|  |
| --- |
| 3GPP TS 33.558 V17.1.0 (2022-06) |
| Technical Specification |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Security aspects of enhancement of support for enabling edge applications;Stage 2(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.© 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

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 Overview 7

5 Security requirements 7

5.1 General security requirements 7

5.1.1 Authentication and Authorization. 7

5.1.2 Interface security 8

5.1.3 User Consent Requirements 8

6 Procedures 8

6.1 Security for the EDGE interfaces 8

6.2 Authentication and Authorization between EEC and ECS 8

6.3 Authentication and Authorization between EEC and EES 9

6.4 Authentication and Authorization between EES and ECS 9

6.5 Authentication and Authorization in EES capability exposure 9

Annex A (informative): Change history 11

# Foreword

This Technical Specification 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 specifies the security features and mechanisms to support the application architecture for enabling Edge Applications in 5G, i.e. security for the interfaces, procedures for the authentication and authorization between the entities of the application architecture, and procedures for the EES capability exposure.

# 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 TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

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

[4] 3GPP TS 33.187: "Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements".

[5] 3GPP TS 23.558: "Architecture for enabling Edge Applications."

[6] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

[7] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs"

[8] Void

[9] Void

[10] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[11] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[12] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[13] IETF RFC 7540: " Hypertext Transfer Protocol Version 2 (HTTP/2)".

[14] RFC 2818: "HTTP Over TLS".

[15] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[16] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[17] IETF RFC 7519: "JSON Web Token (JWT)".

[18] IETF RFC 7515: "JSON Web Signature (JWS)".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1].

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

# 4 Overview

The overall application architecture for enabling Edge Applications that is given in TS 23.558 [5], includes several entities, such as 3GPP core network, Edge Enabler Client (EEC) deployed in the UE, Edge Configuration Server (ECS), Edge Enabler Server (EES), and Edge Application Server (EAS). The application architecture for enabling Edge Applications, is defined in TS 23.558 [2] clause 6.2.

This specification captures the following security requirements and procedures:

- Security for the EDGE interfaces: the set of security features that enable network nodes to exchange signalling data and user plane data securely.

- Authentication and Authorization between EEC and ECS/EES: the set of security features that enable the authentication between EEC and ECS/EES, and enable the EEC to be authorized by the ECS/EES.

- Authentication and Authorization between EES and ECS: the set of security features that enable the authentication between EES and ECS, and enable the EES to be authorized by the ECS.

- Authentication and Authorization in EES capability exposure: the set of security features that enable the EAS to be authenticated and authorized by the EES in EES capability exposure.

- Authentication and Authorization in 3GPP Core Network capability exposure: the set of security features that enable the ECS/EES/EAS to be authenticated and authorized by the 3GPP Core Network in 3GPP Core Network capability exposure.

# 5 Security requirements

## 5.1 General security requirements

The Edge application architecture defined in the TS 23.558 [xx] shall satisfy the following requirements.

### 5.1.1 Authentication and Authorization.

**Authentication and Authorization between Edge Enabler Client (EEC) and Edge Configuration Server (ECS):** Edge Configuration Server (ECS) shall be able to provide mutual authentication with Edge Enabler Client (EEC) over EDGE-4 Interface. ECS shall determine whether EEC is authorized to access ECS's services.

**Authentication and Authorization between EEC and EES:** Edge Enabler Server (EES) shall provide mutual authentication with EEC over EDGE-1 Interface. EES shall determine whether EEC is authorized to access EES's services.

**Authentication and Authorization between Edge Enabler Server (EES) and ECS**: ECS shall provide mutual authentication with EES over EDGE-6 Interface. ECS shall determine whether EES is authorized to access ECS's services.

**Authentication and Authorization in EES capability exposure to EAS**: EES shall provide mutual authentication with EAS over EDGE-3 Interface. EES shall determine whether EAS is authorized to access EES's services and expose EEC Capabilities. The Edge application architecture shall support EASs to obtain the user's authorization to access sensitive information (e.g. user's location).

NOTE1: The corresponding security requirements defined in TS 23.558 [5] is AR-5.2.6.2-a/b/d/e/f/g.

### 5.1.2 Interface security

Confidentiality, integrity, and replay protection shall be supported on the EDGE-1-4 and EDGE 6-9 interfaces.

NOTE 1: The interfaces are defined in the Figure 6.2.4 of TS 23.558 [5]. The corresponding security requirement defined in TS 23.558 [5] is AR-5.2.6.2-c.

NOTE 2: The security requirement of EDGE 5 is out of the scope of this specification, since its details are out of the scope of this release of this specification, according to TS 23.558 [5].

The privacy requirements AR-5.2.6.2-h defined in TS 23.558 [5] are implicitly supported, since all the interfaces will be confidentiality and integrity protected.

### 5.1.3 User Consent Requirements

User consent for edge computing shall comply with TS 33.501 [3] (Annex V).

If EES, trusted by the 3GPP Core Network, is utilizing 5GC services without NEF, the EES acts as the consent enforcing entity. Otherwise, if the EES is utilizing 5GC services via NEF, the NEF acts as the consent enforcing entity.

User consent architecture in the present document is only applicable when EES or NEF and data provider are operated by the same entity.

# 6 Procedures

## 6.1 Security for the EDGE interfaces

For the interfaces (EDGE-1/4), the EEC, EES and ECS shall support TLS and HTTPS as specified in RFC 7540 [13] and RFC 2818 [14]. TLS profile shall follow the profile given in clause 6.2 of TS 33.210 [1] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [13]. TLS shall be used for transport protection..

For the interfaces EDGE-2/7/8,

- If the NEF APIs are selected, security aspects of Network Exposure Function including the protection of NEF-AF interface and support of CAPIF defined in TS 33.501 clause 12 [2] shall be reused, i.e., use of TLS.

- If the SCEF APIs are selected, the Security procedures for reference point SCEF-SCS/AS defined in TS 33.187 clause 5.5 [3] can be reused here, i.e., use of TLS.

For the interfaces (EDGE-3/6/9), the EAS, EES and ECS shall support TLS and HTTPS as specified in RFC 7540 [13] and RFC 2818 [14]. TLS profile shall follow the profile given in clause 6.2 of TS 33.210 [1] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [13]. TLS shall be used for transport protection, unless security is provided by other means, e.g.,. physical security.

## 6.2 Authentication and Authorization between EEC and ECS

 The ECS shall be configured with the information of authorization methods (token-based authorization or local authorization) used by EESes.

Authentication between EEC and ECS shall be done during the execution of the TLS handshake protocol.. Details of the authentication method (e.g., TLS certificates, usage of AKMA [11] or GBA [12] as methods to arrange the PSK for TLS) are out of scope of the present document. If the EEC sends the GPSI to the ECS, then the ECS shall also authenticate the GPSI. The details of how to authenticate the GPSI is out of scope of the present document.

After successful authentication, the ECS shall authorize the EEC by its local authorization policy.

After successful authentication and authorization, the ECS decides whether OAuth 2.0 [15] access tokens are required for the candidate EESes using the configuration information and issues separate EES access tokens to be used for each candidate EESes that use token-based authorization. The ECS, EEC and EES respectively assume the role of authorization server, client and resource server roles defined in [15]. "Client Credentials" grant type and bearer tokens [16] shall be used. JSON Web Token (JWT) as specified in IETF RFC 7519 [17] for encoding and the JSON signature profile as specified in IETF RFC 7515 [18] for protection of tokens shall be followed. This token profile also applies for clause 6.3 of the present document. The claims of the EES service tokens in the form of JWT [17] shall include the ECS FQDN (issuer), EEC ID (client\_id), GPSI (subject), expected EES service name(s) (scope), EES FQDN (audience), expiration time (expiration). The ECS shall send the service response back to the EEC, which may include EES access token(s).

## 6.3 Authentication and Authorization between EEC and EES

Authentication between EEC and EES shall be done during the execution of the TLS handshake protocol.. Details of the authentication method (e.g., TLS certificates, usage of AKMA [11] or GBA [12] as methods to arrange the PSK for TLS) are out of scope of the present document. If the EEC sends the GPSI to the EES, then the EES shall also authenticate the GPSI. The details of how to authenticate the GPSI is out of scope of the present document.

For authorization of EEC by the EES, the EEC shall send the OAuth 2.0 [15] access token, if received from the ECS, to the EES. The token profile is specified in clause 6.2 of the present document. If the EES requires access token for authorization, then the EES shall authorize the EEC by using the token. Otherwise, the EES shall authorize the EEC by its local authorization policy.

After successful authentication and authorization, the EES shall process the request and sends the service response back to the EEC.

## 6.4 Authentication and Authorization between EES and ECS

6.4.1 General

The detailed service procedures between EES and ECS are described in TS 23.558 [5].

6.4.2 Procedure for the Authentication and Authorization between EES and ECS

Pre-requisite:

- EES obtains onboarding information within the same PLMN domain or from a third-party domain. The information includes the Edge Configuration Server Address and Root CA certificate details, it may include an enrolment token.

NOTE1: The provisioning and usage of the onboarding information are out of the scope of this document.

- The EES and ECS are provisioned with credentials for the mutual authenticated TLS.

TLS shall be used to provide integrity protection, replay protection, and confidentiality protection for the interface between the EES and the ECS.

Security profiles for TLS implementation and usage shall follow the profiles given in TS 33.210 [2] Annex E and F, and TS 33.310 [11]. The identities in the end-entity certificates shall be used for authentication and policy checks. Identities in the end-entity certificate shall be based on endpoint information (e.g., URI, FQDN, IP address) as described in the TS 23.558[5].

The ECS shall authorize the EES based on local authorization policy.

## 6.5 Authentication and Authorization in EES capability exposure

According to clause 8.7.3 of TS 23.558 [5], the EES may re-expose the network capabilities of the 3GPP core network to the EAS(s) as per the CAPIF architecture specified in TS 23.222 [6]. If the CAPIF architecture is used, the CAPIF functional security model specified in TS 33.122 [7] shall be used for Authentication and authorization in EES capability exposure.

If CAPIF is not used, mutual authentication with TLS certificates using TLS shall be used. The TLS and certificates shall follow the profiles defined in TS 33.210 [2] and TS 33.310 [10], and the authorization is based on local authorization policy at the EES.

NOTE: Void

Annex A (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 2022-03 | SA#95e | SP-220189 |  |  |  | Presented for information and approval | 1.0.0 |
| 2022-03 | SA#95e |  |  |  |  | Upgrade to change control version | 17.0.0 |
| 2022-06 | SA#96 | SP-220558 | 0001 | 2 | F | Editorial corrections and technical clarifications | 17.1.0 |
| 2022-06 | SA#96 | SP-220558 | 0002 | 1  | F | Clarification of access token usage in EC | 17.1.0 |