|  |
| --- |
| 3GPP TR 33.850 V0.3.0 (2020-11) |
| 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://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 members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® 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 9

5.2.3 Potential security requirements 9

5.3 Key Issue #3: Security protection of key distribution 9

5.3.1 Key issue details 9

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 10

5.4.3 Potential security requirements 10

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: protect MBS traffic in transport layer 11

6.1.1 Solution overview 11

6.1.2 Solution details 11

6.1.3 Solution evaluation 13

6.2 Solution #2: protect MBS traffic in service layer 13

6.2.1 Solution overview 13

6.2.2 Solution details 13

6.2.2.1 MBS group key distribution and update 15

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 17

6.3.3 Solution evaluation 18

6.4 Solution #4: Authentication and authorization for multicast communication service 18

6.4.1 Solution overview 18

6.4.2 Solution details 18

6.4.3 Solution evaluation 20

6.5 Solution #5: Authorization revocation 20

6.5.1 Solution overview 20

6.5.2 Solution details 20

6.5.3 Solution evaluation 21

6.6 Solution #6: Authentication and authorization for multicast communication service based on AKMA 21

6.6.1 Solution overview 21

6. 6.2 Solution details 21

6.6.3 Solution evaluation 22

6.7 Solution # 7: security protection between AF and 5GC 22

6.7.1 Solution overview 22

6.7.2 Solution details 22

6.7.3 Solution evaluation 22

6.X Solution #X: <Solution name> 22

6.X.1 Solution overview 22

6.X.2 Solution details 22

6.X.3 Solution evaluation 22

7 Conclusions 22

Annex <A>: <Informative annex title for a Technical Report> 24

Annex <X> (informative): Change history 25

# 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".

# 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

MSF Multicast Service Function

MSF-C MSF Control Plane

MSF-U MSF User Plane

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

# 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 |  |
| #X: <Solution name> |  |  |  |  |  |

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

## 6.1 Solution #1: protect 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 identifier.
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.
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.

1. The MBS security context is distributed from RAN to UE. The RRC config message further contains the current PDCP COUNT value for the K\_group. If the K\_group is newly created, the PDCP COUNT is set to the initial value (e.g., 0).
2. UE receives and stores the MBS security context for the multicast group.
3. 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.

Editor’s Note: The message name and flow may be updated to align with the conclusion from SA2 and RAN WGs.

Editor’s Note: The support for mobility of UEs is FFS.

### 6.1.3 Solution evaluation

TBD

## 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 baseline architecture 2 in TR 23.757 [2], the MBSU (Multicast/Broadcast Service User plane) is defined as a new entity to handle the payload part to cater for the service level functions and management. Similarly, MSF User Plane (MSF-U) in baseline architecture 1 is also defined in service layer. This solution protects the MBS traffic between the MBSU/MSF-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 MBSU/MSF-U respectively. The UEs, which belongs to a multicast group, acquire the same keys in the MBSU/MSF-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

MBSU/

MSF-U

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.

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. IP address of MBSU/MBS-U may be included if needed for UE to find MBSU/MBS-U,
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. When re-authentication runs, the UE generates a new MUK and deletes the old MUK.

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

Editor’s Note: Key update procedure after reauthentication is FFS.

1. 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 generates a new MUK and deletes the old MUK.
3. AUSF responds to SMF with MUK.
4. SMF distributes MUK to MBSU/MSF-U.
5. MBSU/MSF-U receives and stores the MUK. Afterwards, ACK is reponded to SMF.
6. Continue with the multicast service initiation procedure.
7. MBSU/MSF-U 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, MBSU/MSF-U generates K\_group and derives the K\_group\_enc and K\_group\_int. The encryption and integrity algorithms are selected.

1. UE calculates token based on MUK and requests traffic key to MBSU/MSF-U. 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. MBSU/MSF-U verifies the token using MUK and distributes the MBS security context to UE if succeeded.

Editor’s Note: The message name and flow may be updated to align with the conclusion from SA2 and RAN WGs.

Editor’s Note: Whether the roaming aspect is addressed based on the conclusion from SA2.

### 6.2.2.1 MBS group key distribution and update

This section explains the logic of step 18a and 18b in Figure 6.2.2.1. using two approaches:

**Default approach:**

The default version uses key hierarchy:

 MUK -> K\_group

Step 18a relies on K=K\_group, i.e., this message is used to directly update K\_group by means of MUK. If K\_group needs to be updated and the group size is N, this approach requires the exchanged of N messages.

In Step 18a, EK1{K2} means authenticated encryption of key K2 with key K1 and is used to indicate the secure delivery of K2.

**Communication optimized approach:**

Alternatively, a key hierarchy” MUK -> K\_transport\_i-> K\_group” can be used. This alternative is useful to decrease the communication overhead to roughly 2 SQRT(N). 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.

Each UE has three keys: a device specific key, MUK; a transport key K\_transport\_i shared with other L-1 devices in the same set S\_i; a group key shared with all N devices and used to protect the MBS traffic. 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. The key hierarchy is as follows where the arrow indicates protection.

 MUK -> K\_transport\_i -> K\_group

The distribution and update of the group key is done by means of two messages:

* Message 18a: in this meassage, K=K\_transport\_i and is used to provide 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.

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=1600, M=40, L=40, then the key update only requires 39 point-to-point messages for the update of the transport key associated to the set of the device that is leaving and 40 messages for the group key update. This choice is good since 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.

Editor’s note: Reliability of the scheme is FFS

Editor’s note: the relationship between K\_transport and K\_group is FFS.

Editor’s note: the detailed description of key hierarchy is FFS.

### 6.2.3 Solution evaluation

TBD

## 6.3 Solution #3: MBS Traffic Protection

### 6.3.1 Solution overview

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

According to TR 23.757 [2], in the baseline architecture 2, the MBSU (Multicast/Broadcast Service User plane) is defined as a new entity to handle the payload part to cater for the service level functions and management; Similarly, MSF User Plane (MSF-U) in baseline architecture 1 is also defined. Also the MBSF (Multicast/Broadcast Service Function) is defined as a new entity to handle the signalling aspects; similarly, MSF Control Plane (MSF-C) in baseline architecture 1 is also defined.

In this solution, MBS traffic is protected between the MBSU/MSF-U in the operator domain and the UE, and it is transparent to the content provider. MBS Traffic Key (MTK) is generated by MBSF/MSF-C and distributed to the UEs through the control plane. MBSU/MSF-U uses the MTK to protect the MBS traffic before sending them out to the UE.

###  6.3.2 Solution details

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

NOTE X: (MB-)SMF is either the MB-SMF defined in the baseline architecture 2 or the enhanced SMF in the baseline architecture 1, as defined in the TR 23.757 [2] on 5G MBS.



**Figure 6.3.2-1: Authentication and authorization procedure**

1. The AF of the content provider provisions to the MBSF/MSF-C the information on the MBS application including the security policy. The NEF is involved in the provision if the content provider belongs to a 3rd party.
2. If the security policy indicates the MBS application needs security protection, MBSF/MSF-C shall generate a MTK and the associated key identifier (KID) for the MBS application. MBSF/MSF-C provisions the received information on the MBS application and the generated MTK and the KID to the UDM/UDR.

Editor’ Note: How to generate the MTK and KID is FFS.

1. UE sends a request to use the MBS application. The request is forwarded to the (MB-)SMF. According to the TR 23.757 [2], there are two ways for step 1, the control plane join and the user plane join. For the control plane join, the UE initiates the request for a PDU session establishment/modification and includes in the requires the identifier for the MBS application. The request is forwarded to the (MB-)SMF through the control plane. For the user plane join, the UE sends an IGMP/MLR message to a UPF including the identifier of the MBS application. The UPF forwards the IGMP/MLR message the (MB)-SMF.

Editor's note:  The identifier for the MBS application is to be aligned with SA2 progress.

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 UDM/UDR replies with the requested subscription and the received MTK in step 2.
3. The (MB-)SMF sends the received MTK and the KID to the UE.
4. The MTK and the KID are delivered to the MBSU/MSF-U from the MBSF/MSF-C.
5. When MBS traffic is received at the MBSU/MSF-U, the MBSU/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 6 to process the MBS traffic.

### 6.3.3 Solution evaluation

TBC

## 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.

### 6.4.2 Solution details

In the solution below, the (MB-)SMF is an enhanced SMF supporting 5G MBS, (MB-)UPF is an enhanced UPF supporting 5G MBS. The solution works with both baseline architectures defined in the TR 23.757 [2].

NOTE X: (MB-)SMF is either the MB-SMF defined in the baseline architecture 2 or the enhanced SMF in the baseline architecture 1, defined in the TR 23.757 [2] on 5G MBS. (MB-) UPF is either the MB-UPF defined in the baseline architecture 2 or the enhanced UPF in the baseline architecture 1, defined in the TR 23.757 [2] on 5G MBS.



Figure 6.4.2-1: Authentication and authorization procedure

1. UE sends a request to join a multicast service/application. The request is forwarded to the (MB-)SMF. According to the TR 23.757 [2], there are two ways for step 1, the control plane join and the user plane join. For the control plane join, the UE initiates the request for a PDU session establishment/modification and includes the identifier of the multicast service/application that the UE wishes to join. The request is forwarded to the (MB-)SMF through the control plane. For the user plane join, the UE sends an IGMP/MLR message including the identifier of the multicast service/application to a UPF. The UPF forwards the IGMP/MLR message the (MB)-SMF.

Editor's note:  The identifier of the multicast service/application is to be updated according to SA2 progress.

1. If not available locally, the (MB-)SMF retrieves the subscription data from the UDM.
2. The (MB-)SMF determines that authentication and authorization is needed for the MBS communication service based on the subscription data.
3. The (MB-)SMF sends an EAP request and the identifier of the multicast service/application to the UE to request the EAP identity used for the multicast service/application.
4. The UE responds with an EAP response with the EAP identity and the identifier of the multicast service/application.

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

6-7. The (MB-)SMF sends the received EAP identity and the identifier of the multicast service/application to the AAA server through a (MB-)UPF.

1. EAP messages are exchanged between the AAA server and the UE.
2. After the successful completion of the authentication procedure, DN AAA server shall send EAP Success message to the (MB-)SMF.
3. If the UE is authorized to join the multicast service/application based on the subscription, then the (MB-SMF) will proceed with PDU session establishment/modification. The (MB-)SMF sends the EAP access and the identifier of the multicast service/application to the UE.

### 6.4.3 Solution evaluation

TBC

## 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 an enhanced SMF supporting 5G MBS. The solution works with both baseline architectures defined in TR 23.757 [2] on 5G MBS.

Note:  (MB-SMF) is the MB-SMF in the baseline architecture 2 or the enhanced SMF in the baseline architecture 1, as defined in the TR 23.757 [2] on 5G MBS.



Figure 6.5.2-1: Authorization revocation

1. The AF of the content provider provisions the information on the multicast service/application 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 service/application and the PDU session for the multicast service/application has been established.
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.
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 identifier of the multicast service/application and UE identifier (i.e. SUPI) is included in the notification.
6. The (MB-)SMF releases the PDU session for the multicast service/application identified by the received identifier.

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.

Editor's note:  The identifier for the multicast service/application is to be updated according to SA2 progress.

### 6.5.3 Solution evaluation

TBC

## 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.

Editor’s Note: It is FFS how to discover the correct AAnF.

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

Editor’s Note: It is ffs whether primary authentication is sufficient to authenticate the UE towards the MBSF.

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

TBD

## 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.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

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 |