|  |
| --- |
| 3GPP TS 33.558 V0.2.0 (2021-10) |
| 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.© 2021, 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 7

5 Security requirements 7

5.1 General security requirements 7

5.1.1 Authentication and Authorization. 7

5.1.2 Interface security 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 8

6.4 Authentication and Authorization between EES and ECS 9

6.5 Authentication and Authorization in EES capability exposure 9

Annex <A> (normative): <Normative annex for a Technical Specification> 10

Annex <B> (informative): <Informative annex for a Technical Specification> 11

Annex <X> (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] 3GPP TS 23.558: "Architecture for enabling Edge Applications."

# 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].

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].

Abbreviation format (EW)

<ABBREVIATION> <Expansion>

# 4 Overview

The overall application architecture for enabling Edge Applications that is given in TS 23.558 [8], 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 securely exchange signalling data and user plane data.

- 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.

Editor’s Note: “EEC authentication towards EES/ECS to be confirmed”.

# 5 Security requirements

## 5.1 General security requirements

The Edge application architecture defined in the TS 23.558 [5] 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 be able to determine whether EEC is authorized to access ECS’s services.

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

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

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

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

### 5.1.2 Interface security

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

NOTE1: The interfaces is defined in the Figure 6.2.4 of TS 23.558 [5]. The corresponding security requirements defined in TS 23.558 [5] is AR-5.2.6.2-c.

NOTE2: Security requirement of EDGE 5 is out of scope of this specification, since its details is out of scope of this release of this specification, according to TS 23.558 [5].

The security requirements AR-5.2.6.2-b defined in TS 23.558 [5] that relies on the Edge Computing Service Provider, is out of scope of this specification. The privacy requirements AR-5.2.6.2-h defined in TS 23.558 [5] is implicitly supported, since all the interfaces will be security protected.

Editor’s Note: It is FFS whether the security requirements AR-5.2.6.2-b defined in TS 23.558 [5] that relies on the Edge Computing Service Provider, is out of scope of this specification.

# 6 Procedures

## 6.1 Security for the EDGE interfaces

For the interfaces (EDGE-1/4), TLS specified in TS 33.210 [1] shall be used if HTTP protocol is selected.

For the interfaces EDGE-2/7/8,

- If the NEF APIs is 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 is 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), TLS shall be used as specified in TS 33.210 [1], unless security is provided by other means, e.g. physical security.

## 6.2 Authentication and Authorization between EEC and ECS

Editor’s Notes: Authentication and Authorization between EEC and ECS is to be added.

## 6.3 Authentication and Authorization between EEC and EES

Editor’s Notes: Authentication and Authorization between EEC and EES is to be added.

## 6.4 Authentication and Authorization between EES and ECS

Editor’s Notes: Authentication and Authorization between EES and ECS is to be added.

## 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 3GPP 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.

Annex <A> (normative):
<Normative annex for a Technical Specification>

Start each annex on a new page.

Annexes are labelled A, B, C, etc. and designated either "normative" or "informative" depending on their content.

Normative annexes only to appear in Technical Specifications. Use style "Heading 8".

Annex <B> (informative):
<Informative annex for a Technical Specification>

Informative annexes may appear in both Technical Specifications and Technical Reports. Use style "Heading 8" for use in TSs.

Informative annexes shall not contain requirements for the implementation of the Technical Specification.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2021-08 | SA3 #104-e | S3-212647 |  |  |  | TS Skeleton | 0.0.0 |
| 2021-08 | SA3 #104-e | S3-213227 |  |  |  | Implemented S3-212650, S3-212325, and, S3-212326. | 0.1.0 |
| 2021-10 | SA3 #104-e-Ad-hoc | S3-213668 |  |  |  | Implemented S3-213663, and, S3-213664. | 0.2.0 |

Change history of this template:

|  |  |  |
| --- | --- | --- |
| 2001-07 | Copyright date changed to 2001; space character added before TTC in copyright notification; space character before first reference deleted. | 1.3.3 |
| 2002-01 | Copyright date changed to 2002. | 1.3.4 |
| 2002-07 | Extra Releases added to title area. | 1.3.5 |
| *2002-12* | *"TM" added to 3GPP logo.* | *1.3.6* |
| *2003-02* | *Copyright date changed to 2003.* | *1.3.7* |
| *2003-12* | *Copyright date changed to 2004. Chinese OP changed from CWTS to CCSA* | *14.0* |
| *2004-04* | *North American OP changed from T1 to ATIS* | *1.5.0* |
| *2005-11* | *Stock text of clause 3 includes reference to 21.905.*  | *1.6.0* |
| *2005-11* | *Caters for new TSG structure. Minor corrections.* | *1.6.1* |
| *2006-01* | *Revision marks removed.* | *1.6.2* |
| *2008-11* | *LTE logo line added, © date changed to 2008, guidance on keywords modified; acknowledgement of trade marks; sundry editorial corrections and cosmetic improvements* | *1.7.0* |
| *2010-02* | *3GPP logo changed for cleaner version, with tag line;LTE-Advanced logo line added; © date changed to 2010;editorial change to cover page footnote text;trade marks acknowledgement text modified;additional Releases added on cover page;proforma copyright release text block modified* | *1.8.0* |
| *2010-02* | *Smaller 3GPP logo file used.* | *1.8.1* |
| *2010-07* | *Guidance note concerning use of LTE-Advanced logo added.* | *1.8.2* |
| *2011-04-01* | *Guidance of use of logos on cover page modified; copyright year modified.* | *1.8.3* |
| *2013-05-15* | *Changed File Properties to MCC macro default.* *Removed R99, added Rel-12/13.**Modified Copyright year.**Guidance on annex X Change history.* | *1.8.4* |
| *2014-10-27* | *Updated Release selection on cover. In clause 3, added "3GPP" to TR 21.905.* | *1.8.5* |
| *2015-01-06* | *New Organizational Partner TSDSI added to copyright block.Old Releases removed.* | *1.9.0* |
| *2015-12-03* | *Provision for LTE Advanced Pro logo Update copyright year to 2016* | *1.10.0* |
| *2016-03-08* | *Standarization of the layout of the Change History table in the last annex.(Unreleased)* | *1.11.0* |
| *2016-06-15* | *Minor adjustment to Change History table heading* | *1.11.1* |
| *2017-03-13* | *Adds option for 5G logo on cover* | *1.12.0* |
| *2017-05-03* | *Smaller 5G logo to reduce file size* | *1.12.1* |
| *2019-02-25* | *Replacement of frames on cover pages by in-line text.**Clarification of help text on when to use 5G logo.Removal of defunct keywords frame on page 2.Add Rel-16, Rel-17 options, eliminated earlier, frozen, Releases (cover page, below title)Corrections to some guidance text, addition of guidance text concerning automatic page headers under Word 2016 ff.Use of modal auxiliary verbs added to Foreword.More explicit guidance on Bibliography and Index annexes.Converted to .docx format.* | *1.13.0* |
| *2019-09-12* | *Cover page table outline shown dotted for ease of logo selection. (Author to hide outline after logo selection.) User now needs to delete whole table rows instead of individual cells, which proved to be tricky.**Change of style for "notes" in the Foreword to normal paragraphs.**Insertion of new bookmarks, correction of location of existing bookmarks. (To improve navigation.)**Improvements to guidance text.* | *1.13.1* |
| *2021-06-18* | *Provision for 5G Advanced logo Update copyright year to 2021Additional guidance on the use of Heading 8/9 in annexes C, D and X.* | *1.14.0* |