|  |  |
| --- | --- |
| 3GPP TR 33.862 V0.4.0 (2021-03) | |
| 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 address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 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".

[4] 3GPP TS 33.434: "Service Enabler Architecture Layer (SEAL); Security aspects for Verticals".

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

[6] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security".

[7] 3GPP TS 22.262: " Message Service within the 5G System; Stage 1 ".

[8] 3GPP TR 22.824: " Feasibility study on 5G message service for MIoT; Stage 1 ".

[9] 3GPP TR 23.700-24: " Study on support of the 5GMSG Service ".

[10] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

# 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

3GPP TS 22.262[7] and 3GPP TR 22.824[8] define the stage 1 requirements of the MSGin5G Service (message service for MIoT over 5G System), 3GPP TR 23.700-24[9] is under progress of defining the architecture and procedures to support the MSGin5G service. The above specifications form the baseline for the present study on security aspects of MSGin5G Service for the 5G system (5GS).MSGin5G Service enables an UE sending/receiving message of text, voice, video or data to/from another UE or application server. It is basically designed for IoT device communication, including thing-to-thing communication and person-to-thing communication. The emerging IoT device communication will introduce new requirements of messaging service in terms of service capabilities, performance, charging, and security etc.

For example, for the following scenarios from TS 22.262[7], the content of the messages are required to be integrity and confidentially protected. For each scenario and for different UE types (5GMSGS UE, Legacy 3GPP UE, Non-3GPP UE), whether existing security mechanisms can be used to achieve the integrity and confidentiality protection under the architecture defined by TR 23.700-24[9] need to be investigated.

a) point-to-point message

b) application-to-point message

c) group message

d) broadcast message

# 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.

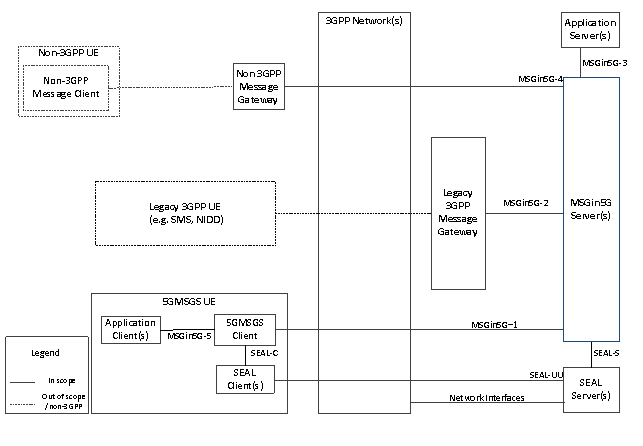


Figure 5.1.1-1: Application Architecture of the MSGin5G Service

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

## 5.4 Key issue #4: Authentication and Authorization between message Gateway and MSGin5G Server

### 5.4.1 Key Issue Details

As per 23.700-24 [2], MSGin5G-4 is 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.

Also, MSGin5G-2 is the interface between legacy 3GPP message gateway and MSGin5G server. This reference point supports registration of Legacy 3GPP Message Gateway to MSGin5G Server and exchange of MSGin5G messages.

During registration, the MSGin5G server should be able to verify the non-3GPP message Gateway , and legacy 3GPP message gateway otherwise malicious Gateway may connect to MSGin5G server, so that sensitive information such as 5GMSGS Client ID, service ID may leak out.

### 5.4.2 Security Threats

During registration, if the MSGin5G server transfers information without verify the Gateway, Gateway may connect to MSGin5G server, so that sensitive information such as 5GMSGS Client ID, service ID may leak out. Malicious Gateway may use this information to launch attacks on MSGin5G server.

These information’s can be used by malicious Gateway to mount an attack to get services from MSGin5G server without authorization.

### 5.4.3 Potential Security Requirements

MSGin5G shall support mutual authentication and authorization for communication between MSGin5G server and Non-3GPP message gateway.

MSGin5G shall support mutual authentication and authorization for communication between MSGin5G server and legacy 3GPP message gateway.

# 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: Authentication and authorization between 5GMSGS client and MSGin5G server

### 6.1.1 Solution overview

This solution addresses the security requirement for the Authentication and Authorization between 5GMSGS client and MSGin5G server in key issue #2.

This solution uses SEAL server as an access token issuer and validator. SEAL Client authenticates with SEAL server as a result of which it receives access token using OpenID Connect protocol as specified in TS 33.434 [4].

Access token is used for authorization of the 5GMSGS UE Client to access/obtain the MSGin5G services.

### 6.1.2 Solution details



**Figure 6.1.2-1: Authentication/Authorization framework for 5GMSGS client and MSGin5G servers**

Step 1: SIM-C establishes a secure tunnel with the SIM-S. In this step the SIM-C provides the 5GMSGS UE identifier in case to associate the SIM-C with the 5GMSGS client.

Step 2: SIM-C sends an OpenID Connect Authentication Request to the SIM-S. The request contains an indication of authentication methods supported by the UE.

NOTE: This solution works only if OpenID Connect protocol is supported by the system.

Step 3: User Authentication is performed between SIM-C and the SIM-S. On receiving OpenID Connect Authentication Request, SIM-S provides HTML page to the SIM-C.

Step 4: SIM-C authenticates itself by giving username and password.

NOTE: The primary credentials for user authentication (e.g., username/password) are based on MSGin5G service provider policy. The method chosen by the service provider is neither defined nor limited to the example (username/password) provided in this solution.

Step 5: SIM-S verifies the username and password and authenticates the UE.

Step 6: SIM-S sends an OpenID Connect Authentication Response to SIM-C containing an authorization code (AuthCode).

Step 7: SIM-C sends an OpenID Connect Token Request to the SIM-S, passing the AuthCode.

Step 8: SIM-S sends an OpenID Connect Token Response to the UE containing an ID\_token and an access token (each which uniquely identify the user of the MSGin5G service). The access token is used by the 5GMSGS UE client to communicate and authorize the identity of the 5GMSGS UE client to the MSGin5G server. The access token and ID-token format is same as format defined in TS 33.434, Annex A.2.1 and A.2.2.

Step 9: 5GMSGS UE client gets the ID\_Token and access token from the SIM-C.

Step 10: A secure IPSec tunnel is established between 5GMSGS UE client and MSGin5G server.

Step 11: The 5GMSGS UE client initiates application registration procedure with the MSGin5G server, including the access token obtained from SIM-S at step 6 required for the 5GMSGS Client to register to the MSGin5G Server.

The request also includes a 5GMSGS Client Profile for the 5GMSGS Client initiating the registration request. The 5GMSGS client profile includes UE ID, 5GMSGS Client ports, 5GMSGS Client ID, 5GMSGS Client capabilities.

Step 12: The authorization check for the application registration request is performed by verification of the access token issued by the SIM-S. The MSGin5G server obtains the access token validation service from the SIM-S.

Step 13: MSGin5G server sends the application accept or reject response based on the result of access token validation.

Editor’s Note: Whether SEAL supports handling 5GMSGS identifiers is FFS.

Editor’s Note: ID\_Token format and its usage is FFS.

Editor’s Note: Further details on Authentication at step 10 is FFS.

### 6.1.3 Solution evaluation

TBD

## 6.2 Solution #2: Authentication and authorization between 5GMSGS UE client and MSGin5G server using secondary authentication

### 6.2.1 Solution overview

This solution addresses the security requirement for the Authentication and Authorization between 5GMSGS UE client and MSGin5G server in key issue #2.

This solution proposes to reuse the secondary authentication procedure for the authentication between the 5GMSGS Client and the MSGin5G server as specified in TS 33.501 [5].

### 6.2.2 Solution details



**Figure 6.2.2-1: Authentication/Authorization framework for 5GMSGS UE client and MSGin5G servers using secondary authentication**

1. The UE registers to the network and perform the primary authentication procedure.

2. When the UE triggers the MSGin5G service it sends the PDU session establishment request to the AMF to setup the PDU session for the MSGF.

3-6. The following steps 3, 4, 5, 6 are the same as in clause 11.1.2 of TS 33.501[5]. The secondary authentication procedure is performed. The SMF should trigger EAP Authentication procedure and perform the role of the EAP Authenticator. The MSGF is the EAP server (AAA) of the DN.

7-8. After the successful completion of the secondary authentication procedure, the MSGF sends EAP Success message to the SMF including the registration response.

9. The SMF sends a Namf\_Communication\_N1N2MessageTransfer to the AMF with the EAP success message.

10. The AMF forwards PDU Session Establishment Response message along with EAP Success.

### 6.2.3 Solution evaluation

TBD

## 6.3 Solution #3: Transport security protection for MSGin5G-1 interfaces

### 6.3.1 Solution overview

This solution addressed the transport security requirements for MSGin5G-1 interface defined in key issue#1. As specified in SEAL specification TS 33.434[4], NDS/IP should be used for the data protection over MSGin5G-1 interface.

### 6.3.2 Solution details

The protection of this interface should be supported according to NDS/IP as specified in TS 33.210 [6] as per VAL-UU protection defined in TS 33.434[4].

NOTE: NSD/IP is used only when SEAL enabler is supported by the UE.

### 6.3.3 Solution evaluation

TBD

## 6.4 Solution #4: Authentication and Authorization between 5GMSGS Client and MSGin5G server based on AKMA

### 6.4.1 Introduction

This solution addresses the security requirement for the Authentication and Authorization between 5GMSGS UE client and MSGin5G server in key issue #2.

This solution proposes to use AKMA (as specified in TS 33.535 [10]) for the authentication between the 5GMSGS Client and the MSGin5G server.

### 6.4.2 Solution details

Pre-requisite: UE with 5G MSG Client functionality registers in the 5G network, and retrieves the information of AKMA capability from 5GC. The AKMA capability indicates that 5G MSG Server supports to use AKMA, thus the UE and the 5GC generates KAKMA as specified in [10].



Step 1-3: UE communicates with the 5G MSG Server to negotiate the key K5GMSG, of which the UE and the 5G MSG Server both are in possession after step 3.

Step 4: The UE and the 5G MSG Server establish the TLS security tunnel based on the key K5GMSG. The authentication between the UE and the 5G MSG Server is fulfilled based on the TLS.

### 6.4.3 Evaluation

TBD

## 6.5 Solution #5: Authentication and authorization for 5GMSGS UE

### 6.5.1 Introduction

This solution proposes to use TLS-PSK based authentication for the authentication between MSGin5G UE and the MSGin5G server.

### 6.5.2 Solution details



**Figure 6.5.2-1: Authentication and authorization between 5GMSGS UE and MSGin5G server**

Step 1-2: The UE performs the procedures (for example, Initial Registration procedure) as defined in TS 23.502 to get the 5GC network access. At the end of the network access authentication procedure (Primary authentication and key agreement [TS 33.501, clause 6.1]), the UE and the AMF are in possession of the key KAMF derived from KSEAF.

The UE and AMF performs the capability exchange procedure and agree upon the method of authentication for MSGin5G service during PDU session establishment.

Step 3: Then the UE initiate the Initial service provisioning procedure with the SEAL server.

Step 4: SEAL server sends a key request to the designated AMF. The AMF/SEAF derives the KMSG from the KSEAF/KAMF. The SEAL server identifies the AMF using the 5G-GUTI which has the GAUMI which uniquely identifies one AMF.

Step 5a-5b: The UE derives the KMSG key for MSGin5G service, whenever there is trigger to get MSG service. Based on the UE’s capability to support MSGin5G service, the SEAF/AMF derives the KMSG. Key derivation step is skipped, if the UE and AMF holds a valid KMSG.

Step 6: After key material (KMSG) is generated, the SEAF/AMF sends the generated KMSG and ngKSI to the SEAL server together with UE ID and/or SUPI and/or MSGin5G service ID of the 5GMSGS client in the key response. The SEAL server stores the latest information sent by the SEAF/AMF.

Step 7: Once KMSG is established, PSK is generated from KMSG.

Step 8-10: SEAL server sends the initial service provisioning response to the 5GMSGS client. On receiving the initial service provisioning response, the 5GMSGS client derives the KMSG-PSK. On successful initial service provisioning procedure, the 5GMSGS client and SEAL server establishes a TLS session using pre-shared key KMSG-PSK.

Step 11-14: On successful TLS session establishment the 5GMSGS client sends a trigger message to the SEAL client to trigger an access token request. Accordingly, SEAL client sends an application token request to the SEAL server. SEAL server provides the SEAL client with an access token. The acquired access token is shared with 5GMSGS client.

Step 15: Before sending the access token for authorization to the MSGin5G server, the 5GMSGS client establishes a secure channel using certificates.

Step 16: The 5GMSGS client sends the access token in an application registration request to the MSGin5G server along with the MSGin5G service ID.

Step 17-19: SEAL server validates the received access token and the MSGin5G server validates the service request by validating the MSGin5G service ID. On successful verification MSGin5G server sends the application registration response.

Editor's Note: How to protect the spoofing of Service ID by a malicious UE is FFS.

### 6.5.3 Evaluation

*TBD*

## 6.6 Solution #6: Authentication and authorization for legacy UE

### 6.6.1 Introduction

This solution proposes to use TLS-PSK based authentication for the authentication between legacy UE and the MSGin5G server where SMSF acts as the key management function.

### 6.6.2 Solution details



**Figure 6.6.2-1: Procedure for authentication and authorization between legacy UE and MSGin5G server.**

Step 1-2: The UE performs the procedures (for example, Initial Registration procedure) as defined in TS 23.502 to get the 5GC network access. At the end of the network access authentication procedure (Primary authentication and key agreement [TS 33.501, clause 6.1]), the UE and the AMF are in possession of the key KAMF derived from KSEAF.

The UE and AMF performs the capability exchange procedure and agree upon the method of authentication for MSGin5G service during the PDU session establishment.

Step 3: The UE initiates the Initial service provisioning procedure with the SMSF.

Step 4: SMSF sends a key request to the designated AMF. The AMF/SEAF derives the KMSG from the KSEAF/KAMF. The SMSF identifies the AMF using the 5G-GUTI which has the GAUMI which uniquely identifies one AMF.

Step 5a-5b: The UE derives the KMSG key whenever there is trigger to get MSG service. Based on the UE’s capability to support MSGin5G service, the SEAF/AMF derives the KMSG. Key derivation step is skipped, if the UE or AMF holds a valid KMSG.

Step 6: After key material (KMSG) is generated, the SEAF/AMF sends the generated KMSG and ngKSI to the SMSF together with UE ID and/or SUPI and/or MSGin5G Service ID of the UE in the key response. The SMSF stores the latest information sent by the SEAF/AMF.

Step 7: Once KMSG is derived, PSK is generated from KMSG.

Step 8-10: SMSF sends the initial service provisioning response to the UE. On receiving the initial service provisioning response, the UE derives the KMSG-PSK. On successful initial service provisioning procedure, the UE and SMSF establishes a TLS session using pre-shared key KMSG-PSK.

Step 11-12: On successful TLS session establishment the UE sends an application token request to the SMSF. SMSF provides the access token to the UE.

Step 13: The legacy UE establishes a secure connection with the Legacy 3GPP message gateway. The legacy UE registers with the MSGin5G server via legacy 3GPP message gateway. The communication between legacy UE and the gateway is out of scope of the study.

Step 14: Before sending the access token for authorization to the MSGin5G server, the gateway establishes a secure channel using certificates.

Step 15: The gateway sends the access token in an application registration request to the MSGin5G server along with the MSGin5G service ID.

Step 16-18: SMSF validates the received access token and the MSGin5G server validates the service request by validating the MSGin5G service ID. On successful verification MSGin5G server sends the application registration response.

Editor's Note: How to protect the spoofing of Service ID by a malicious UE is FFS.

### 6.6.3 Evaluation

*TBD*

## 6.7 Solution #7: Authentication and authorization for Non-3GPP UE

### 6.7.1 Introduction

This solution proposes to use TLS-PSK based authentication for the authentication between non-3GPP UE and the MSGin5G server.

### 6.7.2 Solution details



**Figure 6.7.2-1: Procedure for authentication and authorization between Non-3GPP UE and MSGin5G server.**

UE here refers to the non-3GPP UE or the non-3GPP gateway. Based on SA2 specification the TR 23.700-24, the Service ID in non-3GPP UE is translated as the MSGin5G service ID.

Detailed procedure is provided below:

Step 1-2: The UE initiates the initial registration procedure as defined in TS 23.502 to get the 5G Core network access. At the end of the network access authentication procedure (Primary authentication and key agreement [TS 33.501, clause 6.1]), the UE and the AMF are in possession of the key KAMF.

The UE and AMF performs the capability exchange procedure and agree upon the method of authentication for MSGin5G service during the PDU session establishment.

Step 3: Then the UE initiate the Initial service provisioning procedure with the N3IWF which acts as the key management server. The MSGin5G service Key KMSG is derived from KAMF.

Step 4: N3IWF sends a key request to the designated AMF.

Step 5a-6: AMF derives the MSGin5G service key (KMSG) from KAMF/KSEAF. The AMF sends back the derived KMSG in the key response.

Step 7-9: N3IWF derives the pre-shared key KMSG-PSK from KMSG and sends the initial service provisioning response to the UE. On receiving the initial service provisioning response, the UE derives the KMSG-PSK.

Step 10: On successful initial service provisioning procedure the UE and N3IWF establishes a TLS session using pre-shared key KMSG-PSK.

Step 11-12: On successful TLS session establishment the UE sends an application token request to the N3IWF. N3IWF provides the UE with an access token.

Step 13: The non-3gpp UE establishes a secure connection with the Non-GPP message gateway. The non-3gpp UE registers with the MSGin5G server via Non-3GPP message gateway. The communication between non-3gpp UE and the gateway is out of scope of the study.

Step 14: Before sending the access token for authorization to the MSGin5G server, the non-3gpp gateway establishes a secure channel using certificates.

Step 15: The gateway sends the access token in an application registration request to the MSGin5G server along with the MSGin5G service ID.

Step 16-18: N3IWF validates the received access token and the MSGin5G server validates the service request by validating the MSGin5G service ID. On successful verification MSGin5G server sends the application registration response.

Editor's Note: How to protect the spoofing of Service ID by a malicious UE is FFS.

### 6.7.3 Evaluation

*TBD*

# 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 | S3-202765 |  |  |  | S3-202304,S3-202533,S3-201615,S3-202616,S3-202617 | 0.1.0 |
| 2020/11/16 | 3GPP SA3 101-e | S3-203464 |  |  |  | S3-203139, S3-203365, S3-203366, S3-203241 | 0.2.0 |
| 2021/01/25 | 3GPP SA3 102-e | S3-210673 |  |  |  | S3-210319, S3-210320, S3-210578, S3-210579, S3-210580, S3-210582 | 0.3.0 |
| 2021/03/08 | 3GPP SA3 102bis-e | S3-211323 |  |  |  | S3-211200 | 0.4.0 |