|  |
| --- |
| 3GPP TR 33.883 V0.3.0 (2022-10) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security enhancements for 5G multicast-broadcast services phase 2(Release 18) |
|   |
|  | 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.© 2022, 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 7

3.3 Abbreviations 7

4 Assumptions 7

5 Key issues 7

5.1 Key issue#1: security handling in MOCN network sharing scenario 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential security requirements 8

5.2 Key issue#2: TMGI Protection 8

5.2.1 Key issue details 8

5.2.2 Security threats 8

5.2.3 Potential security requirements 8

5.X Key issue #X: <Title> 8

5.X.1 Key issue details 8

5.X.2 Threats 8

5.X.3 Potential security requirements 8

6 Proposed solutions 9

6.1 Mapping of solutions to key issues 9

6.2 Solution #1: MBS Traffic Key distribution for MOCN deployment scenarios 9

6.2.1 Introduction 9

6.2.2 Solution details 9

6.2.3 System impact 10

6.2.4 Evaluation 10

6.3 Solution #2: MOCN security handling for MBS 10

6.3.1 Introduction 10

6.3.2 Solution details 11

6.3.2.1 MOCN Broadcast Procedure 11

6.3.2.2 Common MOCN TMGI 12

6.3.2.3 MOCN keys MSK MTK 12

6.3.3 System impact 14

6.3.4 Evaluation 14

6.A Solution #A: <Title> 14

6.A.1 Introduction 14

6.A.2 Solution details 14

6.A.3 System impact 14

6.A.4 Evaluation 14

7 Conclusions 14

Annex <A>: <Informative annex title for a Technical Report> 15

Annex X: Change history 15

# 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

This clause is optional. If it exists, it shall be the second unnumbered clause.

# 1 Scope

The present document is to identify key issues, potential security and privacy requirements and solutions with respect to Rel-18 enhancement for 5G multicast-broadcast services. Specifically:

- Study the security enhancement enabling UE's receiving Multicast MBS Session data in RRC Inactive state. Analysis whether existing security mechanisms for UE in RRC connected state can be reused or new security enhancement are needed.

- Study the security impact and potential enhancement if supporting feasible and efficient resource utilization for the same broadcast content to be provided to 5G MOCN network sharing scenarios.

- Other security issues if identified in the enhancements made by other WGs in Rel-18.

# 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 23.700-47: "Study on architectural enhancements for 5G multicast-broadcast services ".

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

[4] 3GPP TS 23.003: "Numbering, addressing and identification".

[5] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification".

[6] 3GPP TS 23.247: "5G multicast-broadcast services; Stage 2".

# 3 Definitions of terms, symbols and abbreviations

This clause and its three subclauses are mandatory. The contents shall be shown as "void" if the TS/TR does not define any terms, symbols, or 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].

Definition format (Normal)

**<defined term>:** <definition>.

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

## 3.2 Symbols

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

Symbol format (EW)

<symbol> <Explanation>

## 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].

MOCN Multi-Operator Core Network

TMGI Temporary Mobile Group Identity

# 4 Assumptions

This clause contains assumptions for the study. If there are no assumptions at the end of the study, the clause will be removed before sending for approval.

# 5 Key issues

## 5.1 Key issue#1: security handling in MOCN network sharing scenario

### 5.1.1 Key issue details

In MOCN network sharing scenario, multiple CNs are connected to the same NG-RAN. As documented in TR 23.700-47 [2], the efficiency of resource utilization for the same broadcast content is studied. For the same broadcast content, the AF will set up multiple broadcast MBS sessions towards those CNs. Each CN will deliver the same content towards the same shared NG-RAN node. The NG-RAN node only delivers one copy of the broadcast content over the air.

As specified in clause W.4 of TS 33.501 [3], user-plane procedure is applicable for broadcast service. MBSTF may protect the traffic transmission with encryption and/or integrity. The security protection of MBS traffic is supported in service layer. In MOCN network sharing scenario, the multiple CNs may enable their own security towards the content. The UE will receive the MBS keys from their serving PLMN. However, the NR-RAN broadcasts only one copy of the content. The security impact needs analysis if security are activated for the same content to be provided to 5G MOCN network sharing scenarios. For example, UEs from PLMN1 may be unable to decipher the content if the NG-RAN node chooses to broadcast the ciphered content from the CN of PLMN2, since the MTK generated and distributed by the PLMN1 may be different from the MTK that will be used by the PLMN2 to protect the MBS traffic.

If the content is protected using CN-specific keys, which is not a serving PLMN for an UE in the shared RAN, then UEs not having the key will fail to properly process the content, should the network send only one of the copies.

### 5.1.2 Security threats

If the content is not protected by application (in another words, CA/DRM does not apply) then reusing the existing security procedure in service layer may cause processing failure in UEs in MOCN network sharing scenario. The UEs will be out of MBS if it is not served by the PLMN that is protecting the MBS traffic, as the UE does not have the appropriate MTK (key that will be used to protect the MBS content at the service layer) to handle the protected traffic.

### 5.1.3 Potential security requirements

The 5G system should provide the means to protect the traffic in the service layer in MOCN network sharing scenario.

NOTE: If the content is protected by application, the security protection in service layer is not required.

## 5.2 Key issue#2: TMGI Protection

### 5.2.1 Key issue details

According to TS 23.003 [4] and TS 38.331 [5], TMGI is defined as Temporary Mobile Group Identity. Temporary Mobile Group Identity (TMGI) is used within MBMS to uniquely identify Multicast and Broadcast bearer services. The TMGI is composed of MBMS Service ID, Mobile Country Code (MCC), and Mobile Network Code (MNC).

TMGI is used by the Core Network (CN) of MBS UEs and by MBS UEs as a temporary identity for monitoring of the Paging channel for CN paging if configured by upper layers for MBS multicast reception (e.g., see clause 7.2.5.2 of TS 23.247 [6]).

TMGI is a temporary identity. However, since it is being utilized for MBS group paging and its value reused for paging different UEs, as well as being transmitted in cleartext, the privacy attack and DoS attack may be possible.

### 5.2.2 Security threats

An attacker eavesdrop over the paging channel for MBS UEs may be capable of the following privacy attacks:

- inferring members of the MBS group presence in the paging area.

### 5.2.3 Potential security requirements

The 5G system may provide means to mitigate the privacy attack which infers the members of the MBS group by group paging with TMGI.

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

### 5.X.1 Key issue details

### 5.X.2 Threats

### 5.X.3 Potential security requirements

# 6 Proposed solutions

## 6.1 Mapping of solutions to key issues

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 |
| #1: MBS Traffic Key distribution for MOCN deployment scenarios | X |  |  |
| #2: MOCN security handling for MBS | X |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 6.2 Solution #1: MBS Traffic Key distribution for MOCN deployment scenarios

### 6.2.1 Introduction

This solution addresses Key Issue #1 to provision appropriate keys (keys that will be used to protect the MBS content at the service layer) to the UE to handle the protected MBS traffic over the MOCN deployment scenarios. The MBS Traffic Key (MTK) is generated by the AF and provided to the CN NF to distribute and use it.

The AF performs the MTK generation and provides the MTK for all deployment scenarios.

### 6.2.2 Solution details

If the MTK is derived by the AF and provided it to the PLMNs, then all the PLMNs of the MOCN will distribute the same MTK to all the MBS authorized UEs it serves. Therefore the UEs in a shared RAN even if the serving PLMN are different, will have the same MTK and UEs will be able to handle the protected content even if it is protected by the non-serving PLMN.



Fig 6.2.2-1: MTK generation and distribution for MOCN deployment scenario

Figure 6.2.2-1 includes only the relevant steps specified in TS 23.247 [6] for the AF to provide the MTK to the NEF/MBSF and details of distribution of the MTK by the NEF/MBSF for MBS traffic protection. As shown in the Figure 6.2.2-1, the steps 1 to 6 are performed for the PLMN-1 and also for the PLMN-2 for the MBS session ID.

0) The AF generates the MTK and selects the security algorithm for the MBS session ID.

1) The AF provides the security data (MTK, MTK ID and selected algorithm(s)) to the NEF/MBSF.

2-3) The MBSF includes the received security data in the multicast session security context and provides it to the MB-SMF. The SMF obtains the multicast session security context from the MB-SMF and provides it to the UE, as specified in TS 33.501 [3].

4-5) The NEF/MBSF provides the received security data to the MBSTF. Upon receiving the security data from the NEF/MBSF, the MBSTF uses the provided MTK for MBS traffic protection, instead of deriving a MTK for the specified MBS session ID.

6) The NEF/MBSF provides response for the received Nnef\_MBSSession\_Create request.

Editor’s note: Handling of MTK refresh is FFS.

### 6.2.3 System impact

The key distribution procedure aligns with the session management procedure as defined in TS 23.247 [6].

### 6.2.4 Evaluation

This solution details the distribution of the MTK key (that will be used to protect the MBS content at the service layer) to the UE to handle the protected MBS traffic over the MOCN deployment scenarios.

Editor’s note: Further system impact and evaluation details are FFS.

## 6.3 Solution #2: MOCN security handling for MBS

### 6.3.1 Introduction

This solution addresses the key issue #1 “security handling in MOCN network sharing scenario” from present document.

### 6.3.2 Solution details

#### 6.3.2.1 MOCN Broadcast Procedure



Figure 6.3.2.1-1: MOCN broadcast procedure

UE#1 belong to PLMN A, UE#2 belong to PLMN B, UE#3 belongs to PLMN C. And corresponding MBSTF, MB-SMF, MB-UPF is independently present for each operator / PLMN A, B and C.

Step 1 MOCN TMGI allocation is performed by MB-SMF. TS 23.247 can be referred for normal TMGI allocation. Same procedure is followed but the TMGI structure used is MOCN TMGI shown in this document in section 6.3.2.2.

Step 2 Separate service announcement is made for broadcast services to UE#1, UE#2 and UE#3 by respective PLMNs.

Step 3 This step is without involving AF option. All operators use unique key id for MOCN and derive the keys for MSK, MTK which is common for MOCN broadcast scenario.

Step 4 Traffic protection uses common one across all operators.

Step 5 when the media stream from AF is received to each MB-UPF of PLMN A, B, C. Each MB-UPF of each PLMN will forward the media stream to MOCN RAN.

Step 6 MOCN RAN considers only one media stream content and ignores the rest of the media stream content received from rest of the TMGI. RAN decides based on the common MOCN TMGI ID used in media stream. Clause 6.3.2.2 describes possible ways to arrive at a common MOCN TMGI.

Step 7 PTM transmission is made from MOCN RAN to all UE of different operators.

#### 6.3.2.2 Common MOCN TMGI

Current Temporary Mobile Group Identity (TMGI) is used within MBMS to uniquely identify Multicast and Broadcast bearer services. But this ID is unique to a particular PLMN. Different PLMNs uses their own TMGI id for set of UEs belong to them.

Considering the MOCN for broadcast usecase in 5G, TMGI can’t be unique only to one operator and it has to be common across the different PLMNs. This solution proposes four possible ways to arrive at a common MOCN TMGI. Figure 1 illustrates these mechanisms.

Figure 6.3.2.2-1: Possible mechanisms for a common MOCN TMGI

1. MBMS service ID and default MOCN MCC and MNC configured by the operators. Values for MCC and MNC can be reserved for MOCN usecase and used across different operators.
2. MBMS service ID and AF ID instead of MNC, MCC. AF\_ID is defined in TS 33.535[Z].
3. Addition of new field to include AF\_ID with MBMS service ID and with MCC=MNC=Zero.
4. Addition of new field to include MOCN\_ID with MBMS service ID and with MCC=MNC=Zero.

Editor’s Note: Which of these mechanisms should be standardized is FFS. This can be aligned with SA2.

#### 6.3.2.3 MOCN keys MSK MTK

Considering the MOCN for broadcast usecase in 5G, common mechanisms to derive MSK and MTK are required across the different PLMNs. This solution proposes three possibile mechanisms for MOCN key identification. This proposal considers configurations of common fields for MOCN. For example, setting Key domain ID to a default value for all PLMNs involved in the MOCN. Figure 2 illustrates these proposed mechanisms.

**MOCN MSK**

1. Key domain can be set as default values or set to zero or new MOCN ID can be introduced instead of key domain ID. Differentiation bit must be set to show the difference between MOCN ID or key domain ID.MSK ID remains as before 4 bytes.
2. Key domain ID can be set to Zero or default value. MSK ID can remain as before with 4 bytes. MOCN ID can be introduced, and range of values are defined. For many such MOCN use cases, where different broadcast cases of RAN sharing will be assigned a MOCN ID value. MSK ID remains as before 4 bytes.
3. Key domain ID can be set to Zero or default value. MSK ID remains as before 4 bytes. AF ID is newly introduced and assigned the FQDN of AF & security protocol identifier. MSK ID remains as before 4 bytes.

**MOCN MTK**

1. Key domain can be set as default values or set to zero or new MOCN ID introduced instead of key domain ID. Differentiation bit must be set to show the difference between MOCN ID or key domain ID.MSK ID remains as before 4 bytes & MTK as 2 bytes.
2. Key domain ID can be set to Zero or default. MSK ID remains as before 4 bytes. MOCN ID is newly introduced, and range of values are defined. For many such MOCN use cases, where different broadcast cases of RAN sharing will be assigned a MOCN ID value. MSK ID remains as before 4 bytes & MTK as 2 bytes.
3. Key domain ID can be set to Zero or default. MSK ID remains as before 4 bytes. AF ID is newly introduced and assigned the FQDN of AF & security protocol identifier. MSK ID remains as before 4 bytes & MTK as 2 bytes.



Figure 6.3.2.2-2: Possible options for MSK and MTK for MOCN

Editor’s Note: Which of these mechanisms should be standardized is FFS.

Editor’s Note: How to derive the same key using common identifires is FFS.

Editor’s Note: Need to coordinate with SA2 on proposed TMGI definition.

### 6.3.3 System impact

TBD

### 6.3.4 Evaluation

TBD

## 6.A Solution #A: <Title>

### 6.A.1 Introduction

### 6.A.2 Solution details

### 6.A.3 System impact

### 6.A.4 Evaluation

# 7 Conclusions

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

Annex X:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-07 | SA3#107 Adhoc-e |  |  |  |  | S3-221394, S3-221395, S3-221666, S3-221667 | 0.1.0 |
| 2022-08 | SA3#108-e |  |  |  |  | S3-222070 | 0.2.0 |
| 2022-10 | SA3#108 Adhoc-e |  |  |  |  | S3-223092, S3-223093, S3-223064, S3-222555-r3 | 0.3.0 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |