|  |  |
| --- | --- |
| 3GPP TR 33.850 V0.7.0 (2021-08) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Security Aspects of Enhancements for 5G Multicast-Broadcast Services (MBS) (Release 17) | |
|  | |
| *5G-logo_175px* | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***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 |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

Introduction 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 8

4 Overview of Multicast-Broadcast Services (MBS) 8

5 Key issues 8

5.1 Key issue #1: Security of authentication and authorization for multicast communication services 8

5.1.1 Key issue details 8

5.1.2 Security threats 9

5.1.3 Potential security requirements 9

5.2 Key Issue #2: Security protection of MBS traffic 9

5.2.1 Key issue details 9

5.2.2 Security threats 10

5.2.3 Potential security requirements 10

5.3 Key Issue #3: Security protection of key distribution 10

5.3.1 Key issue details 10

5.3.2 Security threats 10

5.3.3 Potential security requirements 10

5.4 Key Issue # 4: Security protection between AF and 5GC 10

5.4.1 Key issue details 10

5.4.2 Security threats 11

5.4.3 Potential security requirements 11

5.X Key issue #X: <Key issue name> 11

5.X.1 Key issue details 11

5.X.2 Threats 11

5.X.3 Potential security requirements 11

6 Proposed solutions 11

6.0 Mapping of solutions to key issues 11

6.1 Solution #1: Protection of MBS traffic in transport layer 12

6.1.1 Solution overview 12

6.1.2 Solution details 12

6.1.2.1 Security handling in handover 13

6.1.3 Solution evaluation 14

6.2 Solution #2: protect MBS traffic in service layer 14

6.2.1 Solution overview 14

6.2.2 Solution details 14

6.2.2.1 MBS group key distribution and update 16

6.2.3 Solution evaluation 17

6.3 Solution #3: MBS Traffic Protection 17

6.3.1 Solution overview 17

6.3.2 Solution details 18

6.3.3 Solution evaluation 19

6.4 Solution #4: Authentication and authorization for multicast communication service 19

6.4.1 Solution overview 19

6.4.2 Solution details 19

6.4.2.1 Authentication and authorization 20

6.4.2.2 Authorization revocation 21

6.4.3 Solution evaluation 21

6.5 Solution #5: Authorization revocation 21

6.5.1 Solution overview 21

6.5.2 Solution details 22

6.5.3 Solution evaluation 22

6.6 Solution #6: Authentication and authorization for multicast communication service based on AKMA 23

6.6.1 Solution overview 23

6. 6.2 Solution details 23

6.6.3 Solution evaluation 24

6.7 Solution # 7: security protection between AF and 5GC 24

6.7.1 Solution overview 24

6.7.2 Solution details 24

6.7.3 Solution evaluation 24

6.8 Solution #8: MBS Traffic Protection 24

6.8.1 Solution overview 24

6.8.2 Solution details 24

6.8.3 Solution evaluation 26

6.9 Solution #9: Key update solution 26

6.9.1 Solution overview 26

6.9.2 Solution Details 26

6.9.2.1 Comparison between the default and optimized approaches 28

6.9.2.2 Key update conditions 29

6.9.2.3 Applicability to other solutions 30

6.9.3 Evaluation 31

6.10 Solution #10: Secure framework for Key distribution in MBS 31

6.10.1 Solution overview 31

6.10.2 Solution details 32

6.10.2.1 MBS key generation 32

6.10.2.2 MBS procedure for key generation and traffic protection 32

6.10.2.3 MBS procedure for re-keying 34

6.10.3 Solution Evaluation 37

6.11 Solution #11: Update the keys used to protect the MBS traffic 37

6.11.1 Introduction 37

6.11.2 Solution details 37

6.11. 3 Evaluation 38

6.12 Solution #12: Protection of MBS traffic at service layer based on GBA 39

6.12.1 Solution overview 39

6.12.2 Solution details 39

6.12.3 Solution evaluation 40

6.13 Solution #13: Key generation and distribution for MBS 41

6.13.1 Solution overview 41

6.13.2 Solution details 41

6.13.3 Solution evaluation 44

6.14 Solution #14: Secure key delivery in service layer 44

6.14.1 Solution overview 44

6.14.2 Solution details 44

6.14.3 Solution evaluation 46

6.X Solution #X: <Solution name> 46

6.X.1 Solution overview 46

6.X.2 Solution details 46

6.X.3 Solution evaluation 46

7 Conclusions 46

7.1 Conclusions on Key Issue #1 46

7.2 Conclusions on Key Issue #2 46

7.3 Conclusions on Key Issue #4 46

Annex <A>: <Informative annex title for a Technical Report> 47

Annex <X> (informative): Change history 48

# Foreword

This Technical Report 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.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

Editor’s Note: Content is FFS

# 1 Scope

The present document studies the security of 5G multicast-broadcast services based on FS\_5MBS study in TR 23.757 [2]. Potential security requirements are identified and possible security solutions are proposed to address these 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, 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 TR 23.757: " Study on architectural enhancements for 5G multicast-broadcast services ".

[3] 3GPP TS 33.246: " Security of Multimedia Broadcast/Multicast Service (MBMS) ".

[4] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

[5] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[6] 3GPP TS 33.501: " Security architecture and procedures for 5G system".

[7] 3GPP TS 23.468 Group Communication System Enablers for LTE (GCSE\_LTE); Stage 2.

[8] 3GPP TS 33.220 Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA).

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

Editor’s Note: Example needs to be deleted

## 3.2 Symbols

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

<symbol> <Explanation>

Editor’s Note: Example needs to be deleted

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

MBS Multicast/Broadcast Service

MBSF Multicast/Broadcast Service Function

MBSF-C MBSF Control Plane

MBSF-U MBSF User Plane

MBSTF Multicast/Broadcast Service Transport Function

MUK Multicast User Key

PTP Point-to-Point

PTM Point-to-Multipoint

# 4 Overview of Multicast-Broadcast Services (MBS)

Editor’s Note: This clause will contain a brief overview on MBS

5G system aims to enable general Multicast-Broadcast Service (MBS), e.g. public safety, V2X application, group communications and IoT applications, etc.

As in 4G, 5G MBS service also have two modes: Transport Only Mode in which the multicast and broadcast contents are transparent to the 3GPP network functions, and Full Service Mode in which the 3GPP network functions are aware of the contents.

Two delivery methods are envisioned for 5G MBS service, from the view point of 5G core network (5GC): 5GC Individual MBS traffic delivery method, and 5GC shared MBS traffic delivery method. For the former, 5GC receives a single copy of MBS data packets and delivers separate copies of those MBS data packets to individual UEs via per-UE PDU sessions, while for the latter, 5G CN receives a single copy of MBS data packets and delivers a single copy of those MBS packets packet to a RAN node, which then delivers them to one or multiple UEs.

RAN delivers MBS data to UEs using either Point-to-Point delivery or Point-to-Multipoint (PTM) delivery.

The study item includes security aspects on muticast and broadcast service:

* Security of authentication and authorization for multicast communication services
* Security protection of MBS traffic
* Security protection of key distribution
* Security protection between AF and 5GC

NOTE: Different solutions may use different nomenclature for the Service Functionality MBSF/MBSTF, e.g. both MBSF and MBSTF or MBSF-C and MBSF-U.

# 5 Key issues

Editor’s Note: This clause will contain the agreed key issues

## 5.1 Key issue #1: Security of authentication and authorization for multicast communication services

### 5.1.1 Key issue details

Architecture enhancements for 5G MBS services have been studied in TR 23.757 [2]. Two reference architectures for 5G MBS are proposed. Compared to the MBS architecture for LTE and before as specified in TS 23.246 [4], 5G MBS architecture differ, among others, in that MBS signalling is flowing through the control plane of 3GPP. Figure 1a and 1b shows the MBS architecture for LTE and before in TS 23.246 [3], and Figure A.1.2-1 and A.2.2-1 in TR 23.757 [2] shows the MBS architecture alternatives for 5G.

TS 33.246 [3] specifies the security for the MBS for LTE and before. It is required that a UE is authenticated and authorised such that only legitimate users are able to participate in a MBS service. In addition, KI#3 from TR 23.757 [2] is describing authorization for multicast communication services for 5G, which addresses the following security-related issues:

*5.3.1 Description*

*The 5GS is expected to support different use cases of multicast services. The mobile network operators (MNO) and/or application service providers (ASP) may want to provide different levels of authorization (e.g. at session or service level) for the UE to access multicast communication services.*

*This key issue will study the following aspects:*

*- Define and study how to support the necessary level(s) of authorization for UEs to access multicast communication services.*

*- How can a UE join/leave (including authorised or revoked to access) a multicast communication service?*

How that authentication and authorization is realized in the new architecture for 5Gmulticast communication service needs to be studied. The necessary level(s) of authorization could be needed for UEs to access multicast communication services.

### 5.1.2 Security threats

If authentication for multicast communication service is not supported, an attacker may spoof a legitimate UE to gain access to a MBS service. If authorization for multicast communication service is not supported, an attacker may gain free access to content without any knowledge of the service provider. In addition, an attacker may use the 3GPP network to gain "free access" of MBS services and other services on another user's bill.

### 5.1.3 Potential security requirements

The 5GS shall support the authentication and authorization for multicast communication service.

## 5.2 Key Issue #2: Security protection of MBS traffic

### 5.2.1 Key issue details

According to TR 23.757 [2], MBS traffic needs to be delivered from application service provider to multiple UEs through 5GS. Depending on many factors, multiple delivery methods may be used to deliver MBS traffic. As described in clause 4.4 of TR 23.757 [2], Shared PTP or PTM delivery method and Individual delivery method may be used at the same time for a 5G MBS session depending on selected solution.

The 5GS may provide multiple interfaces for transferring MBS data between UE and external services/networks, such as Uu, N3, N6. MBS traffic need to be properly protected especially in air interface. While it is still possible to support security for multicast/broadcast traffic at the application layer, it is necessary to consider a security natively provided by the 5G system for the following reasons: There would be multicast/broadcast services that do not have application level security (e.g., due to protocol overhead) but want to leverage the security provided by 5G system, such as the MBS services provided by operators (e.g., for IoT devices).

As a result, MBS protection independent of application layer protection is to be studied in this key issue. This key issue investigates security protection of 5G MBS PDU sessions/flows at the transport or service level. In Transport layer, the service is provided by the 5G system to deliver multicast datagrams to multiple receivers using minimum network and radio resources, while the service layer is fully separate from the transport layer. This allows for applications that do not require a service layer to establish a multicast transport directly via Nnef (control plane and N6 (user plane data)

Editor’s Note: this key issue may need to be updated based on the progress of the 5G MBS architecture design by SA2 and RAN WGs.

### 5.2.2 Security threats

Attackers may eavesdrop MBS traffic on the air-interface. Users that have not joined and activated a MBS service receiving that service without being charged.

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.

### 5.2.3 Potential security requirements

The 5GS shall support the confidentiality protection, integrity protection, and anti-replay protection of MBS traffic.

## 5.3 Key Issue #3: Security protection of key distribution

### 5.3.1 Key issue details

MBS introduces the concept of a point-to-multipoint service into a 3GPP system. MBS traffic is delivered from application service provider to multiple UEs through 5GS. To securely transmit data to a given set of users, the MBS traffic needs to be protected to mitigate the potential attacks. As the security fundamental basis, the keys for protection of MBS traffic are required.

Compared with UE keys, the keys for protection of MBS traffic are one-to-many keys. When UE joins the MBS session, only authorized users are able to receive the keys delivered from the key generator for protection of MBS traffic. UEs might also leave an MBS session or be compromised.

### 5.3.2 Security threats

If the keys for protection of MBS traffic are not confidentiality protected, an attacker may use the 3GPP network to gain "free access" of MBS services.

If the keys for protection of MBS traffic are not integrity or anti-replay protected, the authorised users may not be able to acquire the MBS traffic properly.

If the keys for protecting the MBS traffic cannot be updated, then:

* If a device in the group leaves, the device might be able to access the content after leaving,
* If a device joins the group, the device might be able to access previous content,
* If a device in the group is malicious, the device might be able to inject fake content.

### 5.3.3 Potential security requirements

The distribution of the keys for protection of MBS traffic between the key generator and the UE shall be confidentiality, integrity and anti-replay protected.

The 5GS shall be able to update the keys used to protect the MBS traffic.

## 5.4 Key Issue # 4: Security protection between AF and 5GC

### 5.4.1 Key issue details

The adopted baseline architecture in TR 23.757 [2] provides the Network Functions including MBSF and NEF at Service Layer and exposure to Application Function. MBSF User Plane Function is denoted MBSF-U and MBSF Control Plane Function is denoted MBSF-C. These NFs support external exposure of capabilities to AF and interaction with provider.

The reference architecture provides the configuration variants for AF interaction with 5G Core Network, usage of NEF or MBSF-C in the control plane, and usage of N6, MB2-C or xMB-U in user plane. Three configuration options are descripted including (1) No MBSF, (2) MBSF, N33 towards AF and (3) MBSF, MB2-C/xMB-C towards AF. The protection between AF and NEF/MBSF-C/MBSF-U is needed.

### 5.4.2 Security threats

If the interface between 5GC and AF is not well protected, the attacker may eavesdrop, modify or replay the message. In addition, the deliberated manipulation of the data between the 5GC and AF may disturb the communication.

If mutual authentication between 5GC and AF is not supported, the attacker may impersonate the actual source and publish fake content.

### 5.4.3 Potential security requirements

Integrity protection, replay protection and confidentiality protection for communication between 5GC and AF shall be supported..

Mutual authentication between 5GC and AF shall be supported.

The 5GC shall be able to determine whether the AF is authorized to interact with the relevant Network Functions.

## 5.X Key issue #X: <Key issue name>

### 5.X.1 Key issue details

### 5.X.2 Threats

### 5.X.3 Potential security requirements

# 6 Proposed solutions

Editor’s Note: This clause will contain the proposed solutions

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Solutions | Key Issues | | | | |
| 1 | 2 | 3 | 4 | X |
| #1: protect MBS traffic in transport layer |  | x | x |  |  |
| #2: protect MBS traffic in service layer |  | x | x |  |  |
| #3: MBS Traffic Protection |  | x | x |  |  |
| #4: Authentication and authorization for multicast communication service | x |  |  |  |  |
| #5: Authorization revocation | x |  |  |  |  |
| #6: Authentication and authorization for multicast communication service based on AKMA | x |  |  |  |  |
| #7: security protection between AF and 5GC |  |  |  | x |  |
| #8: MBS Traffic Protection |  | x | x |  |  |
| #9: Key update solution |  | x |  |  |  |
| #10: Secure framework for Key distribution in MBS |  | x | x |  |  |
| #11: Update the keys used to protect the MBS traffic |  | x |  |  |  |
| #12: Protection of MBS traffic at service layer based on GBA |  | x | x |  |  |
| #13: Key generation and distribution for MBS |  | x | x |  |  |
| #X: <Solution name> |  |  |  |  |  |

Editor's note: This clause describes the mapping between solutions and key issues.

## 6.1 Solution #1: Protection of MBS traffic in transport layer

### 6.1.1 Solution overview

This solution addresses Key Issue 2&3 to support the secure MBS traffic delivery from context provider to multiple UEs through 5GS. The keys for protection of MBS traffic are generated in the RAN nodes and distributed to UEs. The UEs, which belong to a multicast group, acquire the same keys in the RAN node. The security protection is enabled in transport layer.

### 6.1.2 Solution details

UE

(MB-) SMF

AMF

RAN

UPF

UDM

Content Provider

2. Multicast announcement

4.Nsmf PDU session update SMcontext

(multicast\_group\_info)

5.Multicast distribution session check

6.NamfcommunicationN1N2messageTransfer

7.N2 session request

（multicast\_group\_info）

1. UE registration and PDU session establishment

8. generate K\_group, and select the security algorithms

9. RRC reconfiguration request

（key\_ID, K\_group\_enc, K\_group\_int, security algorithms）

10. UE recieves and stores the security info

11. continue with the multicast service initiation procedure

3.PDU session modification request

(multicast\_group\_info)

**Figure 6.1.1-1. The procedure to protect MBS traffic in transport layer**

The procedure is described as follows:

1. The UE registers in 5GS and establishes a PDU session.
2. The content provider announces the availability of multicast using higher layers (e.g., application layer).
3. The UE sends the PDU Session Modification Request. Information about multicast group including identifier of the multicast group, which UE wants to join, shall be sent. Multicast\_group\_ID can be multicast address or other identifiers.
4. The AMF invokes Nsmf\_PDUSession\_UpdateSMContext, in which information about multicast group is included. The SMF checks whether the UE is authorized to receive the requested multicast service based on the UE’s subscription information.

Editor’s Note: Step 3&4 need to be revised if SA2 agrees to support UE’s multicast session join/leave operation via UP e.g. IGMP Join/Leave.

1. If MBS context is not available in (MB-)SMF, (MB-)SMF interacts with UDM to check whether a multicast context for the multicast group exists in the system.
2. (MB-)SMF requests the AMF to transfer a message to the RAN node using the Namf\_N1N2MessageTransfer service to create a multicast context in the RAN, if it does not exist already. In addition, the SMF sends a security policy for the multicast service to the gNB via AMF. Security policy indicates whether confidentiality and/or integrity protection needs to be activated or not for all bearers belonging to that MBS service.
3. The N2 session modification request is sent to the RAN, in which information about multicast group and the security policy is included.
4. RAN check whether the MBS security context for this multicast group is available. MBS security context, which is used for MBS traffic protection, includes the key\_ID, K\_group\_enc, K\_group\_int, encryption and integrity algorithms. The key\_ID is the key identifier and associated with the K\_group\_enc and K\_group\_int. K\_group\_enc and K\_group\_int are used for encryption and integrity protection of MBS traffic respectively.

If not, RAN generates K\_group and derives the K\_group\_enc and K\_group\_int. The encryption and integrity algorithms are selected. The MBS security context is stored until all the UEs in the multicast group have left the RAN.

NOTE 1: The K\_group generation method is randomly generated by the RAN node when needed.

NOTE 2: The RAN node should update K\_group to ensure that the same PDCP COUNT value is not used multiple times to encrypt and/or integrity protect the MRB traffic..

1. The MBS security context is distributed from RAN to UE. The RRC Reconfiguration message further contains the current PDCP COUNT value for the K\_group.

NOTE: Inclusion of the current PDCP COUNT value in RRC Reconfiguration message is to ensure the UE of the current multicast PDCP COUNT at the time of joining the multicast PDU session since PDCP PDU header does not carry the full PDCP PDU count value.

Editor’s Note: PDCP COUNT setting for the MRB should be determined in coordination with RAN WGs.

1. UE receives and stores the MBS security context for the multicast group.
2. Continue with the multicast service initiation procedure. Then, the UE decrypts and/or checks the integrity of PDCP PDUs sent over the K\_group based on the security policy.

NOTE 3: The support for mobility of UEs is addressed in other solutions.

#### 6.1.2.1 Security handling in handover

In handover, if a UE has established an MBS PDU session and the corresponding bearer(s) (i.e., MRB(s)) with the source RAN node, the MRB(s) needs to be handed over to the target RAN node. There are two handover scenarios that need to be considered.

* If the target RAN node has already created an MBS security context for the MBS PDU session that the UE has established with the source RAN node, the target RAN node provides the MBS security context to the UE via the source RAN node.

NOTE 4: It is possible that the target RAN node creates an MBS security context for the MBS PDU session when it has received a Handover request from the source RAN node.

* If the target RAN node has not created the MBS security context associated with the MBS PDU session, the target RAN node configures the DRB(s) for the MBS PDU session for the UE and provides this configuration information to the UE via the source RAN node. The security activation status of DRB(s) is same as the security activation status of MRB(s) for the MBS PDU session.

The above security handling of MBS traffic during the handover is applicable to both Xn-based and N2-based Handover procedures.

### 6.1.3 Solution evaluation

This solution fulfils the potential security requirements for the key issue#2&3. This solution provides the protection for the MBS traffic in transport layer between the RAN node and the UE.

K\_group is a one-to-many key to protect the MBS traffic, and is distributed and updated in a secure way.

## 6.2 Solution #2: protect MBS traffic in service layer

### 6.2.1 Solution overview

This solution addresses Key Issue 2&3 to support the secure MBS traffic delivery from context provider to multiple UEs through 5GS. In the agreed architecture in TR 23.757 [2], the MBSF-U (Multicast/Broadcast Service Function-User plane) is defined as a new entity to handle the payload part to cater for the service level functions and management. MBSF-C (Multicast/Broadcast Service Function-Control plane) is defined as a new entity to functionality to handle the control plane signalling. This solution protects the MBS traffic between the MBSF-U in the operator domain and the UE. It is independent to the protection in the application layer from the content provider.

The keys for protection of MBS traffic are generated in the SMF. Afterwards, the keys are distributed to UEs and MBSF-U respectively. The UEs, which belongs to a multicast group, acquire the same keys in the MBSF-U. The keys can be updated in an efficient way.

### 6.2.2 Solution details

3.PDU session modification request

(multicast\_group\_info)

4.Nsmf PDU session update SMcontext

(multicast\_group\_info)

5.Multicast distribution session check

6.NamfcommunicationN1N2messageTransfer

7.N2 session request

2. Multicast announcement

1. UE registration and PDU session establishment

AMF

RAN

UE

(MB)-SMF

MBSF-C

AUSF

UDM

16. generate K\_group, K\_transport\_i, and select the security algorithms

8. RRC reconfiguration request

9. UE derive MUK based on Kausf and multicast\_group\_info

15. continue with the multicast service initiation procedure

Content Provider

11. AUSF derive MUK based on Kausf and multicast\_group\_info

10.MUK request

(multicast\_group\_info)

12.MUK response

(MUK)

13.MUK distribution

(MUK)

14. ACK

18a. transport key response

EMUK（key\_ID, K\_enc, K\_int, security algorithms）

17. transport and traffic key request

(token)

18b.key response and update

EMUK transport\_1（group\_key\_ID, , K\_group）,…, EK\_transport\_M (group\_key\_ID, K\_group), H=Hash(K\_group\_ID)

**Figure 6.2.2-1.The procedure to protect MBS traffic in service layer**

The procedure is described as follows:

1. The UE registers 5GS and establishs a PDU session.
2. The content provider announces the availability of multicast using higher layers (e.g., application layer).
3. The UE sends the PDU Session Modification Request. Information about multicast group including identifer of the multicast group which UE wants to join, shall be sent. Multicast\_group\_ID can be multicast address or other identifier.
4. The AMF invokes Nsmf\_PDUSession\_UpdateSMContext, in which information about multicast group is included.

NOTE 1: It’s SA2’s choice to decide whether the network and UE support multicast session join/leave operation via UP e.g. IGMP Join/Leave.

1. If MBS context is not available in (MB)-SMF, (MB)-SMF interacts with UDM/UDR to check whether a multicast context for the multicast group exists in the system.
2. (MB)-SMF requests the AMF to transfer a message to the RAN node using the Namf\_N1N2MessageTransfer service to create a multicast context in the RAN, if it does not exist already. IP address of MBSF-C may be included if needed for UE to find MBSF-C.
3. The N2 session modification request is sent to the RAN.
4. RAN sends RRC reconfiguration request message to UE.
5. If UE is allowed to access the MBS service, UE derives Multicast User Key (MUK). The input key KEY is Kausf. The parameters are used to form the input string to the KDF including Multicast\_group\_ID.

This solution assumes that MUK update and re-authentication are independent. If reauthentication is performed, the UE still uses the current MUK. The UE will also try to process the MBS traffic with its known group key to avoid introducing unnecessary delays. The MUK and group key may be updated based on update policy after re-authentication.

NOTE 2: The details of MUK derivation will be discussed in the normative work.

NOTE 3: Depending on which solutions are concluded to be chosen for KI#1 and KI#3, the details related to “reauthentication” and “protection of MBS traffic” and “MUK/group key update” might need to be adapted. This can be left to normative phase.

1. (MB)-SMF requests MUK and sends Multicast\_group\_ID to AUSF.
2. AUSF derives Multicast User Key (MUK) based on Kasuf and Multicast\_group\_ID. When re-authentication runs, the AUSF is not required to generate a new MUK immediately. The MUK is derived when request is received from SMF.
3. AUSF responds to SMF with MUK.
4. (MB)-SMF distributes MUK to MBSF-C.
5. MBSF-C receives and stores the MUK. Afterwards, ACK is reponded to SMF.
6. Continue with the multicast service initiation procedure.
7. MBSF-C checks whether the MBS security context for this multicast group is available. MBS security context, which is used for MBS traffic protection, includes the key\_ID, K\_group\_enc, K\_group\_int, encryption and integrity algorithms. The key\_ID is used to indicate which key pair is used. K\_group\_enc and K\_group\_int are used for encryption and integrity protection of MBS traffic respectively.

If not, MBSF-C generates K\_group and derives the K\_group\_enc and K\_group\_int. The encryption and integrity algorithms are selected.

The MBS security context is distributed from MBSF-C to MBSF-U.

1. UE calculates token based on MUK and requests traffic key to MBSF-C. The token is secured with digital signatures or Message Authentication Codes (MAC). The input parameter includes UE\_id, Multicast\_group\_ID, and fresh parameters.
2. MBSF-C verifies the token using MUK and distributes the MBS security context to UE if succeeded.

NOTE 4: If roaming aspect is supported, MUK is calculated in home network.

The above text describes the security handling when SMF and MB-SMF are co-located. If SMF and MB-SMF are deployed separately, MB-SMF requests MUK from AUSF and distributed MUK to MBSF-C.

### 6.2.2.1 MBS group key distribution and update

This section explains the logic of steps 18a and 18b in Figure 6.2.2-1 to support MBS group key distribution and update based on the two approaches described in Solution #9.

**Default approach:**

This default approach uses only Step 18a.

Step 18a relies on K=K\_group, i.e., this message is used to directly update K\_group by means of MUK.

**Communication optimized approach:**

The distribution and update of the group key is done by means of the two messages shown in Steps 18a and 18b:

* Message 18a: in this meassage, K=K\_transport\_i and is used to provide the UE with the key transport for the set it belongs to protected with the UE’s MUK.

Upon reception, a UE first verifies the message authentication code, and if it is correct, it decrypts its transport key. Freshness can be achieved in multiple ways. For instance, an increasing initialization vector can be used that depends on the initial access token exchanged in Step 17.

* Message 18b: the new group key is distributed by protecting it with the transport keys in a point-to-point or in multicast messages. The hash of the new group key H is included in this message.

Upon reception, a UE first searches the part of the message that is addressed to its set. For instance, if the UE belongs to set z, the UE needs to look for EK\_transport\_z{K\_group}. Then, the UE verifies the message authentication code, and if it is correct, it decrypts the new group key. Freshness can be achieved by using the same freshness counter as used for the distribution of MBS traffic. Finally, the UE also checks whether the hash of the decrypted key equals the hash H of the group key that is appended at the end of this message.

These two messages 18a and 18b can be combined to address different situations:

1. Initial key distribution to a UE: the UE is provided with its transport key and the group key in a same message combining 18a and 18b.
2. Key update triggered by a too long usage of key group: Message 18b is used to distribute a new group key to all UEs.
3. Key update triggered by a new device joining the group: Message 18a is used to deliver the corresponding transport key to the new UE. Then, Message 18b is used to distribute a new group key to all UEs.
4. Key update triggered by a UE leaving/being revoked: If a UE leaves or is revoked, its transport key associated to its set and the group key are compromised. To deal with this situation, Message 18a is sent to the L-1 UEs in its set to update the transport key. Afterwards, message 18b is used to distribute a new group key to all UEs.

### 6.2.3 Solution evaluation

The solution fulfils the potential security requirements given in the key issues#2&3. This solution protects the MBS traffic in service layer between the MBSF-U in the operator domain and the UE.

MUK is UE-specific key derived based on Kausf and Multicast\_group\_ID. K\_group is a one-to-many key to protect the MBS traffic, and is distributed and updated in user plane in a secure way.

This solution requires a new security protocol between the UE and the MBSF-C for mutual authentication and transport of the MBS keys.

Editor’s Note: Further evaluation if FFS.

## 6.3 Solution #3: MBS Traffic Protection

### 6.3.1 Solution overview

This solution addresses both KI#2 and KI#3. It is based on the converged architecture in TR 23.757 [2] which is concluded as the adopted architecture for 5G MBS.

According to TR 23.757 [2], in the adopted architecture, the MBSTF (Multicast Broadcast Service Transport Function ) and MBSF(Multicast Broadcast Service Function ) are two functional components introduced at Service Layer. MBSTF is the media anchor for MBS data, performs generic packet transport functionalities such as framing, packet encoding, etc. MBSF provides service level functionality to support MBS, interacts with AF and MB-SMF for session operations and transport, controls MBSTF, and etc. Both MBSTF and MBSF belong to the operator domain.

In this solution, the MBS traffic is protected between the MBSTF and the UE, and the protection is transparent to the content provider. MBS Traffic Key (MTK) is generated by MBSF and securely distributed to the MBSTF and the UEs through the control plane. MBSTF uses the MTK to protect the MBS traffic before sending them out to the UE.

### 6.3.2 Solution details

Figure 6.3.2-1 shows the call flow for secure MTK distribution and multicast data protetion. The call flow in Figure 6.3.2-1 is based on the concluded multicast call flow in TR 23.757 [2]. In the call flow MB-SMF is another functional component introduced in the adopted architecture in TR 23.757 [2]. MB-SMF is used for MBS session management (including QoS control), control of MBS transport, and etc. MB-SMF may be standalone or co-located with existing network function.



**Figure 6.3.2-1: MBS key distribution**

Step 1. The AF of the content provider provisions to the MBSF the information on a multicast session including the the multicast group ID and the security policy for the multicast session. The multicast group ID, which identifies the multicast session, can eithr be a TMGI or source specific IP multicast address. The NEF is involved in the provision if the content provider belongs to a 3rd party.

Step 2. If the security policy indicates the multicast session needs security protection, MBSF will generate a MTK and the associated key identifier (KID) for the multicast session. MBSF sends a request message including the multicast group ID to request MB-SMF to reserve source for the session. MBSF also provisions the MTK and the KID to MB-SMF in the request message.

MTK needs to be different for each multicast session, therefore, the multicast group ID may be used to generate MTK. The KID consists of a Key Domain ID and a MTK ID. The Key Domain ID is MCC|| MNC. A MTK ID is a number that is different for each MTK.

Step 3. MBSF sends the security policy and the MTK and KID to MBSTF.

Step 4. There are other steps defined in concluded multicast call flows in TR 23.757 [2] for the multicast session configuration at the core network (e.g. RAN configuration), the details of which are omitted in this solution as they are irrelevant to solving the key issue #2 and #3.

Step 5. To join a multicast group via control plane, UE sends to SMF the request for a PDU session establishment/modification and includes in the request the multicast group ID the UE wishes to join.

Step 6. SMF sends to MB-SMF a request for the contexts of the multicast session identified by the multicast group ID.

Step 7. MB-SMF replies to SMF with MTK and KID in the response message.

Step 8. There are other steps for the PDU session establishment/modification (e.g. N4 session creation or modification).

Step 9. SMF sends the received MTK and the KID to UE.

Step 10. When the multicast data of the session identified by the multicast group ID is received at MBSTF, MBSTF uses the received MTK to protect the multicast data if the received security policy from step 3 indicates security policy is needed. The protected multicast data along with the KID are sent to the UE. Based on the received KID, the UE uses the received MTK in step 9 to decrypt the protected multicast data and/or verify the integrity of the protected multicast data.

### 6.3.3 Solution evaluation

In the solution, the multicast data protection is performed between UE and MBSTF, the anchor point of the multicast data. This is similar to the MBS protection before 5G, in which the protection is performed between BM-SC (the data anchor) and UE.

The MTK and KID，used for the multicast data protection, is generated by MBSF when needed and securely distributed to UE over the control plane, and to MBSTF. The solution conforms to the call flows concluded in TR 23.757 [2].

The solution does not affect RAN or UPF or MB-UPF. Moreover, during the transmission of the multicast data, the solution exposes the unprocted multicast data to the least network functions possible, i.e. only MBSTF has access to the unprotected multicast data.

The protection provided by the solution is transparent to UE mobility.

The solution does not rely on GBA or AKMA.

Editor’s Note: Further evaluation is FFS.

## 6.4 Solution #4: Authentication and authorization for multicast communication service

### 6.4.1 Solution overview

This solution, which is based on existing EAP based secondary authentication, addresses the key issue #1 Security of authentication and authorization for multicast communication service. This solution also comprises authorization revocation aspects. The solution is based on the concluded architecture in TR 23.757 [2].

### 6.4.2 Solution details

In the solution below, the (MB-)SMF is either SMF, which is for managing in the MBS session, controlling of MBS transport and etc, or SMF for managing the per-UE PDU session. The two may be co-located.

#### 6.4.2.1 Authentication and authorization



Figure 6.4.2-1: Authentication and authorization procedure

1. UE initiates multicast session join, specificall, UE sends the request for a PDU session establishment/modification and includes the multicast session ID identifying the multicast session that UE wishes to join. The request is forwarded to the (MB-)SMF.. The multicast session ID can either be a TMGI (Temporary Mobile Group Identifier) or a source specific IP multicast address.

If not available locally, the (MB-)SMF retrieves the subscription data from the UDM.

1. The (MB-)SMF determines that authentication and authorization is needed for the multicast session based on the subscription data.
2. The (MB-)SMF sends a message to the UE to request the EAP identity used for the multicast session authentication and authorization. The message includes the multicast session ID.
3. The UE responds with the EAP identity and the multicast session ID to (MB-)SMF.

To avoid the round-trip in step 3 and 4, the UE may also send the EAP identity in step 1, similar to the EAP based secondary authentication by an external DN-AAA server in 33.501.

5-6. The (MB-)SMF sends the received EAP identity and multicast session ID to the AAA server through a (MB-)UPF.

1. EAP messages are exchanged between the AAA server and UE.
2. After the successful completion of the authentication procedure, the AAA server sends EAP Success message to the (MB-)SMF.
3. (MB-)SMF sends the EAP access and the multicast session ID to the UE.

Note: SMF and MB-SMF may or may not be co-located. If they are co-located, the above procedure apparently applies. If they are not, the above procedure still applies with the adataption that (MB-)SMF is replaced with MB-SMF and the communication between MB-SMF and UE is via SMF.

#### 6.4.2.2 Authorization revocation



Figure 6.4.2-2: Authentication Revocation procedure

Step 1: AAA Server sends to (MB-)UPF the request to revoke UE’s authorization to use the multicast communication service. The multicast service ID and UE ID is included. The multicast service ID may be a TMGI (Temporary Mobile Group Identifier) or a source specific IP multicast address. UE ID may be GPSI or UE IP address.

Step 2: (MB-)UPF sends to (MB-)SMF the request to revoke UE’s authorization to use the multicast communication service, including the received UE ID and multicast service ID.

Step 3: (MB-)SMF may release the corresponding session for the multicast service.

Step 4: (MB-)SMF sends the response to (MB-)UPF, including UE ID and multicast service ID.

Step 5: (MB-UPF) sends the resonse the AAA Server, including the received UE ID and multicast service ID.

Note: SMF and MB-SMF may or may not be co-located. If they are co-located, the above revocation procedure apparently applies. If they are not, the above revocation procedure still applies with the adataption that in (MB-)SMF is replaced with MB-SMF and in step 3, MB-SMF requests SMF to release the corresponding PDU session.

### 6.4.3 Solution evaluation

This solution addresses KI#1 “Security of authentication and authorization for multicast communication service”. It re-uses the EAP based secondary authentication and authorization in TS 33.501[6] with the adaptation that a TMGI or a source specific IP multicast address is used to identify a multicast service.

Editor's Note: Further evaluation is FFS.

## 6.5 Solution #5: Authorization revocation

### 6.5.1 Solution overview

This solution proposes how the authorization revocation is performed, for KI#1. When the content provider decides that the user authorization for a multicast service needs to be revoked, the content provider will inform the UDM/UDR about the revocation. The UDM/UDR will accordingly instructs the SMF to release the corresponding resources established for the user for the multicast service.

### 6.5.2 Solution details

In the solution below, the (MB-)SMF is either the MB-SMF, which is for managing in the MBS session, controlling of MBS transport and etc., or the SMF for managing the per-UE PDU session. MB-SMF and SMF may be co-located.



Figure 6.5.2-1: Authorization revocation

1. The AF of the content provider provisions the information on the multicast session including the authorization information to the UDM/UDR. The NEF is involved in the provisioning if the content provider belongs to a 3rd party.
2. The UE has successfully joined a multicast session.
3. The (MB-)SMF subscribes to the UDM/UDR on the changes of the multicast information including the authorization information. Step 2 may also be performed during step 1. (MB-)SMF may get data from UDR via UDM/PCF/NEF.
4. The content provider updates the multicast information. The NEF is involved in the provisioning if the content provider belongs to a 3rd party.
5. The UDM/UDR notifies the (MB-)SMF when the authorization for a UE to join the multicast service/application is revoked. The multicast session ID and UE identifier (i.e. SUPI) is included in the notification. The multicast session ID can either be a Temporary Mobile Group Identifier (TMGI) or a source specific IP multicast address.
6. The (MB-)SMF may release the PDU session for the multicast session identified by the received multicast session ID if no UE is left using the multicast session.

When a UE decides to revoke the authorization, the UE may send a request to the content provider in the application layer, then the step 3, 4, and 5 of the solution apply, or the UE may release the PDU session for the mulicast session.

Note: If MB-SMF and SMF are co-located, the above procedure applies. If MB-SMF and SMF are not co-located, the above procedure still apply with the adaptation that (MB-)SMF is replaced by MB-SMF and the communication between MB-SMF and UE is via SMF .

### 6.5.3 Solution evaluation

The solution provides the authorization revocation for a multicast session, for KI#1

## 6.6 Solution #6: Authentication and authorization for multicast communication service based on AKMA

### 6.6.1 Solution overview

This solution, which is based on AKMA, addresses the key issue #1 Security of authentication and authorization for multicast communication service.

### 6.2 Solution details

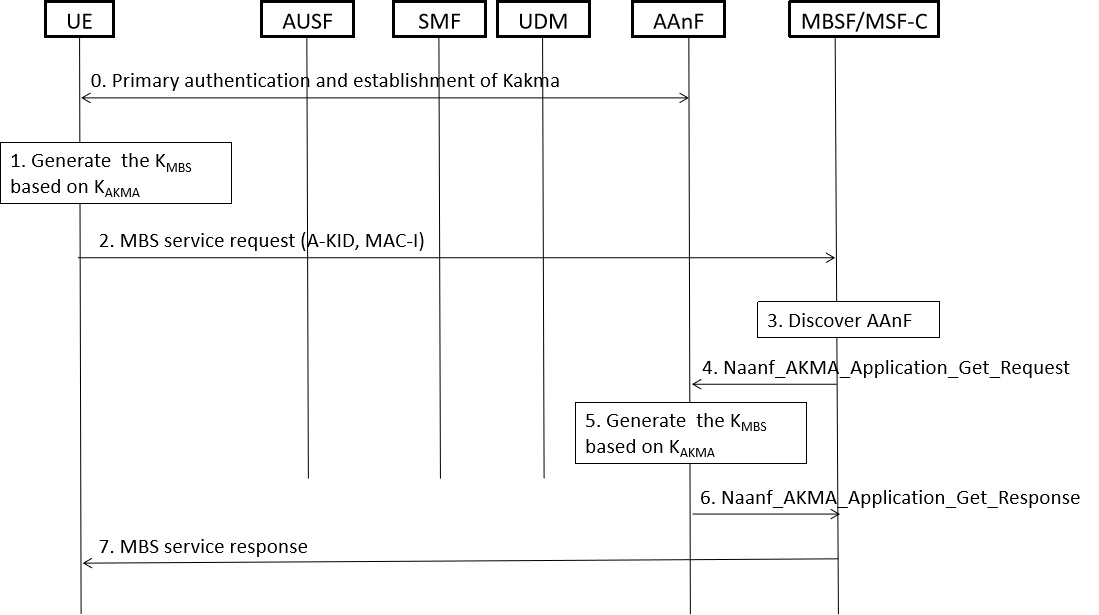


Figure 6.6.2-1 Authentication between the MBSF/MSF-C and UE based AKMA

1. UE shall generate the AKMA Anchor Key (KAKMA) and the A-KID from the KAUSF before initiating communication with an AKMA Application Function, i.e MBSF/MSF-C, as specified in TS 33.535 [5].
2. UE derive a key KMBS for authentication with the MBSF/MSF-C .
3. When UE try to join the multicast service, UE computes MAC-I and then UE sends a MBS service request to MBSF/MSF-C. The service request include A-KID and MAC-I.

Editor’s Note: How to derive the MAC-I is FFS.

3-6. Upon receiving the request, the MBSF/MSF-U discovers the AAnF, then AAnF generates KMBS and sends the KMBS to MBSF/MSF-C. The AAnF discovery and selection is specified in the TS 33.535[5] clause 6.7. The MBSF/ MSF-C computes the MAC-I using KMBS, and check if it is the same with the received MAC-I from UE. If so, it means that the UE is authenticated and authorized to use the service.

Editor’s Note: How MBSF/MSF-C obtains authorization information is FFS.

7. The MBSF/MSF-C verifies the MAC-I using the KMBS, when the verification is succeed, and if the UE is authorized to perform the operation,Then the MBSF/MSF-C sends a service response to the UE.

### 6.6.3 Solution evaluation

This solution use AKMA framework to address security of authentication and authorization for multicast communication service.

Editor’s Note: Further evaluation is FFS

## 6.7 Solution # 7: security protection between AF and 5GC

### 6.7.1 Solution overview

This security solution is related to the key issue #4: "Security protection between AF and 5GC". The interface between the NEF/MBSF-C/MBSF-U and the AF used needs to be properly secured by providing confidentiality, integrity and replay protection. Mutual authentication is also needed. TS 33.501 [6] already defined the security aspects of NEF, which can be reused.

### 6.7.2 Solution details

The security aspects defined in clause 12 in TS 33.501[6] is applicable for both NEF, MBSF-C and MBSF-U. TLS based solution are reused to protect the interface between AF and 5GC.

### 6.7.3 Solution evaluation

The proposed solution fulfils the potential security requirements given in the related key issue.

## 6.8 Solution #8: MBS Traffic Protection

### 6.8.1 Solution overview

This solution addresses both KI#2 and KI#3.

According to TR 23.757 [2], in the adopted baseline architecture 3, the MBSF-U (Multicast/Broadcast Service Function-User plane) is defined as a new entity to handle the payload part to cater for the service level functions and management.

In this solution, MBS traffic is protected between the MBSF-U in the operator domain and the UE, and it is transparent to the content provider. MBS Traffic Key (MTK) is generated by (MB-)SMF and distributed to the UEs through the control plane. In addition, key update is also supported. MBSF-U uses the MTK to protect the MBS traffic before sending them out to the UE.

### 6.8.2 Solution details

In the procedure below, (MB-)SMF is the enhanced SMF that supports MBS.

UE

(MB-)SMF

UDM

MBSF-U

Content Provider

1. Multicast request

3. MBS subscription Response

5. MTK establish/update request message

(MTK, KID)

8.MBS data

4. If MTK is not available in UDM or key update is needed, generate MTK and KID

2. MBS subscription Request

6. MTK establish/update request message

(MTK, KID)

7. PDU session establish/modification

(MTK, KID)

8.MBS data

1. Multicast configuration

**Figure 6.8.2-1: MBS traffic protection procedure**

1. The AF of the content provider provides the multicast configuration information to UDM. The information includes UE authorization information and indicates whether the security protection provided by PLMN is needed. The NEF is involved in the provision if the content provider belongs to a 3rd party.
2. The UE initiates the request for a PDU session establishment/modification. The identifier for the MBS application is included. The request is forwarded to the (MB-)SMF through the control plane.

Note: Multicast session join operation via UP may be supported based on the conclusion from SA2.

1. If the (MB-)SMF does not have the subscription data already, the (MB-)SMF sends a request for the subscription data to the UDM/UDR.
2. The UE authorization information is included in the response message. If the security protection provided by PLMN is needed and MTK and KID is available, the UDM/UDR replies with the stored MTK and KID. Step 4-7 are skipped if key updated is not needed.
3. If MTK and KID is not available in UDM/UDR or the MTK needs to be updated based on local policy, (MB-)SMF shall generate a MTK and the associated key identifier (KID) for the MBS application. KID contains the Key Group part and the Key Number part. Key Group part could be the MBS Session ID. Key number part is used to distinguish MTKs that have the same Key Group part.

If MBSF-C is determined to generate MTK and KID, (MB-)SMF retrieves MTK and KID from MBSF-C when needed.

1. (MB-)SMF provisions the generated MTK and the KID to the MBSF-U.
2. (MB-)SMF provisions the generated MTK and the KID to the UDM/UDR.
3. If UE is authorised to use the MBS feature and allowed to access the data from the MBS application, the (MB-)SMF sends the MTK and the KID to the UE. The UP security policy is set to “not needed” which indicates UP confidentiality and/or UP integrity protection shall not be activated for all DRBs belonging to that MBS session to avoid redundant protection.
4. When MBS traffic is received at the MBSF-U/MSF-U, the MBSF-U/MSF-U uses the received MTK to protect the MBS traffic. The protected MBS traffic along with the KID are sent to the UE.

The UE uses the received MTK in step 7 to process the MBS traffic.

The above text descripts the security handling when SMF and MB-SMF are co-located. If SMF and MB-SMF are deployed separately, MB-SMF performs step 2-6. For step 8, the MB-SMF sends the MTK and the KID to the UE via SMF.

### 6.8.3 Solution evaluation

This solution fulfils the potential security requirements given in the key issue#2&3. This solution provides the protection for the MBS traffic between the MBSF-U in the operator domain and the UE.

MTK is a one-to-many key to protect the MBS traffic, and is distributed and updated in control plane in a secure way.

## 6.9 Solution #9: Key update solution

### 6.9.1 Solution overview

This solution addresses Key Issue 3 to support the update or revocation of the group key.

This solution is described in the context of Solution 1. The keys for protection of MBS traffic are generated in the RAN nodes and distributed to UEs. The UEs, which belong to a multicast group, acquire the same group keys in the RAN node. The security protection is enabled in transport layer. MUK and GK in this description refer to UE\_K and K\_group in Solution #1, respectively.

The solution includes two approaches, a basic and a communication optimized approach that provides better performance, in particular, when the number of subscribed UEs is high.

This key update solution can be applied to service layer solutions, e.g., Solution 2 uses it in Section 6.2.2.1.

### 6.9.2 Solution Details

This subsection explains how the group key is to be updated. Reasons to trigger this procedure include UE mobility, presence of malicious UEs, or long usage of the group key.

**Default approach:**

The default group key update version uses key hierarchy:

MUK 🡪 GK

In this approach, each UE has two keys: a device specific key, MUK, and a group key GK shared with all N devices in a RAN subscribed to the same MBS service and used to protect the MBS traffic. MUK refers the device specific UE keys used to protect message 9 in 6.1.1-1, i.e., the RRC reconfiguration request.

In the following, K1 🡪 K2 means that K1 is used to protect the transport of K2 by ensuring its confidentiality, integrity, and freshness. In the following, EK1{K2} is used to indicate the secure delivery of K2 by protecting it with K1.

Group key update in the following situations:

1. Initial group key distribution,
2. Key update due to a too long usage,
3. Key update triggered by a new device joining the group, and
4. Key update triggered by a UE leaving/being revoked

might involve the following steps:

* RAN generating a new group key (Step 8 in Figure 6.1.1-1 and Step 8 in Figure 6.9.2-1).
* RAN sending RRC reconfiguration request unicast messages to all UEs subscribed to a given MBS service (Step 9 in Figure 6.1.1-1 and Step 9 in Figure 6.9.2-1).
* UE receiving and storing the security information (Step 10 in Figure 6.1.1-1 and Step 10 in Figure 6.9.2-1).



**Figure 6.9.2-1. Default key update**

**Communication optimized approach:**

Alternatively, the following key hierarchy is used:

MUK 🡪 TK\_i 🡪 GK

In this approach, each UE has three keys: a device specific key, MUK; a transport key TK\_i shared with L - 1 devices in the same set S\_i; a group key GK shared with all N devices and used to protect the MBS traffic. The transport keys and the group key shall be generated independently from each other in a secure way. The MUK is used to securely deliver transport keys in a point-to-point connection. The transport keys are used to securely deliver the group key.

In this approach, a multicast group with N members is divided into M disjoint sets S\_i of UEs with i={1,…,M}. Each set has roughly L ~ N/M UEs.

The transport keys are used to securely deliver the group key updates as part of the data exchanged over the regular MBS traffic. The process to extract this data is as follows:

* any UE decrypts, checks the integrity, and freshness of the multicast data sent over the transport layer using the current GK.
* a UE belonging to set z looks for ETK\_z{GK}. Then, the UE verifies the message authentication code, and if it is correct, it decrypts the new group key. Freshness can be achieved by using the same freshness counter as used for the distribution of MBS traffic. Finally, the UE also checks whether the hash of the new decrypted group key equals the hash H of the group key that is appended at the end of this multicast group key message. This multicast group key message (MGKM) is:

MGKM: ETK \_1{GK}, …, ETK\_M{GK }, H=Hash(GK)

The group key update procedure might involve – depending on the key update policy -- the following steps:

1. **During initial group key distribution**: MUK is used in the initial group key distribution to securely distribute transport keys and GK in a point-to-point connection by means of RRC reconfiguration request messages (Step 9 in Figure 6.1.1-1 and Steps 8, 9, and 10 in Figure 6.9.2-2).
2. **Group key update due to a too long usage** might require the gNB generating a new group key and sending the MGKM over the MBS transport layer. Steps 8 and 12 in Figure 6.9.2-2.
3. **Key update triggered by a new device joining the group or a** **UE leaving/being revoked** might require (1) RAN generating a new group key and a new transport key (Steps 8 and 9 in Figure 6.9.2-2), (2) sending L-1 RRC reconfiguration request messages to the L-1 UEs that were in the same set as the device that is leaving or has been revoked by means of RRC reconfiguration request messages (Step 9 in Figure 6.1.1-1 and Steps 10 in Figure 6.9.2-2); and (3) sending the MGKM over the MBS transport layer (Step 12 in Figure 6.9.2-2).

NOTE: The above steps are aligned with the key update conditions in 6.9.2.2 derived from TS 33.246. The specific required steps can be defined during normative phase or depend on the operator’s policy.



**Figure 6.9.2-2. Communication optimized key update**

### 6.9.2.1 Comparison between the default and optimized approaches

This communication optimized approach is useful to decrease the communication overhead to roughly 2 SQRT(N) compared with the default approach. This approach is efficient and resilient since the update of the group key due to a device leaving the group only requires L – 1 + M messages instead of N that would be required when only point-to-point messages are involved. For instance, if N=64, M=8, L=8, then the key update only requires L-1=7 point-to-point messages for the update of the transport key associated to the set of the device that is leaving and the multicast distribution of the MGKM for the group key update. This MGKM message trasports the group key protected with M different transport keys. The total number of messages is minimized when L=M=SQRT(N). Another choice might be M=1 so that there is a single transport key or M=N so that there are N transport keys. The following table provides a comparison in the number of messages required to update a transport key (TK) and the group key (GK) depending on the key update method (default or optimized) and configuration (number of transport keys).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Group size (N) | Number of transport keys (M) | Number of devices per set (L) | Number of messages required to the TK  (unicast) | Size of the MGKM multicast message  (in number of encrypted keys) |
| Default approach | 256 | 0 | 256 | 255 | 0 |
| 1600 | 0 | 1600 | 1599 | 0 |
| 10000 | 0 | 10000 | 9999 | 0 |
| Communication Optimized Approach | 256 | 1 | 256 | 255 | 1 |
| 1600 | 1 | 1600 | 1599 | 1 |
| 10000 | 1 | 10000 | 9999 | 1 |
| 256 | 16 | 16 | 15 | 16 |
| 1600 | 40 | 40 | 39 | 40 |
| 10000 | 100 | 100 | 99 | 100 |

The trade-offs between default and optimized approaches can also be compared from a computational view. To this end, we can consider the default approach and assume that 256 users in the same area, e.g., at a concert, are willing to receive the MBS traffic. We assume M= 16 independent groups, each group with a different group key. For instance, 16 groups in a RAN, each group with L= 16 devices. In this case, if a device leaves the MBS session, only the group key in the affected multicast group needs to be updated. The overhead of updating the group key is now as low as in the communication optimized approach; however, this approach requires encrypting/protecting the MBS bulk traffic with M = 16 different group keys, one per group. Thus, the computational overhead is a factor M worse. Note that this configuration also involves transmitting the same MBS content M times in parallel.

Since M transport keys are used, an attacker that compromises a UE can only try to update the group key of up to L-1 devices. This limits the impact of such an attack, in particular, compared with a situation in which a single transport key is used to protect the update of the group key where N-1 would be affected.

Furthermore, the hash of the group key is included so that devices in other sets – that potentially might also receive this fake group key update -- can check the consistency by means of H, detect the group key update attack, and inform the RAN.

### 6.9.2.2 Key update conditions

Refering to TS 33.246-C.4 (R5c), the key update conditions depend on the operator and might include:

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

The key update protocol supports the operator to perform re-keying as frequently as necessary in an efficient way.

* To address 1), the GK must be updated in a regular basis based on a policy deployed to RAN.
* To address 2) and 3), a new GK must be distributed to all devices. In the case of the communication optimized approach, the corresponding TK must be updated first.



**Figure 6.9.2.2-1. Definition and distribution of key update conditions**

To implement these key update conditions, the (MB-)SMF has to define and deploy key update policies to RAN via AMF (Step 1 and 2 in Figure 6.9.2.2-1) and the (MB-)SMF has to monitor key update condition events, e.g., when a user leaves or joins, and inform RAN via AMF (Step 4 and 5 in Figure 6.9.2.2-1). The RAN key update actions (Step 3 and 6 in Figure 6.9.2.2-1) might be any of the actions done by RAN in Figures 6.9.2-1 and 6.9.2-2.

### 6.9.2.3 Applicability to other solutions

The communication optimized approach described above has been used in the context of Solution #1 and Solution #2 (Section 6.2.2.1) and it is easily applicable to other solutions to reduce the key update signaling overhead. For instance, in Solution #11, the communication overhead of the key update mechanism in terms of point to point messages – Step 6 in Figure 6.11.2 -1 – can be reduced from N messages to ~ SQRT(N) messages, where N is the number of UEs in connected state that joined the MBS session, as follows:

* In Step 1, the MBSF-C has to generate M different Transport Keys (TKs) and distribute them to MBSF-U and UEs. As in the communication optimized approach:
  + (1) each UE has a unique security key (NAS security), a TK, and a MTK. This section uses the term MTK as in Solution #11 whose role is equivalent to GK used in this section above. These keys are independent of each other;
  + (2) a NAS protected message is used to securely distribute the TK and the TK is used to securely distribute the MTK. Both TK and MTK can also be distributed to the UE at the same time; and
  + (3) disjoint sets of L UEs receive the same TK so that M•L ≥ N, where N is the total number of devices.
* In Step 3, the MBSF-C has to generate a new TK for the L-1 UEs in the same set of a UE whose authorization info has changed.
* In Step 4, KID2 is replaced by KID2’. KID2’ includes the identifier of the new MTK, KID2, concatenated (indicated as “|”) with the MGKM message defined above:

KID2’ := KID2|MGKM

Note 1: The MGKM message is generated by the MBSF-C and combined with KID2 into KID2’ to avoid the integration of any security functionalities into the MBSF-U.

Note 2: Details on the structure of KID2’ that acts as a container of KID2 and MGKM can be discussed during normative phase.

* In Step 5, the MBSF-C distributes the new TK to the (MB-)SMF.
* In Step 6, **ONLY** the L-1 UEs that shared the same TK as the UE whose authorization info has changed are updated by means of a point to point connection. This means that only L-1 unicast interactions are required, instead of N. These unicast messages are NAS protected.
* In Step 8, the MBSF-U uses MTK2 to protect the MBS traffic. The MBSF-U appends KID2’ to the message. A UE uses: (1) KID2 in KID2’ to determine the usage of a new MTK and (2) if the UE did not receive MTK2 in Step 6 by means of a unicast message, the UE uses the MGKM in KID2’ to access the new MTK2 by using its TK to decrypt/verify MTK2.

With this modifications, the key update overhead in Solution #11 is proportional to the square root of the number of UEs in the MBS session. This optimized signalling approach in 6.11.2.1 also facilitates interoperability with LTE networks.

## 6.9.3 Evaluation

This solution addresses Key issue #3 to manage, distribute, and update the keys required to protect the MBS traffic in the context of transport layer solution #1.

This solution can be applied to service layer solutions, e.g., Solution #2 uses it.

This solution describes a default and a communication optimized approach.

The communication optimized approach allows updating the group key used to protect the MBS traffic in a group with N devices with around root square of N (SQRT(N)) unicast messages in contrast with the default approach that requires N unicast messages. This means that *for the same key update signaling overhead*, the communication optimized approach allows supporting MBS groups a quadratic factor larger compared with the default approach without increasing the computational or communication overhead to protect/transmit the MBS traffic.

The choice M~L~SQRT(N) minimizes the total message size required to distribute a new group key and the total number of required encryptions to update the group key. This is because L-1 unicast messages need to be sent to L-1 UEs and the MGKM message includes M = N/L (rounded upwards) protected group keys. Thus, the total overhead in terms of protected group keys is L-1+N/L. This is minimized when L~SQRT(N).

Using M>1 transport keys and including the hash of the group key makes the communication optimized solution more resilient.

The communication overhead of the default approach is similar to the communication overhead of the rest of solutions of KI#3 in this TR in terms of the number of unicast messages required to distribute/update a group key.

Editor’s Note: Further evaluation is FFS.

## 6.10 Solution #10: Secure framework for Key distribution in MBS

### 6.10.1 Solution overview

This solution addresses the key issue #2 “security protection of MBS traffic” and Key issue #3 “security protection of key distribution”.

Encryption key for MBS session is generated at RAN and UE from parmeters like TMGI, multicast group token, rekeying token (needed only when rekeying, otherwise by default it is zero for initial key generation),encryption algorithm and algorithm ID. Integrity key for MBS session is generated at RAN and UE from parameters like Temporary Mobile Group Identifier (TMGI), multicast group token, rekeying token (needed only when rekeying, otherwise by default it is zero for initial key generation),integrity algorithm and algorithm ID.

When UE joins the multicast group identified by the TMGI and its session, after the PDU session establishment, SMF shares the multicast group token, TMGI, Rekeying token list , rekeying token ID to RAN via AMF. Rekeying token list contains many pre-generated re-keying token needed for this particular MBS session. Rekeying ID and respective rekeying token list is stored in RAN for future use. RAN and UE generates independently the encryption and integrity keys for this MBS session.MBS traffic is encrypted, and integrity protected at RAN level. Received MBS traffic is decrypted, and integrity check is performed at UE.

When a UE or few UEs leaves the MBS group, then rekeying token from the stored list in RAN is retrieved. Using this rekeying token, new keys are generated at RAN and UEs in the ongoing MBS session and further sessions, till another member leaves the group.

### 6.10.2 Solution details

Multicast key generation and the procedure to distribution of those keys from network to the UEs belonging to a multicast group identified by TMGI and rekeying procedure is described below in detail.

#### 6.10.2.1 MBS key generation



Figure 6.10.2-1 Key generation at UE and RAN

For the multicast broadcast encryption key generation for traffic KMTenc, the parameters like TMGI (Temporary mobile group identifier), multicast group token, re-keying token (if available, otherwise default value “0” is used), encryption algorithm and encryption algorithm ID are used. For the multicast broadcast integrity key generation for traffic KMTint, the parameters like TMGI (Temporary mobile group identifier), multicast group token, re-keying token (if available, otherwise default value “0” is used), integrity algorithm and integrity algorithm ID are used.

NOTE 1: As long as the “Multicast group Token” is not updated, the security of KMTenc and KMTint depends only on the rekeying token.

Figure 6.10.2-1 shows the key generation at UE and RAN.

(RAN node (Base stations) get the parameters for the key generation from the 5G core network nodes MB-SMF/AMF as detailed in TR 23.757).

#### 6.10.2.2 MBS procedure for key generation and traffic protection

Step 1: UE registers in the PLMN (see clause 4.2.2.2 of TS 23.502) and request the establishment of a PDU session (see clause 4.3.2.2 of TS 23.502). The UE also indicates its capability to receive multicast data over the radio. The AMF obtains information from the UDM whether the UE can join multicast sessions as part of the SMF Selection Subscription data. If so, for direct discovery, the AMF selects an SMF capable of handling multicast sessions based on locally configured data or a corresponding SMF capability stored in the NRF and also indicates the UE's capability to receive multicast data over the radio to the SMF.

Step 2: The content provider announces the availability of multicast using higher layers (e.g., application layer). The announcement includes at least the multicast address of a multicast group that UE can join.

Step 3: To join the multicast group session, steps 4 to 9 as described in TR 23.757 are followed.



Figure 6.10.2.2-1 MBS Procedure for key generation and traffic protection

Step 4: SMF requests AMF to transfer a message to RAN node using Namf\_N1N2Message Transfer service with multicast information along with multicast group token, TMGI, Rekeying token list, Rekying token id etc. Rekeying token list contains many pre-generated re-keying token and corresponding ids needed for this particular multicast group mangement.

NOTE 2: As an option, rekeying token id and rekeying token list sent during initial configuration from SMF to RAN, can be simplified by reducing the list to single key. This will avoid key management at RAN.

Step 5: N2 session request is sent to RAN with multicast related information received from SMF.

Step 6: Rekeying token list is stored in RAN for future purposes (in case of re-keying).

Step 7: RAN generates multicast key hierarchy (both encryption key and integrity key) needed for the traffic as shown in Figure 6.10.2.1-1.

Step 8: RAN shares in an integrity protected and encrypted RRC message, the multicast group token and MBS session ID TMGI to the respective UE. The multicast group token which palys the role of a group master key should of sufficient length for e.g.128bits.

Step 9: UE which joins the session will generate the MBS related keys (both encryption KMTenc and integrity keys KMTint).

Step 10: UPF(MB-UPF) receives multicast PDUs, either directly from the content provider or via the MBSF-U that can manipulate the data.

Step 10a: UPF(MB-UPF) sends multicast PDUs in the N3/N9 tunnel associated to the multicast distribution session to the RAN. There is only one tunnel per multicast distribution session and RAN node, i.e., all associated PDU sessions share this tunnel.

Step 10b: RAN performs the encryption of traffic using encryption key KMTenc and integrity protection by KMTint. RAN selects PTM or PTP radio bearers to deliver the multicast PDUs to UEs that joined the multicast group.

Step 11a: RAN performs the transmission using selected bearer.

Step 11b: Receiving multicast UEs which are part of this MBS session (matching the MBS group ID) will decrypt the traffic using encryption keys and also verifies the integrity check of the packets received.

Figure 6.10.2.2-1 shows the MBS procedure for key generation and traffic protection

NOTE 3: Security policies for PTM and PTP needs to be the same. RAN may decide to switch between PTM and PTP for a UE, if the security policies for PTM and PTP is not the same (e.g. PTM is protected but PTP is not protected), then security may be breached.

#### 6.10.2.3 MBS procedure for re-keying



Figure 6.10.2.3-1 MBS procedure for re-keying

Step 1: If a UE in a Multicast broadcast, is leaving the Multicast group, then respective SMF is informed about the UE leaving the Multicast group and the TMGI. If a UE joins a session, then PDU session estabilishment or modification happens with respective SMF.

Step 2: SMF informs the respective RAN via AMF about a UE leaving an MBS group and initiate a new MBS group management procedure. As one or few UEs leaving the group, same keys can not be used for ongoing MBS traffic.

Step 3: It is also possible that few of the UEs are actively listening to the ongoing MBS session while few of the UEs are in idle mode, may or may not be listening to the traffic. In order to update all the UE which belongs to the new (modified) multicast group, AMF pages the UEs which are in Idle state (which belongs to new multicast group), so that they will listen to the page (example: with cause mbskeyupdate) and further connect to the network. The UEs which have left the multicast group are excluded from the to be paged list.

NOTE: The privacy issue with group paging to be addressed during normative phase.

Step 4: UEs which were in Idle mode establishes connection to the respective base stations. UEs which were active UEs (already in connected mode) are aligned and will be in connected mode with the respective RAN. So, all the UEs in the MBS group identified by the TMGI under the coverage of a given base station are connected to the base station now.

Step 5: RAN selects the rekeying token from the list already received form SMF, as instructed by the SMF. All the RAN nodes have to select the same rekeying token, so to aid the same rekeying token selection, SMF also would have sent the rekeying token id to the RAN node. It is also option to send the rekeying token to the RAN nodes at this step directly without token id , to avoid sending the rekeying token list upfront.

NOTE 1: An alternative is to use different rekeying tokens per RAN node indicated by SMF. This would result in different multicast keys (both integrity key KMTint and encryption key KMTenc) at every RAN node.

Step 6: RAN shares in an integrity protected and encrypted RRC message, the rekeying token to respective UEs. The re-keying token should be of sufficient length, for e.g.128 bits.

Step 7: New multicast keys (both integrity key KMTint and encryption key KMTenc) are generated at RAN and UE using rekeying token (Procedure shown in Figure 6.10.2.1-1).

Figure 6.10.2.3-2 shows the procedure how and when RAN updates the offset information and rekeying token in RRC reconfiguration message (step 2 and 3) to all UEs. Traffic protected with newly generated keys are received from network according to configured timing offset(the value indicates the timing offset with respect to subframe#0 of SFN#0 in milliseconds.).

NOTE 2: Same MBS security context is used for any MBS data transmission.

Editor´s Note: It is FFS when to activate the new keys at UE and RAN, after rekeying token is delivered.

Step 8: Fresh new multicast keys (both integrity key KMTint and encryption key KMTenc) are generated at UEs using rekeying token.

NOTE 3: Rekeying token is never delivered to the UE which left the MBS session and so with older MBS keys, the MBS traffic can’t be decrypted, and integrity protection check will fail.



Figure 6.10.2.3-2 MBS procedure for re-keying token delivery for multiple UEs

Mobility usecase:

**Usecase where no key update required:** When the SMF distributes the same rekeying token to all RANs , then there is no need for rekeying procedure during handover. Target and source RANs will use the same keys for that particular MBS session.

Usecase where key update required: When SMF provides different rekeying token for different RANs, then during of the UE handover, it needs to update the keys. Assume Source NG-RAN has received the multicast group token, which is same for target NG-RAN. The difference considered is the rekeying token received at each RAN . Example: rekeying\_token\_A is received in source NG-RAN and corresponding MBS keys are generated. Similarly rekeying\_token\_B is received in target NG-RAN and corresponding MBS keys are generated. UE\_A connected to source NG-RAN will have the same key material and traffic is protected with MBS key\_A. UE\_B connected to target NG-RAN will have the same key material and traffic is protected with MBS key\_B.

When handover is triggered, then SMF will share the rekeying token\_B to UE\_A, so the new MBS keys are generated at UE\_A and target NG-RAN (updated in security context). UE\_A , UE\_B which is connected to target NG-RAN will have same MBS key\_B, which can be used for decrypting the incoming traffic.

### 6.10.3 Solution Evaluation

As SMF controls rekeying token, UE handover scenarios doesn’t need any rekeying token (in case target and source RAN uses same rekeying token). In case target and source RAN maintains different rekeying token, SMF provides the same rekeying token (used in target RAN) to UE during handover. So in handover scenarios, it has no or less impact on RAN modules. Mobility issue and dynamic switch between PTM and PTP needs security handling in PDCP layer.

Editor´s Note: further evaluation is FFS

## 6.11 Solution #11: Update the keys used to protect the MBS traffic

### 6.11.1 Introduction

This solution addresses Key issue #3 to update the keys to protect the MBS traffic. The MBS traffic is protected between MBSF-U and UEs. The basic idea is to use the signalling messages for the key update procedure. The UEs, which belong to a multicast group, acquire the same group keys as in the MBSF-U. The security protection is enabled in service layer.

### 6.11.2 Solution details

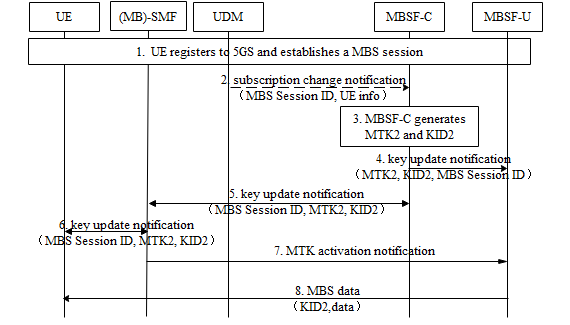


Figure 6.11.2 -1: Procedure for MTK update

1. The UE registers to 5GS and establishes a MBS session, during which MBSF-C generates MTK1&KID1 and distributes them to MBSF-U and UEs. MTK1&KID1 are used to protect the MBS traffic. Details can be found in solution 3 or solution 8.

2. MBSF-C subscribes to the UDM/UDR on the changes of the multicast information including the authorization information. The UDM/UDR notifies the MBSF-C when the authorization for a UE to join the multicast service/application is revoked by AF. The MBS Session ID and UE info (i.e. GPSIs, number of UEs) are included in the notification. The MBS Session ID may be a Temporary Mobile Group Identifier (TMGI) or a multicast address. UE info indicates the change of authorization info.

3. MBSF-C triggers the MTK update based on the changes of authorization info or the key lifetime of MTK1. MBSF-C generates MTK2 and KID2 for this MBS session. For example, if the number of UEs whose authorization is revoked reached the threshold, the MBSF-C triggers the MTK update. It’s operator’s choice to decide the policy for different event.

4-5. MBSF-C distributes MTK2, KID2 and MBS Session ID to (MB)-SMF and MBSF-U respectively.

6. (MB)-SMF distributes MTK2, KID2 and MBS Session ID to the authorized UEs in the connected state whose MBS sessions are not released. Confirmation for update notification is responded to (MB)-SMF. With the confirmation info, (MB)-SMF determines to activate MTK2 based on local policy. For UEs in idle or inactive state UEs, the updated key are delivered when UE joins or actives the MBS session.

7. If the procedure to update the key in UE side is finished, (MB)-SMF indicates MBSF-U to activate the MTK2 for the corresponding MBS session via MBSF-C.

8. MBSF-U uses MTK2 and KID2 to protect the MBS traffic.

The above text describes the security handling when SMF and MB-SMF are co-located. If SMF and MB-SMF are deployed separately, MBSF-C distributes MTK2, KID2 and MBS Session ID to MB-SMF. Afterwards, MB-SMF distributes MTK2, KID2 and MBS Session ID to the authorized UEs via SMF. MB-SMF indicates MBSF-U to activate the MTK2

### 6.11. 3 Evaluation

This solution addresses Key issue #3 to update the key for protecting the MBS session. The solution protects the MBS traffic between MBSF-U and UEs.

AF provides the subscription changes to UDM via NEF.

MBSF-C decides to trigger the MTK update procedure based on the changes of authorization info or the key lifetime of MTK. The new MTK and KID are sent to UE and MBSF-U respectively. The key update procedure by SMF to the UEs incurs signalling overhead proportional to the number of UEs in connected state that joined the MBS session. NAS SM messages need to be delivered to those UEs when a key change happens.

This doesn’t require idle or inactive state UEs to transition to the connected state to receive the key update.

## 6.12 Solution #12: Protection of MBS traffic at service layer based on GBA

### 6.12.1 Solution overview

This solution addresses Key Issue 2 and 3 to protect the MBS key and traffic at service-layer. This solution leverages the MBMS security architecture specified in TS 33.246 [3].

### 6.12.2 Solution details

In order to receive an MBS service, the UE establishes a secure connection with the MBS service function and obtains security materials



Figure 6.12.2-1: Message flows for MBS key delivery and MBS traffic protection

0. The UE is registered to 5GS.

1. The UE requests a PDU session establishment or modification to receive an MBS service.

2. The UE establishes a secure connection with MBSF-U based on GBA similar to MBMS [3] or AKMA [5]. In both scenarios, MBSF-U is considered an AF and UE and MBSF-U communicate using Ua/Ua\* protocol. Both the UE and MBSF-U derive Multicast User Key (MUK) from the AF key (e.g., Ks\_(int/ext)\_NAF for GBA or KAF for AKMA). Over the secure connection, the UE and MBSF-U performs authentication and key derivation as specified in TS 33.246 [3].

NOTE: The key management function is located in the MBSF-U as in BM-SC [3].

3. The UE receives the Multicast Service Key (MSK) from the MBSF-U. The MSK is protected using the MUK and delivered using a unicast message over the secure connection.

4. The UE receives the Multicast Traffic Key (MTK) protected using MSK from the MBSF-U. The MTK can be delivered either a unicast or a multicast message. The MTK is used as a root key to derive application/protocol specific keys to protect (e.g., encrypt or integrity protect) MBS service traffic.

5. Using the MTK received in step 4, the UE derives application/protocol specific keys and decrypts or verifies the MBS traffic.

The key hierarchy, rekeying and key usage for MBS traffic protection is illustrated in Figure 6.12.2-2 and Figure 6.12.2-3. The MUK derived either based on GBA or AKMA is used to protect MSKs, and each MSK is used to protect MTKs. MBSF-U decides to trigger the MSK/MTK update procedure based on the changes of authorization info or the key lifetime. MSK rekeying is done over unicast to each UE joined to the MBS PDU session, and MTK rekeying is done over unicast or multicast to UEs joined to the MBS session.

NOTE: When GBA is used, MUK derivation follows as specified in TS 33.303. When AKMA is used, MUK is set to KAF based on AKMA derivation.

Editor’s Note: Use of AKMA for MUK rekeying requires further explanation



**Figure 6.12.2-2 Usage of MSK for a single session or a channel**



**Figure 6.12.2-3 Usage of MSK for multiple sessions or channels**

### 6.12.3 Solution evaluation

This solution reuse the LTE MBMS security architecture, both GBA and AKMA are used to protect the MBS key and traffic at service-layer.

This solution addresses Key issue #2 and 3 to protect the MBS key and traffic at service-layer.

MBSF-U decides to trigger the MTK update procedure based on the changes of authorization info or the key lifetime of MTK. The new MTK and KID are sent to UE and MBSF-U respectively. The MSK update procedure by MBSF-U to the UEs incurs overhead proportional to the number of UEs in connected state that joined the MBS session. The user plane messages need to be delivered to those UEs when a MTK change happens.

## 6.13 Solution #13: Key generation and distribution for MBS

### 6.13.1 Solution overview

This solution addresses Key Issue 2&3 to support the secure MBS traffic delivery between the UE and the NG-RAN. The MBS session key is derived by the MB-SMF and provided to the UE and also to the NG-RAN. Further keys are derived by the UE and the NG-RAN to protect the MBS data traffic over the air. For MBS data traffic protection (integrity and/or confidentiality protection) between the UE and the NG-RAN is performed at the PDCP layer.

Editor's note: Call flow needs to be re-visited once SA2 has conclusion.

### 6.13.2 Solution details

6.13.2.1 Key generation and distribution



**Figure 6.13.2.1-1: MBS Session Key generated and distribution**

1. MB Session Announcement (see e.g., TS 23.468 [7]).

2. UE sends a MB Session Join Request (TMGI) message to the AMF, to join an MB Session.

3. If the AMF does not already have a MB Session Context for the received TMGI, the AMF selects an MB-SMF for the TMGI by querying the NRF. A MB Session Request (TMGI, AMF ID) message is sent to the MB-SMF to announce the AMF's interest in the MB Session. The MB-SMF generates a session key (KMBS, as detailed in clause 6.13.2.2) for the TMGI, selects the security algorithm(s) (encryption algorithm and/or Integrity protection algorithm) and generates a MBS Key index for the TMGI.

The MB-SMF selects the security algorithm(s) (encryption algorithm and/or Integrity protection algorithm), if there is network wide usage of the same algorithm for the TMGI.

If multiple MB-SMFs are used within the network, then a Key Management Server (KMS) is used to generate the session key (KMBS, as detailed in clause 6.13.2.2) for the TMGI, selects the security algorithm(s) (encryption algorithm and/or Integrity protection algorithm) and generates a MBS Key index for the TMGI. The MB-SMF fetch the MBS session security context data from the KMS. If the KMS does not already have a MBS session security context for the received TMGI from the MB-SMF, then the KMS generates the MBS session security context for the TMGI and provides it to the MB-SMF.

4. The MB-SMF provides the MBS session security context data to the AMF. The AMF stores the MBS session security context data for the TMGI, in the MBS Session Context.

5. The AMF creates a DL NAS MB Session Join Response message (which includes MBS session security context data) and piggy backs that on a N2 MB Session Join (NGAP ID, TMGI) message. The DL NAS message is protected using the NAS security context.

6. The AF requests activation of an MB Session by sending an Activate MBS Bearer Request (TMGI, Service Requirement) message to the NEF/MBSF.

7. NEF/MBSF sends a MB Session Start (TMGI, Service Requirement) message to the MB-SMF.

8. MB-SMF sets the MB Session Context to active and sends MB Session Start (TMGI) messages to all AMFs that has earlier joined the MB Session.

9. The AMF sends a MB Session Resource Setup Request (TMGI, MBS session security context data) message to all RAN nodes where CM CONNECTED UEs that has joined the TMGI resides.

The NG-RAN selects the security algorithm(s) (encryption algorithm and/or Integrity protection algorithm), instead of MB-SMF selecting (as detailed in step 3), if NG-RAN specific selection of the security algorithm is supported for the MBS traffic.

The NG-RAN creates a MB Session Context (if it not already exists), sets it to 'active' state, stores the TMGI and MBS session security context data in the MB Session Context.

10. If NG-RAN prefers to use N3 multicast transport, the NG-RAN joins the multicast group.

11. NG-RAN establishes PTM or PTP DL resources for the MB Session.

For the TMGI’s PTM MB sessions, the NG-RAN activates the security context and indicates the key index and information required to derive the RAN specific keys (as detailed in clause 6.13.2.2).

Editor's note: The details of the exact message which will transport the security parameters and activation of MBS security depends on the work progress in RAN2. Once RAN2 make working assumptions, then the solution will be updated with further details.

12. The NG-RAN transmits the received DL media stream using DL PTM or PTP resources. The NG-RAN uses the MBS session security context data of the TMGI to protect (encryption and/or integrity protection) the DL media stream.

6.13.2.2 Key hierarchy



**Figure 6.13.2.2-1: Key hierarchy generation**

- KMBS is an anchor/master/primary key, for a particular TMGI, generated by the MB-SMF. KMBS is provided to the UE and to the RAN. The network entity/function generates KMBS (for example, random key generated from a random number generation function).

- KMBS-RAN is a key generated by ME and NG-RAN from MBS key KMBS. The KMBS-RAN is used to derive further keys that are used between the UE and the NG-RAN to protect MBS.

- KMRBint is a key generated by ME and NG-RAN from MBS RAN specific key KMBS-RAN, which is used for the protection of MBS traffic with a particular integrity algorithm.

- KMRBenc is a key generated by ME and NG-RAN from MBS RAN specific key KMBS-RAN, which is used for the protection of MBS traffic with a particular encryption algorithm.

Key generation is performed using the key derivation function (KDF) specified in Annex B.2.0 of TS 33.220. When deriving a key, the input parameters are used to form the input S to the KDF.

The NG-RAN and the UE derives cell specific key from the session key (KMBS) as follows:

KMBS-RAN  = KDF {KMBS, TMGI, RANDMBS, CountMBS, PCI, ARFCN-DL}

KMRB-enc = KDF {KMBS-RAN, Algorithm type distinguisher value, Algorithm identifier value}

KMRB-int = KDF {KMBS-RAN, Algorithm type distinguisher value, Algorithm identifier value}

Details of the input parameters used to derive MBS keys:

- TMGI: is included in the key generation as to bind the key to a specific TMGI.

- PCI and ARFCN-DL: are included in the key generation as to bind the key to a specific RAN Cell.

- CountMBS: is used as a freshness parameter in refreshing the key. The NG-RAN associates a counter, called a CountMBS, with the MBS security context. The CountMBS is used as freshness input into keyderivations. The NG-RAN sends the value of the CountMBS to the UE over the RRC signalling path when it is required to generate a new MBS key. The NG-RAN maintains the value of the counter for a duration of the current MBS security context between UE and NG-RAN. The NG-RAN initializes the CountMBS to 0x00 0x01 when the KMBS-RAN is derived. The UE and the NG-RAN maintains the CountMBS for lifetime of the KMBS-RAN. The CountMBS is incremented by the NG-RAN for every new computation of the KMBS-RAN. The NG-RAN sends the value of the CountMBS (used to generate the KMBS-RAN) to the UE. The UE accepts CountMBS value that is greater than stored CountMBS value.

- RANDMBS: is used as a freshness parameter in refreshing the key (in other words, not to generate the same key every time), as to generate unique key for every key generation and to provide it to only authorised UEs. RANDMBS is used to prevent the UE from deriving the keys, which are not authorized for the current session, but obtained the MBS security context for the previous sessions. The size of the RANDMBS should be long enough to prevent predicting the KMBS-RAN, even if KMBS is known to a revoked UEs.

MBS bearer can comprise of MRB (PTM) or DRB (PTP) or a combination of MRB (PTM) and DRB (PTP). PTM path is protected with using the key (KMBS-enc/KMBS-int) and PTP path is protected using the UP key (KUPenc/KUPint). In case of combination of PTM and PTP delivery methods, same security policy is applied for both MRB and DRB bearers.

Editor's note: How MB-SMF or KMS selects AS security algorithms is FFS.

Editor's note: Details on KMS is FFS, e.g., how it interfaces and interacts with MB-SMF.

6.13.2.3 Key Refresh

The MBS keys used to protect the MBS traffic needs to be updated:

- to prevent the UE to access the MBS content after leaving the group (e.g., cancel a MBS subscription)

- if a UE joins the group newly (newly subscribes for MBS), then the UE should not able to access the already broadcasted content, and

- to prevent use of same key stream blocks repeatedly (due to PDCP COUNT wrap-around).

If the NG-RAN nodes decides to refresh the KMRB-RAN, then the NG-RAN provides a new RANDMBS and also the increased CountMRB value to the authorised UEs over SRB using RRC Re-configuration message. Once the parameters required for the key derivation is provided by the NG-RAN, then the UE and the NG-RAN derives new keys (KMBS-RAN,KMRB-enc and KMRB-int). The NG-RAN, then establish a new MRB and starts using the new keys to protect the MBS traffic.

### 6.13.3 Solution evaluation

This solution provides the protection for the MBS traffic between the RAN and the UE (at PDCP layer). This solution provides the following aspects:

Supporting all deployment scenarios. As per SA2 MBS TS 23.247 (c.f., Clause 5.1), MBSF and MBSTF are optional entities (Excerpt from TS 23.247: *NOTE 1: The MBSF is optional and may be collocated with the NEF or AF/AS, and the MBSTF is an optional network function.*), leading to deployment scenarios with/without MBSF & MBSTF.

- In case if any MBS group member leaves the group, it is efficient to do the key update at RAN level by refreshing the key KMBS-RAN, instead of updating the session key (KMBS) to all member.

- The key distribution procedure aligns with the session management procedure as defined in SA2 and RAN groups.

- The security granularity is cell-level

Editor’s Note: Further evaluation on SMF managing key should be done

Editor’s Note: Further evaluation is FFS (after resolving Editor’s Notes in the solution)

## 6.14 Solution #14: Secure key delivery in service layer

### 6.14.1 Solution overview

This solution addresses Key Issue #3: Security protection of key distribution, which includes the security requirement as “The distribution of the keys for protection of MBS traffic between the key generator and the UE shall be confidentiality, integrity and anti-replay protected.”

As the NAS confidentiality protection between AMF and UE is not mandatory and it is not always enabled. Whenever there is no NAS confidentiality protection, KMBS will be sent in the clear, which is a huge damage for MBS service. That’s the motivation to design this solution. For the case when the NAS confidentiality protection is enabled, the protection in this solution is optional but also no harm to enable.

This solution proposes a method to protect the KMBS used for MBS traffic protection based on KMBS-UE which is derived based on KAUSF. With this solution, KMBS delivery from MB-SMF to UE can be confidentially protected.

### 6.14.2 Solution details

Diagram

Description automatically generated

**Figure 6.x.2-1. The procedure of key delivery of KMBS**

The procedure is described as follows:

Step 0a: UE initiates the Primary Authentication and establishes the KAUSF with AUSF in HPLMN.

Step 0b: Service announcement procedure, following the current Clause 7.1.1 in TS 23.247.

Step 1. MB-SMF generates KMBS and KID for the specific MB service.

Step 2. To join the multicast group, the UE sends the PDU Session Modification Request (MBS Session ID). MBS Session ID indicates the multicast group that UE wants to join.

Step 3.0. AMF sends MBS Key Request to AUSF to ask for the encryption key.

Step 3.1. AUSF generates a KMBS-UE using KAUSF and TMGI.

Editor’s Note: it's FFS how AUSF knows TMGI

Step 3.2. UE generates a KMBS-UE and using KAUSF and TMGI.

Step 3.3. AUSF send the KMBS-UE to AMF.

Step 4. By using Nsmf\_MBSSession\_Create request (MBS Session ID), SMF interacts with MB SMF to retrieve multicast QoS flow information of the indicated MBS session.

Step 5. MB-SMF sends the KMBS and KID to SMF using Nsmf\_MBSSession\_Create response.

Step 6. SMF responds to AMF through Nsmf\_PDUSession\_UpdateSMContext response(N2 SM information (PDU Session ID, MBS Session ID, MB-SMF ID, multicast QoS flow information, updated PDU Session information, mapping between unicast QoS flow and multicast QoS flow information), N1 SM container (PDU Session Modification Command, KMBS and KID)

Step 7. AMF send the PDU session modification command (EKMBS-UE(KMBS)) to UE, including the encrypted KMBS and KID.

Step 8. UE decrypt the EKMBS-UE(KMBS) and gets the KMBS

KMBS is used for the future protection of the MBS traffic.

Editor’s Note: It is FFS whether the KMBS will be used as the root key or the session key.

NOTE: The UE leaving group procedure will be handled separately.

Editor’s Note: Whether other keys (e.g Kamf) can be used is FFS.

Editor’s Note: What algorithms should be used is FFS.

### 6.14.3 Solution evaluation

TBD

## 6.X Solution #X: <Solution name>

### 6.X.1 Solution overview

### 6.X.2 Solution details

### 6.X.3 Solution evaluation

# 7 Conclusions

Editor’s Note: This clause will contain the conclusion of the TR

## 7.1 Conclusions on Key Issue #1

Following conclusions are made on Key Issue #1: Authentication and authorization for multicast communication services:

* Solution #4 (Secondary based authentication and authorization) will form the basis for the authentication and authorization method for multicast PDU session and it is optional-to-use.

## 7.2 Conclusions on Key Issue #2

Following conclusions are made on Key Issue #2 " Security protection of MBS traffic ":

* Service-layer solution is used as a baseline for the normative work. MBSTF provides the security protection for MBS traffic. The MTK is used as a root key to derive application/protocol specific keys to protect (e.g., encrypt or integrity protect) MBS service traffic. This will be optional to implement in both UE and network.

## 7.3 Conclusions on Key Issue #4

Following conclusions are made on Key Issue #4 " Security protection between AF and 5GC":

* Solution #7 will form the basis of normative work for key issue #4.

Annex <A>:  
<Informative annex title for a Technical Report>

Annex <X> (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-08 | SA3#100-e |  |  |  |  | TR skeleton (approved in S3-201722) | 0.0.0 |
| 2020-08 | SA3#100-e |  |  |  |  | Inclusions of documents approved at SA3#100-e: S3-202120, S3-202121, S3-202123, S3-202125 | 0.1.0 |
| 2020-10 | SA3#100-bis-e |  |  |  |  | Inclusions of documents approved at SA3#100-bis-e: S3-202475, S3-202476, S3-202761, S3-202762, S3-202746, S3 202491, S3-202745 | 0.2.0 |
| 2020-11 | SA3#101-e |  |  |  |  | Inclusions of documents approved at SA3#101-e: S3-203422, S3-203423, S3-203424, S3-203427, S3-203428, S3-203429, S3-203031, S3-203361 | 0.3.0 |
| 2021-01 | SA3#102-e |  |  |  |  | Inclusions of documents approved at SA3#102-e: S3-210290, 210369, S3-210677, S3-210693, S3-210286, S3-210690, S3-210610, S3-210134, S3-210672, S3-210641, S3-210642, S3-210643 | 0.4.0 |
| 2021-03 | SA3#102-bis-e |  |  |  |  | Inclusions of documents approved at SA3#102-bis-e: S3-211278, S3-211307, S3-211294, S3-211197, S3-210886, S3-211308, S3-210920, S3-210963, S3-211069, S3-211127, S3-211270, S3-211271, S3-210935, S3-211317, S3-210917 | 0.5.0 |
| 2021-05 | SA3#103-e |  |  |  |  | Inclusions of documents approved at SA3#103-e: S3-211635, S3-212255, S3-211590, S3-212192, S3-212173, S3-212239, S3-211878, S3-211879, S3-212250, S3-212096, S3-212139, S3-212140, S3-212174 | 0.6.0 |
| 2021-08 | SA3#104-e |  |  |  |  | Inclusions of documents approved at SA3#104-e: S3-213084, S3-213085, S3-213038, S3-213104, S3-212555, S3-213077, S3-213078, S3-212720, S3-213127, S3-213126, S3-213136, S3-213123 | 0.7.0 |