|  |  |
| --- | --- |
| 3GPP TR 33.839 V0.2.0 (2020-10) | |
| 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 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 6

Introduction 7

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 9

3.1 Terms 9

3.2 Symbols 9

3.3 Abbreviations 9

4 Overview of Edge Computing (EC) 9

5 Key issues 9

5.1 Key issue #1: Authentication and Authorization between EEC and EES 10

5.1.1 Key Issue Details 10

5.1.2 Security Threats 10

5.1.3 Potential Security Requirements 10

5.2. Key issue #2: Authentication and Authorization between EEC and ECS 10

5.2.1 Key Issue Details 10

5.2.2 Security Threats 11

5.2.3 Potential Security Requirements 11

5.3 Key issue #3: Authentication and Authorization between EES and ECS 11

5.3.1 Key Issue Details 11

5.3.2 Security Threats 11

5.3.3 Potential Security Requirements 12

5.6 Key issue #6: Transport security for the EDGE-1-9 interfaces 13

5.6.1 Key issue details 13

5.6.2 Threats 14

5.6.3 Potential security requirements 14

5.7 Key Issue #7: Security of Network Information Provisioning to Local Applications with low latency procedure 14

5.7.1 Key issue details 14

5.7.2 Security threats 15

5.7.3 Potential Security requirements 15

5.8 Key Issue #8: authentication and authorization in EES capability exposure 15

5.8.1 Key issue details 15

5.8.2 Security threats 16

5.8.3 Potential security requirements 16

5.9 Key Issue #9: Security of EAS discovery procedure 16

5.9.1 Key issue details 16

5.9.2 Security threats 16

5.9.3 Potential Security requirements 17

5.10. Key issue #10: Authorization during Edge Data Network change 17

5.10.1 Key issue details 17

5.10.2 Security threats 17

5.10.3 Potential security requirements 17

5.X Key issue #X: <Key issue name> 17

5. X.1 Key issue details 17

5. X.2 Security threats 17

5. X.3 Potential security requirements 17

6 Proposed solutions 17

6.0 Mapping of Solutions to Key Issues 18

6.1 Solution #1: DNS request protection 18

6.1.1 Introduction 18

6.1.2 Solution details 18

6.1.3 Solution Evaluation 19

6.2 Solution #2: Authentication between EEC and ECS based on primary authentication 19

6.2.1 Introduction 19

6.2.2 Solution details 19

6.2.2.1 Procedure 19

6.2.2.2 Derivation of Kedge and Kedge ID 20

6.2.2.3 Generation of MACEEC 20

6.2.3 Solution Evaluation 20

6.3 Solution #3: Authentication/Authorization framework for Edge Enabler Client and Servers 21

6.3.1 Introduction 21

6.3.2 Solution details 21

6.4 Solution #4: Authentication/Authorization framework for Edge Enabler Client and Servers 23

6.4.1 Introduction 23

6.4.2 Solution details 23

6.5 Solution #5: Authentication and Authorization between the Edge Enabler Client and the Edge Enabler Server 25

6.5.1 Introduction 25

6.5.2 Solution details 25

6.5.3 Solution Evaluation 26

6.6 Solution #6: Authentication and Authorization between the Edge Enabler Client and the Edge Enabler Server 26

6.6.1 Introduction 26

6.6.2 Solution details 27

6.6.3 Solution Evaluation 27

6.7 Solution #7: Authentication and Authorization with the Edge Data Network 27

6.7.1 Solution overview 27

6.7.2 Solution details 28

6.7.3 Solution evaluation 30

6.8 Solution #8: Authentication between EEC and EES 30

6.8.1 Solution overview 30

6.8.2 Solution details 30

6.8.3 Solution evaluation 31

6.9 Solution #9: Authentication and authorization between EEC and ECS based on AKMA 31

6.9.1 Introduction 31

6.9.2 Solution details 32

6.9.3 Solution Evaluation 33

6.10 Solution #10: Authentication and Authorization between the Edge Enabler Client and the Edge Configuration Server 33

6.10.1 Introduction 33

6.10.2 Solution details 33

6.10.3 Evaluation 34

6.11 Solution #11: Authentication between EEC and ECS 34

6.11.1 Solution overview 34

6.11.2 Solution details 34

6.11.3 Solution evaluation 35

6.12 Solution #12: Onboarding and authentication/authorization framework for Edge Enabler Server and Edge Configuration Server 35

6.12.1 Introduction 35

6.12.2 Solution details 35

6.12.3 Solution evaluation 37

6.13 Solution #13: Transport security for EDGE-1-9 interfaces 37

6.13.1 Introduction 37

6.13.2 Solution details 37

6.13.2.1 Type A 37

6.13.2.2 Type B 37

6.13.2.3 Type C 38

6.13.3 Evaluation 38

6.14 Solution #14: Protection of Network Information Provisioning to Local AF directly 38

6.14.1 Solution overview 38

6.14.2 Solution details 39

6.14.3 Solution evaluation 39

6.15 Solution #15: Service capability re-exposure 39

6.15.1 Introduction 39

6.15.2 Solution details 40

6.15.3 Solution Evaluation 40

6.X Solution #X: <Solution name> 41

6.X.1 Solution overview 41

6.X.2 Solution details 41

6.X.3 Solution evaluation 41

7 Conclusions 41

Annex <A>: <Informative annex title for a Technical Report> 41

Annex <X> (informative): Change history 42

# 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.

NOTE: The user consent for exposure of information to Edge Applications is not addressed in the present document, it will be discussed in TR 33.867 [yy].

# 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 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)".

[7] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[8] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[9] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

[10] 3GPP TS 33.501: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[11] 3GPP TS 33.187: "Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements".

[12] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[13] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

# 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

EAS Edge Application Server

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 within 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[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. 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 ECS
  + 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 EAS
  + EDGE-8: between 3GPP Core network and ECS
* 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.

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

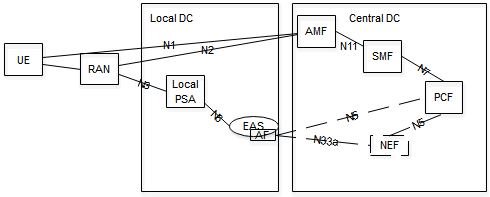


For this case, the following two alternatives proposed:

- 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).

- 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).

- UPF exposes the network information to local AF directly.



For this case, the following two alternatives proposed:

- 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).

- 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 [9] 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 [3], 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: Authorization during Edge Data Network change

### 5.10.1 Key issue details

TR 23.748 [3] clause 5.2 describes a key issue #2 "Edge relocation", which raises an issue on "How to handle change of the serving EAS (without UE mobility) to support seamless change, e.g. preventing or reducing packet loss". Currently, several solutions (such as solution #22-40) in TR 23.748 [3] were proposed to address this key issue.

Here, Edge Data network connectivity will be modified during the edge relocation, which is different from changing the PDU session anchor only. When a new PDU session is created, secondary authentication will be triggered (distributed anchor with SSC mode 1/2/3 and multiple PDU sessions). This will not happen when additional PSA-UPFs are added to an existing PDU session. Authorization needs to be investigated in relation to session breakout and ULCL as well as IPv6MH.

Specifically, it needs to be studied how the authorization provided by the secondary authentication is addressed during Edge Data network change with requirements on service continuity as studied in Key issue #2 of TR 23.748 [3].

This key issue is to study the authorization requirement between the UE and the target Edge Data network during the Edge Data network change.

### 5.10.2 Security threats

Without the authorization, an unauthorized UE may be able to consume the services provided by the target Edge Data network.

#### 5.10.3 Potential security requirements

Authorization of UE for EAS service access during Edge Data network relocation with seamless change shall be supported.

## 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 |  |  |  |  |  |  |  |  |
| Solution #4: Authentication/Authorization framework for Edge Enabler Client and Servers | x | x |  | x |  | x |  |  |  |  |
| Solution #5: Authentication and Authorization between the Edge Enabler Client and the Edge Enabler Server | x |  |  |  |  |  |  |  |  |  |
| Solution #6: Authentication and Authorization between the Edge Enabler Client and the Edge Enabler Server | x |  |  |  |  |  |  |  |  |  |
| Solution #7: Authentication and Authorization with the Edge Data Network | x | x |  |  |  | x |  |  |  |  |
| Solution #8: Authentication between EEC and EES | x |  |  |  |  |  |  |  |  |  |
| Solution #9: Authentication and authorization between EEC and ECS based on AKMA |  | x |  |  |  |  |  |  |  |  |
| Solution #10: Authentication and Authorization between the Edge Enabler Client and the Edge Configuration Server |  | x |  |  |  |  |  |  |  |  |
| Solution #11: Authentication between EEC and ECS |  | x |  |  |  |  |  |  |  |  |
| Solution #12: Onboarding and authentication/authorization framework for Edge Enabler Server and Edge Configuration Server |  |  | x |  |  |  |  |  |  |  |
| Solution #13: Transport security for EDGE-1-9 interfaces |  |  |  |  |  | x |  |  |  |  |
| Solution #14: Protection of Network Information Provisioning to Local AF directly |  |  |  |  |  |  | x |  |  |  |
| Solution #15: Service capability re-exposure |  |  |  |  |  |  |  | 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 [7] 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 should 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

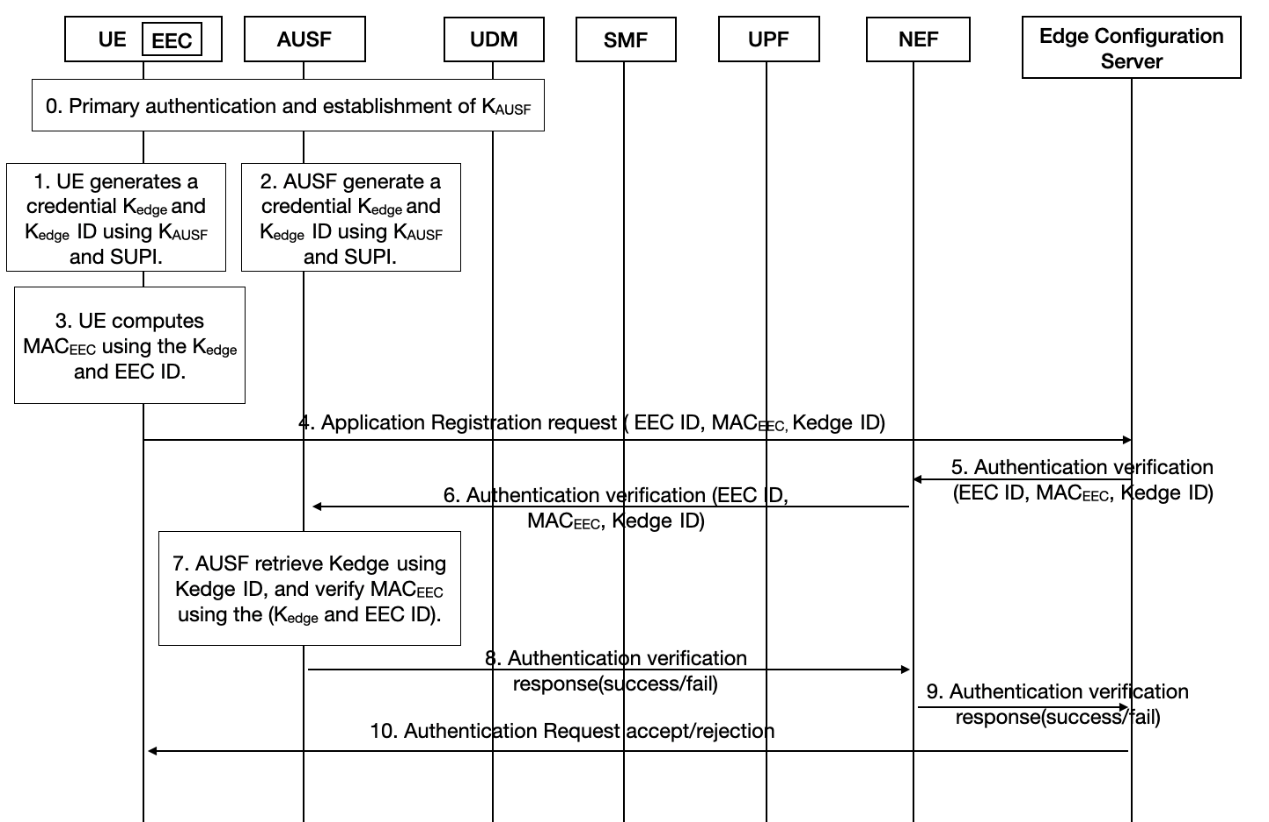


Figure-6.2.2.1-1. Authentication between the EEC and ECS based on primary authentication

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 [2]). 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 discovers the AUSF based on Kedge ID, and sends Authentication verification (EEC ID, MACEEC, Kedge ID) to AUSF for MACEEC verification.

Editor’s Note: How to discover the AUSF is FFS.

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 [8]. When deriving a Kedge from KAUSF, the following parameters should 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 should be KAUSF.

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

Editor’s note: How to generate the Kedge ID in AUSF and UE is FFS.

#### 6.2.2.3 Generation of MACEEC

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

- P0 = Kedge,

- P1 = EEC ID,

The input S should 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, Key issue #6(for EDGE-1, EDGE-4 interfaces).

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 is the AKMA Application Key (KAF) and derived as specified in TS 33.535 [6] . KECS is the AKMA Application Key (KAF) and derived as specified in TS 33.535 [6].

Step 2B: EEC establish a TLS session with the ECS, to secure the communication. TLS should be used to provide integrity protection, replay protection and confidentiality protection for EDGE-4 interface.

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, CounterEEC and MAC-IEEC derived over the request message using the key KECS to prove its authenticity. The MAC-IEEC is derived as specified in sub-clause 6.3.2.1 of this document. The ECS contacts the AAnF (using AKMA key ID) to obtain the corresponding key KECS (KAF) of the UE, if it does not holds a valid KECS of the UE. The key KECS is used by the ECS to verify the MAC-IEEC 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: It is ffs, instead of server certificate and MAC-I, whether TLS based on AKMA PSK can be used.

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. Edge Configuration Server may provide Edge Enabling Client's root CA certificate during the registration response (as specified in clause 8.4 in TS 23.558[2]) to the Edge Enabling Server to validate the Edge Enabling Client's certificate. TLS provides integrity protection, replay protection, and confidentiality protection over the EDGE-1 interface. 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 verifying 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.

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 as shown in figure 6.3.2-2. The access token request message includes 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.

6.3.2.1 MAC-IEEC derivation

MAC-IEEC generation is performed using the key derivation function (KDF) specified in Annex B.2.0 of TS 33.220 [8]. When deriving a MAC-IEEC from KECS, the following parameters, KECS, CounterEEC, Initial Provisioning request message are used to form the input S to the KDF.

The MAC-IEEC is identified with the 128 least significant bits of the output of the KDF.

To generate the MAC-IEEC, the EEC use a counter, called a CounterEEC. The EEC and the ECS associates a 16-bit counter, CounterEEC, with the key KECS. The EEC initializes the CounterEEC to 0x00 0x01 when the KECS is derived. The EEC and the ECS maintains the CounterEEC for lifetime of the KECS. The EEC sets the CounterEEC to 0x00 0x02 after the first calculated MAC-IEEC, and monotonically increment it for each additional calculated MAC-IEEC.

The CounterEEC is incremented by the EEC for every new computation of the MAC-IEEC. The CounterEEC is used as freshness input into MAC-IEEC derivations, to mitigate the replay attack. The EEC sends the value of the CounterEEC (used to generate the MAC-IEEC) along with the MAC-IEEC to the ECS. The ECS accepts CounterEEC value that is greater than stored CounterEEC value. The ECS stores the received CounterEEC, onlyif the verification of the received MAC-IEEC is successful.

The EEC suspends the Initial provisioning procedure, if the CounterEEC associated with the KECS is about to wrap around. When a fresh KECS is generated, the CounterEEC at the EEC is reset to 0x00 0x01 and the EEC resumes the Initial provisioning procedure.

## 6.4 Solution #4: Authentication/Authorization framework for Edge Enabler Client and Servers

### 6.4.1 Introduction

This solution addresses the security requirement for the Authentication and Authorization of EEC in key issue #1 and key issue #2, Key issue 4, Key issue #6(for EDGE-1, EDGE-4 interfaces).

Note: Secondary Authentication is performed in this solution.

### 6.4.2 Solution details



Figure 6.4.2-1: Secondary Authentication Based Authentication/Authorization framework for Edge Enabler Client and Servers

The procedure includes the following steps:

Step 0: UE pre-configuration: If the ECS deployed by MNO is contracted with one or more ECSP(s), the ECS provides EES configuration information of MNO owned, and ECSP owned EESs via MNO ECS as described in clause 8.3.3.2 in 23.558 [2]. If a non-MNO ECSP deploys the ECS, the ECS endpoint address may be configured with the EEC. An EEC that is aware of multiple ECSP's ECS endpoint addresses may perform the service provisioning procedure per ECS ECSP multiple times.

Editor’s Note: Deployment scenarios related to ECS are FFS.

Editor’s Note: Interface security for Edge-1 and Edge-4 are FFS

Step 1: Primary Authentication: In this step, UE performs primary authentication with the network.

Step 2a, 2b: PDU session: As a result of UE initiating the service provisioning procedure with the ECS (as specified in clause 8.3 in TS 23.558 [2]), UE establishes a PDU session. This PDU Session may be established either to a well-known or pre-configured S-NSSAI or DNN, or the 5GC derives the S-NSSAI by using the registration for UE to network in step 1. Based on this information, the AMF selects an SMF, which in turn selects a PSA that provides a data connection to the Edge Cloud Service Provider's (Edge Data Network's) AAA Server. SMF continues secondary authentication as per clause 11.1.2 in 33.501[7]. ECS may act as DN-AAA Server.

Step 3a, 3b: After successful UE-requested PDU Session Establishment authentication/authorization by an EDN-AAA server, the device discovers and connects, at the application level, to a ECS server address (that was preconfigured in the UE in step 0 or is derived from the application identifier and/or Service Provider Identifier provided by the user in step 1) for provisioning EEC with ECS. 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.

After successfully establishing the secure session over EDGE-4 as in step 2, the Edge Enabling Client should send an Initial Provisioning request with Access Token Request message to the Edge Configuration Server as per the OAuth 2.0 specification. The Edge Configuration Server should verify the Access Token Request message per OAuth 2.0 specification. If the Edge Configuration Server successfully verifies the Access Token Request message, the Edge Configuration Server should generate an access token specific to the Edge Enabling Client and return it in an Initial Provisioning Response (Access Token Response) message.

Step 4.a: On EDGE-1, the Edge Enabling Client authenticates to the Edge Enabling Server by establishing a TLS session with the Edge Enabling Server based on the Server (Edge Enabling Server) side certificate authentication or certificate-based mutual authentication) as indicated by Edge Configuration Server. Edge Configuration Server may provide Edge Enabling Client's root CA certificate during the registration response (as specified in clause 8.4 in TS 23.558[2]) to the Edge Enabling Server to validate the Edge Enabling Client's certificate. TLS provides integrity protection, replay protection, and confidentiality protection over the EDGE-1 interface. It is required to protect and to provide the access token to an authentic EES.

Step 4.b: The UE initiates the EEC registration procedure with the EES, including the access token obtained from the ECS in Step 3.b. The authorization check for the EEC registration request is performed by verifying the access token issued by the ECS to the UE. The EES obtains the access token validation service from the ECS.

Editor’s Note: It needs to be clarified if the access token validation service by the ECS could be replaced by an authorization service by the ECS that does not require a token to be issued by the ECS to the UE

Step 5: EEC requests a service (e.g., Discovery) with access token obtained in step 4. The Edge Enabling Server should validate the access token. The Edge Enabling Server verifies the integrity of the access token by verifying the Edge Configuration Server signature. If validation of the access token is successful, the Edge Enabling Server should verify the Edge Enabling Client's Service request against the authorization claims in the access token, ensuring that the Edge Enabling Client has access permission for the requested service.

e.g., When the UE initiates the EAS discovery procedure with the EES by including the same access token obtained from the ECS in Step 3.b if it is valid. Again, the EES obtains the access token validation service from the ECS. The EES also requests and obtains the access token(s) from the ECS for the UE to grant access to the EAS(s). In response to the request, the EES includes the EAS access grant token(s), with relevant information like validity time, to the UE.

If the obtained access token from the ECS (in Step 3.b) is not valid, then the EEC requests ECS for a new access token, as shown in figure 6.3.X-1. The access token request message includes the necessary parameters to identify the EEC security context and parameters for authenticity verification. After verifying the authenticity, the ECS provides a new access token to the EEC in response to the request.

Step 6: 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 5. Before sending the access token to the EAS, the UE and the EAS establish a secure channel using the 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.

6.4.3 Solution evaluation

## 6.5 Solution #5: Authentication and Authorization between the Edge Enabler Client and the Edge Enabler Server

### 6.5.1 Introduction

The following solution addresses the security requirement for the key issue #1 on Authentication and Authorization between the EEC and the EES.

In clause 8.3.2.3 of TS 23.558[2], before the service provisioning procedure, the Edge Enabler Client should been authorized to communicate with the Edge Configuration Server. From the security perspective, three security requirements are specified for the access of UE to Edge Data Network.

- It needs to ensure that only PLMN authorized UE can access to the Edge Data Network.

- It needs to ensure that only edge computing service authorized UE can access to the Edge Data Network.

- The URI or address information of Edge Enabler Server is the entry information for Edge Data Network when the ECS is within the MNO.

This solution proposes a mechanism to reuse the secondary authentication for the authorization of the PLMN PDU session establishment for the authentication between the EEC and the EES.

Based on the secondary authentication procedure, the client is authenticated by the EES.The SMF will allocate the Edge Applicaition Server information to the client. Then the client can use this URI information of the Edge Applicaition Server to consume the edge service.

### 6.5.2 Solution details



Figure 6.5.2-1 Authentication and Authorization between the EEC and the EES

The procedure assumes that the Edge Configuration Server is deployed by the MNO. In thi s case, the EES is the authentication server in the Edge Data Network.

1. The UE registers in the operator network and perform the primary authentication procedure. After primary authentication, the UE has the information of Edge Configuration Server.

2 When the UE triggers the edge service it sends the PDU session establishment request to the AMF to setup the PDU session for the services provided by Edge Data Network. The SMF should trigger EAP Authentication procedure and perform the role of the EAP Authenticator.

3-6. The following steps 3, 4, 5, 6 are the same as steps 5a-13 in clause 11.1.2 of TS 33.501[7]. The secondary authentication procedure is performed. The EES is the authentication server (AAA) of the Edge Data Network.

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

8. The SMF sends a Namf\_Communication\_N1N2MessageTransfer to the AMF with the received information.

9. The AMF forwards NAS SM PDU Session Establishment Response message along with EAP Success, an d the EAS information in the registration response.

Editor's note: It is FFS how to proceed the authentication and authorization if the secondary authentication is not performed.

Editor's note: Whether EAS info can be acquired during the secondary authentication needs to be justified.

### 6.5.3 Solution Evaluation

TBD

## 6.6 Solution #6: Authentication and Authorization between the Edge Enabler Client and the Edge Enabler Server

### 6.6.1 Introduction

The following solution addresses the security requirement for the key issue #1 on Authentication and Authorization between the EEC and the EES.

In clause 8.3.2.3 of TS 23.558[2], before the service provisioning procedure, the Edge Enabler Client should been authorized to communicate with the Edge Configuration Server. From the security perspective, three security requirements are specified for the access of UE to Edge Data Network.

- It needs to ensure that only PLMN authorized UE can access to the Edge Data Network.

- It needs to ensure that only edge computing service authorized UE can access to the Edge Data Network.

- The URI or address information of Edge Configuration Server is the entry information for Edge Data Network when the ECS is deployed by the ECSP.

When the Edge Configuration server is deployed by the ECSP, the ECS information is preconfigured in the UE. This solution proposes a mechanism how the Edge Enabler Client is authenticated and authorized by the Edge Enabler Server when the Edge Configuration server is deployed by the ECSP. The secondary authentication for the authorization of the PLMN PDU session establishment will be reused as service authentication. The SMF should perform the role of the EAP Authenticator and communicates with the ECS (AAA).

Based on the secondary authentication procedure, the client is authenticated. The SMF will allocate the Edge Enabler Server information to the EEC. Then the client can use this URI information of the Edge Enabler Server to communicate with the Edge Date Network. It takes advantage of the secondary authentication between EEC and ECS to realize the authentication between the EEC and the EES. The authorization between the EEC and the EES is performed via the ECS.

### 6.6.2 Solution details



Figure 6.6.2-1 Authentication and Authorization between the EEC and the EES

The procedure assumes that the Edge Data Network is deployed by the ECSP.

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

2. When the UE trigger the edge service it sends the PDU session establishment request to the AMF to setup the PDU session for the services provided by Edge Data Network.

3-6. The following steps 3, 4, 5, 6 are the same as steps 5a-13 in clause 11.1.2 of TS 33.501[7]. The secondary authentication procedure is performed. The ECS is the authentication server of the Edge Data Network.

7. After the successful completion of the authentication procedure, the ECS sends EAP Success message to the SMF including the address information of Edge Enabler Server and the GPSI.

8. The SMF sends a Namf\_Communication\_N1N2MessageTransfer to the AMF with the received information.

9. The AMF forwards NAS SM PDU Session Establishment Response message along with EAP Success, the address information of suitable Edge Enabler Server and the GPSI to the UE/EEC.

10. The EEC sends Edge Enabler Client registration request to the EES.

11. The EES retrieves the authorization information of the EEC from the ECS.

12. After successful service authorization verification, the EES sends Edge Enabler Client registration response to the EEC.

Editor's note: It is FFS how to proceed the authentication and authorization if the secondary authentication is not performed.

Editor's note: details of authorization is FFS.

### 6.6.3 Solution Evaluation

TBD

## 6.7 Solution #7: Authentication and Authorization with the Edge Data Network

### 6.7.1 Solution overview

The solution addresses the following key issues:

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

- Key issue #2: Authentication and Authorization between EEC and ECS

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

The solution is based on the KAMF generated during the primary authentication. The network function that receives a registration request is querying the previous network function for authentication and the key for setting up an IPsec SA. Messages are protected with a MAC-I, which is also used to authenticate the UE.

### 6.7.2 Solution details



**Figure 6.7.2-1: Authentication and Authorization with the Edge Data Network**

1. The UE performs normal primary authentication and registration to the network. The UE is MEC capable and may indicate this in the MEC capabilities to the AMF during the registration procedure.

2. The UE establishes a PDU Session for IP connectivity.

3. If the UE is MEC capable, then the UE and the AMF derive a key KECS for authentication with the ECS from the AMF key KAMF.

4. The UE sends an Application Registration Request with a MAC-IECS to the ECS. The MAC-IECS is computed in a similar way as e.g. the SoR-MAC-IAUSF as defined in Annex A.17 of TS 33.501 [7]. The MAC-IECS is based on the payload of the Application Registration Request, which form the input Application Registration Request Data, and the key KECS to the KDF. The MAC-IECS is identified with the 128 least significant bits of the output of the KDF.

5. The UE is not authenticated at the ECS and the ECS sends a Key Request including the Application Registration Request with the MAC-IECS to the NEF, which selects based on UE ID the serving AMF and forwards the message to this AMF.

Editor's note: A new network entity to handle the EC service requests to the serving AMF is FFS.

Editor's note: Identification of the serving AMF is FFS.

6. The AMF verifies the MAC-IECS of the Application Registration Request, i.e. it computes with the key KECS the MAC-I over the Application Registration Request payload in the similar way as the UE and compares the result with the MAC-IECS included in message. If both are identical, the message can be authenticated to be sent by the UE.

7. The AMF sends a Key Response to the ECS, including the result of the authentication as well as the KECS.

8. Based on the authentication result the ECS decides whether to accept or to reject the Application Registration Request from the UE. The ECS sends the Application Registration Response message to the UE including the authentication result and protects the message with a MAC-IECS based on the received key KECS in a similar way as the UE protected the payload of the message in step 4.

9. The UE verifies the MAC-IECS and if authentication result and verification of the message are successful, then the UE establishes an IPsec SA between the UE and ECS by using the ECS key KECS. All messages are now confidentiality and integrity protected by the IPsec tunnel.

10. The UE derives the key KEES from the key KECS using a MEC Key Distinguisher flag as input to the KDF.

11. The UE sends an Application Registration Request with a MAC-IEES to the EES. The MAC-IEES is computed based on the payload of the Application Registration Request, which form the input Application Registration Request Data, and the key KEES to the KDF. The MAC-IEES is identified with the 128 least significant bits of the output of the KDF.

12. The UE is not authenticated at the EES and the EES sends a Key Request to the ECS. The selection of the ECS may be based on the UE ID.

13. The ECS identifies the UE based on the UE ID and derives the key KEES in a similar way as the UE in step 10. The ECS verifies the MAC-IEES of the Application Registration Request, i.e. it computes with the key KEES the MAC-I over the Application Registration Request payload in the similar way as the UE and compares the result with the MAC-IEES included in message. If both are identical, the message can be authenticated to be sent by the UE.

14. The ECS sends a Key Request Response to the EES, including the result of the authentication as well as the KEES.

15. Based on the authentication result the EES decides whether to accept or to reject the Application Registration Request from the UE. The EES sends the Application Registration Response message to the UE including the authentication result and protects the message with a MAC-IEES based on the received key KEES in a similar way as the UE protected the payload of the message in step 11.

16. The UE verifies the MAC-IEES and if authentication result and verification of the message are successful, then the UE establishes an IPsec SA between the UE and EES by using the EES key KEES. All messages are now confidentiality and integrity protected by the IPsec tunnel.

17. The UE derives the key KEAS from the key KEES using a MEC Key Distinguisher flag as input to the KDF.

18. The UE sends an Application Registration Request with a MAC-IEAS to the EAS. The MAC-IEAS is computed based on the payload of the Application Registration Request, which form the input Application Registration Request Data, and the key KEAS to the KDF. The MAC-IEAS is identified with the 128 least significant bits of the output of the KDF.

19. The UE is not authenticated at the EAS and the EAS sends a Key Request to the EES. The selection of the EES may be based on the UE ID.

20. The EES identifies the UE based on the UE ID and derives the key KEAS in a similar way as the UE in step 17. The EES verifies the MAC-IEAS of the Application Registration Request, i.e. it computes with the key KEAS the MAC-I over the Application Registration Request payload in the similar way as the UE and compares the result with the MAC-IEAS included in message. If both are identical, the message can be authenticated to be sent by the UE.

21. The EES sends a Key Request Response to the EAS, including the result of the authentication as well as the KEAS.

22. Based on the authentication result the EAS decides whether to accept or to reject the Application Registration Request from the UE. The EAS sends the Application Registration Response message to the UE including the authentication result and protects the message with a MAC-IEAS based on the received key KEAS in a similar way as the UE protected the payload of the message in step 3.

23. The UE verifies the MAC-IEAS and if authentication result and verification of the message are successful, then the UE establishes an IPsec SA between the UE and EAS by using the EAS key KEAS. All messages are now confidentiality and integrity protected by the IPsec tunnel.

Editor’s Note: Whether the Kamf can be used to derived the Kecs in case ECS is deployed by the home network is FFS.

Editor’s Note: How to solve the replay attack towards the ECS if the counter is not stored in the AMF is FFS

### 6.7.3 Solution evaluation

TBD

## 6.8 Solution #8: Authentication between EEC and EES

### 6.8.1 Solution overview

This solution addresses the security requirement for the Authentication between EEC and EES in key issue #1.

In this solution, UE knows to use AKMA with EES via interact with ECS before communication with EES. If the EES deployed by MNO is considered to be trusted by the operator, the EES interacts directly with AAnF. Otherwise, the EESs not allowed by the operator to access directly the Network Functions should use the NEF to interact with AAnF.

### 6.8.2 Solution details

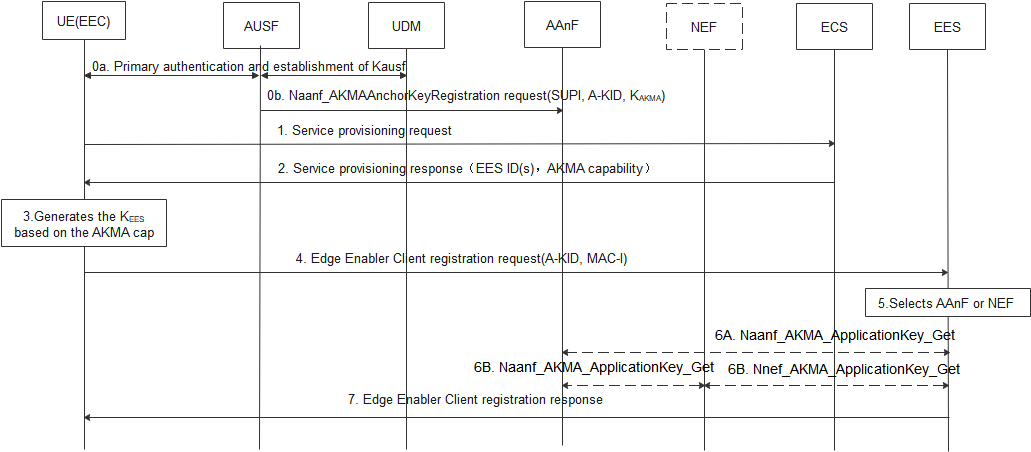


Figure 6.8.2-1 Authentication between the EEC and EES based AKMA

0a. UE performs primary authentication with the network. Then KAUSF is shared between UE and AUSF in Home network. If the AUSF receives the AKMA indication from the UDM, the AUSF should generate the AKMA Anchor Key (KAKMA) and the A-KID from KAUSF after the primary authentication procedure is successfully completed.

0b. After AKMA key material is generated, the AUSF should send the generated A-KID, and KAKMA to the AAnF.

1-2. The UE initiates the service provisioning procedure with the ECS. The ECS provides Edge Enabler Server Information (EES ID (i.e. FQDN or IP address(es) of EES), AKMA capability) to the UE. The AKMA capability indicates the EES support to use AKMA.

3. When the UE determines to communicate with EES, if the UE supports AKMA, the UE derives the AKMA key and the KEES(i.e. Kaf) as specified in TS 33.535 [6] based on the received AKMA capability.

4. The UE computes the MAC-I over the request message using the KEES and sending Edge Enable Client registration request with A-KID and MAC-I.

Editor’s Note: It is FFS whether TLS based on AKMA PSK can be used instead of MAC-I.

5. Upon receiving the request, the Edge Enabler Server discovers the AAnF or NEF.

NOTE : In the case of architecture without CAPIF support, the EES is locally configured with the API termination points for the service. In the case of architecture with CAPIF support, the EES obtains the service API information from the CAPIF core function via the Availability of service APIs event notification or Service Discover Response as specified in TS 23.222 [9].

6. The EES contacts AAnF directly or via NEF to obtains the corresponding key KEES of the UE (as defined in TS33.535 [6])..

7. The EES verifies the MAC-I using the KEES, when the verification is succeed, and if the UE is authorized to perform the operation. The EES computes MAC-I over the response message using KECS and sends Edge Enable Client registration response with the MAC-I to the UE.

### 6.8.3 Solution evaluation

TBD.

## 6.9 Solution #9: Authentication and authorization between EEC and ECS based on AKMA

### 6.9.1 Introduction

This solution addresses the key issue #2. It is assumed that the key used for authentication between EEC and ECS is negotiated based on AKMA. Then, the EEC should initiate the service provisioning request with EEC ID included. To prevent EEC ID impersonation, the ECS should verify the authenticity of UE’s EEC ID before performing authorization based on the EEC ID. Considering the ECS can determine the authenticity of UE’s A-KID based on AKMA procedure, it can confirm the authenticity of UE’s EEC ID in case the association between A-KID and EEC ID can be verified. This solution further transforms the association between A-KID and EEC ID to the association between A-KID and GPSI based on the pre-configured association between EEC ID and GPSI in ECS. Afterwards, the ECS interworks with 5GC to verify the association between A-KID and GPSI.

After successful verification, the ECS may retrieve the edge computing related profile for the EEC from the 3GPP Core Network or from its local database for edge computing. Then, the ECS can determine the EEC’s authorization based on the profile.

### 6.9.2 Solution details



Figure 6.9.2-1: Authentication/Authorization between Edge Enabler Client and ECS

Pre-conditions:

- The EEC and ECS have shared A-KID and KAF via AKMA (as specified in TS 33.535 [1]).

- The ECS or the 5GC is configured with the edge computing related profile for the EEC.

- The ECS and the 5GC share an UE identifier (i.e., GPSI) to identify the EEC.

- The ECS stores the association between EEC ID and UE identifier.

Editor’s Note: Storage of association between the EEC and the UE ID in an entity and retrieval are FFS

Editor’s Note: How to manage the UE ID bindings when the ECS is serving multiple EDNs and is FFS.

Step 1: UE initiates the service provisioning procedure with EEC ID included (as specified in clause 8.3 in TS 23.558 [2]).

Step 2: The ECS retrieves GPSI from EEC ID according to the preconfigured association.

Step 3: In order to prove the authenticity of the UE’s GPSI, the ECS sends an association check request to UDM (if the ECS is located out of 5GC, the request should be sent via NEF), including the GPSI and A-KID.

Step 4: In order to verify the association of GPSI and A-KID, the UDM first contacts the AUSF to obtain the corresponding SUPI of the A-KID. Afterwards, the UDM verifies the association of the GPSI and A-KID according to the association between SUPI and GPSI.

Editor’s Note: Support for verification of the association between the A-KID and SUPI by the AUSF/AAnF is FFS.

Step 5: The UDM sends the association verification response back to the ECS.

Step 6: On successful verification, the ECS retrieves the edge computing related profile for the EEC either from the 5GC or from its local database. Afterwards, the ECS can determine the EEC’s authorization based on EEC’s profile.

Step 7: The ECS sends the provisioning response back to EEC.

### 6.9.3 Solution Evaluation

TBD

## 6.10 Solution #10: Authentication and Authorization between the Edge Enabler Client and the Edge Configuration Server

### 6.10.1 Introduction

The following solution addresses the security requirement for the key issue #2 on Authentication and Authorization between the EEC and the ECS.

In clause 8.3.2.3 of TS 23.558 [2], before the service provisioning procedure, the Edge Enabler Client should been authorized to communicate with the Edge Configuration Server. From the security perspective, two security requirements are specified for the access of UE to Edge Data Network.

* It needs to ensure that only authorized UE in the PLMN can access to the Edge Configuration Server.
* It needs to ensure that only edge computing service authorized UE can access to the Edge Data Network.

This solution proposes a soulution to address how the Edge Enabler Client is authorized to achieve the URI or address information of Edge Configuration Server after authentication when the Edge Configuration Server is deployed by the MNO. It reuses the primary authentication for the service authentication. The service authorization is performed via the 5GC.

Based on the primary authentication procedure, the AMF will allocate the Edge Configuration Server information to the UE. Then the Edge Enabler Client can use this URI information of the Edge Configuration Server to communicate with the Edge Configuration Server.

### 6.10.2 Solution details



Figure 6.10.2-1 Authentication and Authorization between the Edge Enabler Client and the Edge Configuration Server

The procedure assumes that the Edge Configuration Server is deployed by the MNO.   
The authentication between the Edge Enabler Client and the Edge Configuration Server reuses the 5G primary authentication procedure in the PLMN. The UE can obtain information to access the Edge Configuration Server via the registration accept message. The Authorization information of the Edge Enabler Client is retrieved from the UDM in the 5GC.

1. The UE sends a Registration Request with edge computing service capability.

2. The UE and the 5G core network preform the primary authentication procedure as described in clause 6.1.2 of TS 33.501[7].

3. The AMF sends UE the Registration Accept message with suitable ECS address information.

4. The Edge Enabler Client sends service provisioning request to the ECS.

5. The ECS obtains service authorization of the Edge Enabler Client from the UDM via the NEF.

6. The UDM responses with the service authorization response message to the ECS via the NEF.

7. The ECS sends service provisioning response to the Edge Enabler Client.

Editor's note: which information can be used for authorization is FFS.

### 6.10.3 Evaluation

TBD

## 6.11 Solution #11: Authentication between EEC and ECS

### 6.11.1 Solution overview

This solution addresses the security requirement for the Authentication between EEC and ECS in key issue #2.

In this solution, UE knows to use AKMA with ECS via interactions with 3GPP network before communication with ECS. If the ECS deployed by MNO is considered to be trusted by the operator, the ECS interacts directly with AAnF. Otherwise, the ECSs not allowed by the operator to access directly the Network Functions should use the NEF to interact with AAnF.

### 6.11.2 Solution details

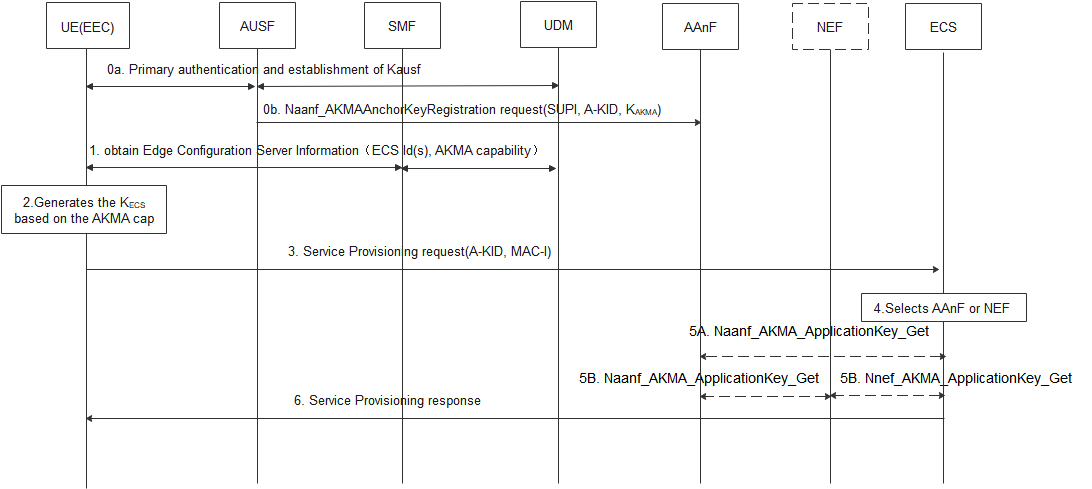


Figure 6.11.2-1 Authentication between the EEC and ECS based AKMA

0a. UE performs primary authentication with the network. Then KAUSF is shared between UE and AUSF in Home network. If the AUSF receives the AKMA indication from the UDM, the AUSF should generate the AKMA Anchor Key (KAKMA) and the A-KID from KAUSF after the primary authentication procedure is successfully completed.

0b. After AKMA key material is generated, the AUSF should send the generated A-KID, and KAKMA to the AAnF.

1. During PDU Session Establishment, the SMF provides Edge Configuration Server Information (ECS ID (i.e. FQDN or IP address(es) of ECS), AKMA capability) to the UE. The AKMA capability indicates the ECS support to use AKMA.
2. When the UE determines to communicate with ECS, if the UE supports AKMA, the UE derives the AKMA key and KECS(i.e KAF) as specified in TS 33.535 [6] based on the received AKMA capability.
3. UE computes the MAC-I over the request message using the KECS and sends service provision request with A-KID, MAC-I.

Editor’s Note: It is FFS whether TLS based on AKMA PSK can be used instead of MAC-I.

1. Upon receiving the request, the Edge Configuration Server discovers the AAnF or NEF.

NOTE : In the case of architecture without CAPIF support, the ECS is locally configured with the API termination points for the service. In the case of architecture with CAPIF support, the ECS obtains the service API information from the CAPIF core function via the Availability of service APIs event notification or Service Discover Response as specified in TS 23.222 [9].

5A-5B. The ECS contacts AAnF directly or via NEF to obtain the corresponding key KECS (KAF) of the UE(as defined in TS33.535).

6. The ECS verifies the MAC-I based on the KECS, when the verification is succeed, and if the UE is authorized to perform the operation. Then the ECS computes MAC-I over the response message using KECS, and sends a service provisioning response with the MAC-I to the UE.

### 6.11.3 Solution evaluation

TBD.

## 6.12 Solution #12: Onboarding and authentication/authorization framework for Edge Enabler Server and Edge Configuration Server

### 6.12.1 Introduction

This solution addresses the security requirement for the Onboarding of EES with ECS, as described in Key issue 3. The solution proposes a framework and procedure that the Edge Enabling Server and the Edge Configuration Server follows to secure and authenticate the Registration, update, and deregistration of the Edge Enabling Server to the Edge Configuration Server.

As a prerequisite to this procedure (step 1), the solution assumes that Onboarding credential information is obtained by EES within the same PLMN domain or from a third party domain. Procedures on how to obtain this information are out of the scope of 3GPP. EES uses onboarding credentials to authenticate and establish a secure TLS communication with the Edge Configuration Server during the registration process. The credential information includes details of the Edge Configuration Server Address and Root CA certificate, and it may also include an onboarding token (e.g., OAuth 2.0 access token).

Note: ECS address that is not belonging to the credentials, is out of scope of this document, and will be determined by SA6.

### 6.12.2 Solution details



Figure 6.12.2-1: Authentication/Authorization framework for EES with ECS

Step 1-2: The Edge Enabling Server and Edge Configuration Server should establish a secure session based on TLS (Server-side certificate authentication). The Edge Enabling Server should use the credential information obtained in step 1 to establish the TLS session with the Edge Configuration Server.

Step 3: After the successful establishment of the TLS session, the Edge Enabling Server should send an Edge Enabler Server Registration message to the Edge Configuration Server along with the credential (OAuth access token) and EES Profile. The Edge Enabling Server generates the key pair {Private Key, Public key} and provides the public key along with the Onboard Edge Enabling Server request.

Editor Note: ECS certificate procedures should be FFS

Step 4: The Edge Configuration Server should validate the enrolment credential (OAuth token). After successful verification of credentials, Edge Configuration Server may generate Edge Enabling Server's certificate on its own, for the assigned Edge Enabling Server identity and public key. For subsequent authentication procedures with the Edge Configuration Server, the Edge Enabling server may use this certificate to establish a secure connection and authentication with the Edge configuration Server.

Editor’s Note: Details of EES verification are FFS.

Step 5: The Edge Configuration Server should respond with a Registration response message. The response should include the Edge Configuration Server assigned Edge Enabling Server Registration ID, Edge Enabling Server Authentication and authorization information (if generated in step 4), Edge Enabling Server's certificate, and the Edge Enabling Server access token (if generated by the Edge Configuration Server).

### 6.12.3 Solution evaluation

## 6.13 Solution #13: Transport security for EDGE-1-9 interfaces

### 6.13.1 Introduction

This solution addressed the transport security requirements for EDGE-1-9 interfaces in key issue #6. Generally, NDS/IP should be used here for data protection.

### 6.13.2 Solution details

There are three types of interfaces related with edge application architecture defined in TR 23.558 [2]. Hence, the transport security will be discussed separately within three subclauses.

#### 6.13.2.1 Type A

Interfaces of type A (Between UE and Edge servers) are as follows:

* EDGE-1: between EEC and EES
* EDGE-4: between EEC and EAS
* EDGE-5: between EEC and Application Client(s)

Editor’s Note: How to protect the EDGE-1 and EDGE-4 interfaces is FFS.

According to TS 23.558[2], details of the EDGE-5 is out of scope of that document. Hence the transport security of EDGE-5 is out of scope of this document, and can be left for implementation.

#### 6.13.2.2 Type B

Interfaces of Type B (Between 3GPP core and Edge servers) are as follows:

* EDGE-2: between 3GPP Core network and EES
* EDGE-7: between 3GPP Core network and ECS
* EDGE-8: between 3GPP Core network and EAS

How to protect the interface between 3GPP Core network and EES/ECS/EAS, depends on the functionality, which will be performed on this interface.

As defined in TS 23.558 clause 6.4.2, it says.

*EDGE-2 reference point enables interactions between the Edge Enabler Server and the 3GPP Core Network. It supports:*

*a) access to 3GPP Core Network functions and APIs for retrieval of network capability information, e.g. via SCEF and NEF APIs as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3], 3GPP TS 29.522 [4], 3GPP TS 23.682 [17], 3GPP TS 29.122 [5], and with the EES acting as a trusted AF in 5GC (see 3GPP TS 23.501 [2] clause 5.13, 3GPP TS 23.503 [12]).*

*NOTE: EDGE-2 reference point reuses 3GPP reference points or interfaces of EPS or 5GS considering different deployment models.*

Similarly, EDGE-7/8 is used to support the same functionality as the EDGE-2.

Therefore, For 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 [10] can be reused here to protect the EDGE-2/7/8 interfaces, 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 [11] can be reused here, i.e. use of TLS.

NOTE: Transport security protection of EDGE-2/7/8 can take the other deployment models in the future.

#### 6.13.2.3 Type C

Interfaces of type C (Between Edge servers) are as follows:

* EDGE-3: between EAS and EES. The supported functionalities include EAS registration, de-registration, etc.
* EDGE-6: between EES and ECS. The supported functionalities include EES registration.
* EDGE-9: between EES(s). The supported functionalities include discovery of target EAS.

As all the exchanged data of EDGE-3/6/9 is in the application layer, transport security protection on the SBI interface can be reused here. Hence TLS should be used as specified in TS 33.210 [12], unless security is provided by other means, e.g. physical security. A SEG may be used to terminate the NDS/IP IPsec tunnels.

For the EDGE-3, if the CAPIF capability is consumed by the EAS, the interface security defined in the TS 33.501 clause 12 can be reused here to protect the CAPIF related data transferred in the EDGE-3 interfaces, i.e. TLS should be used.

NOTE 1: Regardless of whether TLS is used or not, NDS/IP as specified in TS 33.210 [12] and TS 33.310 [13] can be used for network layer protection.

Editor’s Note: whether the above transport security protection mechanism for Type C interfaces is sufficient is FFS.

### 6.13.3 Evaluation

TBD

## 6.14 Solution #14: Protection of Network Information Provisioning to Local AF directly

### 6.14.1 Solution overview

This solution addresses the security requirement for the case that the UPF exposes information to local AF directly in the key issue 7.

Editor’s Note: which interface for UPF and AF communicate over is FFS.

### 6.14.2 Solution details

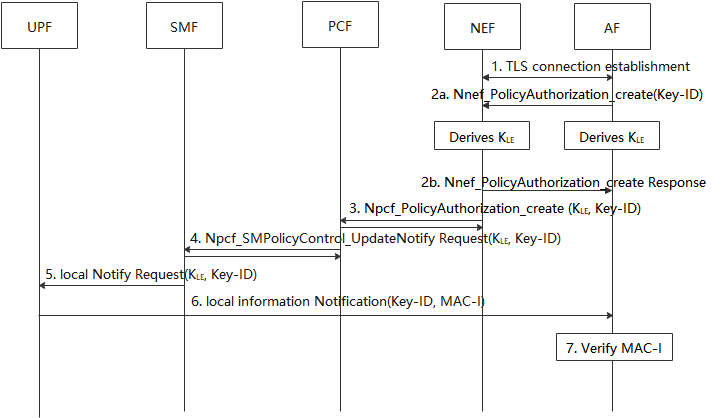


Figure 6.14.2-1 Protection of Network Information Provisioning to Local AF

1. AF establish a TLS session with the NEF, to secure the communication between the AF and NEF.

2a-2b. The AF generates a Key-ID for the UE and derives a KLE. The Key-ID is used to identify the KLE, and the KLE is used to protect the message transmission between UPF and AF. The AF provides the Key-ID to NEF in the request service.

3-4. The NEF initiates the policy authorization with PCF, including the K-ID and KLE received from the AF. PCF initiates the PDU session modification procedure as defined in clause 4.3.3.2 of TS 23.502 [3] and provides the Key-ID and KLE to the SMF.

5. SMF sends the notification information with Key-ID and KLE to the UPF.

6. When the QoS monitoring information is received from RAN, the UPF generates MAC-I over the message using the KLE to prove its authenticity. The UPF sends the message including Key-ID and MAC-I to AF.

7. The AF retrieves the KLE based on the received Key-ID and verify the MAC-I.

### 6.14.3 Solution evaluation

TBD.

## 6.15 Solution #15: Service capability re-exposure

### 6.15.1 Introduction

In clause 5.8 of this document, it describes the key issue on service capability APIs exposed by the Edge Enabler Server to the Edge Application Server(s). It states that the Edge Application Server(s) should be authenticated and authorized, otherwise attackers would potentially be able to perform unauthorized access or trigger DoS attacks .This solution is proposed to address the security requirement for authentication and authorization in EES capability exposure in key issue #8.

In this solution, it is proposed the Edge Enabler Server check whether the EAS is allowed to be authorized for the service capability re-exposure by the 5GC and the UE (EES capabilities and 3GPP Core Network capabilities) via the NEF and the UDM.

### 6.15.2 Solution details

1. The Edge Application Server sends API request message to the Edge Enabler Server with the UE Identifier, related service exposure information and the Edge Application Server ID.

2. If the service can be provided by EES directly, the Edge Enabler Server will check whether the EAS has the authorization token, and it will provide the exposure information to the authorized EAS as specified in clause 8.6.2 in TS 23.558[2]. If the request service cannot be provided EES directly, may be the EES has not been authorized by 5G core network for the service exposure bases on SLA, the Edge Enabler Server should request the NEF to verify whether the service is allows to be exposed to the EAS by the EES with EAS ID and the SLA from the UDM. The authentication and authorization between the EES and NEF reuses the mechanisms specified in clause 12 in TS 33.501[7].

3. The NEF sends a request to the UDM to query whether it is allowed to expose the service to the EAS.

4. The UDM checks the service exposure authorization for the EAS.

5. The UDM returns the corresponding service exposure authorization information to the NEF. If the EAS is allowed to be authorized, the UDM returns the authorization identifier with 1. Otherwise, the UDM replies with 0.

6. After receiving the response message, the NEF send the verification response.

7. If the EAS is authorized, the Edge Enabler Server responds to the Edge Application Server with service exposure information to the EAS.



Figure 6.15.2-1 The authorization for service capability APIs exposure to EAS

### 6.15.3 Solution Evaluation

TBD

## 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, S3-202151, S3-202063, S3-202119, and S3-202062. | 0.1.0 |
| 2020-08 | SA3#100bis-e | S3-202764 |  |  |  | Implemented S3-202729, S3-202521, S3-202620, S3-202697, S3-202318, S3-202319, S3-202320, S3-202321, S3-202733, S3-202743, S3-202744, S3-202731, S3-202742, S3-202781, S3-202779, S3-202778, S3-202777, S3-202776, S3-202759, S3-202758, S3-202757, S3-202756 | 0.2.0 |