|  |
| --- |
| 3GPP TR 33.862 V0.1.0 (2020-10) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of the Message Service for MIoT over the 5G System (MSGin5G)  |
|   |
| *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

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 7

4 Overview of MSGin5G Service 7

5 Key issues 7

5.1 Key issue #1: Transport security for the MSGin5G interfaces 7

5.1.1 Key issue details 7

5.1.2 Threats 8

5.1.3 Potential security requirements 8

5.2 Key issue #2: Authentication and Authorization between 5GMSGS client and MSGin5G Server 8

5.2.1 Key Issue Details 8

5.2.2 Security Threats 9

5.2.3 Potential Security Requirements 9

5.3 Key issue #3: Authentication and Authorization between Application server and MSGin5G Server 9

5.3.1 Key Issue Details 9

5.3.2 Security Threats 9

5.3.3 Potential Security Requirements 9

5.X Key issue #X: <Key issue name> 10

5. X.1 Key issue details 10

5. X.2 Threats 10

5. X.3 Potential security requirements 10

6 Proposed solutions 10

6.0 Mapping of Solutions to Key Issues 10

6.1 Solution #1: <Solution name> 10

6.1.1 Introduction 10

6.1.2 Solution details 10

6.1.3 Evaluation 10

6.X Solution #X: <Solution name> 11

6.X.1 Introduction 11

6.X.2 Solution details 11

6.X.3 Evaluation 11

7 Conclusions 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.

# 1 Scope

The present document studies the security aspects on the support of the 5GMSG Service defined in TR 23.700-24 [2], determines key issues of potential security requirements and proposed possible security solutions to meet 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 23.700-24: " Study on support of the 5GMSG Service ".

[3] 3GPP TS 23.222: " Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

# 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 MSGin5G Service

Editor’s Note: This clause will contain a brief overview on MSGin5G Service

# 5 Key issues

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

## 5.1 Key issue #1: Transport security for the MSGin5G interfaces

### 5.1.1 Key issue details

TR 23.700-24 [2], clause 8.2 describes an application architecture of the MSGin5G Service.



Figure 5.1.1-1: Application Architecture of the MSGin5G Service

New interfaces (i.e. MSGin5G-1-5) were introduced in the architecture for MSGin5G Service. This key issue studies the related transport security, i.e. confidentiality, integrity and replay-protection.

**MSGin5G-1:** Between a 5GMSGS client and a MSGin5G Server. This reference point supports:

- Registration of a 5GMSGS client to a MSGin5G Server when not using IMS base solution; and the exchange of MSGin5G messages.

**MSGin5G-2:** Between a MSGin5G Server and the Legacy 3GPP Message. This reference point supports:

- Indicating the underlying message delivery mechanism to the Legacy 3GPP Message Gateway; and exchange of MSGin5G messages; and registration of Legacy 3GPP Message Gateway to MSGin5G Server.

**MSGin5G-3:** Between an Application Server and a MSGin5G Server. This reference point supports:

- Access to MSGin5G Server and APIs to enable sending and receiving of MSGin5G messages; and Adherence to CAPIF as specified in 3GPP TS 23.222[3].

**MSGin5G-4:** Between a Non-3GPP Message Gateway and a MSGin5G server. This reference point supports:

- Registration of Non-3GPP Message Gateway to MSGin5G Server; and the exchange of MSGin5G messages.

**MSGin5G-5:** Between an application client and a 5GMSGS client. This reference point supports:

- Providing information from application clients required to enable the 5GMSGS client to construct a MSGin5G message to be delivered to other MSGin5G service endpoints.

- Configuring application clients with information required to enable the 5GMSGS client and MSGin5G Server to exchange and route MSGin5G messages to other MSGin5G service endpoints.

- Sending notifications and information in the incoming MSGin5G messages received by the 5GMSGS client to the application clients from other MSGin5G service endpoints.

NOTE: As MSGin5G-5 is an internal interface between application client and a 5GMSGS client within the UE, the protection is taken care by the UE implementation.

### 5.1.2 Threats

Without confidentiality, integrity and replay protection, an attacker may eavesdrop or manipulate or replay the communication or initiate the MitM attacks on the interface.

### 5.1.3 Potential security requirements

Confidentiality protection, integrity protection and replay-protection shall be supported on the MSGin5G-1-4 interfaces.

## 5.2 Key issue #2: Authentication and Authorization between 5GMSGS client and MSGin5G Server

### 5.2.1 Key Issue Details

As per 23.700-24 [2], MSGin5G-1 between a 5GMSGS client and a MSGin5G Server. This reference point supports registration and de-registration of a 5GMSGS client to a MSGin5G Server when not using IMS based solution and the exchange of MSGin5G messages.

During registration, the 5GMSGS Client provides profile/availability information for the 5GMSGS Client and the Application Clients that are serviced by the 5GMSGS Client to the MSGin5G Server. The profile/availability information includes contact information such as UE Identifier(s) and port number(s) which the 5GMSGS Client and the Application Clients listen on for incoming MSGin5G messages, supported MSGin5G capabilities (e.g. MOMT, AOMT, MOAT, Group, Broadcast) and MSGin5G service requirements (e.g. required time windows of service, message latency and data rates).

### 5.2.2 Security Threats

When registration and de-registration is used without authorization, if the registration is a new registration, the MSGin5G Server assigns a unique 5GMSGS Client ID to the malicious 5GMSGS client receive. The malicious 5GMSGS Client stores the identifier and uses it in all future MSGin5G communication with the MSGin5G Server. The Malicious 5GMSGS client may receive information e.g. URI, Application Server Functionalities, protocols which may reveal the security domain topology of the server. Malicious 5GMSGS Client may use this information to launch attacks on MSGin5G server.

### 5.2.3 Potential Security Requirements

MSGin5G Server and 5GMSGS Client shall be mutually authenticated over MSGin5G-1 Interface.

The 5GMSGS client shall be authorized to access MSGin5G services.

## 5.3 Key issue #3: Authentication and Authorization between Application server and MSGin5G Server

### 5.3.1 Key Issue Details

As per 23.700-24 [2], MSGin5G-3 between an Application Server and a MSGin5G Server. This reference point supports access to MSGin5G Server and APIs to enable sending and receiving of MSGin5G messages.

During registration, the MSGin5G server should be able to verify the Application server, otherwise MSGin5G server may share sensitive information to the application server such as 5GMSGS Client ID, APIs like so.

### 5.3.2 Security Threats

During registration, the MSGin5G server should be able to verify the Application server, otherwise MSGin5G server may share sensitive information to the application server such as 5GMSGS Client ID, APIs like so. These informations can be used by the application server to mount an attack to get services from MSGin5G server without the server knowing its liability.

### 5.3.3 Potential Security Requirements

The system shall support mutual authentication and authorization between application server and MSGin5G server over MSGin5G-3 Interface.

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

## 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 | X |  |  |
| #1: <Solution name> | X |  |  |  |
| #X: <Solution name> | X |  |  |  |

Editor’s Note: This clause provides the mapping of Solutions to Key Issues.

## 6.1 Solution #1: <Solution name>

### 6.1.1 Introduction

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 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 Introduction

### 6.X.2 Solution details

### 6.X.3 Evaluation

# 7 Conclusions

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

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020/10/19 | 3GPP SA3 100bis-e |  |  |  |  | S3-202304,S3-202533,S3-201615,S3-202616,S3-202617 | 0.1.0 |