3GPP TSG SA WG3 Security#30 **S3-030583**
6 – 10 October, 2003
Povoa de Varzim, Portugal

Agenda Item: 7.20

Source: Siemens

Title: Key distribution protocol selection

Document for: Discussion/Decision

1. Introduction

At the SA3 Adhoc in Antwerp no key distribution protocol was selected. Ericsson [S3z030027] proposed that the MIKEY protocol should be used. OTA methods (See TS 23.048) could be used as well as indicated by some other companies. This document analyses the aforementioned proposals (section 3). Before the evaluation is started, some relevant requirements from different documents are highlighted (section 2).

2. Requirements

This section covers various requirements that are thought useful in evaluating the different candidate solutions.

Req-1: [TS22.146 V6.2.0] Section 6: '*In case of roaming a user should also be able to subscribe and join Multicast Services that are provided locally in the visited network, as allowed by the user's home environment.*'

Req-2: [LS From SA1 to SA3: S1-030997]: *'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.*'

Req-3: [TS 22.246 V1.0.0 MBMS users services: SP-030511]: This specification describes services that can be delivered to the UE via mechanisms specified in TS 22.146 and TS 23.246. The specification contains many example applications and contains an explicit reference to the use of DRM.

Following requirements could therefore be derived from TS 22.246 usecases:

A) The MBMS keying function (i.e. including the key distribution protocol) shall be a function that applications may use but don't need. An application may also implement own means.

B) The MBMS keying function shall not be incompatible with the use of DRM.

C) The MBMS keying function should be general enough to be useful for many applications.

Req-4: [TS 33.246 V0.2.0: S3z030028 Section 4.1.4]:

'R4a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected.

R4b: The transfer of the MBMS keys between the MBMS key generator and the UE may be integrity protected.

R4c: The UE and MBMS key generator shall support re-keying to ensure that users that have joined a multicast service, but then left, shall not gain further access to the multicast service without being charged appropriately. The re-keying shall also ensure that users joining a multicast service shall not gain access to data from previous transmissions in the multicast service without having been charged appropriately

R4d: Only authorized users that have joined an MBMS multicast service shall be able to receive MBMS keys delivered from the MBMS key generator.

R4e: The MBMS key encryption key shall not allow the BM-SC to infer any information about used UE-keys at radio level (i.e. if they would be derived from it).'

3. Evaluation

This section discusses the alternatives protocols to transport a Key Encryption Key (KEK) or BAK to the UICC or Terminal. The alternatives proposals as known from the SA3 Adhoc in Antwerp were: OTA and MIKEY.

3.1 OTA

A) The use of OTA may cause delays in initial keying or re-keying.
Secure OTA uses secured SMS messages. The transport of SMS has no real-time constraints but uses a push and forward mechanism in the network. If an MBMS user wants to join an already ongoing service then it is unacceptable to receive the BAK/TEK many minutes later. If the delivery latency is low and kept within know acceptable time boundaries then this would pose no problem.

B) OTA does not need an active PDP context.
While OTA bases on SMS, the (re-)keying messages can be delivered whenever the MS is attached to the network. This provides an advantage over solutions that require an active PDP context (e.g. MIKEY, https) as less network resources need to be allocated.

C) The OTA encryption method may be operator specific which limits the use of updating UICC information to HN-services.
The used encryption algorithm within OTA is either proprietary, DES or 3DES. In case only an operator specific algorithm has been pre-configured on the card this poses a problem while within the MBMS model the user shall be able to obtain services from the VN. This will require that HN OTA-servers shall be involved even for MBMS services provided by a visited network.

D) OTA uses a two-layer concept for securing the SMS messages (See TS 23.048) based on HN managed secret keys. Using this for VN-MBMS services seems very inefficient and is in contradiction with the required E2E confidentiality of the MBMS keys.
There are pre-configured keys available (KIK i.e. layer 1) at the UICC that are used to update confidentiality and integrity keys (i.e. layer 2) to the UICC. The layer 2 keys are then used by the sending entity in the network that wants to use secure OTA (e.g. sending secure SMS messages). Typically this is the SMS centre which resides in the HN. Req-1 specifies that the BM-SC may reside outside the HN which contradicts the layer 2 key characteristics which are HN owned and requires an OTA-server which resides in the HN. Figure 1 provides such a configuration that overcomes the key ownership problem. For VN MBMS services the VN will have to interconnect to the OTA-server in the HN of the subscriber for updating the first layer of MBMS keys. **The HN operator will get access to all MBMS keys, even for services from a neighbouring operator's network**. This contradicts Req-4. This problem could be overcome by doing a GBA-run and use dynamically established keys between the MBMS key sender and the receiver to protect the first level of MBMS key. This will however require changes to OTA to be able to refer and use these generated GBA-keys.

E) The use of OTA needs to be supplemented by a terminal mechanism that requests key updates.
Such a mechanism is necessary to allow the terminal to re-synchronise keys after detecting that it has missed a key update. This functionality need to be implemented in the terminal as the UICC is a passive actor. This is not a disadvantage of OTA but due to the UICC characteristics.

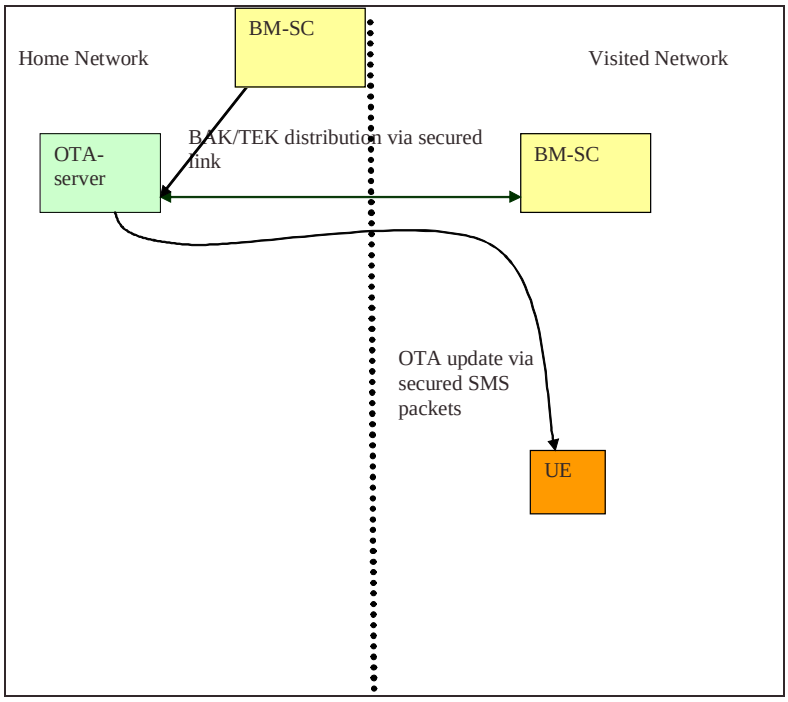

Figure 1: Using OTA server for VN MBMS services

3.2 MIKEY

This section looks specifically at the issues that arise when MIKEY would be selected as a key distribution protocol that terminates at the UICC. The MIKEY-protocol is lightweight, flexible in use and conforms to the requirements listed in section 2.

A) **This will require that AES and Hashing algorithm shall be implemented on the UICC**.
For use in OTA the algorithms DES, 3DES have been implemented on the UICC already. So this should not pose any problem.

B) **The use of MIKEY can provide real E2E key transport security between the Sending entity in the VN and the UE.**
But in order to bootstrap this E2E transport, the sending entity and the UE need a shared secret which may be supplied by a GBA-run. For OTA, these secrets were already in place on the card but posed a problem for VN-MBMS services! Exact mechanism how to bootstrap keys to the UICC for use in MBMS are for ffs.

C) **MIKEY over http needs a active PDP context**
This is less efficient then OTA and not typical to a UICC implementation.

4. Conclusions

OTA has been restricted by design to be used only by the Home Network. If OTA would be selected as the Key distribution mechanism to transfer an MBMS key to the card then many application servers will need to be connected to the HN OTA server. The OTA server in the HN will also get knowledge of MBMS keys of VN MBMS services.

Siemens proposes that OTA should not be adopted as a solution to update MBMS keys to the UICC or to the terminal.