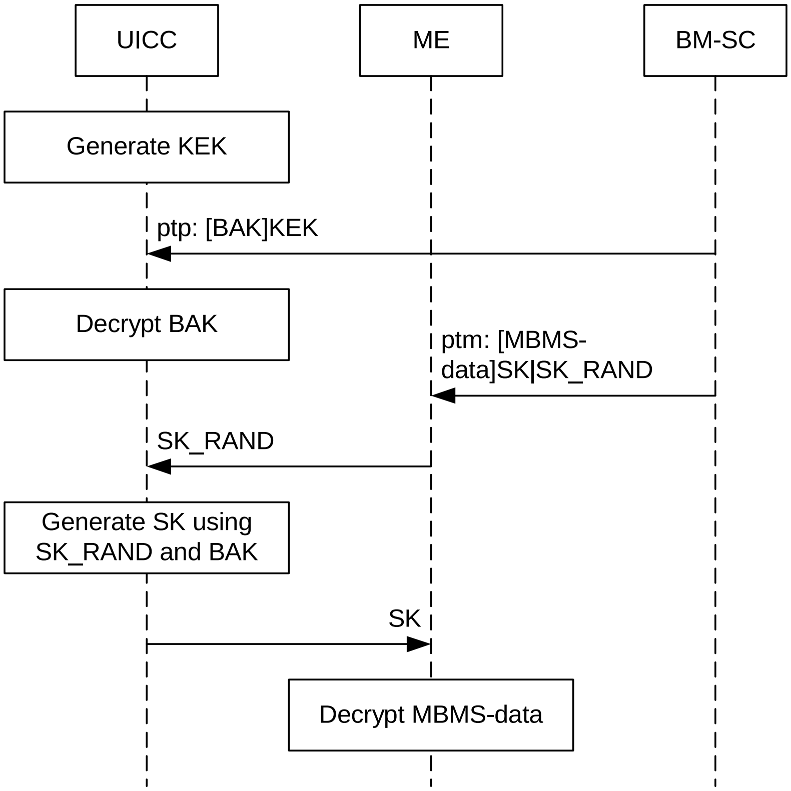

Figure 1 – Two-tiered model sequence diagram

In the two-tiered method [1], a key encryption key (KEK) is generated by the UICC and it is stored inside the UICC. The two-tiered method uses point-to-point messages to deliver BAKs to the UICC. The UICC decrypts the BAK using the KEK. MBMS data is delivered using multicast and data is encrypted using a session key (SK). MBMS data packet contains also SK_RAND in clear text. If the ME has not the current SK, it can request a new SK from the UICC. The UICC generates the SK using the BAK and SK_RAND and delivers it to the ME. After that the ME can decrypt MBMS data using the SK.

The two-tiered method requires change of UICCs, thus introduction cost is high, but re-keying is very fast, because every MBMS data packet can contain SK_RAND. However, if an attacker breaks one UICC and leaks out the BAK, then re-keying is as slow as in the simple point-to-point method because BAK has to be replaced. It should be stressed here that re-keying of BAK is only useful if the "leaking" UICC has been identified somehow first.

2.2 Simple Point-to-Point Method

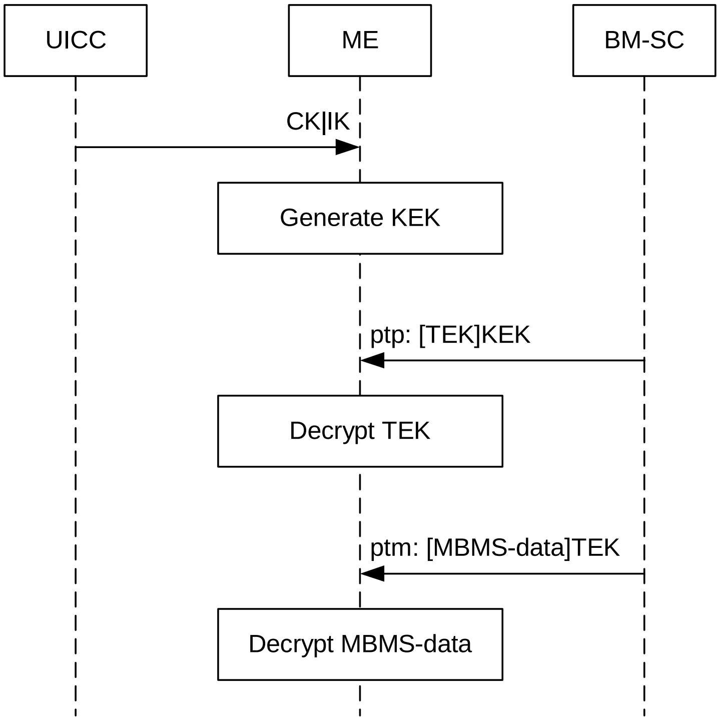

Figure 2 – Simple model sequence diagram

In the simple point-to-point method, a key encryption key (KEK) is generated by the ME. The simple method uses point-to-point messages to deliver encrypted traffic encryption keys (TEKs) to the ME. The ME decrypts the TEK using the KEK. MBMS data is delivered using multicast and data is encrypted using a TEK. The ME can decrypt MBMS data using the TEK.

The simple method has slow re-keying and it may cause heavy load on the RAN if re-keying is performed very frequently.

2.3 LKH

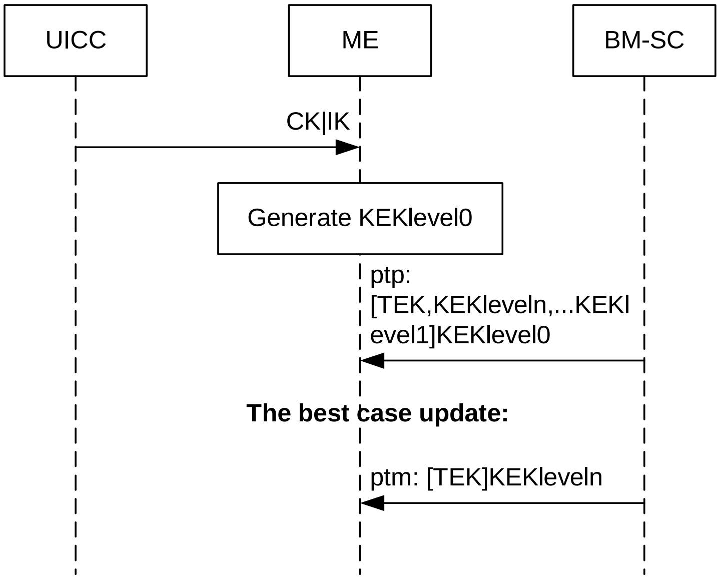

Figure 3 – LKH sequence diagram

In the LKH method, the lowest level key encryption key (KEKlevel0) is generated by the ME and it is stored inside the ME. The LKH uses point-to-point messages to deliver level 1 key encryption keys and point-to-multipoint messages to deliver above keys (level 2 and above), see the Figures 3 and 4. The highest key is a TEK in the key tree and MBMS data is encrypted using it.

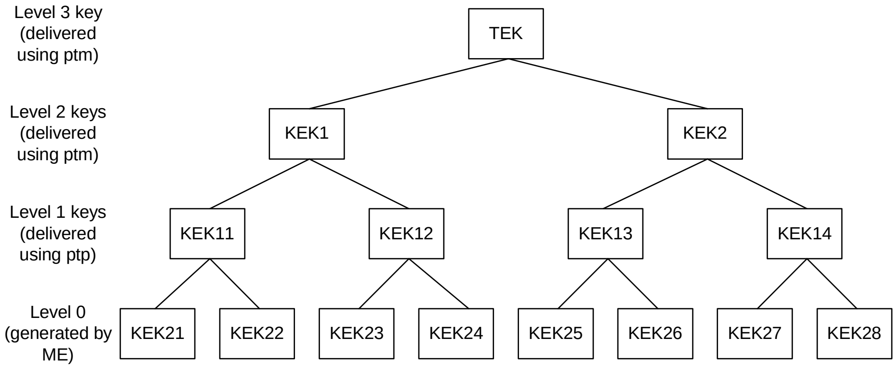
Level 3 key (delivered using ptm)
Level 2 keys (delivered using ptm)
Level 1 keys (delivered using ptp)
Level 0 (generated by ME)
TEK
KEK1
KEK2
KEK11
KEK12
KEK13
KEK14
KEK21
KEK22
KEK23
KEK24
KEK25
KEK26
KEK27
KEK28

Figure 4 - Key Tree

One of the design goals of the LKH was to minimize a number of re-keying messages after a user has left the service. However, this kind of re-keying functionality is unrealistic in the MBMS context. Therefore, LKH model falls back to simple point-to-point re-keying, because users cannot be trusted and users who are leaking keys are typically not traceable. In fact, LKH causes more traffic than the simple point-to-point method, because LKH has multiple key encryption keys. For example: If MBMS service has 100 000 users and every key has two sub keys (i.e. we use a binary tree) then 100 000 point-to-point messages must be sent and every message must contain 17 keys, see RFC 2627 [5], section 5.4.1.

2.4 Hybrid

In the hybrid model [4], a KSO is generated by the ME. The hybrid method uses point-to-point messages to deliver encrypted group sealing key for OTAR (GSKO) to the ME. The ME decrypts GSKO using the KSO. Encrypted TEKs are delivered using point-to-multipoint messages and the ME can decrypt these messages using the GSKO. MBMS data is delivered using multicast and data is encrypted using a TEK. The ME can decrypt MBMS data using the TEK.

The hybrid method is similar to LKH in case the latter has only three layers. It also contains aspects of the two-tiered method if the KSO and/or GSKO are stored in the UICC.

The hybrid method also contains solutions for recovery from situations where the user has not received a key intended to him/her.

2.5 Summary of comparison

The two-tiered, simple point-to-point and hybrid methods can fulfil general security requirements (all keys are uniquely identifiable, regular change of keys, re-keying etc.), but the LKH performance enhancements in re-keying exist only if legitimate users can be trusted. Re-keying methods are compared against the speed, complexity and re-keying reliability in the following table.

	Two-tiered	Simple ptp	LKH	Hybrid
Speed of re-keying in situations where no compromise has happened	Fast (every MBMS data packet contains SK_RAND)	Slow (re-keying using ptp)	Fast (multicast messages protected by high level keys)	Fast
Speed of re-keying if a traitor is leaking all available keys	Fast (Slow if UICC broken and BAK is leaked)	Slow	Slow (even slower than simple ptp, because there are more keys to encrypt and deliver)	Slow (GSKOs are delivered with ptp messages)
Complexity	Simple	Very simple	Complex (many keys to handle, complex key hierarchy)	Complex (on the part of key overlapping, key request)
Reliable key delivery	Yes (ptp for BAK and every MBMS data packet contains SK_RAND)	Yes (ptp)	Requires reliable multicast	Yes (UE requests a new key if multicast message was not received)
Other issues	Requires change of	-	Works well only if	-

	UICCs		legitimate users can be trusted	

3. COMBINED METHOD

The combined method is designed to combine fast and reliable re-keying of two-tiered and low cost of introduction of simple point-to-point method.

Low value MBMS services can allow KEK generation and storage of BAK in the ME, but high value MBMS services can require KEK generation and storage of BAK in the UICC.

This requires that BAK for low value services (BAK_low) is different from the BAK for high value services (BAK_high). Therefore, we have the following cases:

1. For ME with an old UICC only low value services can be accessed; ME contains BAK_low.
2. For ME with a new UICC, all services may be accessed; UICC contains BAK_high and ME (or UICC) contains BAK_low.

The Figure 5 shows combined method with an old UICC:

1. The ME generates a KEK
2. The ME receives a new BAK, which is encrypted using the KEK
3. The ME decrypts the BAK
4. The ME receives a MBMS data packet, which contains encrypted MBMS data, an encrypted TEK and necessary key identification information in clear text
5. If the ME has not the current TEK then it decrypts the TEK using the BAK
6. The ME decrypts MBMS data using the TEK

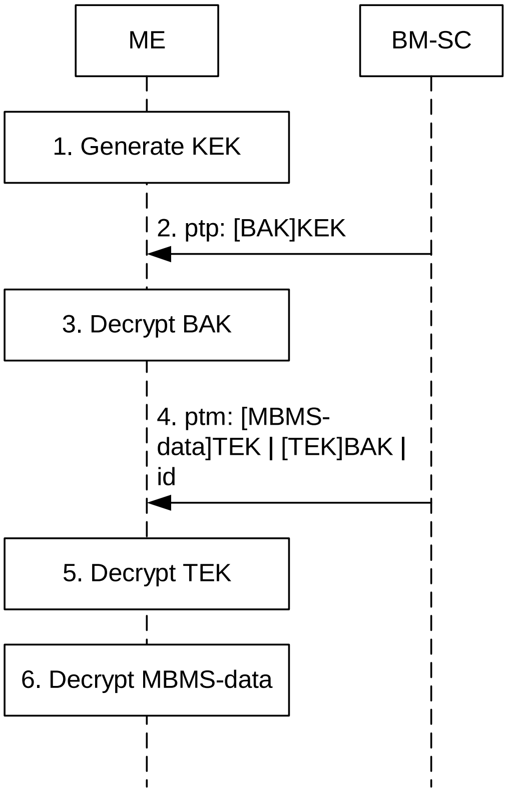

Figure 5 - The combined model with an old UICC

The Figure 6 shows combined method with an old UICC:

1. The UICC generates a KEK
2. The UICC receives an encrypted BAK
3. The UICC decrypts the BAK using the KEK
4. The ME receives encrypted MBMS data, encrypted TEK and necessary key identification information in the clear text
5. If the ME has not the current TEK then it sends a request to the UICC
6. The UICC decrypts the new TEK
7. The ME receives the new TEK
8. The ME decrypts MBMS data

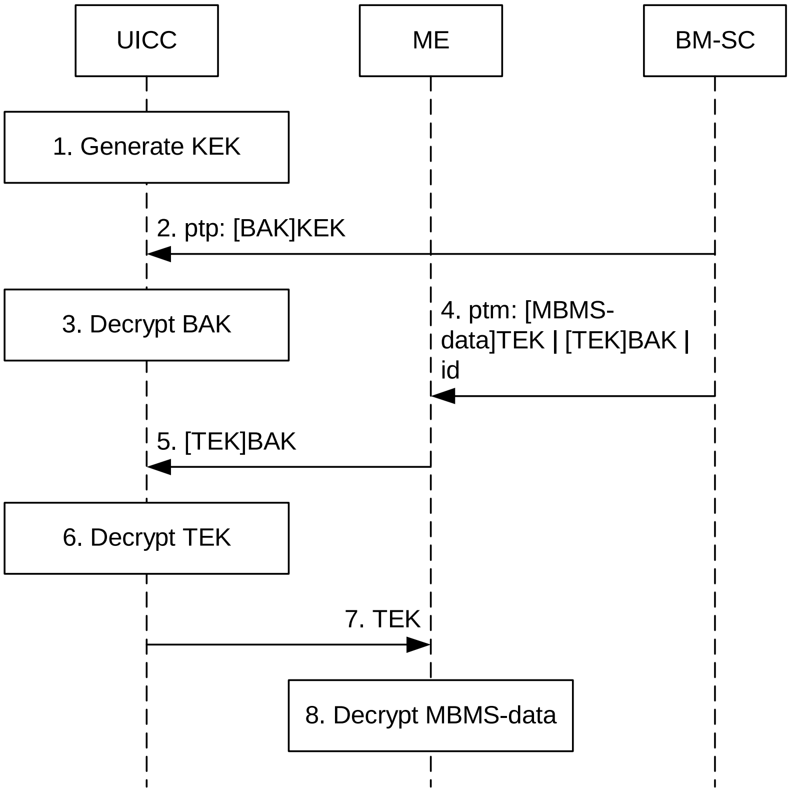

Figure 6 - The combined model with a new UICC

4. REFERENCES

[1] TDoc S3-030360, Levels of Key Hierarchy for MBMS, Qualcomm

[2] TDoc S3-030349, MBMS re-keying: PTP with periodic re-keying, Huawei

[3] TDoc S3-030286, Further consideration of LKH for MBMS re-keying, Samsung

[4] TDoc S3-030335, Hybrid MBMS Key Management Scheme, BT Group

[5] IETF RFC 2627, Key Management for Multicast: Issues and Architectures