3GPP TSG SA WG3 Security ó SA3#34 **S3-040678**
6-9 July 2004
Acapulco, Mexico

Source: **MBMS Security Rapporteur**

Title: **Latest version of MBMS TS**

Document for: **Information**

Agenda Item: **MBMS**

1 Introduction

The attached document is the latest version of the MBMS TS. With the exception of editorial changes, this is version that will be sent to SA plenary in September for approval.

Draft 3GPP TS 33.246 V1.3.0 (2004-07)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security;
Security of Multimedia Broadcast/Multicast Service
(Release 6)

Keywords

UMTS, multimedia, broadcast, security

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The security of MBMS provides different challenges compared to the security of services delivered over point-to-point services. In addition to the normal threat of eavesdropping, there is also the threat that it may not be assumed that valid subscribers have any interest in maintaining the privacy of the communications, and they may therefore conspire to circumvent the security solution (for example one subscriber may publish the decryption keys enabling non-subscribers to view broadcast content). Countering this threat requires the decryption keys to be updated frequently in a manner that may not be predicted by subscribers while making efficient use of the radio network.

1 Scope

The Technical Specification covers the security procedures of the Multimedia Broadcast/Multicast Service (MBMS) for 3GPP systems (UTRAN and GERAN). MBMS is a GPRS network bearer service over which many different applications could be carried. The actual method of protection may vary depending on the type of MBMS application.

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, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.146: "Multimedia Broadcast/Multicast Service; Stage 1".

[3] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 22.246 "MBMS User Services"

[6] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[7] 3GPP TS 31.102: "3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM application"

[8] IETF RFC 2617 "HTTP Digest Authenticationî

[9] IETF: MIKEY: Multimedia Internet KEYing; http://www.ietf.org/internet-drafts/draft-ietf-msec-mikey-08.txt; Work In Progress

[10] IETF RFC 1982 "Serial Number Arithmeticî

[11] IETF RFC 3711 "Secure Real-time Transport Protocolî

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply.

For the definitions of MBMS User Service refer to [5].

MRK = MBMS Request Key: This key is to authenticate the UE to the BM-SC when performing key requests etc.

MSK = MBMS Service Key: The MBMS Service key that is securely transferred (using the key MUK) from the BM-SC towards the UE. For MBMS streaming the MSK is not used directly to protect the MBMS User Service data (see MTK).

MTK = MBMS Traffic Key: A key that is obtained by the UICC or ME by calling a decryption function MGV-F with the MSK. The key MTK is used to decrypt the received MBMS data on the ME.

MUK = MBMS User Key: The MBMS user individual key that is used by the BM-SC to protect the point to point transfer of MSKís to the UE.

NOTE: The keys MSK and MUK may be stored within the UICC or the ME depending on the MBMS service.

3.2 Symbols

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

MUK_I	Integrity key derived from key MUK
MUK_C	Confidentiality key derived from key MUK
MSK_I	Integrity key derived from key MSK
MSK_C	Confidentiality key derived from key MSK

3.3 Abbreviations

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

MBMS	Multimedia Broadcast/Multicast Service
MGV-F	MTK Generation and Validation Function

4 MBMS security overview

4.1 MBMS security architecture

MBMS introduces the concept of a point-to-multipoint service into a 3G network. 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. The point-to-point services in a 3G network use the AKA protocol (see TS 33.102 [4]) to both authenticate a user and agree on keys to be used between that user and the radio network. These keys are subsequently used to provide protection of traffic between the network and the UE.

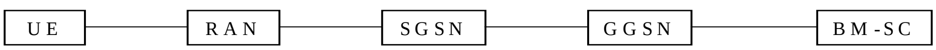

Figure 1: MBMS security architecture

Figure 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 ñ 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 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 MBMS bearer authorisation 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 MBMS data that is received.

4.2 Key management overview

A MBMS User Service may contain one or more MSKs which may be in use at the same time and are managed at the MBMS User Service Level. The BM-SC controls the use of the MSKs towards the different Transport Services. The MSKs are not directly used towards the MBMS Transport Services but as a second level key MTK as specified within clauses 6.4 and 6.5.

NOTE: According to good security practice the use of the same MTK with two different protocols shall be avoided

For MBMS User Services it shall be possible to share one or more MSKs with other MBMS User Service, as according to TS 22.246 [5] there exist MBMS User Services with shared and non-shared Transport Services.

NOTE: 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.

5 MBMS security functions

5.1 Authenticating and authorizing the user

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

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

Editorís 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 delivery procedures (e.g. point to point repair service)

Editorís 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 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.

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 requires no additional protection). This protection will be either confidentiality and integrity or just confidentiality. 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 (GE-)RAN. Although this ìdouble cipheringî is unnecessary from a security point of view it is a (GE-)RAN decision whether to apply ciphering or not in (GE-)RAN.

6 Security mechanisms

6.1 Using GBA for MBMS

GBA[6] is used to agree keys that are needed to run an MBMS Multicast User service. MBMS imposes the following requirements on the MBMS capable UICCs and MEs:

A UICC that contains MBMS key management functions shall implement GBA_U.

An 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.

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 [6] section 5. The BM-SC will act as a NAF according to [6].

The MSKs for an MBMS User service shall be stored on either the UICC or the ME. Storing the MSKs on the UICC requires a UICC that contains the MBMS management functions (and by requirement is GBA aware) and requires that all of the network elements, i.e. HSS, BSF and BM-SC, to be GBA_U aware. As a result of the GBA_U run in these circumstances, 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 to protect MSK deliveries to the UICC as described within clause 6.3. The key Ks_ext_NAF is used as the key MRK within the protocols as described within clause 6.2.

NOTE: A run of GBA_U on a GBA aware UICC will not allow the MSKs to be stored on the UICC, if the MBMS management functions are not present on the UICC.

In any other circumstance, a run of GBA 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 (MBMS Request Key). 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.

6.2 Authentication and authorisation of a user

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

Editorís 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

When the user wants to join (or leave) an MBMS user service, it shall use HTTP digest authentication [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 chapter ìProcedures using the bootstrapped Security Associationî in [6]. The BM-SC will act as a NAF according to [6].

The following adaptations apply to HTTP digest:

- The transaction identifier as specified in [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.

Editorís 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.

6.2.2 Authentication and authorisation in MBMS bearer establishment

The authentication of the UE during 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 [4]. Authorisation for the MBMS bearer establishment happens by the network making an authorisation request to the BM-SC to ensure that the UE is allowed to establish the MBMS bearer(s) corresponding to an MBMS User Service (see TS 23.246 [3] for the details). As MBMS bearer establishment authorisation lies outside the control of the MBMS bearer network (i.e. it is controlled by the BM-SC), there is an additional procedure to remove the MBMS bearer(s) related to a UE that is no longer authorised to access an MBMS User Service.

6.2.3 Authentication and authorisation in MSK request

When the UE requests MSK(s), the UE shall be authenticated with HTTP digest as in subclause 6.2.1.

6.2.4 Authentication and authorisation in post delivery procedures

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

6.3 Key update procedures

Editorís Note: The contents of the http client payloads are FFS and may require input from TSG SA WG4.

6.3.1 General

In order to protect an MBMS User service, it is necessary to transfer both MSKs and MTKs from the BM-SC to the UE. Subclause 6.3.2 describes the possible procedures for transferring MSKs, while subclause 6.3.3 deals with the transfer of MTKs.

6.3.2 MSK procedures

6.3.2.1 MSK identification

Every MSK is uniquely identifiable by its Network ID, Key Group ID and MSK ID

where

Network ID = MCC || MNC and is 3 bytes long. It is carried in the ID_I payload in MIKEY message

Key Group ID is 2 bytes long and is used to group keys together in order to allow redundant MSKs to be deleted. It is carried in the CSB ID field of MIKEY common header.

MSK ID is 2 bytes long and is used to distinguish MSKs that have the same Network ID and Key Service ID. It is carried in the MSK-ID field of MIKEY extension payload.

If the UE receives an MSK and already contains two other MSKs under the same Network ID and Key Group ID, then the UE shall delete the older of these two MSKs.

Editorís Note: The handling of MSKs may need some enhancement to cover download services, where the MSK is fetched after the UE has received the encrypted data.

6.3.2.2 UE initiated MSK update procedure

When a UE detects that it needs the MSK(s) for a specific MBMS User service, the UE should try to get the MSKs that will be used to ëprotectí the data transmitted as part of this multicast service. Reasons for UE to retrieve the MSK(s) include e.g.:

- Retrieval of initial MSKs e.g. when the UE has joined the MBMS user service

Editorís note: The initial key request may also be part of User Service joining procedure if SA4 decides to have such procedure. In this case the MSKs will be transported after the joining procedure has completed.

- Retrieval of MSKs when the UE has missed a key update procedure e.g. due to being out of coverage

If the UE fails to get hold of the MSK or receives confirmation that no updated MSK is necessary or available at this time, then, unless the UE has a still-valid, older MSK, the UE shall leave the MBMS user service.

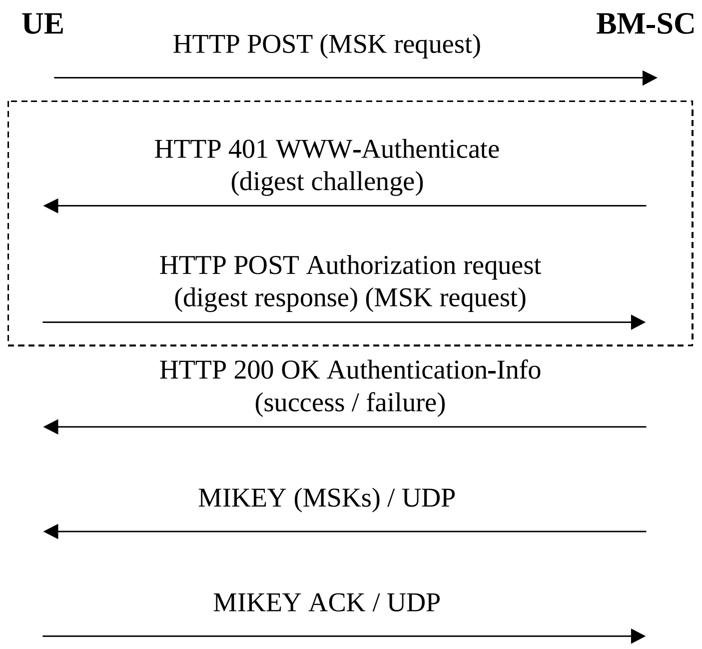

Figure x. UE initiated MSK delivery

The UE requests for the MSKs using the HTTP POST message. The key identification information is included in the client payload of the HTTP message.

The BM-SC may challenge the UE with HTTP response including WWW-Authenticate header and digest-challenge. Upon receiving the digest-challenge, the UE calculates the digest response and re-sends HTTP POST message including the key request and Authorization Request header including the digest response.

The BM-SC sends a response in HTTP 200 OK message with Authentication-Info header. The response in client payload includes cause code for success or reject.

If the key request procedure above resulted to success, the BM-SC sends MIKEY messages 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.

6.3.2.3 BM-SC initiated MSK update procedures

6.3.2.3.1 Pushing the MSKs to the UE

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

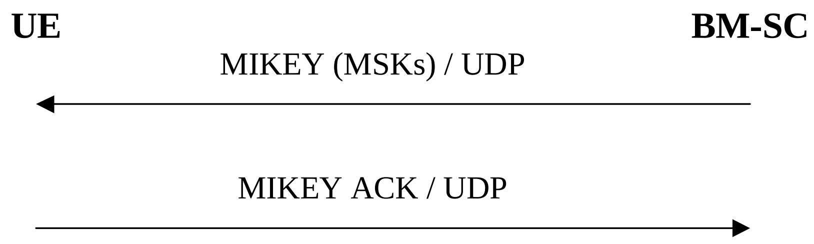

Figure x. Pushing the MSKs to the UE

When the BM-SC decides to 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.

6.3.2.3.2 Push solicited pull

While the push is the regular way of updating the MSK to the UE, there may be situations where the BM-SC solicits the UE to contact the BM-SC and request for new MSKs. An example of such situation is when the BM-SC wants the UE to authenticate itself during the service or when the MUK has expired.

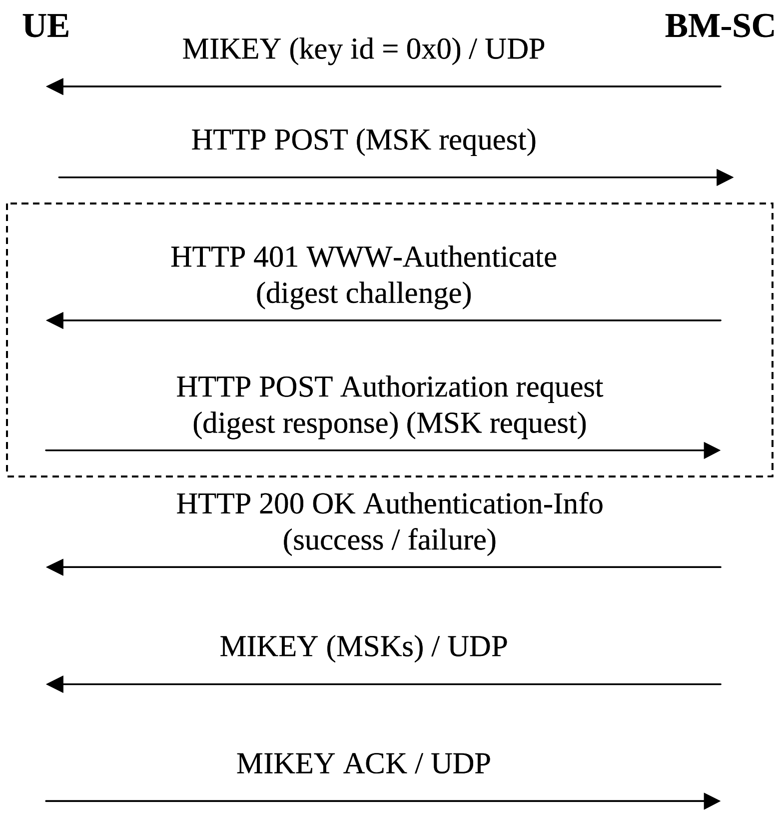

Figure x. Push solicited pull

The BM-SC sends MIKEY message over UDP to the UE. The key IDs in the extension payload of the MIKEY message set to 0x0 to indicate that the UE should request for current MSK from the BM-SC.

When the UE contacts the BM-SC, the BM-SC may trigger re-authentication of the UE or even re-run of GBA procedure to update the MUK.

The rest of the procedure is the same as in 6.3.1.

6.3.3 MTK procedures

6.3.3.1 MTK identification

Every MTK is uniquely identifiable by its Network ID, Key Group ID, MSK ID and MTK ID

where

Network ID, Key Group ID and MSK ID are as defined in subclause 6.3.2.1.

Editorís Note: The format of MTK is ffs.

6.3.3.2 MTK update procedure

The MTK is delivered to the UE as in 6.3.2.1 but the MIKEY ACK is not used.

6.4 MIKEY message creation and processing in the ME

Editorís note: The need for salting keys in processing of MIKEY messages is for further study.

6.4.1 General

MIKEY is used to transport the MSKs and MTKs from the BM-SC to the UE. Subclauses 6.4.2, 6.4.3, 6.4.4 and 6.4.5 describe how to create the MIKEY messages, while subclause 6.6.6 describe the initial processing by the ME on these messages. The final processing is done by the MGF-V and is described in subclause 6.5.

6.4.2 MIKEY common header

MIKEY shall be used with pre-shared keys as described in [9].

MSKs shall be carried in MIKEY messages with a Data Type value of 0x07 in the MIKEY common header that signals that the message contains an MBMS MSK. This allows legacy MIKEY implementations to discard the message early in the processing stage. 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.

To keep track of MSKs and MTKs, a new Extension Payload is added to MIKEY (see Section 6.3.2). The Extension contains the identities of MSKs and the MTKs.

Once the MSK is in place in the UE, the UE can make use of the broadcast MTK messages sent by the BM-SC. The MTK is carried in messages conforming to the structure defined by MIKEY and use the MSK as pre-shared secret. A Data Type value of 0x08 is used in the MIKEY common header to signal that the message contains an MBMS MTK.

If the BM-SC requires an ACK for a 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 shall carry the Key Group ID.

6.4.3 Replay protection

Each MIKEY message contains the timestamp field (TS) of type 2. This means that the contents of the timestamp field is a 32-bit counter. The counter is increased by one for each message sent from the BM-SC to the UE. Note that there is one counter per UE for MSK delivery, and one counter common to all UE:s for MTK delivery. The counter is used for replay protection; messages with a counter less than or equal to the current counter are discarded. Less than or equal is to be taken in the meaning of RFC1982. If the less than or equal relation is undefined in the sense of RFC1982, the message should be considered as being replayed. The counter in the TS field shall be reset for MSK transport messages when the MUK is updated. The counter in the TS field shall be reset for MTK transport messages when the MSK is updated.

NOTE: The counter in TS field in MTK transport messages is used to detect replay attacks while the counter in MTK ID field of EXT payload is used to detect the resendings of the same MTK keys.

6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in MIKEY [9]. To be able to keep track of the keys, an new general Extension Payload (EXT) is defined that conforms to the structure defined in 6.15 of MIKEY[9]. The ID:s of the involved keys are kept in the EXT, to enable the UE to look up the identity of the key which was used to protect the message, and which key is contained in the message. This EXT is incorporated in the MIKEY messages (see Figure 1). When an MSK is delivered to a UE, the MIKEY message contains an EXT that holds the MUK ID of the MUK used to protect the delivery, and the MSK ID of the MSK delivered in the message. For messages that contains a MTK, the EXT contains the MSK ID of the MSK used to protect the delivery, and the MTK ID of the MTK contained in the message. The MSK ID and MTK ID areis increased by 1 every time the corresponding key is updated. It is possible that the same MTK is delivered several times in multicast, 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 Section 6.4) 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 integer counters, 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.

Outer Key ID	Inner Key ID

Figure 1. The figure shows the Extension payload used with MIKEY. The Inner Key ID is the ID of the key that is transported in the message (i.e. an MSK or MTK). The Outer Key ID is the ID of the key used as pre-shared secret for the key delivery (i.e. an MUK or MSK).

6.4.5 MIKEY message structure

6.4.5.1 MSK message structure

The structure of the MIKEY message carrying a MSK key is depicted in Figure 2. The actual key that is delivered is kept in the KEMAC payload. The MIKEY-RAND is used to derive e.g. encryption and authentication keys from the received keys. It is sent only in the initial MSK delivery message. The identity payloads of the initiatorís and responderís IDs shall be included in the MSK transport messages. ID_I is the ID of the BM-SC and ID_r is the ID of the UE. Security Policy (SP) payload includes information for the security protocol such as algorithms to use, key lengths, initial values for algorithms etc. The Key Validity Data subfield is present in the KEMAC payload when MSK is transported but it is not present for MTK transport. The field defines the Key Validity Time for MSK in terms of sequence number interval (i.e. lower limit of MTK ID and upper limit of MTK ID). The lower limit of the interval defines the SEQs in the MTK Generation and Validation Function.

Editorís note: The type (URI or NAI) of identity payloads to use are for further study.

Editorís Note: The contents of the Security Policy payload depends on the used security protocols. MIKEY [9] has defined Security Policy payload for SRTP, but for other security protocols there is a need to define new Security Policy payloads. The exact definitions of these are FFS.

Common HDR
Timestamp (counter)
(MIKEY RAND)
ID_I
ID_R
(SP)
EXT
KEMAC

Figure 2. The logical structure of the MIKEY message used to deliver MSK.

6.4.5.2 MSK Verification message

If the BM-SC expects a response to the MSK-transport message (i.e., the V-bit in the MIKEY common header is equal to 1), the UE shall send a verification message as a response. The verification message shall be constructed according to Section 3.1 of MIKEY, and shall consist of the following fields: HDR || TS || ID_i || ID_r || V, where ID_I is the ID of the BM-SC and ID_r is the ID of the UE. Note that the MAC included in the verification payload, shall be computed over both the initiatorís and the responderís IDs as well as the timestamp in addition to be computed over the response message as defined in [9]. The key used in the MAC computation is the MUK_I.

Common HDR
Timestamp (counter)
ID_I
ID_R
V

Figure 3. The logical structure of the MIKEY message used to deliver MSK.

The verification message shall not be sent as a response to MIKEY messages delivering MTK.

The verification message shall be constructed by the ME, except for the MAC field, and then be given to the MGV-F that will perform the MAC computation and will return the verification message appended with the MAC to the ME. The ME shall send the message to the BM-SC.

6.4.5.3 MTK message structure

The structure of the MIKEY message carrying a MTK key is depicted in Figure 3. The actual key that is delivered is kept in the KEMAC payload. The network identity payloads (ID_I) shall be used in MTK transport messages.

Common HDR
Timestamp (counter)
ID_I
EXT
KEMAC

Figure 4. The logical structure of the MIKEY message used to deliver MTK.

6.4.6 Processing of received messages in the ME

6.4.6.1 MSK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following Section 5.3 of [9]).

1. The Data Type field of the common MIKEY header (HDR) is examined, and if it indicates an MSK delivery, the MUK ID is extracted from the Extension Payload.

2. The Timestamp Payload is checked, and the message is discarded if the Counter is larger or equal to the current MIKEY replay counter associated with the given MUK (the Counter value is retrieved from MGV-S). To avoid issues with wrap around of the ID fields ``smaller than¥should be in sense of RFC1982 [10].

3. The Security Policy payload is stored if it was present.

4. The message is transported to MGV-F for further processing, cf 6.5.2.

5. The MGV-F replies success or failure.

6.4.6.2 MTK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following Section 5.3 of [9]).

1. The Data Type field of the common MIKEY header (HDR) is examined, and if it indicates an MTSK delivery, the MSK ID is extracted from the Extension Payload.

2. The Timestamp Payload is checked, and the message is discarded if the Counter is larger or equal to the current MIKEY replay counter associated with the given MUSK (the Counter value is retrieved from MGV-S). To avoid issues with wrap around of the ID fields ``smaller than¥should be in sense of RFC1982 [10].

3. If the MTK ID extracted from the Extension payload is less than or equal to the current MTK ID (kept in the ME), the message must be discarded.

4. The message is transported to MGV-F for further processing, cf 6.5.3.

5. The MGV-F replies success (i.e. sending the MTK) or failure.

6.5. Validation and key derivation functions in MGV-F

6.5.1 General

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 but for certain type of MBMS services the UICC shall be used as determined by the service provider. The MGV-F is implemented inside MGV-S.

Editorís note: The choice between MIKEY key derivation algorithms and other suitable key derivations has not been made as there could be algorithms already in the UE.

6.5.2 MUK derivation

When a MUK has been installed in the MGV-S, i.e. as a result of a GBA run, it is used as pre-shared secret together with the MIKEY-RAND and the Key Group ID from the MIKEY message to derive encryption and integrity keys (MUK_C and MUK_I) as defined in Section 4.1.4 of MIKEY. MUK_I and MUK_C are used to verify the integrity of the MSK transport message and decrypt the key carried in the KEMAC payload.

6.5.3 MSK validation and derivation

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common header. If the key in the message is an MSK, MGV-F retrieves the MUK with the ID given by the Extension payload.

The MAC in the KEMAC payload is verified using MUK_I, and the message is discarded upon failure. If the MAC verification is successful the MUK_C is used to decrypt the Key Data sub-payload, and the MSK can be installed in the key management module. The MSK is used as pre-shared secret together with the MIKEY-RAND and the Key Group ID from the MIKEY message to derive (as specified in section 4.1.4 of [9]) encryption and integrity keys (MSK_I and MSK_C). The Key Validity data is extracted from the message and stored (in the form of MTK ID interval). The lower limit of the interval defines the SEQs.

NOTE: The MSK is not necessarily updated in the message, since a MSK transport message can be sent e.g. to update the Key Validity data.

The MGV-F shall update in MGV-S the Counter value in the Time Stamp payload associated with the corresponding MUK ID.

6.5.4 MTK validation and derivation

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common header. If the key inside the message is an MTK, MGV-F retrieves the MSK with the ID given by the Extension payload.

It is assumed that the MBMS service specific data, MSK and the sequence number SEQs, have been stored within a secure storage (MGV-S). Both MSK and SEQs were transferred to the MGV-S with the execution of the MSK update procedures. The initial value of SEQs is determined by the service provider.

The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh.

The MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored SEQs. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME. If SEQp is greater than SEQs then the MGV-F shall calculate the MAC as defined in [9] using the received MIKEY message and MSK as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message.. If the MAC defers then the MGV-F will indicate a failure to the ME. If the MAC is equal then the MGV-F shall update SEQs with SEQp value and start with the generation of MTK. The MGV-F provides the MTK to the ME.

The MGV-F shall update in MGV-S the value in the Time Stamp payload associated with the corresponding MSK ID.

NOTE: MIKEY includes functionality to derive further keys from MTK if needed by the security protocol. The key derivation is defined in Section 4.1.3 of MIKEY [9].

6.6 Protection of the transmitted traffic

6.6.1 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 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 a Key_ID is included with the protected data. The Key_ID will uniquely identify the MSK and contain other information needed to calculate the MTK. The MTK is derived according to the methods described in clauses 6.4 and 6.5. Whenever data from an MBMS User Service has been decrypted, if it is to be stored on the UE it will be stored decrypted.

Note: including the Key_ID with the protected data stops the UE trying to decrypt and render content for which it does not have the MSK.

6.6.2 Protection of streaming data

Editorís Note: The content of this clause will be checked after the joint meeting with SA4

6.6.2.1 Usage of SRTP

When it is required to protect MBMS streaming data SRTP (Secure Real-time Transport Protocol) as defined in [11] shall be used to protect MBMS streaming data. The MTK is carried to the UEs from the BM_SC using extended MIKEY. MTK shall be used as the master key in SRTP key derivation to derive the SRTP session keys as defined in chapter 4.3 of [9]. 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 [11]. 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 [9].

SRTP security policy parameters, such as encryption algorithm, are transported in MIKEY Security Policy payload as defined in chapter 6.10.1 in [9].

6.6.2.2 Packet processing in the UE

When the SRTP module receives a packet, it will check if it has the MTK corresponding to the value in the MKI field in the cryptographic context.

NOTE: The SRTP module does not need to interpret the MKI field semantics. It only checks whether it has the MTK corresponding to the MKI value.

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 for MTK corresponding to the MKI from the key management module. When the key management module returns a new MTK, 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 the clause 6.3.

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

Figure x. Delivery of protected streaming content to the UE

6.6.3 Protection of download content

Data that belongs to a download 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.

Annex A (informative): Trust model

The following trust relationship between the roles that are participating in MBMS services are proposed:

The user trusts the home network operator to provide the MBMS service according to the service level agreement. .

The user trusts the network operator after mutual authentication.

The network trusts an authenticated user using integrity protection and encryption at RAN level.

The network may have trust or no trust in a content provider.

The home network and visited network trust each other when a roaming agreement is defined, in the case the user is roaming in a VPLMN.

Annex B (informative): Security threats

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 sub-chapters:

unauthorized access to multicast 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 data

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

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

A3: Users that have joined and then left a MBMS multicast service continuing to receive the MBMS multicast 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.

B.1.2 Threats to integrity

B1: Modifications and replay of messages in a way to fool the user of the content from the actual source, e.g. replace the actual content with a fake one.

B.1.3 Denial of service attacks

C1: Jamming of radio resources. Deliberate manipulation of the data to disturb the communication.

B.1.4 Unauthorised access to MBMS services

D1: An attacker using the 3GPP network to gain ìfree accessî of MBMS services and other services on another userís bill.

D2: An attacker using MBMS shared keys (MSK, MTK) to gain free access to content without any knowledge of the service provider.

Note: It cannot be assumed that keys held in a terminal are secure. No matter how the shared keys (MSK, MTK) are delivered to the terminal, we have to assume they can be derived in an attack. For example, the shared keys, while secure in the UICC, may be passed over an insecure SIM-ME interface.

B.1.5 Privacy violation

E1: The user identity could be exposed to the content provider, in the case the content provider is located in the 3GPP network, and then linked to the content.

B.2 Threats associated with attacks on other parts of the system

The threats associated with attacks on other parts of the system are split into the following categories, which are described in the following sub-chapters:

unauthorized access to data;

threats to integrity;

denial of service;

A malicious UE generating MTKs for malicious use later on;

Unauthorized insertion of MBMS user data and key management data.

B.2.1 Unauthorised access to data

F1: It is assumed that the BM-SC and the GGSN are located in the same network. The BM-SC can though be located in a different place than the GGSN, and therefore can open up for intruders who may eavesdrop the new interface Gi and Gmb between the BM-SC and GGSN.

F2: Intruders may eavesdrop the new interface between the content provider and the BM-SC.

B.2.2 Threats to integrity

G1: It is assumed that the BM-SC and the GGSN are located in the same network. The BM-SC can though be located in a different place than the GGSN, and therefore can open up for new attacks on the new interfaces Gi and Gmb between the BM-SC and GGSN.

G2: The new interface between the content provider and the BM-SC may open up for attacks as modifications of multimedia content.

B.2.3 Denial of service

H1: Deliberated manipulation of the data between the BM-SC <-> Content Provider to disturb the communication.

H2: Deliberated manipulation of the data between the BM-SC <-> GGSN to disturb the communication.

B.2.4 A malicious UE generating MTKs for malicious use later on.

I1: A malicious ME querying the MTK generation function for MTKís to use them later on in an attack (e.g. in order to use the retrieved MTKs within an unauthorized data insertion attacks (See B.2.5)).

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 stream.

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

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

Annex C (normative): Multicast security requirements

C.1 Requirements on security service access

C.1.1 Requirements on secure service access

R1a: A valid USIM shall be required to access MBMS User Services.

R1b: It shall be possible to prevent intruders from obtaining unauthorized access of MBMS User Services by masquerading as authorized users.

C.1.2 Requirements on secure service provision

R2a: It shall be possible for the network (e.g. BM-SC) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to MBMS User Services.

R2b: It shall be possible to prevent the use of a particular USIM to access MBMS User Services.

NOTE: No security requirements shall be placed on the UE that requires UE to be customised to a particular customer prior to the point of sale.

C.2 Requirements on MBMS transport Service signaling protection

R3a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS transport service signaling on the Gmb reference point.

Editorís note: When the Gmb reference point is IP-based then NDS/IP methods according to TS 33.210 may be applied to fulfill requirement R3a. The Gmb interface is ffs.

R3b: Unauthorized modification, insertion, replay or deletion of all transport service signaling, on the RAN shall be prevented when the RAN selects a point-to-multipoint (ptm) link for the distribution of MBMS data to the UE

NOTE: UTRAN Bearer signalling integrity protection will not be provided for point to multipoint MBMS signalling and GERAN has no bearer signalling integrity protection, even for point to point signalling.

C.3 Requirements on Privacy

R4a: 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 3GPP operatorís network.

R4b: MBMS identity and control information shall not be exposed when the RAN selects a point-to-multipoint link for the distribution of MBMS data to the UE.

NOTE: UTRAN and GERAN Bearer confidentiality protection will be not be provided for point to multipoint MBMS sessions

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 Requirements on integrity protection of MBMS User Service data

R6a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS User Service data sent to the UE on the radio interface. The use of integrity shall be optional.

NOTE: It may be possible to detect the deletion of MBMS data packets, but it is impossible to prevent the deletion. Packets may be lost because of bad radio conditions, providing integrity protection will not help to detect or recover from this situation.

NOTE: The use of shared keys (integrity and confidentiality) to a group of untrusted users only prevents attacks of lower levels of sophistication, such as preventing eavesdroppers from simply listening in

R6b: The MBMS User Service data may be integrity protected with a common integrity key, which shall be available to all users that have joined the MBMS User Service.

R6c: It may be required to integrity protect the ìBM-SC - GGSNî interface i.e. reference point Gi.

C.6 Requirements on confidentiality protection of MBMS User Service data

R7a: It shall be possible to protect the confidentiality of MBMS User Service data on the radio interface.

R7b: The MBMS User Service data may be encrypted with common encryption keys, which shall be available to all users that have joined the MBMS User Service.

R7c: It may be required to encrypt the MBMS User Service data on the ìBM-SC - GGSNî interface, i.e. the reference points Gi.

R7d: It shall be infeasible for a man-in-the-middle to bid down the confidentiality protection used on protect the MBMS User Service from the BM-SC to the UE.

R7e: It shall be infeasible for an eavesdropper to break the confidentiality protection of the MBMS User Service when it is applied.

C.7 Requirements on content provider to BM-SC reference point

R8a: The BM-SC shall be able to authenticate and authorize a 3rd party content provider that wishes to transmit data to the BM-SC.

R8b: It shall be possible to integrity and confidentiality protect data sent from a 3rd party content provider to the BM-SC.

NOTE: This reference point will not be standardised.

Annex D (normative): UICC-ME interface

D.1 MSK Update Procedure

This procedure is part of the MSK update procedure as described in 6.4 (Validation and key derivation functions in MGV-F).

The ME has previously performed a GBA_U bootstrapping procedure as described in TS 33.220. The UICC stores the corresponding Ks_int_NAF together with the NAF_Id associated with this particular bootstrapping procedure.

The ME receives a MIKEY message containing an MSK update procedure. After performing some validity checks, the ME sends the whole message to the UICC. The ME also includes in this request NAF_Id to identify the stored Ks_int_NAF.

The UICC then uses Ks_int_NAF as the MUK value for MUK derivation and MSK validation and derivation (as described in chapter 6.4.1 and 6.4.2)

After successful MSK Update procedure the UICC stores the Network ID, Key Group ID, MSK ID, MSK and MSK Validity Time (in the form of MTK ID interval).

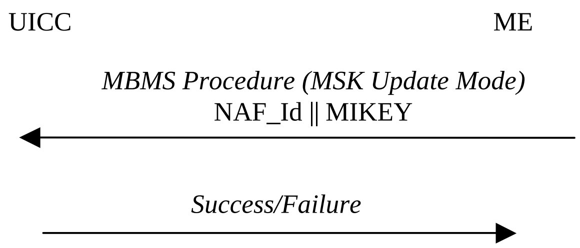

Figure x: MSK Update Procedure

D.2 MSK Verification Message Generation

This procedure is part of the MSK Verification Message as described in 6.3.6.2 (MSK Verification message)

The ME constructs the verification message in response to the MSK-transport message when it is required by BMSC.

The ME shall then give the constructed MIKEY verification message, with an empty MAC field, to the UICC. The ME also includes in this request NAF_Id to identify the stored Ks_int_NAF=MUK to be used in the MSK Verification Message Generation.

The UICC will verify that the Time Stamp MIKEY field correspond to the previous MSK Update procedure. Then, the UICC shall compute and send the MIKEY packet to the ME (including the calculated MAC field) as defined in 6.3.6.2. (MSK Verification message).

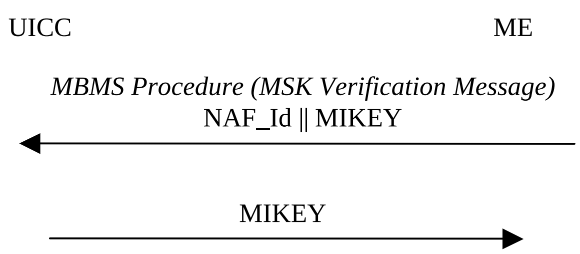

Figure x: MSK Verification Message

D.3. MTK generation and validation

This procedure is part of the MTK generation and validation function as described in 6.4.3 (MTK validation and derivation)

The ME receives the MIKEY message (containing Header, Time stamp, Network ID, Key Group ID, MSK ID, MTK ID = SEQp, MSK_C[MTK] and MAC). After performing some validity checks, the ME sends the whole message to the UICC. The UICC computes the MGV-F function as described in section 6.4. (Validation and key derivation functions in MGV-F). After successful MGV-F procedure the UICC returns the MTK.

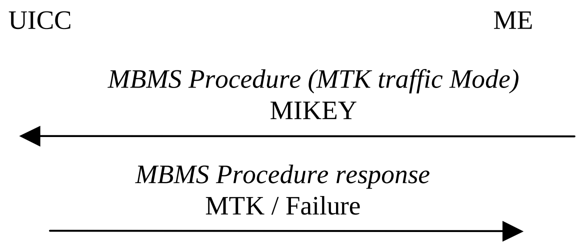

Figure x: MTK Generation and Validation

Annex <X> (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2002-09					Initial version supplied by Rapporteur		0.0.1
2002-11					Updated to include the threat and requirements discussed at SA3 #25.	0.0.1	0.0.2
2003-02					Updated to reflect changes to the requirements agreed at SA#26	0.0.2	0.0.3
2003-04					Updated to reflect changes agreed at the SA#27	0.0.3	0.10.0
2003-07					Updated to reflect the decision on TEK distribution and independence of the MBMS keys from radio level keys	0.1.0	0.1.1
2003-08					Updated to reflect agreement in SA#29 on adding confidentiality requirements, editorís note about double ciphering, and text indicating that different security mechanisms may be needed to protect different protocols/codec that may be used in MBMS and re-organisation of the requirements section.	0.1.1	0.2.0
2003-09					Updated to reflect decision at Antwerp ad-hoc.	0.2.0	0.2.1
2003-11					Updated to reflect changes to requirements and threat at SA3#30	0.2.1	0.2.2
2003-11					Updated to reflect decisions taken at SA3#31while discussing tdoc 755 and attached pseudo CR.	0.2.2	0.2.3
2003-11					Updated to reflect all the other decisions taken at SA3#31	0.2.3	0.3.0
2003-11					Updated with some editorial modification and presented to the SA plenary for information	0.3.0	1.0.0
2004-02					Updated to reflect changes agreed at SA3#32	1.0.0	1.1.0
2004-04					Minor corrections agreed by e-mail discussion	1.1.0	1.1.1
2004-05					Updated to reflect the decisions taken at SA3#33	1.1.1	1.2.0
2004-06					Small editorial corrections	1.2.0	1.2.1
2004-07					Updated to reflect the decisions taken at SA#34 S3-040470, S3-040469, S3-040553, S3-040535, S3-040489, S3-040565, S3-04573, S3-040620 (update of S3-040582), S3-040676 (update of S3-040497 via S3-040618) and S3-040677 (update of s3-040582 via S3-040619)	1.2.1	1.3.0