|  |
| --- |
| 3GPP TR 33.850 V0.1.0 (2020-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Security Aspects of Enhancements for 5G Multicast-Broadcast Services (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 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 6

4 Overview of Multicast-Broadcast Services (MBS) 7

5 Key issues 7

5.1 Key issue #1: Security of authentication and authorization for multicast communication services 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential security requirements 7

5.2 Key Issue #2: Security protection of MBS traffic 8

5.2.1 Key issue details 8

5.2.2 Security threats 8

5.2.3 Potential security requirements 8

5.3 Key Issue #3: Security protection of key distribution 8

5.3.1 Key issue details 8

5.3.2 Security threats 8

5.3.3 Potential security requirements 9

5.X Key issue #X: <Key issue name> 9

5.X.1 Key issue details 9

5.X.2 Threats 9

5.X.3 Potential security requirements 9

6 Proposed solutions 9

6.0 Mapping of solutions to key issues 9

6.1 Solution #1: <Solution name> 9

6.1.1 Solution overview 9

6.1.2 Solution details 9

6.1.3 Solution evaluation 9

6.X Solution #X: <Solution name> 10

6.X.1 Solution overview 10

6.X.2 Solution details 10

6.X.3 Solution evaluation 10

7 Conclusions 10

Annex <A>: <Informative annex title for a Technical Report> 11

Annex <X> (informative): Change history 12

# 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".

# 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].

<ABBREVIATION> <Expansion>

Editor’s Note: Example needs to be deleted

# 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 4G 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 4G 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 4G 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, 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.

### 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 intergrity or anti-replay protected, the authorisaed users may not be able to acquire the MBS traffic properly.

### 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, intergrity and anti-replay protected.

## 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 | X |
| #1: <Key issue name> |  |  |  |  |
| #X: <Key issue name> |  |  |  |  |

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

## 6.1 Solution #1: <Solution name>

### 6.1.1 Solution overview

Editor’s Note: This clause starts with the (part of) the key issue(s) addressed and is followed with a brief overview of the solution

### 6.1.2 Solution details

Editor’s Note: This clause provides the details of the solution

### 6.1.3 Solution evaluation

Editor’s Note: This clause provides the evaluation of the solution

Editor’s Note: This below provides a generic set of headings for a new solution and need to be deleted before the TR goes for approval

## 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 agreed in SA3#100: S3-202120, S3-202121, S3-202123, S3-202125 | 0.1.0 |