3GPP TSG-SA WG3 Meeting S3#37
Sophia, France, 21-25 February, 2005

Tdoc ⌘S3-050090

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**051**	⌘**rev**	**-** ⌘	Current version: **6.1.0** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Alignment to SA4 terminology		
Source:	⌘	Ericsson		
Work item code:	⌘	MBMS	***Date:*** ⌘	14/2/2005
Category:	⌘	**D**	***Release:*** ⌘	Rel-6
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *Ph2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)* *Rel-7 (Release 7)*

Reason for change:	⌘	SA3 TS 33.246 describes how the MBMS user services described in SA4 TS are protected. The terminology of the specifications should be consistent.
Summary of change:	⌘	• MBMS multicast service is corrected to MBMS user service • Post delivery procedure is corrected to Associated delivery procedure • All references to application layer joining are removed since should procedure does not exist in SA4 terminology In case some other CRs modify the same text as this CR, it is proposed that the correct terminology is used in the other CR and the modification is removed from this CR.
Consequences if not approved:	⌘	Terminology will be inconsistent.

Clauses affected:	⌘	4.1, 5.1, 5.2, 6.1, 6.2, 6.2.1, 6.2.4, 6.3.2.3.1, 6.4.2, 6.4.4, B.1, B.1.1, B.2.5, C, C.4,			
		Y	**N**		
Other specs Affected:	⌘		**N**	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

******* NEXT CHANGE *******

4.1 MBMS security architecture

MBMS introduces the concept of a point-to-multipoint service into a 3GPP system. A requirement of a ~~multicast~~MBMS user service is to be able to securely transmit data to a given set of users. In order to achieve this, there needs to be a method of authentication, key distribution and data protection for a ~~multicast~~MBMS user service.

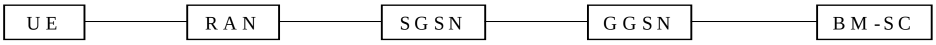

Figure 4.1: MBMS security architecture

Figure 4.1 gives an overview of the network elements involved in MBMS from a security perspective. Nearly all the security functionality for MBMS (beyond the normal network bearer security) resides in either the BM-SC or the UE.

The Broadcast Multicast – Service Centre (BM-SC) is a source for MBMS data. It could also be responsible for scheduling data and receiving data from third parties (this is beyond the scope of the standardisation work) for transmission. It is responsible for generating and distributing the keys necessary for ~~multicast~~ MBMS security to the UEs and for applying the appropriate protection to data that is transmitted as part of a ~~multicast~~MBMS user service. The BM-SC also provides the MBMS bearer authorisation for UEs attempting to establish ~~multicast~~ MBMS bearer.

The UE is responsible for receiving or fetching keys for the ~~multicast~~MBMS user service from the BM-SC and also using those keys to decrypt the MBMS data that is received.

MBMS imposes the following requirements on the MBMS capable elements:

- a UICC that contains MBMS key management functions shall implement GBA_U;
- a ME that supports MBMS shall implement GBA_U and GBA_ME, and shall be capable of utilising the MBMS key management functions on the UICC as well as providing key management functions itself;
- a BM-SC shall support using GBA_U keys to enable UICC key management.

******* NEXT CHANGE *******

5.1 Authenticating and authorizing the user

A UE is authenticated and authorised in the following situations when participating in an MBMS User Service. That is:

~~- when the UE performs User Service joining (or leaving) on the application level;~~

~~Editor's Note: The final decision on application level join procedures relies of work in SA4.~~

- when the UE establishes (or releases) the MBMS bearer(s) to receive an MBMS User Service;
- when the UE requests and receives MSKs for the MBMS User Service;
- when the UE performs ~~post~~ associated delivery procedures (e.g. point to point repair service).

~~Editor's Note: The final decision on post delivery procedures relies of work in SA4.~~

NOTE: The list above does not reflect the order of authentications.

5.2 Key management and distribution

Like any service, the keys that are used to protect the transmitted data in a ~~Multicast~~MBMS user service should be regularly changed to ensure that they are fresh. This ensures that only legitimate users can get access to the data in the

MBMS service. In particular frequent re-keying acts as a deterrent for an attacker to pass the MBMS keys to others users to allow those other users to access the data in an MBMS service.

The BM-SC is responsible for the generation and distribution of the MBMS keys to the UE. A UE has the ability to request a key when it does not have the relevant key to decrypt the data. This request may also be initiated by a message from the BM-SC to indicate that a new key is available.

******* NEXT CHANGE *******

6.1 Using GBA for MBMS

TS 33.220 [6] (Generic Bootstrapping Architecture) is used to agree keys that are needed to run an MBMS ~~Multicast~~ MBMS ~~U~~user service.

Before a user can access an MBMS User service, the UE needs to share GBA-keys with the BM-SC. If no valid GBA-keys are available at the UE, the UE shall perform a GBA run with the BSF of the home network as described within clause 5 of TS 33.220 [6]. The BM-SC will act as a NAF (Network Application Function) according to TS 33.220 [6].

The MSKs for an MBMS User service shall be stored on either the UICC if the UICC is capable of MBMS key management or the ME if the UICC is not capable of MBMS key management.

Storing the MSKs on the UICC requires a UICC that contains the MBMS management functions.

As a result of a GBA_U run, the BM-SC will share a key Ks_ext_NAF with the ME and share a key Ks_int_NAF with the UICC. This key Ks_int_NAF is used by the BM-SC and the UICC as the key MUK (MBMS User Key) to protect MSK (MBMS Service Key) deliveries to the UICC as described within clause 6.3. The key Ks_ext_NAF is used as the key MRK (MBMS Request Key) within the protocols as described within clause 6.2.

A run of GBA_ME results in the BM-SC sharing a key Ks_(ext)_NAF with the ME. This key Ks_(ext)_NAF is used by the BM-SC and the ME to derive the key MUK and the key MRK. The key MUK is used to protect MSK deliveries to the ME as described within clause 6.3. The key MRK is used to authenticate the UE towards the BM-SC within the protocols as described within clause 6.2.

The MUK is identified by the combination of B-TID and NAF-ID and the MRK is defined by B-TID, where B-TID and NAF-ID are defined as specified in TS 33.220 [6].

For ME based key management:

- All MBMS keys (MUK, MRK, MSK and MTK) shall be deleted from the ME when a different UICC is inserted. Therefore the ME needs to store in non-volatile memory the last inserted UICC-identity to be able to compare that with the used UICC-identity at UICC insertion and power on.
- All MBMS keys (MRK, MSK and MTK) may be deleted from the ME when the ME is powered down. If the ME does not delete the MBMS keys at power down then the MBMS keys need to be stored in non-volatile memory. The ME should store the MUKs in non-volatile memory in order to be able to authenticate the first MIKEY message of a push solicited pull procedure (see clause 6.3.2.2.4).

NOTE: If the ME deletes the MSK at power down, then the MBMS client would need to request MSK to the BM-SC and may need to run GBA to reconvene an MBMS session.

6.2 Authentication and authorisation of a user

Editor's Note: The exact details on how to derive the keys MRK and MUK from the GBA keys are for ffs.

~~Editor's Note: According to S3-040212, SA4 has a working assumption to use HTTP as the transport protocol but this is only agreed for the download repair service.~~

6.2.1 Authentication and authorisation in ~~application level joining~~HTTP based procedures

When the user wants to join (or leave) an MBMS user service, it shall use HTTP digest authentication RFC 2617 [8] for authentication. HTTP digest is run between BM-SC and ME. The MBMS authentication procedure is based on the general user authentication procedure over Ua interface that is specified in clause "Procedures using the bootstrapped Security Association" in TS 33.220 [6]. The BM-SC will act as a NAF according to TS 33.220 [6].

The following adaptations apply to HTTP digest:

- the transaction identifier as specified in TS 33.220 [6] is used as username;
- MRK (MBMS Request Key) is used as password;
- the joined MBMS user service is specified in client payload of HTTP Digest message.

Editor's Note: The contents of the client payload are FFS and may require input from TSG SA WG4. ~~The final decision on application level join and leave procedures relies of work in SA4.~~

******* NEXT CHANGE *******

6.2.4 Authentication and authorisation in ~~post~~ associated delivery procedures

When the UE requests ~~post~~ associated delivery procedures, the UE shall be authenticated with HTTP digest as in clause 6.2.1.

******* NEXT CHANGE *******

6.3.2.3.1 Pushing the MSKs to the UE

The BM-SC controls when the MSKs used in a ~~multicast~~MBMS user service are to be changed. The below flow describes how MSK changes are performed.

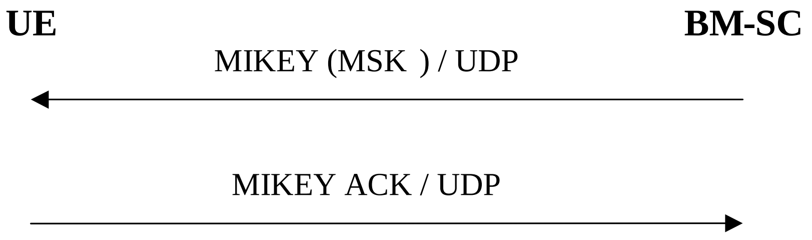

Figure 6.3: Pushing the MSKs to the UE

When the BM-SC decides that it is time to update the MSK, the BM-SC sends MIKEY message over UDP transporting the requested MSKs to the UE.

If requested by the BM-SC, the UE sends a MIKEY acknowledgement message to the BM-SC.

******* NEXT CHANGE *******

6.4.2 MIKEY common header

MSKs shall be carried in MIKEY messages. The messages are sent point-to-point between the BM-SC and each UE. The messages use the MUK shared between the BM-SC and the UE as the pre-shared secret in MIKEY.

Once the MSK is in place in the UE, the UE can make use of the ~~multicast~~ MTK messages sent by the BM-SC over MBMS bearer. The MTK is carried in messages conforming to the structure defined by MIKEY and use the MSK as the pre-shared secret.

If the BM-SC requires an ACK for an MSK key update message this is indicated by setting the V-bit in the MIKEY common header. The UE shall then respond with a MIKEY message containing the verification payload. In the case the server does not receive an ACK, normal reliability constructions can be used, e.g., start a timer when the message is sent and then resend the message if no ACK is received before the timer expires.

The CSB ID field of MIKEY common header is not used.

******* NEXT CHANGE *******

6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in RFC 3830 [9] (MIKEY). To be able to keep track of the key that is derived in the message, a general Extension Payload (EXT) with Type field value x is used that conforms to the structure defined in reference [16].

Editor's Note: The type value will be replaced by value requested from IANA.

The EXT includes a Key Domain ID and one or two Key Type ID sub-payloads depending on the message. These are used as follows.

For MSK delivery the EXT includes the Key Domain ID and a Key Type ID sub-payload. The Key Domain ID has the value as specified in clause 6.3.2.1. The Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MSK ID, see figure 6.4a. The key that is used to protect the message, i.e. MUK, is identified as specified in clause 6.1.

For MTK delivery the EXT includes the Key Domain ID and two Key Type ID sub-payloads. The Key Domain ID has the value as specified in clause 6.3.2.1. The first Key Type ID sub-payload includes the type and ID of the key that is used to protect the message, i.e. the MSK ID, and the second Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MTK ID, see figure 6.4b.

Editor's Note: The Key Domain ID needs to be added to [16]. It may need an extension payload type of its own.

See. clauses 6.3.2.1 and 6.3.3.1 for definition of MSK ID and MTK ID. The MTK ID is increased every time the corresponding key is updated. It is possible that the same MTK is delivered several times ~~in multicast~~ over MBMS bearer, and the ME can then discard messages related to a key it already has instead of passing them to the MGV-F.

The MGV-F (see clause 6.5) protects itself from a possibly malicious ME by checking the integrity and freshness of the MIKEY message.

The format of the key IDs shall be represented by unsigned integers, different from zero. The reason for disallowing zero is that it is reserved for future use. Note that this means that there can only be 2^n - 1 different keys in use during the same session, where n is the number of bits in the ID field.

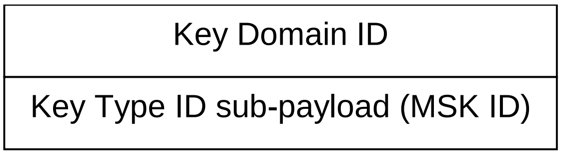

Figure 6.4a: Extension payload used with MIKEY MSK message

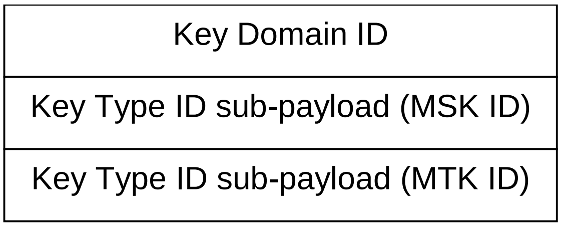
Key Domain ID
Key Type ID sub-payload (MSK ID)
Key Type ID sub-payload (MTK ID)

Figure 6.b: Extension payload used with MIKEY MTK message

******* NEXT CHANGE *******

B.1 Threats associated with attacks on the radio interface

The threats associated with attacks on the radio interface are split into the following categories, which are described in the following clauses:

- unauthorized access to ~~multicast~~ MBMS user service data;
- threats to integrity;
- denial of service;
- unauthorized access to MBMS services;
- privacy violation.

The attacks on the MBMS service announcements to the users on the radio interface are not discussed here, as these will most likely be transferred on a point-to-point connection (e.g. PS signaling connection), which is already secured today (integrity protected and optionally encrypted RAN level).

B.1.1 Unauthorised access to ~~multicast~~ MBMS user service data

A1: Intruders may eavesdrop MBMS ~~multicast~~ user service data on the air-interface.

A2: Users that have not joined and activated a MBMS ~~multicast~~ user service receiving that service without being charged.

A3: Users that have joined and then left a MBMS ~~multicast~~ user service continuing to receive the MBMS ~~multicast~~ user service without being charged.

A4: Valid subscribers may derive decryption keys (MTK) and distribute them to unauthorized parties.

NOTE: It is assumed that the legitimate end user has a motivation to defeat the system and distribute the shared keys (MSK, MTK) that are a necessary feature of any broadcast security scheme.

******* NEXT CHANGE *******

B.2.5 Unauthorised insertion of MBMS user data and key management data

J1: An ME, which deliberately inserts key management and malicious data, encrypted with valid (previously retrieved) MTK from the MTK generation function, within the ~~multicast~~ MBMS user service stream.

J2: An ME, which deliberately inserts key management and malicious data, encrypted with old (using replayed key management messages) MTK, within the ~~multicast~~ MBMS user service stream.

J3: An attacker, which deliberately inserts incorrect key management information within the ~~multicast~~ MBMS user service stream to cause Denial of Service attacks.

Annex C (normative): ~~Multicast~~ MBMS security requirements

******* NEXT CHANGE *******

C.4 Requirements on MBMS Key Management

R5a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected.

R5b: The transfer of the MBMS keys between the MBMS key generator and the UE shall be integrity protected.

R5c: The UE and MBMS key generator shall support the operator to perform re-keying as frequently as it believes necessary to ensure that:

- users that have joined an MBMS User Service ~~multicast service~~, but then left, shall not gain further access to the MBMS User Service without being charged appropriately
- users joining an MBMS User Service shall not gain access to data from previous transmissions in the MBMS User Service without having been charged appropriately
- the effect of subscribed users distributing decryption keys to non-subscribed users shall be controllable.

R5d: Only authorized users that have joined an MBMS User Service shall be able to receive MBMS keys delivered from the MBMS key generator.

R5e: The MBMS keys 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).

R5f: All keys used for the MBMS User Service shall be uniquely identifiable. The identity may be used by the UE to retrieve the actual key (based on identity match, and mismatch recognition) when an update was missed or was erroneous/incomplete.

R5g: The BM-SC shall be aware of where all MBMS specific keys are stored in the UE (i.e. ME or UICC).

R5h: The function of providing MTK to the ME shall only deliver a MTK to the ME if the input values used for obtaining the MTK were fresh (have not been replayed) and came from a trusted source.

C.5