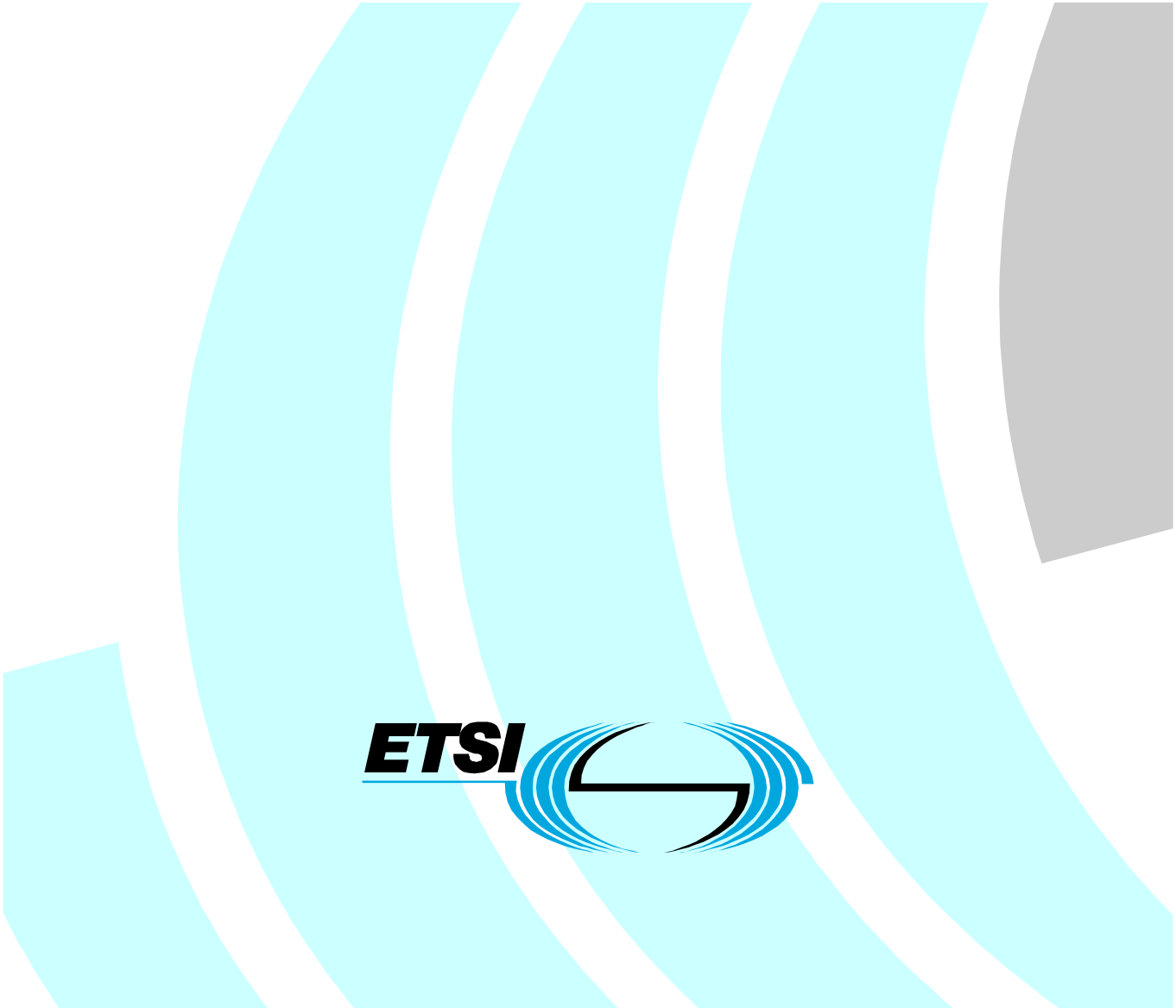
ETSI TS 102 442-6 V1.1.1 (2006-11)

Technical Specification

Satellite Earth Stations and Systems (SES);
Satellite Component of UMTS/IMT-2000;
Multimedia Broadcast/Multicast Services;
Part 6: Security



Reference
DTS/SES-00251-6

Keywords
broadcast, IMT-2000, satellite, service, UMTS, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Satellite Earth Stations and Systems (SES).

The present document is part 6 of a multi-part deliverable covering Satellite Earth Stations and Systems (SES); Satellite Component of UMTS/IMT-2000; Multimedia Broadcast/Multicast Services, as identified below:

Part 1: "Services definitions";

Part 2: "Architecture and functional description";

Part 3: "Introduction in the Radio Access Network (RAN)";

Part 4: "Interworking with terrestrial UMTS networks";

Part 5: "Performances over the radio interface";

Part 6: "Security".

Introduction

S-UMTS stands for the Satellite component of the Universal Mobile Telecommunication System. S-UMTS systems will complement the terrestrial UMTS (T-UMTS) and inter-work with other IMT-2000 family members through the UMTS core network. S-UMTS will be used to deliver 3rd generation mobile satellite services (MSS) utilizing either low (LEO) or medium (MEO) earth orbiting, or geostationary (GEO) satellite(s). S-UMTS systems are based on terrestrial 3GPP specifications and will support access to GSM/UMTS core networks.

NOTE 1: The term T-UMTS will be used in the present document to further differentiate the Terrestrial UMTS component.

Due to the differences between terrestrial and satellite channel characteristics, some modifications to the terrestrial UMTS (T-UMTS) standards are necessary. Some specifications are directly applicable, whereas others are applicable with modifications. Similarly, some T-UMTS specifications do not apply, whilst some S-UMTS specifications have no corresponding T-UMTS specification.

- Since S-UMTS is derived from T-UMTS, the organization of the S-UMTS specifications closely follows the original 3rd Generation Partnership Project (3GPP) structure.

An S-UMTS system is defined by the combination of a family of S-UMTS specifications and 3GPP specifications, as follows:

- If an S-UMTS specification exists it takes precedence over the corresponding 3GPP specification (if any). This precedence rule applies to any references in the corresponding 3GPP specifications.

NOTE 2: Any references to 3GPP specifications within the S-UMTS specifications are not subject to this precedence rule. For example, an S-UMTS specification may contain specific references to the corresponding 3GPP specification.

- If an S-UMTS specification does not exist, the corresponding 3GPP specification may or may not apply. The exact applicability of the complete list of 3GPP specifications shall be defined at a later stage.

1 Scope

The present document intends to specify security requirements.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

[1] ETSI TS 133 246 (Release 6): "Universal Mobile Telecommunications System (UMTS); 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS) (3GPP TS 33.246 Release 6)".

[2] IETF RFC 2617: " HTTP Authentication: Basic and Digest Access Authentication ".

[3] IETF RFC 3711: "The Secure Real-time Transport Protocol (SRTP)".

[4] IETF RFC 3830: "MIKEY: Multimedia Internet KEYing". .

[5] OMA-DRM-DCF-V2-0: "OMA DRM Content Format".

NOTE: Available at: www.openmobilealliance.org.

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BM-SC	Broadcast/Multicast Service Centre
DRM	Digital Right Management
GBA	Generic Bootstrapping Architecture
ME	Mobile Equipment
MSK	S-MBMS Service Key
MTK	S-MBMS Transport Key
NAF	Network Application Function
RAN	Radio Access Network
S-MBMS	Multimedia Broadcast/Multicast Services
UE	User Equipment
UICC	UMTS Integrated Circuit Card
USIM	UMTS Subscriber Identity Module

4 Security requirements

4.1 S-MBMS security requirements

The requirements of [1] shall apply.

Adaptations for the case BM-SC located outside the mobile operator.

4.2 General security requirements

4.2.1 Service level security

4.2.1.1 Secure access to S-MBMS services

It shall be possible to prevent intruders, including relay nodes, from obtaining unauthorized access to S-MBMS services by masquerading as authorized users.

It shall be possible to prevent intruders, including relay nodes, from hijacking a service already provided to a user.

It shall not be possible for unjustified charges to be imposed on users.

It shall be possible for users to be able to verify that serving networks are authorized to offer S-MBMS service on behalf of the user's Home Environment at the start of, and during, service delivery.

It shall not be possible for simultaneous access to S-MBMS services by multiple users from the same terminal to jeopardize the security of individual access to S-MBMS service.

It shall be possible to protect against unauthorized modification of multicast, signalling and control data, particularly on radio interfaces.

It shall be possible to protect the confidentiality of multicast, signalling and control data, particularly on radio interfaces.

4.2.1.2 Protection of user-related transmitted data

It shall be possible to protect the confidentiality of user traffic, particularly on radio interfaces, including protection against eavesdropping from relay nodes.

It shall be possible to protect the confidentiality of user identity data, particularly on radio interfaces, including protection against eavesdropping from relay nodes.

It shall be possible to protect the confidentiality of location data about users, particularly on radio interfaces, including protection against eavesdropping from relay nodes.

It shall be possible to protect against the unauthorized disclosure of location data about users participating in a particular S-MBMS service to other parties participating in the same S-MBMS service.

It shall be possible to protect against unauthorized modification of user traffic.

It shall be possible for the user to be able to check whether or not his user traffic is protected, particularly on radio interfaces.

4.2.1.3 Protection of user-related stored data

It shall be possible to protect against unauthorized modification of user-related data which is stored or processed by a provider.

It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider.

It shall be possible to protect against unauthorized modification of user-related data stored in the terminal or in the USIM.

It shall be possible to protect the confidentiality of user-related data stored in the terminal or in the USIM.

4.2.2 Provider security requirements

4.2.2.1 USIM security

A valid USIM shall be required to access any S-MBMS service except for emergency broadcast messages where the network should be allowed to decide whether or not emergency calls should be permitted without a USIM.

It shall be possible to prevent the use of a particular USIM to access S-MBMS services.

It shall be possible to control access to a USIM so that it can only be used to access S-MBMS services by the subscriber to whom it was issued or by users explicitly authorized by that subscriber.

It shall be possible to control access to data in a USIM. For instance, some data may only be accessible by an authorized home environment.

It shall not be possible to access data in a USIM that is only intended to be used within the USIM, e.g. authentication keys and algorithms.

If a UICC contains more than one USIM (to access services from different home environments) then different home environments shall only have access to the USIMs of their own users.

If a UICC contains more than one USIM (to access services from different home environments) then security management data (e.g. authentication information) of each USIM shall be protected independently against unauthorized access and modification.

It shall be possible to control access to, and selection of, USIMs and other non-S-MBMS applications stored on the same UICC. In particular, it shall be possible to have shared directories between applications where appropriate.

It shall be possible to ensure that the origin and integrity of applications and/or data downloaded to the UICC can be checked. It may also be necessary to ensure that the confidentiality of downloaded applications and/or data can be ensured.

4.2.2.2 Secure provision of S-MBMS services

It shall be possible for providers to authenticate users at the start of, and during, service delivery to prevent intruders (including relay nodes) from obtaining unauthorized access to S-MBMS services by masquerade or misuse of priorities.

It shall be possible to detect and prevent the fraudulent use of services. Alarms will typically need to be raised to alert providers to security-related events. Audit logs of security related events will also need to be produced.

It shall be possible for a home environment to cause an immediate termination of all services provided to users associated with that home environment.

It shall be possible for the serving network to be able to authenticate the origin of user traffic, signaling data and control data on radio interfaces.

It shall be possible to prevent intruders from restricting the availability of services by logical means.

It shall be possible to prevent intruders from significantly disrupting services by failing to relay packets as expected.

It shall be possible to prevent intruders from abusing legitimate relay nodes to obtain a free communications medium.

4.2.3 S-MBMS signalling protection requirements

It shall be possible to protect against unauthorized modification, insertion, replay or deletion of S-MBMS signaling on the Gmb reference point.

Unauthorized modification, insertion, replay or deletion of all signaling, on the RAN shall be prevented.

4.2.4 Requirements on Privacy

The User identity should not be exposed to the content provider or linked to the content in the case the Content Provider is located outside the operator's network.

S-MBMS identity and control information shall not be exposed.

4.2.5 Key management requirements

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

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

The UE and S-MBMS key generator shall support the operator to perform re-keying as frequently as it believes necessary 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 users joining a multicast service shall not gain access to data from previous transmissions in the multicast service without having been charged appropriately the effect of subscribed users distributing decryption keys to non-subscribed users shall be controllable.

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

The S-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).

All keys used for the S-MBMS 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.

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

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

4.2.6 S-MBMS multicast data

4.2.6.1 Integrity protection requirements

It shall be possible to protect against Unauthorized modification, insertion, replay or deletion of S-MBMS multicast data sent to the UE on the radio interface. The use of integrity shall be optional.

The S-MBMS multicast data may be integrity protected with a common integrity key, which shall be available to all users that have joined the S-MBMS service.

It may be required to integrity protect the "BM-SC - GGSN" interface, i.e. reference point Gi.

4.2.6.2 Confidentiality protection requirements

It shall be possible to protect the confidentiality of S-MBMS multicast data on the radio interface.

The S-MBMS multicast data may be encrypted with a common encryption key, which shall be available to all users that have joined the S-MBMS service.

It may be required to encrypt the S-MBMS multicast data on the "BM-SC - GGSN" interface, i.e. the reference points Gi.

It shall be infeasible for a man-in-the-middle to bid down the confidentiality protection used on S-MBMS multicast session from the BM-SC to the UE.

It shall be infeasible for an eavesdropper to break the confidentiality protection of the S-MBMS multicast session when it is applied.

4.2.7 Digital Rights Management

The requirements of [1] apply.

4.2.8 User Equipment

The requirements of [1] apply.

4.2.9 Infrastructure Security

4.2.9.1 BM-SC protection

The requirements of [1] apply.

4.2.9.2 3rd party content provider

The requirements of [1] apply.

4.2.9.3 Satellite environment protection

No additional security requirements are needed.

4.2.9.4 IMRs protection

It should be possible to authenticate the entity.

4.2.9.5 Inter domain security

Key transmission in an hybrid Satellite/terrestrial network (see S-MBMS security signalling transiting through terrestrial 3G system).

5 S-MBMS Security overview

5.1 S-MBMS- security architecture

S-MBMS introduces the concept of a point-to-multipoint service into a S-UMTS. 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.

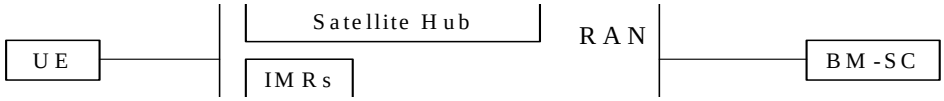


Figure 5.1: S-MBMS security architecture (hub refers to Gateway)

Figure 5.1 gives an overview of the network elements involved in S-MBMS from a security perspective. Nearly all the security functionality for S-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 S-MBMS data. It could also be responsible for scheduling data and receiving data from third parties for transmission. It is responsible for generating and distributing the keys necessary for multicast security to the UEs and for applying the appropriate protection to data that is transmitted as part of a multicast service. The BM-SC also provides the S-MBMS bearer authorization for UEs attempting to establish multicast bearer.

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

S-MBMS imposes the following requirements on the S-MBMS capable elements:

- a UICC that contains S-MBMS key management functions shall implement GBA_U;
- a ME that supports S-MBMS shall implement GBA_U and GBA_ME, and shall be capable of utilizing the S-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.

An S-MBMS User Service is composed of one or more S-MBMS Streaming Sessions and/or S-MBMS Download Sessions. S-MBMS streaming/download sessions may be transported over one or more S-MBMS Transport Services. S-MBMS security is used to protect S-MBMS streaming/download sessions.

5.2 Key management overview

The BM-SC controls the use of the S-MBMS Service Keys (MSKs) to secure the different S-MBMS Streaming/Download Sessions that make up the S-MBMS User Service. The MSKs are not directly used to secure the S-MBMS Streaming/Download Sessions, but they are used to protect the delivery of S-MBMS Transport Keys (MTKs), which are used to secure the S-MBMS Streaming/Download Sessions. MSKs and MTKs are managed at the S-MBMS User Service Level.

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.

There exist S-MBMS User Services with shared and non-shared Transport Services. It shall be possible for S-MBMS User Services to share one or more MSKs for the shared Transport Services with other S-MBMS User Services.

5.2.1 Key transmission for pay per view

The requirements of [1] shall apply.

5.2.2 Key transmission for Subscription

The requirements of [1] shall apply.

5.2.3 Key management with access network

The requirements of [1] shall apply.

5.2.4 Key management without access network

The requirements of [1] shall apply.

6 Security functions

6.1 Authenticating and authorizing the user

A UE is authenticated and authorized in the following situations when participating in an S-MBMS User Service:

- when the UE performs User Service joining (or leaving) on the application level;
- when the UE establishes (or releases) the S-MBMS bearer(s) to receive an S-MBMS User Service;

- when the UE requests and receives MSKs for the S-MBMS User Service;
- when the UE performs post delivery procedures (e.g. point to point repair service).

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

The BM-SC is responsible for the generation and distribution of the S-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.

6.3 Protection of the transmitted traffic

The traffic for a particular S-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 S-MBMS service is actually protected by the DRM security method and hence might not require additional protection. However, S-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.

6.4 Protection of Intermediate Module Repeaters

Void.

7 Security mechanisms

7.1 Using GBA for S-MBMS

Generic Bootstrapping Architecture (GBA) (see TS 133 220 in Bibliography) is used to agree keys that are needed to run an S-MBMS Multicast User service.

Before a user can access an S-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. The BM-SC will act as a NAF (Network Application Function) according to TS 133 220 (see Bibliography).

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

Storing the MSKs on the UICC requires a UICC that contains the S-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 (S-MBMS Service Key) deliveries to the UICC as described within clause 6.3. The key Ks_ext_NAF is used as the key MRK (S-MBMS Request Key).

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 133 220 (see Bibliography).

For ME based key management:

- All S-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 S-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 S-MBMS keys at power down then the S-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.

7.2 Authentication and authorization of user

7.2.1 Authentication and authorization in application level joining

When the user wants to join (or leave) an S-MBMS user service, it shall use HTTP digest authentication RFC 2617 [2] for authentication. HTTP digest is run between BM-SC and ME. The S-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 133 220 (see Bibliography). The BM-SC will act as a NAF according to TS 133 220 (see Bibliography).

The following adaptations apply to HTTP digest:

- the transaction identifier as specified in TS 133 220 (see Bibliography) is used as username;
- MRK (S-MBMS Request Key) is used as password;
- the joined S-MBMS user service is specified in client payload of HTTP Digest message.

7.2.2 Authentication and authorization in S-MBMS bearer establishment

The authentication of the UE during S-MBMS bearer establishment relies on the authenticated point-to-point connection with the network, which was set up using network security described in TS 33.102 (see Bibliography). Authorization for the S-MBMS bearer establishment happens by the network making an authorization request to the BM-SC to ensure that the UE is allowed to establish the S-MBMS bearer(s) corresponding to an S-MBMS User Service. As S-MBMS bearer establishment authorization lies outside the control of the S-MBMS bearer network (i.e. it is controlled by the BM-SC), there is an additional procedure to remove the S-MBMS bearer(s) related to a UE that is no longer authorized to access an S-MBMS User Service.

7.2.3 Authentication and authorization in MSK request

When the UE requests MSK(s), the UE shall be authenticated with HTTP digest as in clause 7.2.1.

7.2.4 Authentication and authorization in post delivery procedures

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

7.3 Key update procedures

Key update procedures shall be compliant with the procedure defined in [1].

7.4 Protection of the transmitted traffic

7.4.1 General

The data transmitted to the UEs is protected by a symmetric key (an MTK) that is shared by the BM-SC and UEs that are accessing the S-MBMS service. The protection of the data is applied by the BM-SC. In order to determine which key was used to protect the data key identification information is included with the protected data. The key identification information will uniquely identify the MSK and MTK. The MTK is processed according to the methods described in TS 133 220 (see Bibliography). Whenever data from an S-MBMS User Service has been decrypted, if it is to be stored on the UE it will be stored decrypted.

7.4.2 Protection of streaming data

7.4.2.1 Usage of SRTP

When it is required to protect S-MBMS streaming data SRTP (Secure Real-time Transport Protocol) as defined in RFC 3711 [3] shall be used. The MTK is carried to the UEs from the BM-SC using RFC 3830 [4] (MIKEY) with extensions defined according to [1]. MTK shall be used as the master key in SRTP key derivation to derive the SRTP session keys as defined in section 4.3 of RFC 3830 [4]. The correct MTK to use to decrypt the data is indicated using the MKI (Master Key Identifier) field, which is included in the SRTP packets as defined in RFC 3711 [3]. The form of MKI shall be a concatenation of MSK ID and MTK ID, i.e. MKI = (MSK ID || MTK ID).

If the SRTP packets are to be integrity protected, the SRTP authentication tag is appended to the packets as defined in RFC 3830 [4].

SRTP security policy parameters, such as encryption algorithm, are transported in MIKEY Security Policy payload as defined in section 6.10.1 in RFC 3830 [4].

7.4.2.2 Packet processing in the UE

When the SRTP module receives a packet, it will retrieve the correct cryptographic context identified by destination transport address, destination port and SSRC (according to RFC 3711 [3]), check if it has the MTK corresponding to the value in the MKI field in the SRTP cryptographic context.

If the check is successful, the SRTP module processes the packet according to the security policy.

If the SRTP module does not have the MTK, it will request the MTK corresponding to the MKI from the key management module. When the key management module returns a new MTK, the SRTP module will derive new session keys from the MTK and process the packet. However, if the key management module does not have the MSK indicated by MKI, then it should fetch the MSK using the methods discussed in [1].

If the correct MTK is not present in the UE when RTP traffic arrives, the UE shall wait for the next MTK update procedure from the BM-SC as described in [1].

If the SRTP module has lost synchronization on the ROC (Roll-Over Counter) of the SRTP stream, it shall wait for the next MTK update message received within the ptm stream. The BM-SC shall deliver the current ROC-value within the CS ID map info payload of the MIKEY common header payload.

The flow below shows how the protected content is delivered to the UE.

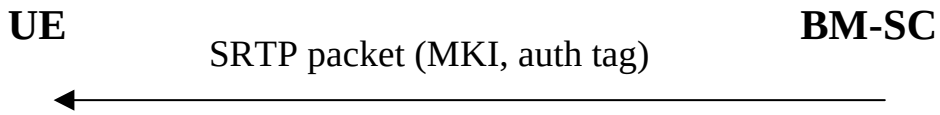


Figure 7.1: Delivery of protected streaming content to the UE

7.4.3 Protection of download content

7.4.3.1 General

Data that belongs to a download S-MBMS User Service is decrypted as soon as possible by the UE, if the MSK needed to provide the relevant MTK is already available on the UE.

7.4.3.2 Usage of OMA DRM DCF

When it is required to protect S-MBMS download content, OMA DRM V2.0 DCF as defined in [5] shall be used. S-MBMS download contents are indicated by the 3GPP-MBMS-DCF flag in the Common Headers Box of a DCF. OMA DRM Rights Objects are not utilized. Instead, encryption and authentication keys are generated from MTK. For integrity protection, an S-MBMS Signature as specified below is attached in the FreeSpaceBox of the DCF.

The range of data for the HMAC calculation shall be according to section 5.3 of [5].

The correct MTK for decrypting and verifying the integrity of the download content is indicated by the key_id in the RightsIssuerURL field as follows:

S-MBMS-key://key_id

where key_id is defined as the base 64 encoded concatenation (Key Domain ID || MSK_ID || MTK ID).

In case the FDT of the FLUTE protocol needs to be protected, the FDT may also be wrapped in a different DCF. Confidentiality and/or integrity protection of FDT can be provided this way.

Annex A (informative): Bibliography

- ETSI TS 133 102: "Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture (3GPP TS 33.102)".
- ETSI TS 133 220: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture (3GPP TS 33.220)".

History

Document history		
V1.1.1	November 2006	Publication