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

***Tdoc ⌘S3-050134***

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **33.246** **CR** **052** ⌘ **rev** **1** ⌘ 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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Introduction of BM-SC subfunctions |
| ***Source:*** | ⌘ | SA WG3 |
| ***Work item code:*** | ⌘ | MBMS |
| ***Date:*** | ⌘ | 23/2/2005 |
| ***Category:*** | ⌘ | **C** |
| ***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:*** | ⌘ | The current specification lacks a proper security architecture overview and description of security sub-functions as defined in SA4 TS 26.346. |
| ***Summary of change:*** | ⌘ | New text is added to describe the MBMS security sub-functions. The Security architecture is clarified. |
| ***Consequences if not approved:*** | ⌘ | The specification will not be aligned with SA4 TS 26.346. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 4.1.1 (New), 4.1.2 (New), 4.1.3 (New), 4.2, 5.1, 5.2, 5.3 |

| ***Other specs Affected:*** | ⌘ | Y | N | | |
|---|---|---|---|---|---|
| | | Y | | Other core specifications | ⌘ TS 26.346 |
| | | | N | Test specifications | |
| | | | N | O&M Specifications | |

| | | |
|---|---|---|
| ***Other comments:*** | ⌘ | |

# 4 MBMS security overview

## 4.1 MBMS security architecture

### 4.1.1 General

MBMS introduces the concept of a point-to-multipoint service into a 3GPP system. A requirement of a multicast 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 service.

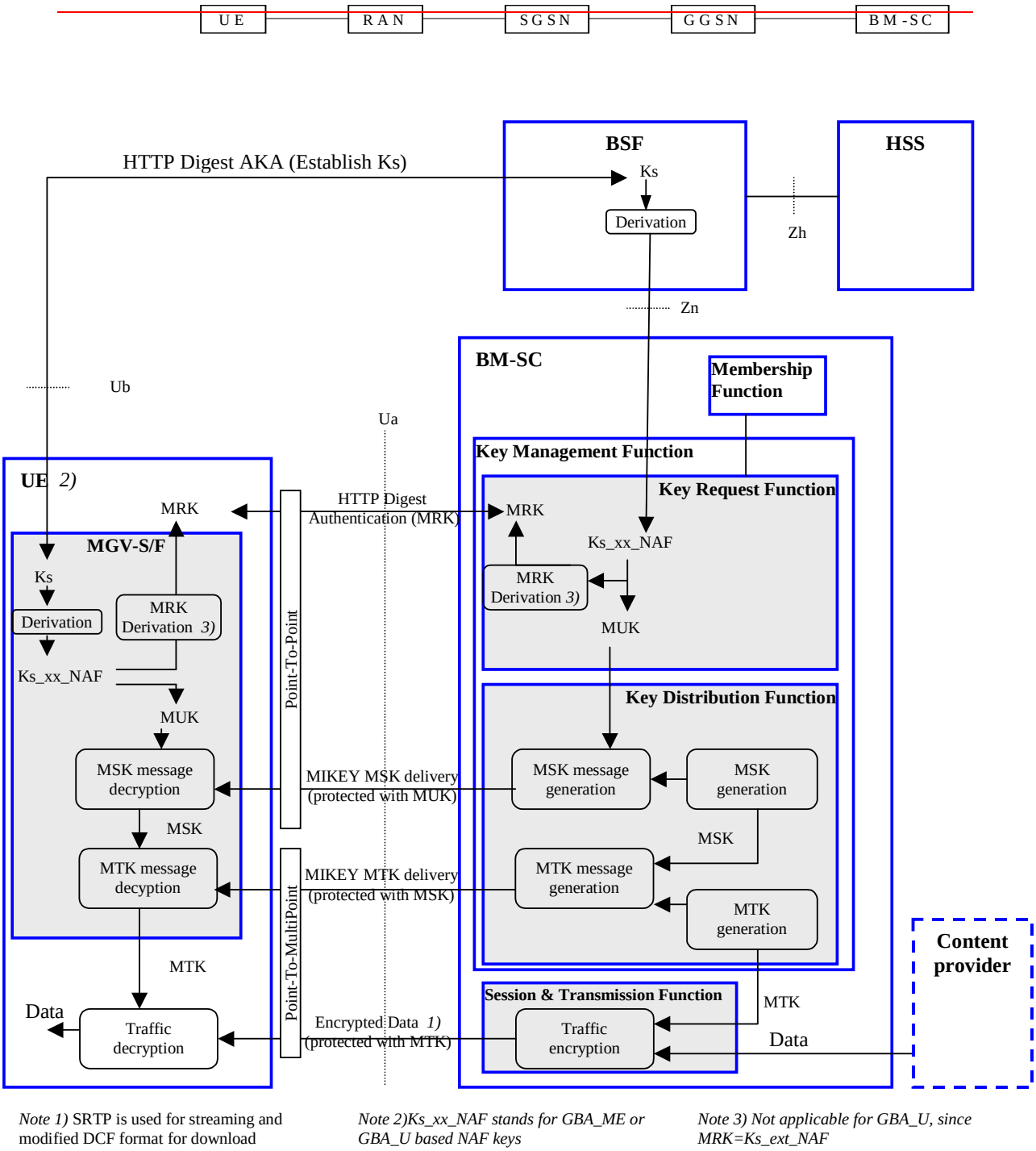


**Figure 4.1: MBMS security architecture**

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~~except for the normal network bearer security~~)~~ resides in either the BM-SC or the UE. The BSF is a part of GBA [6]. The UE and the BM-SC use GBA to establish shared keys that are used to protect the point-to-point communication between the UE and the BM-SC.

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~~ BM-SC is responsible for establishing shared secrets with the UE using GBA, authenticating the UE with HTTP digest authentication mechanism, registering and de-registering UEs for MBMS User Services, generating and distributing the keys necessary for ~~multicast~~ MBMS security to the UEs with MIKEY protocol and for applying the

appropriate protection to data that is transmitted as part of a MBMS user ~~multicast~~ service. The BM-SC also provides the MBMS bearer authorisation for UEs attempting to establish ~~multicast~~ MBMS bearer.

The UE is responsible for establishing shared secrets with the BM-SC using GBA, registering to, and de-registering from, MBMS User Services, requesting and 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.

## 4.1.2 BM-SC sub-functions

The BM-SC has the following sub-functions related to MBMS security, cf. Figure 4.1.

- **Key Management function**: The Key Management function includes two sub-functions: Key Request function and Key Delivery function.
- **Key Request function**: The sub-function is responsible for retrieving GBA keys from the BSF, deriving MUK and MRK from GBA keys, performing MBMS User Service Registration, Deregistration and MSK request procedures and related user authentication using MRK, providing MUK to Key distribution function, performing subscription check from Membership function. The sub-function implements the following procedures:
  - Bootstrapping initiation
  - Bootstrapping re-negotiation
  - HTTP digest authentication
  - MRK derivation
  - MBMS User Service Registration procedure
  - MBMS User Service Deregistration procedure
  - MSK request procedure
- **Key distribution function**: The sub-function is responsible for retrieving MUK from Registration function, generating and distributing MSKs and MTKs to the UE, providing MTK to Session and Transmission function. The sub-function implements the following security procedures:
  - MSK delivery procedure
  - MTK delivery procedure
  - BM-SC solicited pull procedure
- **Session and Transmission function**: The sub-function is responsible for session and transmission functions cf. TS 26.346 [13]. As part of these session and transmission functions, this function performs protection of data with MTK (encryption and/or integrity protection). The sub-function implements the following security procedures:
  - Protection of streaming data
  - Protection of download content
- **Membership function**: The Membership function is used to verify if a user is authorized to register, receive keys or to establish a MBMS bearer. The Membership function is defined in [3].

### 4.1.3 UE security architecture

It is assumed that the UE includes a secure storage (MGV-S). This MGV-S may be realized on the ME or on the UICC. The MGV-F is implemented in a protected execution environment to prevent leakage of security sensitive information such as MBMS keys. MGV-S stores the MBMS keys and MGV-F performs the functions that should not be exposed to unprotected parts of the ME. An overview of ME based key management and UICC based key management in UE is described in Figure 4.y.

In particular in ME based key management it shall be ensured that the keys are not exposed to unprotected parts of the ME when they are transmitted from the UICC to the MGV-S or during the key derivations.

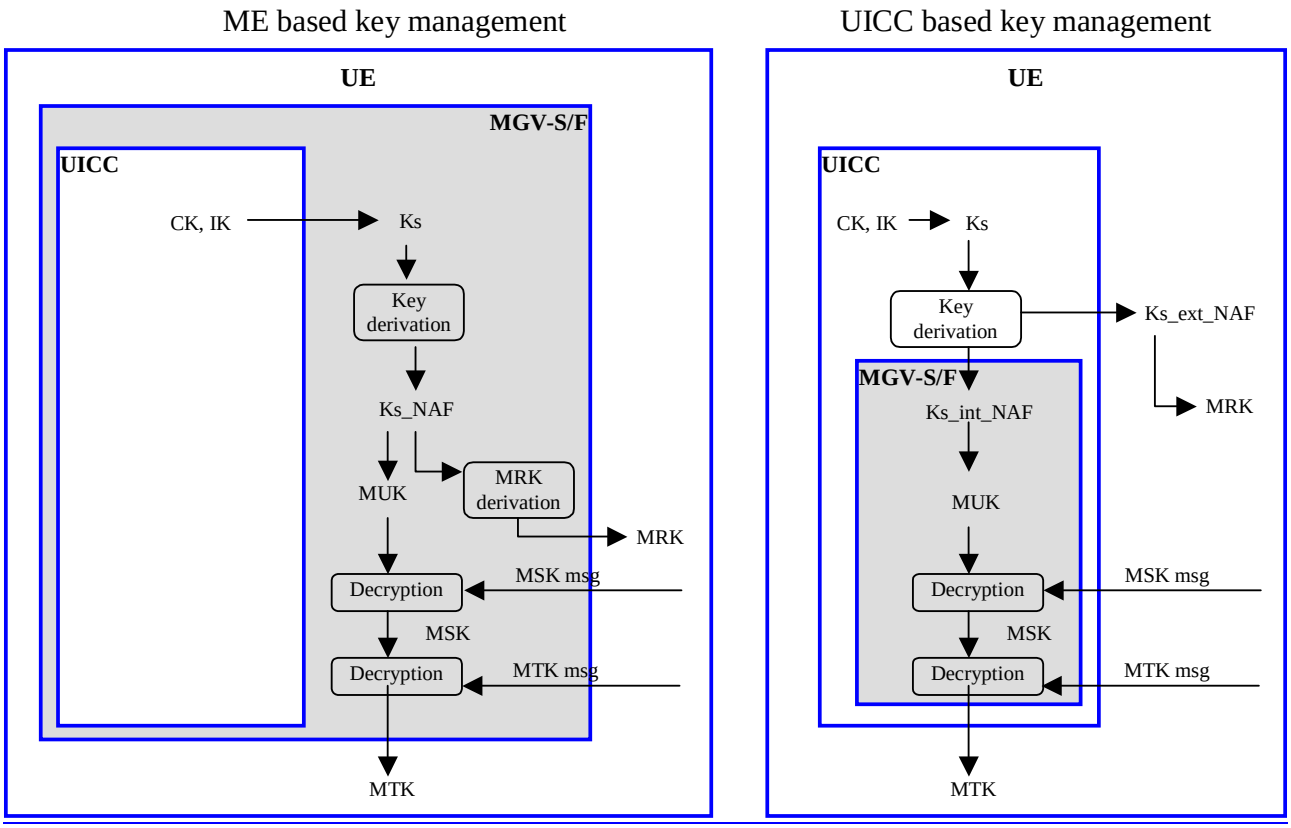


**Figure 4.y: ME and UICC based key management in UE**

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

## 4.2 Key management overview

The BM-SC controls the use of the MBMS Service Keys (MSKs) to secure the different MBMS Streaming/Download Sessions that make up the MBMS User Service. The MSKs are not directly used to secure the MBMS Streaming/Download Sessions, but they are used to protect the delivery of MBMS Transport Keys (MTKs), which are used to secure the MBMS Streaming/Download Sessions~~.~~ as specified within clauses 6.5 and 6.6. MSKs and MTKs are managed at the MBMS User Service Level. The usage of MSKs and MTKs for one Key group is depicted in figure 4.x.

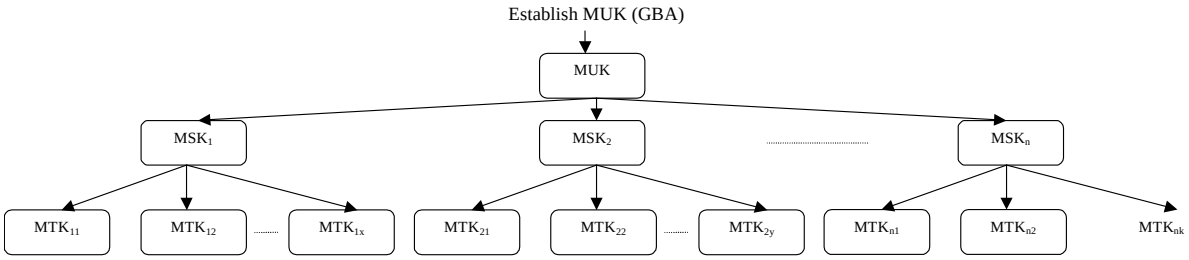


**Figure 4.x: MBMS key hierarchy**

There shall be only one MSK and MTK in use within one Key Group ID. I.e. parallel use of two or more MSKs (with different MSK IDs) or MTKs (with different MTK IDs) within a Key Group ID shall not be allowed.

The use of the same MTK (this implies also the same MSK) with two different transport services (or user services) should be avoided.

NOTE 1: This is to avoid synchronization problems in the UE when a new MTK is taken into use in the traffic, i.e. if the MTK is not changed synchronously in the traffic flows the UE would discard the traffic with smaller MTK ID.

According to TS 22.246 [5] there exist MBMS User Services with shared and non-shared Transport Services. It shall be possible for MBMS User Services to share one or more MSKs for the shared Transport Services with other MBMS User Services.

NOTE 2: While sharing MSKs among different MBMS User Services, care shall be taken that the Users are not given access to data that they are not entitled to.

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

# 5 MBMS security functions

## 5.1 Authenticating and authorizing the user

A UE is authenticated and authorised ~~in the following situations~~ such that only legitimate users ~~when~~ are able to participate~~ing~~ 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;~~

~~-~~ ~~w~~When the UE ~~requests and receives MSKs for the MBMS User Service~~uses HTTP protocol towards the BM-SC, the UE is authenticated with HTTP digest as described in clause 6.2.1. The Membership function within the BM-SC is used to verify the subscription information~~;~~

The following procedures use HTTP digest authentication:

- MBMS User Service Registration procedure (clause 6.3.2)
- MBMS User Service Deregistration procedure (clause 6.3.2)
- MSK request procedure. This can have many triggers (clause 6.3.2)
- Associated delivery procedures (specified in TS 26.346 [13])

When the UE establishes (or releases) the MBMS bearer(s) to receive an MBMS User Service, it is authenticated as defined in clause 6.2.2;

~~- when the UE performs post 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 derivation, management and distribution

Like any service, the keys that are used to protect the transmitted data in a Multicast 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.

The following procedures are involved in Key management and distribution:

- MRK derivation (clause 6.1)
- MBMS User Service Registration procedure (clause 6.3.2)
- MBMS User Service Deregistration procedure (clause 6.3.2)
- MSK request procedure (clause 6.3.2)
- MSK delivery procedure (clause 6.3.2)
- MTK delivery procedure (clause 6.3.3)
- BM-SC solicited pull (clause 6.3.2)

## 5.3 Protection of the transmitted traffic

The traffic for a particular MBMS service may require some protection depending on the sensitivity of the data being transmitted (e.g. it is possible that the data being transmitted by the MBMS service is actually protected by the DRM security method and hence might not require additional protection. However, MBMS protection is independent of DRM protection). If this protection is required, it will be either confidentiality and integrity or confidentiality only, or integrity only. The protection is applied end-to-end between the BM-SC and the UEs and will be based on a symmetric key shared between the BM-SC and the UEs that are currently accessing the service. The actual method of protection specified may vary depending on the type of data being transmitted, e.g. media streaming application or file download.

NOTE: When MBMS data is received over a point-to-point MBMS radio bearer, it would be ciphered between the BM-SC and UE and may also ciphered over the radio interface. This "double ciphering" is unnecessary from a security point of view and hence the decision of whether or not to apply radio interface ciphering to a point-to-point MBMS radio bearer is outside the scope of this specification.

The following procedures are involved in Key management and distribution:

- Protection of streaming data (clause 6.6.2)
- Protection of download content (clause 6.6.3)