|  |
| --- |
| 3GPP TR 33.839 V0.1.0 (2020-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Security Aspects of Enhancement of Support for Edge Computing in 5GC(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.© 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 5

Introduction 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 8

3.3 Abbreviations 8

4 Overview of Edge Computing (EC) 8

5 Key issues 8

5.1 Key issue #1:Authentication and Authorization between EEC and EES 8

5.1.1 Key Issue Details 8

5.1.2 Security Threats 9

5.1.3 Potential Security Requirements 9

5.2. Key issue #2: Authentication and Authorization between EEC and ECS 9

5.2.1 Key Issue Details 9

5.2.2 Security Threats 9

5.2.3 Potential Security Requirements 10

5.3 Key issue #3: Authentication and Authorization between EES and ECS 10

5.3.1 Key Issue Details 10

5.3.2 Security Threats 10

5.3.3 Potential Security Requirements 10

5.6 Key issue #6: Transport security for the EDGE-1-9 interfaces 12

5.6.1 Key issue details 12

5.6.2 Threats 12

5.6.3 Potential security requirements 12

5.7 Key Issue #7: Security of Network Information Provisioning to Local Applications with low latency procedure 13

5.7.1 Key issue details 13

5.7.2 Security threats 14

5.7.3 Potential Security requirements 14

5.8 Key Issue #8: authentication and authorization in EES capability exposure 14

5.8.1 Key issue details 14

5.8.2 Security threats 14

5.8.3 Potential security requirements 14

5.9 Key Issue #9: Security of EAS discovery procedure 15

5.9.1 Key issue details 15

5.9.2 Security threats 15

5.9.3 Potential Security requirements 15

5.10 Key Issue #10: User's consent for exposure of information to Edge Applications 15

5.10.1 Key issue details 15

5.10.2 Security threats 16

5.10.3 Potential security requirements 16

5.X Key issue #X: <Key issue name> 16

5. X.1 Key issue details 16

5. X.2 Security threats 16

5. X.3 Potential security requirements 16

6 Proposed solutions 16

6.0 Mapping of Solutions to Key Issues 16

6.1 Solution #1: DNS request protection 17

6.1.1 Introduction 17

6.1.2 Solution details 17

6.1.3 Solution Evaluation 17

6.2 Solution #2: Authentication between EEC and ECS based on primary authentication 17

6.2.1 Introduction 17

6.2.2 Solution details 17

6.2.2.1 Procedure 17

6.2.2.2 Derivation of Kedge and Kedge ID 19

6.2.2.3 Generation of MACEEC 19

6.2.3 Solution Evaluation 19

6.3 Solution #3: Authentication/Authorization framework for Edge Enabler Client and Servers 19

6.3.1 Introduction 19

6.3.2 Solution details 19

6.X Solution #X: <Solution name> 21

6.X.1 Solution overview 21

6.X.2 Solution details 21

6.X.3 Solution evaluation 21

7 Conclusions 21

Annex <A>: <Informative annex title for a Technical Report> 21

Annex <X> (informative): Change history 22

# 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

# 1 Scope

The present document studies the security enhancements on the support for Edge Computing in the 5G Core network define in TR 23.748 [x], and application architecture for enabling Edge Applications defined in TR 23.758 [y] and TS 23.558 [z].

Potential security requirements are provided and possible security enhancements to 5GS and edge application architecture are proposed that 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 23.558: "Architecture for enabling Edge Applications."

[3] 3GPP TR 23.748: "Study on enhancement of support for Edge Computing in the 5G Core network (5GC)".

[4] 3GPP TR 23.758: "Study on application architecture for enabling Edge Applications".

[5] 3GPP TS 23.502: "Procedure for the 5G System; Stage 2".

[6] 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].

AC Application Client

ECS Edge Configuration Server

EEC Edge Enabler Client

EES Edge Enabler Server

FQDN Fully Qualified Domain Name

LADN Local Area Data Network

<ABBREVIATION> <Expansion>

Editor’s Note: Example needs to be deleted

# 4 Overview of Edge Computing (EC)

Editor’s Note: This clause will contain a brief overview on edge computing

# 5 Key issues

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

## 5.1 Key issue #1:Authentication and Authorization between EEC and EES

### 5.1.1 Key Issue Details

As per [2], EDGE-1 reference point enables interactions between the Edge Enabler Server and the Edge Enabler Client. EDGE-1 reference point supports registration and de-registration of the Edge Enabler Client to the Edge Enabler Server, retrieval and provisioning of Edge Application Server configuration information; and discovery of Edge Application Servers available in the Edge Data Network.

Edge Enabler server provides functionalities to Edge Enabler client over EDGE-1 reference point such as provisioning of configuration information to Edge enabler client and support the functionalities of application context transfer.

Edge Enabler Client performs the functionalities like configuration information retrieval from the edge enabler server and discovering of the edge application servers available in Edge Data Network. The Edge Data Network is a local Data Network. Edge Application Server(s) and the Edge Enabler Server are contained within the EDN.

The UE is initially provisioned with the configurations required to connect to the Edge Data Network. Upon initial provisioning, the Edge Enabler Client of the UE registers with the selected Edge Enabler Server(s) from the list of provisioned Edge Enabler Server(s). Edge Enabler Client consumes service offered by the Edge Enabler Server, e.g. discovering Edge Application Servers in an area of interest. The procedure enables initialization or update of the Edge Enabler Client context information at the Edge Enabler Server. The Edge Enabler Client sends Edge Enabler Client registration request to the Edge Enabler Server. Edge Application Server discovery enables Edge Enabler Clients to obtain information about available Edge Application Servers of interest. The identification of the Edge Application Servers is based on matching query filters or Application Client Profiles provided in the request.

### 5.1.2 Security Threats

When Registration, Discovery , Deregistration is used without authorization, malicious Edge enabler client receive a list of Services and topology structure withing Edge Data Network from Edge Enabler Server discovery response message. Received information can reveal Edge Data Network’s topology (e.g. URI, IP address, number of Edge Application Servers, Application Server Functionalities, API type, protocols). Malicious Edge Enabler Client may use this information to launch attacks on Edge Data Network or use this information for competitive reasons.

### 5.1.3 Potential Security Requirements

Edge Enabler Server shall be able to provide mutual authentication with Edge Enabler Client over EDGE-1 Interface.

Edge Enabler Server shall be able to determine whether Edge Enabling client is authorized to access Edge Enabling Server’s services.

## 5.2. Key issue #2: Authentication and Authorization between EEC and ECS

### 5.2.1 Key Issue Details

As per [2], the EDGE-4 reference point enables interactions between the Edge Configuration Server (ECS) and the Edge Enabler Client. Edge Configuration Server (ECS) (Edge Configuration Server (ECS)) provides supporting functions needed for the Edge Enabler Client to connect with an Edge Enabler Server(EES). EDGE-4 reference point supports provisioning of Edge configuration information (e.g., URI or LADN service information) to the Edge Enabler Client.

Edge Enabler Client performs the functionalities like configuration information retrieval from the edge configuration sever over the EDGE-4 interface.

As per 23.558[2], The Edge Configuration Server(ECS) can be deployed in the MNO domain or can be deployed in 3rd party domain by the service provider in which one Edge Enabling Client may communicate with one or more Edge Configuration Server(ECS)(s) concurrently. If the Edge Configuration Server (ECS) is deployed by MNO, the Edge Configuration Server (ECS) provides one or more Edge Enabling Server configuration information. If the Edge Configuration Server (ECS) is deployed by a non-MNO Edge computing service provider, the Edge Configuration Server(ECS) endpoint address is pre-configured with the Edge Enabling Client. The Edge enabling client that is configured with multiple Edge Configuration Server (ECS) endpoint addresses (es), may perform the service provisioning procedure per the Edge Configuration Server(ECS) of each Edge Configuration Server(ECS) multiple times. UE can contain a single Application Client (AC) or multiple Application Client(AC)s, which are served by a single Edge Configuration Server(ECS). In another scenario, UE has multiple Application Client(AC)s where each Application Client(AC) can be served by an Edge Application Server, which in turn served by a different Edge Configuration Server(ECS)'s Edge Enabling Server.

### 5.2.2 Security Threats

If access to Provisioning and configuration information is retrieved without authentication and authorization, malicious Edge enabler client will be able to receive a list of Edge Enabling Server configuration information and topology structure within Edge Data Network from the provisioning response message. The received information can reveal Edge Data Network's topology (e.g., URI, FQDN, IP address, LADN service information, Application Server Functionalities, API type, protocols).

Malicious Edge Enabler Client may use this information to launch attacks on Edge Data Network or use this information for competitive reasons.

### 5.2.3 Potential Security Requirements

Edge Configuration Server(ECS) Requirements:

Edge Configuration Server(ECS) shall be able to provide mutual authentication with Edge Enabler Client over EDGE-4 Interface.

Edge Configuration Server(ECS) shall be able to determine whether Edge Enabling the client is authorized to access provisioning services offered by Edge Configuration Server(ECS).

## 5.3 Key issue #3: Authentication and Authorization between EES and ECS

### 5.3.1 Key Issue Details

As per 23.558[2], the EDGE-6 reference point enables interactions between the Edge Configuration Server (ECS) and the Edge Enabler Server. EDGE-6 supported the registration and registration updates, deregistration, of Edge Enabler Server information to the Edge Enabler Network Configuration Server. The Edge Enabler Server Registration procedure allows an Edge Enabler Server to provide information to an Edge Configuration Server to request the use of its edge configuration capabilities. The Edge Enabler Server registration update procedure allows an Edge Enabler Server to update the Edge Configuration Server if there is a change in the information at the Edge Enabler Server. The Edge Enabler Server uses the Edge Enabler Server deregistration procedure to remove its information from the Edge Configuration Server. As per 23.558[XX], The Edge Configuration Server(ECS) can be deployed in the MNO domain or can be deployed in 3rd party domain by the service provider in which one Edge Enabling Client may communicate with one or more Edge Configuration Server(ECS)(s) concurrently. One Edge Enabling Server may concurrently connect to one or more Edge Configuration Server with a separate EDGE-6 reference point interface. The Edge enabling server that is configured with multiple Edge Configuration Server (ECS) endpoint addresses (es) may perform the service registration, updates, or deregistration procedures per the Edge Configuration Server(ECS) of each Edge Configuration Server(ECS) multiple times. In this context, the Security Context of each of EDGE-6 interfaces needs to be separate from each other as the trust domain may be different.

### 5.3.2 Security Threats

Without Authentication or authorization, the Malicious Edge Enabling server may be able to register with the Edge configuration server, further exposing its services to UE's Edge, enabling clients and applications running on UE.

Registration updates without any confidentiality or integrity may be able to help a Man In the middle actor impersonating the Edge configuration server to Edge Enabling server exposing and possibly altering the registration updates with falsified Edge Enabling Server profile to Edge configuration server. Also, this attack leads to exposing the topology details, server information within the PLMN domain. Malicious actors can use this exposed information for the benefit of PLMN's or Edge Computing Service provider's competitors.

### 5.3.3 Potential Security Requirements

The Edge Configuration Server and the Edge Enabling Server shall perform mutual authentication, to register and update the server profile information.

The Edge Configuration Server shall be able to authorize the Edge Enabling Server to register and update the server profile information.

5.4 Key Issue #4 Edge Data Network Authentication and Authorization

5.4.1 Key issue detail

The concept of edge computing is analogous to that of (external) data network in the sense in that the UE’s edge client and the edge application server needs to be authenticated and authorized before UE can access the edge data network. In the case of edge data network, the data network itself is much closer to the UE than a traditional data network. UE authentication and authorization are normal part of UE network access. For UEs accessing edge data network, the authentication to the edge data network is in addition to the primary authentication for 3GPP network access. However, depending on the relationship between the edge data network operator and the 3GPP PLMN, the authentication to the edge data network may be implicit.

5.4.2 Security threats

Authentication and authorization are fundamental necessity in establishing security and providing access to the UEs by the network. Without it, there is no security and unauthenticated and unauthorized UEs may be able to enjoy the services provided by an edge data network that the UEs have not subscribed to.

5.4.3 Potential security requirements

UEs and Edge Data Network shall be mutually authenticated. When the Edge Data Network is outside of the 3GPP domain, non-3GPP credentials may be used.

UE’s access to Edge Data Network shall be authorized.

Existing security mechanisms shall be re-used as much as possible (e.g. secondary authentication or slice-specific authentication).

5.5 Key Issue #5 Edge Data Network User Identifier and Credential Protection

5.5.1 Key issue detail

For each UE, there may be multiple sets of user identifiers and credentials that are used between UE and different edge data networks that are different from the longterm identifiers and credentials (i.e. 5G AKA credentials) used for primary authentication. These user identifiers and credentials used in edge data network authentication are stored in the UE and in the edge data networks. The identifiers and credentials need to be identified and protected in the UE, in the network, and in transition, even in case where the edge data network is operated by a third party.

5.5.2 Security threats

If user identifiers and credentials are not protected, a number of well documented attacks can result in the loss of privacy, user data, and other sensitive information for the users.

5.5.3 Potential security requirements

Edge data network application user identifiers and credentials shall be protected in storage and in transit.

NOTE: How edge data network application user identifiers and credentials are provisioned in the UE is out of the scope of the current study.

## 5.6 Key issue #6: Transport security for the EDGE-1-9 interfaces

### 5.6.1 Key issue details

TS 23.558 [2], clause 6.2 describes a new architecture for enabling edge applications, i.e.



New interfaces (i.e. EDGE-1-9) were introduced in the architecture for enabling Edge Applications. This key issues studies the related transport security, i.e. confidentiality, integrity and replay-protection.

* Type A (Between UE and Edge servers):
	+ EDGE-1: between EEC and EES
	+ EDGE-4: between EEC and EAS
	+ EDGE-5: between EEC and Application Client(s)

NOTE: Details of the EDGE-5 is out of scope of this release of this specification, according to TS 23.558[xx]

* Type B (Between 3GPP core and Edge servers):
	+ EDGE-2: between 3GPP Core network and EES
	+ EDGE-7: between 3GPP Core network and ECS
	+ EDGE-8: between 3GPP Core network and EAS
* Type C (Between Edge servers):
	+ EDGE-3: between EAS and EES
	+ EDGE-6: between EES and ECS
	+ EDGE-9: between EES(s)

### 5.6.2 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.

### 5.6.3 Potential security requirements

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

## 5.7 Key Issue #7: Security of Network Information Provisioning to Local Applications with low latency procedure

### 5.7.1 Key issue details

In the solutions for network information provisioning to local application procedure in TR 23.748 [3], the following two ways are proposed to perform network information exposure to local application.

1. UPF exposes the network information (i.e. QoS monitoring) to local AF via Local NEF.

For this case, the following two alternatives proposed:

1. The EAS/AF subscribes the network information notification according to the blue dashed line path, and the local PSA provisions the networking information to EAS/AF via local NEF (i.e. according to the blue solid line path).
2. The EAS/AF subscribes the network information notification according to the red dashed line path, in this case, the local NEF retrieves the UPF information before subscribing the event from UPF for AF which is not showed in the figure. When the request event happens, the local PSA provisions the networking information also to EAS/AF via local NEF (i.e. according to the blue solid line path).
3. UPF exposes the network information to local AF directly.



For this case, the following two alternatives proposed:

1. The EAS/AF subscribes the network information notification according to the blue dashed line path, and the local PSA provisions the networking information to EAS/AF directly (i.e. according to the blue solid line path).
2. The EAS/AF subscribes the network information notification with UPF directly (i.e. according to the red dashed line path).

New interface between UPF and local NEF/local AF/EAS was introduced, we need to study the security issue on the new interface.

### 5.7.2 Security threats

Without authentication and protection, an attacker may eavesdrop or manipulate or replay the communication on the new interface.

### 5.7.3 Potential Security requirements

For the case that UPF exposes the network information to local AF via Local NEF.

* Mutual authentication mechanism between UPF and local NEF shall be supported.
* Confidentiality protection, integrity protection and replay-protection shall be supported on the new interface between UPF and local NEF.

For the case that UPF exposes the network information to local AF directly:

* The UPF enable secure provision of information in the 3GPP network by authenticated and authorized Application Functions.

Confidentiality protection, integrity protection and replay-protection shall be supported on the new interface between UPF and Application Functions.

## 5.8 Key Issue #8: authentication and authorization in EES capability exposure

### 5.8.1 Key issue details

TS 23.558, clause 8.6 [2] describes service capability APIs exposed by the Edge Enabler Server to the Edge Application Server(s). The service capability APIs exposed include EES capabilities and re-exposed 3GPP Core Network capabilities. To support EES capability exposure, the following open issues need to be studied：

- Whether and how to support the Edge Application Server to access the EES capability exposure function directly, e.g., how CAPIF as specified in 3GPP TS 23.222 [xx] can be utilized, and whether there is a need to enhance functionalities of CAPIF?

- How the Edge Enabling Server re-exposes service API(s) to the Edge Application Server, where the service API(s) are relying on the SCEF/NEF northbound API(s)?

### 5.8.2 Security threats

If the access to EES capability APIs is not authenticated and authorized, attackers would potentially be able to perform the following types of attacks:

- Requesting service from the EES that unauthorized parties are not allowed to consume, e.g. in order to gain user’s privacy information

- Flooding the EES with resource-demanding operations that may lead to a Denial of Service situation

### 5.8.3 Potential security requirements

EES capability exposure to EAS shall be authenticated and authorized.

## 5.9 Key Issue #9: Security of EAS discovery procedure

### 5.9.1 Key issue details

In the solutions for EAS discovery procedure in TR 23.748 [2], the following DNS based solution is proposed. The solution requires a new Functionality, an enhanced DNS Forwarder here referred to as "LDNSR". LDNSR supports Edge AS Discovery using DNS using knowledge of the 5GC connectivity of the UE.



Figure 5.9.1-1 Options for the EAS discovery using LDNSR for PDU session breakout

New function LDNSR is introduced for EAS discovery, and the interaction between SMF and LDNSR is also introduced. The SMF may provide knowledge of the 5GC connectivity of the UE to LDNSR, the information about the knowledge of the 5GC connectivity of the UE is sensitive material which should be security protected.

In above solution, DNS request is send for query the Edge Server's address. If the DNS destination address is modified by the attacker, DNS request will be send to compromised DNS server, then wrong Edge Server address may be allocated. This attack may make UE connected to a far Edge Server and ruin the advantage of the MEC, even worse, the compromised DNS server may lead UE to connect to a compromised Edge Server.

### 5.9.2 Security threats

Without protection, an attacker may eavesdrop or manipulate or replay the communication on the new interface.

Without protection about the DNS message, an attacker may manipulate the DNS message which may cause the UE is not able to find a suitable EAS.

### 5.9.3 Potential Security requirements

The interaction message between the SMF and LDNSR shall be confidentiality, integrity, and replay protected. Secure discovery of EDGE Services should be supported.

## 5.10 Key Issue #10: User's consent for exposure of information to Edge Applications

### 5.10.1 Key issue details

EES exposes UE Identifier API to the EAS in order to provide an identifier uniquely identifying a UE. Further, the Edge Enabler Server exposes the UE location API to the Edge Application Server in order to support tracking or checking the valid location of the UE. In order to expose such user related private information to the Edge Application servers, consent from the user is needed.

EES capability exposure to EAS as defined in TS 23.558 [xx], mandates the end user's consent for reporting UE's information, particularly for UE Identifier API and UE location API. Following editor’s note is captured in the TS 23.558 [2] for obtaining the user's consent: *“Editor's note: Whether and how user's consent is obtained to share the UE identifier with a particular EAS is SA3's responsibility.”*

### 5.10.2 Security threats

Use of user’s information to identify and track the user or user’s behavior without the permission or knowledge of the user, poses huge threat to user’s privacy.

### 5.10.3 Potential security requirements

Editor’s Note: the security requirements are TBA.

Editor’s Note: When defining any procedures obtaining user's consent, it is needed to clarify “when” user’s consent is obtained, on “what” information it is obtained and provide details on “why” user’s consent is obtained (e.g. for what purposes the user consented information will be used).

Editor’s Note: If SA3 agrees for a study item to study on a common architecture to obtain user's contest, then this Key Issue will be moved under that study item.

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

### 5. X.1 Key issue details

### 5. X.2 Security 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 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Solution #1: DNS request protection |  |  |  |  |  |  |  |  | x |  |
| Solution #2: Authentication between EEC and ECS based on primary authentication |  | x |  |  |  |  |  |  |  |  |
| Solution #3: Authentication/Authorization framework for Edge Enabler Client and Servers | x | x |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| #X: <Solution name> | X |  |  |  |  |  |  |  |  |  |

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

## 6.1 Solution #1: DNS request protection

### 6.1.1 Introduction

A new key issue is proposed to protect the DNS request modification attack. In edge computing environment, DNS request is needed to query the Edge Server's address. If the DNS destination address is modified by the attacker, then wrong Edge Server address may be allocated. This attack may make UE connected to a far Edge server and ruin the advantage of the MEC, even worse, the false DNS server may lead UE to connect to a compromised Edge Server.

TS 33.501 has an informative annex P.2 on the security aspects on DNS for 5G, and it is proposed to reuse the enhanced DNS on MEC system.

### 6.1.2 Solution details

DNS server shall support DNS over (D)TLS, as specified in RFC 7858 and RFC 8310. The DNS server(s) that are deployed within the 3GPP network can enforce the use of DNS over (D)TLS. The UE can be pre-configured with the DNS server security information (out-of-band configurations specified in the IETF RFCs like, credentials to authenticate the DNS server, supported security mechanisms, port number, etc.), or the core network can configure the DNS server security information to the UE. When DNS over (D)TLS is used, a TLS cipher suite that supports integrity protection needs to be negotiated.

### 6.1.3 Solution Evaluation

TBD.

## 6.2 Solution #2: Authentication between EEC and ECS based on primary authentication

### 6.2.1 Introduction

A new key issue is proposed that Edge Computing system needs to support the 3GPP credential based authentication. This solution proposes the authentication between EEC (Edge Enabler Client) and ECS (Edge Configuration Server). To be more specific, it is proposed to use the Kausf derived from the primary authentication as the trust root to perform the authentication between EEC and ECS.

It is assumed in this solution that ECS is located outside of the MNO’s network.

### 6.2.2 Solution details

#### 6.2.2.1 Procedure



Figure-6.2.2.1-1. Authentication between the EEC and ECS based on primary authentication

The authentication procedure details are as following:

Step 0: UE performs primary authentication with the network. Then KAUSF is shared between UE and AUSF in Home network. UE performs PDU session establishment procedure as defined in TS 23.502.

Step 1: UE generates a credential Kedge and Kedge ID using KAUSF and SUPI, and stored securely. The method to derive generate Kedge and Kedge ID is in 6.2.2.2.

Step 2: AUSF generates a credential Kedge and Kedge ID using KAUSF and SUPI, and stored securely.

Step 3: UE computes MACEEC using the Kedge and EEC ID (defined in TS 23.558). The method to generate MACEEC is in 6.2.2.3.

Step 4: UE sends Application Registration request (EEC ID, MACEEC, Kedge ID) to ECS. Whether this message is send using NAS or user plane is based on SA2’s decision.

Step 5: ECS sends Authentication verification (EEC ID, MACEEC, Kedge ID) to NEF for verification.

Step 6: NEF sends Authentication verification (EEC ID, MACEEC, Kedge ID) to AUSF for MACEEC verification.

Step 7: AUSF retrieves Kedge using KedgeID, and verify MACEEC using the (Kedge and EEC ID).

Step 8: If verification in AUSF succeed, then AUSF sends Authentication verification response(success) back to NEF, otherwise, AUSF sends Authentication verification response(fail) to NEF.

Step 9: NEF sends Authentication verification response(success/fail) from AUSF to ECS.

Step 10: Based on the verification results, ECS decides whether to accept or reject the authentication request, and sends Authentication Request accept/rejection to EEC in the UE.

Editor’s Note: it is FFS what is the impact on the existing key hierarchy.

Editor’s Note: How the AUSF can be aware of each specific Kedge per UE is FFS

#### 6.2.2.2 Derivation of Kedge and Kedge ID

Kedge is generated using KDF defined in Annex B.2.0 of TS 33.220. When deriving a Kedge from KAUSF, the following parameters shall be used to form the input S to the KDF:

- FC = xxxx(to be allocated by 3GPP)

- P0 = <SUPI>,

- L0 = length of <SUPI>.

The input key KEY shall be KAUSF.

Kedge ID is generated by AUSF, and uniquely identify only one Kedge.

#### 6.2.2.3 Generation of MACEEC

When deriving MACEEC in the UE and AUSF, the following parameters shall be used to form the input S to the SHA-256 hashing algorithm:

- P0 = Kedge,

- P1 = EEC ID,

The input S shall be equal to the concatenation P0||P1 of the P0 and P1.

The MACEEC is identified with the 32 least significant bits of the output of the SHA-256 function.

Editor’s Note: This derivation is dependent on SA6’s decision on making EEC ID mandatory or not

### 6.2.3 Solution Evaluation

TBD.

## 6.3 Solution #3: Authentication/Authorization framework for Edge Enabler Client and Servers

### 6.3.1 Introduction

This solution addresses the security requirement for the Authentication and Authorization of EEC in key issue #1 and key issue #2.

The Edge Configuration Server (ECS) act as the token server for issuance and validation of access tokens to the UE and also to the EES/EAS. Access tokens are issued to EEC for the Edge Computing service, after verification of the UE authenticity using AKMA service. AKMA service is used as to use the network access credentials for the UE’s authentication. Access token is used for authorization of the UE to access/obtain the Edge Computing service.

### 6.3.2 Solution details



Figure 6.3.2-1: Authentication/Authorization framework for Edge Enabler Client and Servers

Step 1: The UE performs the procedures as defined in TS 23.502 [5] to get the 5GC network access.

Step 1A: At the end of the network access authentication procedure (Primary authentication and key agreement [TS 33.501, clause 6.1]), the UE and the AUSF are in possession of the key KAUSF.

Step 2A: The UE derives the AKMA key as specified in TS 33.535 [6] and the further keys for Edge Computing service.

 KECS = KDF{KAKMA, ECS IP Address, AKMA Key ID}

Editor’s Note: Derivation of KECS needs to be revisited to be in-line with AKMA KAF derivation.

Step 2B: Optionally the EEC establish a TLS session with the ECS, to secure the communication.

Step 2C-2J: Then the UE initiates the service provisioning procedure with the ECS (as specified in clause 8.3 in TS 23.558 [2]). ECS is Application Function (AF) for the AAnF [TS 33.535]. The UE includes the AKMA Key ID and also generates MAC-I over the request message using the key KECS to prove its authenticity. The ECS contacts the AAnF (using AKMA key ID) to obtain the corresponding key KECS (KAF) of the UE. The key KECS is used by the ECS to verify the MAC-I and then provide the response. If the UE is authorised to access the EES, then the ECS generates and provide the access token to the UE in a secure way (the access token is encrypted using the KECS).

Editor’s Note: Calculation of MAC-I needs to be detailed.

 Editor’s Note: Details of the access token generation to be detailed.

Step 3: The UE performs EEC registration (as specified in clause 8.4.2 in TS 23.558 [2]) and discovery (as specified in clause 8.5 in TS 23.558 [2]) with the EES.

Step 3A: Before sending the access token to the EES, the UE and the EES establish a secure TLS connection using EES server certificate. It is required to protect and to provide the access token to an authentic EES.

Step 3C-3E: The UE initiates EEC registration procedure with the EES, including the access token obtained from the ECS in Step 2J. The authorization check for the EEC registration request is performed by verification of the access token issued by the ECS to the UE. The EES obtains the access token validation service from the ECS.

Step 3F-3I: When the UE initiates EAS discovery procedure with the EES by including the same access token obtained from the ECS in Step 2J, if it is valid. Again the EES obtains the access token validation service from the ECS. The EES also request and obtains the access token(s) from the ECS for the UE to grant access to the EAS(s). Then in response to the request, the EES includes the EAS access grant token(s), with relevant information like validity time, to the UE.

In case, if the obtained access token from the ECS (in Step 2J) is not valid (due to time limitation), then the EEC requests ECS for a new access token. The access token request message include the necessary parameters to identify the EEC security context and parameters for authenticity verification. After verification of the authenticity, the ECS provides a new access token to the EEC, in response to the request.

Step 4A-4F: The UE obtains service from EAS, by producing the access token obtained from the EES, over the secure TLS connection. The UE also obtains security policy and the relevant access token from the EES in Step 3I. Before sending the access token to the EAS, the UE and the EAS establish a secure channel using EAS server certificate. It is required to protect and to provide the access token to an authentic EAS. The EAS obtains the access token validation service from the ECS via EES. After successful validation of the access token, the UE obtains the Edge Computing service from the EAS.

Editor’s Note: Details and the need for the security policy (mentioned in step 4A-4F) needs to be clarified.

Editor’s Note: Whether the authorization between EAC and EAS (step 4C) is in the scope of SA3 is FFS.

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

### 6.X.1 Solution overview

### 6.X.2 Solution details

### 6.X.3 Solution evaluation

# 7 Conclusions

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

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

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-08 | SA3#100-e | S3-202073 |  |  |  | TR Skeleton | 0.0.0 |
| 2020-08 | Sa3#100-e | S3-202085 |  |  |  | Implemented S3-201903, S3-201832, S3-201750, S3-201669, S3-1668, S3-201833, S3-202074, S3-202117, S3-202116, S3-202115, S3-201907r2, S3-201971r4, S3-201749r2, and S3-201970r2. | 0.1.0 |

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* |