3GPP TSG SA WG3 Security — S3#31 **S3-030700**
18 - 21 November 2003
Munich, Germany

Agenda Item: 6.20

Source: Siemens

Title: MBMS (re-)keying models

Document for: Discussion/Decision

1. Introduction

At the SA3 meeting in Povoa no decisions where taken to select a (re-)keying model. This contribution provides an analysis to come to a decision on the used model. Section 2 compares different solutions and intentionally distinguishes between a UE and a UICC based solution. In section 3 the co-existence of UE and UICC-based solutions is discussed.

2. Re-keying models for streaming

This section discusses the alternative (re-)keying solutions. The solutions that are currently on the table are the SK_RAND model, the combined model and a simple ptp model. In principle all three models can be realized both on UE and UICC.

a) SK_RAND model: This two-tiered model uses a key BAK as master key to generate a session key from a received RAND. The session key encrypts the actual streaming data. The key BAK has to be transferred by other means and in advance to the MBMS user using a secure authenticated ptp delivery.

b) Combined model: This two-tiered model uses a key BAK to encrypt the actual TEK during ptm streaming delivery. The key BAK has to be transferred by other means and in advance to the MBMS user using a secure ptp delivery.

c) Simple ptp model: This one-tiered model uses an authenticated ptp connection to transmit a key TEK to the MBMS user.

An important point for evaluation of the models was provided by an LS from S1 to SA3 (LS S1-030997 says "***In keeping with the purpose of MBMS, it is preferable that security and charging mechanisms make efficient use of the radio spectrum by minimising two-way traffic***").

2.1 UE-based solutions

As was highlighted by contribution S3-030539 (Ericsson) to SA3#30 the provided security of the combined model, the SK_RAND model and the simple ptp model are the same for a UE-based keying solution. If the assumption is that UE-keys are stored insecure (*a worst-case insecurity assumption*), then the highest level key from the two-tiered model will be distributed by the malicious mobile, so it doesn't matter if a two tiered model is available. Models (a) and (b) will only add additional bytes to the stream and require extra UE-processing without providing additional security. To provide the same level of security all mentioned models have to re-key the highest level ptp-key with the same frequency.

Proposed principle[1]: 'For UE-based keying solutions the ptp-rekeying shall be as efficient as possible in viewpoint of consumed radio resources. The ptm-rekeying of a second level key will not add to security under the worst-case 'insecurity assumption' of the UE. A decision in favour of a two-tiered

[1] In case only a UE-based solution would be developed.

model for a UE-based solution cannot be defended from a viewpoint of security and performance but may be decided to ensure compatibility with a UICC based solution'

The security level is not augmented for the two-tiered model that requires at the same time a higher UE-performance. **For a UE-based solution the adaptation of DRM methods should be considered as they are specifically designed to run in a UE-based environment**. *The required amount of signalling to get the DRM rights objects to the UE should be comparable to the required ptp key delivery as the main cost is the ptp set-up. Both RO-transfer and MBMS key transfer shall happen before the streaming starts*. DRM does not have a streaming solution yet, but the PSS solution may be reusable. For MBMS download, the solutions provided by OMA DRMDL seems to be usable.

2.2 UICC-based solutions

In this case a two-tiered model makes sense as the highest level key can be stored (*the best-case assumption*) securely on the UICC, where the actual decryption key for streaming is used on the UE. Furthermore, both combined and SK_RAND model take advantage of the adding additional data to the ptm data stream. In this way both models make an efficient use of radio resources. There seems to be no major difference in security and required performance at UE and UICC for both models.

Proposed principle: 'The design of a UICC-based solution shall take care that the security is as high as possible but the solution shall at the same time be cost-efficient[2]. This requires that the costs involved by a UICC based solution are fully understood.'

The MBMS market cannot risk that this model would be flawed. In particular; there has to be a way to relatively easy recover from a situation where one UICC has been completely broken. The one-tiered ptp model does not fulfil this requirement with current technology. **[3]**

2.3 Deciding on UE and/or UICC-based solutions

SA3's decision to select one or both solutions for securing MBMS streaming data may be guided by various arguments as are cost, complexity, market demand, migration possibility, compatibility, time pressure for realization and charging possibilities. This could result in one of following decisions (this list may not be extensive):

a) Only provide a UE-based keying solution for streaming within Rel-6.

b) Only provide a UICC-based keying solution for streaming.

c) Provide a UE-Based keying solution for streaming within Rel-6 and a UICC based keying solution within a later release.

d) Provide both a UE-based and a UICC based keying solution within Rel-6.

The argument that speaks in favour of an UICC-based solution (option (b)) is enhanced security. But is this really needed by the market at the moment? The cost and complexity of UICC-based solutions seems an overkill regarding the expected value of the content for the first streaming services. Given that the list of open issues for a UICC-based solution was still large after SA3#30, deciding for a UICC-based solution may risk an incomplete solution within Rel-6 timeframe. This contradicts the proposed principle from previous section that the 'design of a UICC-based solution shall take care that the security is as high as possible and that the costs of such a solution are fully understood'. Realizing Option (d) is even more challenging.

Conclusion: A UICC-based solution could be a migration path if MBMS streaming gets known by the customers. Option (c) looks the most preferable under the condition that the migration issues can be solved at this meeting. Also a co-existence analysis needs to be made. Section 4 provides a first start.

---

[2] **With respect to costs involved by the manual distribution and updating of UICCs.**

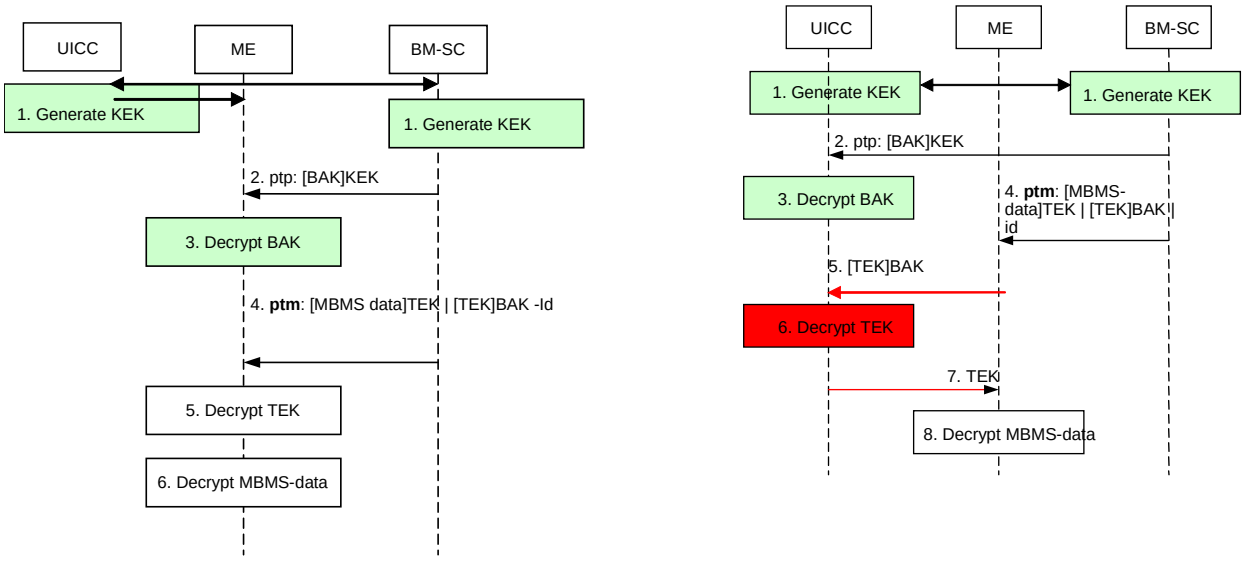
[3] **It is supposed thereby that decryption of the data stream is still not feasible with current smart card technology at acceptable card cost.**

The above conclusion assumes that compatibility between the two solutions can be reached. This is surely a must for the actual ptm data-stream and assumes that we know now which parameters are needed for a UICC-based solution. There is certainly an advantage from the network point of view if the UICC based and the UE-based solution use similar mechanisms. The next section discusses the co-existence consequences and derives some requirements on the UICC-based solution.

3. Co-existence of terminal and UICC based solutions

In a UICC-based concept a key has to be securely transferred to the card and may never leave the card. The terminal interacts with the MBMS functions on the UICC asking to give back the current key with which the traffic has been encrypted.

The pictures below shows the combined model realized with ME and with UICC based key storage.



Note that if OTA would be used for step 1 then the ‘generate KEK’ step could be called ‘transfer KEK’.

Note also that in the left-hand side figure the ‘generate KEK’ step could be realized by GBA-mechanism.

Below we explain why the critical step in viewpoint of security for a UICC-based solution is the ‘Generate KEK’-step.

Following requirement seem to apply with co-existing solutions: **It shall not be possible for a malicious UE to defeat the network such that the KEK can be retrieved making the BM-SC think the key was stored securely at the UICC and was not given out to the ME**. A requirement on the ptp key delivery procedures for the ‘generate KEK’-step is that the BM-SC shall be reliably informed about whether the key KEK has been securely stored on the UICC (and not be given out on the ME). A possible solution may be to incorporate some assertion from the UICC which can only be generated by using some key material that already resides in the UICC. The UE shall not be able to simulate or replay any assertion during that procedure.
Furthermore it may **be important from the viewpoint of service subscription to know from the operators viewpoint if a UE based MBMS application or UICC based MBMS application is involved**. This is important if the operators want to multicast the more valued service only to those users involving a UICC-based solution. If both UICC and UE based solutions have access to the same service, then the BAK/KEK may be leaked through the less secure solution.

Careful design may be needed to guarantee the above requirements. It may end up with two different protocols for the ‘generate-KEK’-step for both UICC and ME-based solution.

4. Conclusions

Siemens proposes to adopt following working assumptions:

- If only a UE-based solution will be developed then the ptp (re)-keying solution shall be as efficient as possible in viewpoint of consumed radio resources’. For a UE-based solution the adoption of DRM methods should be considered as they are specifically designed to run in a UE-based environment. In particular the OMA DRMDL solution should be considered for MBMS download, while for MBMS streaming more study is needed.

- If a UICC-based solution will be developed then the design of a UICC-based solution shall take care that the security is as high as possible but the solution shall at the same time be cost-efficient. In particular there has to be a way to recover from the situation where secrets from within one single UICC are revealed by an attacker.

Following requirement for a UICC-based solution (to be incorporated within TS 33.246) is proposed:

- The ptp key delivery procedures for the ‘generate KEK’-step shall give assurance to the BM-SC where the KEK has been stored. The UE shall not be able to simulate or replay any assurance indication during that procedure.