|  |  |
| --- | --- |
| 3GPP TR 33.739 V18.1.0 (2023-12) | |
| Technical Specification|Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on security enhancement of support for  edge computing phase 2  (Release 18) | |
|  | |
|  | 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.  © 2023, 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 7

1 Scope 9

2 References 9

3 Definitions of terms, symbols and abbreviations 10

3.1 Terms 10

3.2 Symbols 10

3.3 Abbreviations 10

4 Overview of Edge Computing - Phase 2 10

5 Key issues 10

5.1 General 10

5.2 Key issues related with 5G System Enhancements for Edge Computing 10

5.2.1 Key issue #1.1: How to authorize PDU session to support local traffic routing to access an EHE in the VPLMN 10

5.2.1.1 Key issue details 10

5.2.1.2 Threats 11

5.2.1.3 Potential security requirements 11

5.2.2 Key issue #1.2: Security of EAS discovery procedure via V-EASDF in VPLMN 11

5.2.2.1 Key issue details 11

5.2.2.2 Threats 11

5.2.2.3 Potential security requirements 11

5.3 Key issues related with enhanced architecture for enabling Edge Applications 11

5.3.1 Key Issue #2.1: Authentication and authorization of the EEC/UE by the ECS/EES 11

5.3.1.1 Key issue details 11

5.3.1.2 Security threats 12

5.3.1.3 Potential security requirements 12

5.3.2 Key issue #2.2: Authentication mechanism selection between EEC and ECS/EES 12

5.3.2.1 Key issue details 12

5.3.2.2 Security threats 12

5.3.2.3 Potential security requirement 12

5.3.3 Key issue #2.3: Authentication and Authorization between V-ECS and H-ECS 13

5.3.3.1 Key issue details 13

5.3.3.2 Threats 13

5.3.3.3 Potential security requirements 13

5.3.4 Key issue #2.4: Transport security for the EDGE10 interface 13

5.3.4.1 Key issue details 13

5.3.4.2 Threats 13

5.3.4.3 Potential security requirements 13

5.3.5 Key issue #2.5: Authentication and Authorization between AC and EEC 13

5.3.5.1 Key issue details 13

5.3.5.2 Threats 14

5.3.5.3 Potential security requirements 14

5.3.6 Key issue #2.6: New KI on authorization between EESes 14

5.3.6.1 Key issue details 14

5.3.6.2 Threats 14

5.3.6.3 Potential security requirements 14

5.3.7 Key issue #2.7: EEC provided information verification 15

5.3.7.1 Key issue details 15

5.3.7.2 Threats 15

5.3.7.3 Potential security requirements 15

6 Proposed solutions 15

6.0 Mapping of Solutions to Key Issues 15

6.1 Solution #1: Authentication and authorization between EEC hosted in the roaming UE and ECS 17

6.1.1 Solution overview 17

6.1.2 Solution details 17

6.1.3 Solution evaluation 18

6.2 Solution #2: Authentication and authorization between EEC hosted in the roaming UE and EES 18

6.2.1 Solution overview 18

6.2.2 Solution details 19

6.2.3 Solution evaluation 20

6.3 Solution #3: Authentication mechanism selection between EEC and ECS 21

6.3.1 Solution overview 21

6.3.2 Solution details 21

6.3.2.1 ECS configuration 21

6.3.3 Solution evaluation 22

6.4 Solution #4: Authentication mechanism selection between EEC and EES 22

6.4.1 Solution overview 22

6.4.2 Solution details 22

6.4.2.1 EES profile 23

6.4.3 Solution evaluation 23

6.5 Solution #5: 5GC-based authentication mechanism selection between EEC and ECS/EES 23

6.5.1 Solution overview 23

6.5.2 Solution details 24

6.5.3 Solution evaluation 25

6.6 Solution #6: ECS/EES authentication method information provisioning 25

6.6.1 Solution overview 25

6.6.2 Solution details 25

6.6.3 Solution evaluation 25

6.7 Solution #7: Negotiation procedure for the Authentication and Authorization 26

6.7.1 Solution overview 26

6.7.2 Solution details 26

6.7.3 Solution evaluation 27

6.8 Solution #8: Authentication mechanisms selected by ECS/EES 27

6.8.1 Solution overview 27

6.8.2 Solution details 27

6.8.2.1 Authentication between EEC and ECS 27

6.8.2.2 Authentication between EEC and EES 27

6.8.3 Solution evaluation 27

6.9 Solution #9: Authentication mechanism selection procedure between EEC and ECS 27

6.9.1 Solution overview 27

6.9.2 Solution details 27

6.9.3 Solution evaluation 28

6.10 Solution #10: Authentication mechanism selection procedure between EEC and EES 28

6.10.1 Solution overview 28

6.10.2 Solution details 28

6.10.3 Solution evaluation 28

6.11 Solution #11: Authentication mechanism selection procedure among EEC, ECS, and EES 29

6.11.1 Solution overview 29

6.11.2 Solution details 29

6.11.3 Solution evaluation 30

6.12 Solution #12: Authorization for PDU session supporting local traffic routing to access an EHE in the VPLMN 31

6.12.1 Introduction 31

6.12.2 Solution details 31

6.12.3 Solution evaluation 31

6.13 Solution #13: A solution for authentication of EEC/UE and GPSI verification by EES/ECS 31

6.13.1 Solution overview 31

6.13.2 Solution details 31

6.13.3 Solution evaluation 33

6.14 Solution #14: A solution for authentication of UE and GPSI verification by EES/ECS 33

6.14.1 Solution overview 33

6.14.2 Solution details 33

6.14.3 Solution evaluation 34

6.15 Solution #15: Authentication algorithm selection procedure between EEC and ECS 34

6.15.1 Solution overview 34

6.15.2 Solution details 34

6.15.3 Solution evaluation 36

6.16 Solution #16: Authentication algorithm selection procedure between EEC and EES 36

6.16.1 Solution overview 36

6.16.2 Solution details 36

6.16.3 Solution evaluation 37

6.17 Solution #17: Using existing AKMA/GBA negotiation mechanism 38

6.17.1 Solution overview 38

6.17.2 Solution details 38

6.17.2.1 Shared key based EEC/UE authentication and certificate based ECS/EES authentication 38

6.17.2.2 Shared key based mutual authentication 38

6.17.2.2.1 Shared key based mutual authentication in TLS 1.2 38

6.17.2.2.2 Shared key based mutual authentication in TLS 1.3 39

6.17.2.3 Handling EEC authentication negotiation failure 39

6.17.2.4 GPSI verification 39

6.17.3 Solution evaluation 39

6.18 Solution #18: Authentication and Authorization between V-ECS and H-ECS 39

6.18.1 Solution overview 39

6.18.2 Solution details 40

6.19 Solution #19: Authorization of V-ECS in roaming scenario 40

6.19.1 Solution overview 40

6.19.2 Solution details 40

6.19.3 Solution evaluation 41

6.20 Solution #20: Transport security for the EDGE10 interface 41

6.20.1 Solution overview 41

6.20.2 Solution details 41

6.20.3 Solution evaluation 41

6.21 Solution #21: Using local policy on authorization between EESes 41

6.21.1 Solution overview 41

6.21.2 Solution details 41

6.21.3 Solution evaluation 41

6.23 Solution #23: EAS discovery procedure protection 43

6.23.1 Solution overview 43

6.23.2 Solution details 43

6.23.3 Solution evaluation 43

6.24 Solution #24: Public key signature based ECS/EES authentication 43

6.24.1 Solution overview 43

6.24.2 Solution details 43

6.24.3 Solution evaluation 44

6.25 Solution #25: Utilizing Token-Based Solutions for EEC authentication 44

6.25.1 Solution overview 44

6.25.2 Solution details 44

6.25.3 Solution evaluation 45

6.26 Solution #26: Using authorization token on authorization between EESes 45

6.26.1 Solution overview 45

6.26.2 Solution details - Target EES Decided ACR 45

6.26.3 Solution details: Source EAS decided ACR 47

6.26.4 Solution details: S-EES executed ACR 48

6.26.5 Solution evaluation 50

6.27 Solution #27: Token-based solution for authorization between EESes 50

6.27.1 Solution overview 50

6.27.2 Solution details 50

6.27.3 Solution evaluation 51

6.28 Solution #28: Usage of randomly generated ticket to verify EEC provided IP address 51

6.28.1 Solution overview 51

6.28.2 Solution details 51

6.28.3 Solution evaluation 52

6.29 Solution #29: Authorizing the Service Consumer when Resolving an IP Address to a UE ID 53

6.29.1 Solution overview 53

6.29.2 Solution details 53

6.29.3 Solution evaluation 53

6.30 Solution #30: Usage of existing public IP address to verify EEC provided IP address 56

6.30.1 Solution overview 56

6.30.2 Solution details 56

6.30.3 Solution evaluation 57

6.31 Solution #31: AKMA/GBA based verification of EEC provided IP address 58

6.31.1 Solution overview 58

6.31.2 Solution details 58

6.31.3 Solution evaluation 59

6.32 Solution #32: KDF based verification of EEC provided IP address 59

6.32.1 Solution overview 59

6.32.2 Solution details 59

6.32.3 Solution evaluation 59

6.33 Solution #33: Verification of EEC provided IP address 60

6.33.1 Solution overview 60

6.33.2 Solution details 60

6.33.3 Solution evaluation 60

6.34 Solution #34: Verification of EEC provided IP address using access token 61

6.34.1 Solution overview 61

6.34.2 Solution details 61

6.34.3 Solution evaluation 61

7 Conclusions 62

7.1 Conclusions for Key Issue #2.4 62

7.2 Conclusions for Key Issue #2.3 62

7.3 Conclusions for Key Issue #2.5 62

7.4 Conclusions for Key Issue #1.1 62

7.5 Conclusions for Key Issue #2.1 62

7.6 Conclusions for Key Issue#2.2 62

7.7 Conclusions for Key Issue #2.6 63

7.8 Conclusions for Key Issue #1.2 63

7.9 Conclusions for Key Issue #2.7 63

Annex A: Change history 64

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document studies the security aspects related to the new features and procedures resulting from the continuation of the work on Edge Computing support in 5G Systems, i.e. 5G System Enhancements for Edge Computing in 3GPP TR 23.700-48 [2], and enhanced architecture for enabling Edge Applications in 3GPP TR 23.700-98 [3]. The study bases on the work done in the 3GPP TS 33.558 [4] and 3GPP TR 33.839 [5].

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.700-48: "5G System Enhancements for Edge Computing; Phase 2".

[3] 3GPP TR 23.700-98: "Study on Enhanced architecture for enabling Edge Applications ".

[4] 3GPP TS 33.558: "Security aspects of enhancement of support for enabling edge applications".

[5] 3GPP TR 33.839: "Study on security aspects of enhancement of support for edge computing in the 5G Core (5GC)".

[6] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

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

[8] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[9] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[10] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[11] 3GPP TS 23.558: "Architecture for enabling Edge Applications".

[12] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[13] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security".

[14] GSMA TS.43: "Service Entitlement Configuration".

[15] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

[16] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[17] IETF RFC 7858: "Specification for DNS over Transport Layer Security (TLS)".

[18] IETF RFC 8310: "Usage Profiles for DNS over TLS and DNS over DTLS".

# 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].

**Application Client:** Application software resident in the UE performing the client function.

**Application Context:** A set of data about the Application Client that resides in the Edge Application Server.

**Application Context Relocation**: End-to-end service continuity procedure described in clause 8.8.

**Application Context Transfer**: Refers to the transfer of the Application Context between the source Edge Application Server and the target Edge Application Server, which is a part of the service continuity procedure described in clause 8.8.

**Application Server**: Application software resident in the cloud performing the server function.

**Edge Application Server:** An Application Server resident in the Edge Hosting Environment.

**Edge Computing:** A concept, as described in 3GPP TS 23.501 [2], that enables operator and 3rd party services to be hosted close to the UE's access point of attachment, to achieve an efficient service delivery through the reduced end-to-end latency and load on the transport network.

**Edge Computing Service Provider**: A mobile network operator or a 3rd party service provider offering Edge Computing service.

**EEC Context:** A set of data about the Edge Enabler Client that resides in the Edge Enabler Server.

**Edge Data Network:** A local Data Network that supports the architecture for enabling edge applications.

**Edge Enabler Client:** A functional entity resident in the UE providing services for the Application Clients.

**Edge Enabler Layer:** The overall functionality provided by the entities such as Edge Enabler Client, Edge Enabler Server and Edge Configuration Server, in support of applications as per the architecture defined in clause 6.

**Edge Enabler Server:** A functional entity resident in the Edge Hosting Environment providing services for the Edge Application Servers and Edge Enabler Clients

**Edge Hosting Environment:** An environment providing support required for Edge Application Server's execution.

## 3.2 Symbols

Void.

## 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].

AAnF AKMA Anchor Function

AC Application Client

ACID Application Client Identification

ACR Application Context Relocation

ACT Application Context Transfer

AF Application Function

AKMA Authentication and Key Management for Applications

AMF Access and Mobility Management Function

API Application Programming Interface

AUSF Authentication Server Function

BSF Binding Support Function

DNAI Data Network Access Identifier

DNN Data Network Name

DNS Domain Name System

EAS Edge Application Server

EASDF Edge Application Server Discovery Function

EASID Edge Application Server Identification

ECS Edge Configuration Server

ECSP Edge Computing Service Provider

EDN Edge Data Network

EEC Edge Enabler Client

EEL Edge Enabler layer

EES Edge Enabler Server

EESID Edge Enabler Server Identification

EHE Edge Hosting Environment

FQDN Fully Qualified Domain Name

GBA Generic Bootstrapping Architecture

GPSI Generic Public Subscription Identifier

GSM Global System for Mobile Communications

GSMA GSM Association

H-ECS Home Edge Configuration Server

HSS home subscriber server

IP Internet Protocol

KDF Key Derivation Function

MNO Mobile Network Operator

NAT Network Address Translation

NEF Network Exposure Function

NRF Network Repository Function

OPG Operator Platform Group

PCF Policy Control Function

PCO Protocol Configuration Option

PSA PDU Session Anchor

PDU Protocol Data Unit

RAT Radio Access Technology

S-EAS Source Edge Application Server

S-EES Source Edge Enabler Server

SMF Session Management Function

S-NSSAI Single Network Slice Selection Assistance Information

T-EAS Target Edge Application Server

T-EES Target Edge Enabler Server

TLS Transport Layer Security

UDM Unified Data Management

UE User Equipment

UPF User Plane Function

URI Uniform Resource Identifier

V-ECS Visited Edge Configuration Server

V-EES Visited Edge Enabler Server

# 4 Overview of Edge Computing - Phase 2

The present document studies the security enhancements on the support for Edge Computing of phase 2 in the 5G Core network defined in 3GPP TS 23.548 [15], and application architecture for enabling Edge Applications of phase 2 defined in 3GPP TS 23.558 [11].

For the EC supported in 5GC, refer to 3GPP TS 23.548 [15].

For more details on enabling Edge Applications, it is proposed to refer to 3GPP TS 23.558 [11].

# 5 Key issues

## 5.1 General

Clause 5 describes the security key issues related with 5G System Enhancements for Edge Computing of 3GPP TR 23.700‑48 [2] in clause 5.2, and Enhanced Architecture for Enabling Edge Applications of 3GPP TR 23.700‑98 [3] in clause 5.3.

## 5.2 Key issues related with 5G System Enhancements for Edge Computing

### 5.2.1 Key issue #1.1: How to authorize PDU session to support local traffic routing to access an EHE in the VPLMN

#### 5.2.1.1 Key issue details

Two scenarios (i.e. UE accessing EHE in VPLMN via an LBO PDU Session and UE accessing EHE in VPLMN via a PDU Session established as HR) are described in 3GPP TR 23700-48 [2], clause 5.1.2. One issue is left for study from the security point of view for the scenario using a PDU Session with a PSA in the HPLMN, i.e. how to authorize the PDU session to support local traffic routing to access an EHE in the VPLMN.

It is suggested to study whether the existing secondary authentication can be reused here for this new scenario.

#### 5.2.1.2 Threats

Unauthorized UE could access the PDU session to support local traffic routing to access an EHE in the VPLMN.

#### 5.2.1.3 Potential security requirements

5G system should support PDU session authorization to support the local traffic routing to access an EHE in the VPLMN.

### 5.2.2 Key issue #1.2: Security of EAS discovery procedure via V-EASDF in VPLMN

#### 5.2.2.1 Key issue details

In 3GPP TS 23700-48 [2], two scenarios on how the UE accesses the EHE in VPLMN are described: the UE accesses EHE via an LBO PDU Session or the UE accesses EHE via a Home Routed (HR) PDU Session. For the discovery of the EAS located in EHE in VPLMN, the V-EASDF will be selected by the V-SMF and the V-EASDF address is sent to UE by the V-SMF directly (i.e. LBO case) or via H-SMF (i.e. HR case). The UE then exchanges DNS messages with V-EASDF to perform EAS discovery. Therefore, if the DNS message is modified by an attacker, then the DNS message could be sent to a compromised DNS server, in which case a wrong EAS address is allocated. Alternatively, the attacker could modify the EAS address and replace it with an address to a malicious AS.

According to clause 6.7.2.3 of 3GPP TS 23.548 [15], when the target FQDN of the DNS query cannot be resolved by the V-EASDF, then the V-EASDF can send the DNS request to the DNS server address of HPLMN. Investigation on whether this communication between the V-EASDF and DNS server of the HPLMN also needs to be protected against unauthorized access and modifications by the attackers is required.

#### 5.2.2.2 Threats

Without protection of the DNS message, an attacker could manipulate the DNS messages causing a disruption to the discovery procedure and edge services or misleading the UE to malicious servers.

If the communication between V-EASDF and DNS server of HPLMN is not security protected, then a malicious or compromised entity who can monitor the incoming and outgoing traffic of V-EASDF can learn the DNS query of the UE. Also, that entity could manipulate the DNS messages causing a disruption to the discovery procedure and edge services or misleading the UE to malicious servers.

#### 5.2.2.3 Potential security requirements

The system should support secure EAS discovery procedure via V-EASDF.

## 5.3 Key issues related with enhanced architecture for enabling Edge Applications

### 5.3.1 Key Issue #2.1: Authentication and authorization of the EEC/UE by the ECS/EES

#### 5.3.1.1 Key issue details

This key issue aims at addressing authentication and authorization problem for the EEC/UE by the ECS/EES considering both the non-roaming and roaming cases.

Regarding the non-roaming case, Rel-17 security specification of edge computing support, 3GPP TS 33.558 [4], the authentication methods for EEC are left as out of scope for Rel-17. From the standardization point of view, these mechanisms need to be standardized to solve interoperability issues.

Regarding the roaming case, in 3GPP TR 23.700-98 [3], it is stated that "It is required to clarify how an EEC hosted in the roaming UE can be authenticated and authorized to access the edge computing services available in the VPLMN. The related requirement is described in GSMA OPG as follows: 'Access of roaming subscribers to edge applications in the visited network shall be subject to authorization by the subscriber's Home OP and the Visited OP'.".

However, the edge computing authorization procedures for roaming scenarios, which may need the cooperation of home network and visiting network, are still unclear. Moreover, mechanisms which can be utilized to authenticate EEC hosted in the roaming UE or the roaming UE itself and data protection are not defined. Therefore, the procedures and mechanisms about authenticating and authorizing EEC hosted in the roaming UE or the roaming UE itself and data protection need to be studied.

Regarding both the non-roaming and roaming cases, investigations about UE authentication and authorization by the EES/ECS and about whether UE authentication and authorization is enough instead of EEC authentication and authorization by the EES/ECS are required.

#### 5.3.1.2 Security threats

If the EEC hosted in the UE or the UE is not authenticated and authorized both in the non-roaming and roaming cases, an attacker can impersonate the EEC/UE, manipulate the data communicated with edge computing servers, and track victim UEs.

#### 5.3.1.3 Potential security requirements

Mutual authentication and authorization between EEC/UE and edge servers considering both the non-roaming and roaming scenarios should be supported.

Communication between EEC/UE and edge servers considering both the non-roaming and roaming scenarios should be securely protected.

### 5.3.2 Key issue #2.2: Authentication mechanism selection between EEC and ECS/EES

#### 5.3.2.1 Key issue details

In 3GPP TS 33.558 [4], clauses 6.2 and 6.3 introduce the authentication and authorization between EEC and ECS, EEC and EES. And it is concluded for authentication between EEC and ECS, EEC and EES, TLS authentication methods shall be used, and the details of TLS authentication method, (e.g. TLS with AKMA as specified in 3GPP TS 33.535 [8], TLS with GBA as specified in 3GPP TS 33.222 [10], other TLS authentication methods that uses other than 3GPP subscription credential(s) which is out of 3GPP) are out of scope of the present document.

However, with these multiple authentication methods, how to select which authentication mechanism to use between the EEC and EES, EEC and ECS is not addressed. Not knowing which authentication to use between EEC and EES, EEC and EES would lead to mis-synchronization between the EEC and EES, EEC and ECS.

For EDGE authentication mechanism selection, the roaming scenario needs to be taken into consideration.

For EDGE authentication mechanism selection, the authentication capability supported by the UE and the network entities needs to be taken into consideration.

This key issue is to study the selection of authentication mechanism for the authentication procedures between EEC and ECS, EEC and EES for Edge service.

#### 5.3.2.2 Security threats

If the authentication between the EEC and ECS or EEC and EES is done without the security method selection, it would cause mis-synchronization between the EEC and EES/ECS.

#### 5.3.2.3 Potential security requirement

Selection of authentication mechanism for the authentication procedures between EEC and EES and between EEC and ECS shall be supported.

### 5.3.3 Key issue #2.3: Authentication and Authorization between V-ECS and H-ECS

#### 5.3.3.1 Key issue details

In 3GPP TR 23.700-98 [3], it defines roaming architecture, the roaming architecture uses ECSs provided in HPLMN and VPLMN, in which the EEC in the UE obtains services from V-ECS and V-EES. In the architecture, the H-ECS is associated with HPLMN, while the V-ECS and the EDN which the UE accesses is associated with VPLMN. A new reference point EDGE-10 is defined between ECSs (i.e. V-ECS and H-ECS). The new interface is introduced for EES discovery in roaming PLMN in solution 5 or V-ECS information retrieval in solution 14.

#### 5.3.3.2 Threats

Without authentication or authorization, the Malicious H-ECS may be able to obtain EES information or V-ECS information from V-ECS. This attack leads to exposing the topology details, server information within the V-PLMN domain. A malicious V-ECS may obtain UE information from H-ECS, which may cause exposure of UE privacy.

#### 5.3.3.3 Potential security requirements

V-ECS and H-ECS shall perform mutual authentication.

The V-ECS shall be able to authorize the H-ECS to get the EES information or V-ECS information.

H-ECS shall only communicate with an authorized V-ECS.

### 5.3.4 Key issue #2.4: Transport security for the EDGE10 interface

#### 5.3.4.1 Key issue details

In 3GPP TR 23.700-98 [3], it defines roaming architecture, the roaming architecture uses ECSs provided in HPLMN and VPLMN, in which the EEC in the UE obtains services from V-ECS and V-EES. In the architecture, the H-ECS is associated with HPLMN, while the V-ECS and the EDN which the UE accesses is associated with VPLMN. A new reference point EDGE-10 is defined between ECSs (i.e. V-ECS and H-ECS). The new interface is introduced for EES discovery in roaming PLMN in solution 5 or V-ECS information retrieval in solution 14. This key issues studies the related transport security, i.e. confidentiality, integrity, and replay-protection.

#### 5.3.4.2 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.

#### 5.3.4.3 Potential security requirements

Confidentiality protection, integrity protection, and replay-protection shall be supported on the EDGE-10 interface.

### 5.3.5 Key issue #2.5: Authentication and Authorization between AC and EEC

#### 5.3.5.1 Key issue details

As per 3GPP TR 23.700-98 [3], EDGE-5 reference point enables interactions between the Application Client (AC) and the Edge Enabler Client (EEC). EDGE-5 reference point supports AC registration, EAS discovery, ACR request, AC subscription, and AC notification.

AC may request the EEC for EEL service and also can request AC subscription. The EEC creates the subscription and when required, performs necessary operations such as EAS discovery, ACR etc., delivering notifications to the AC as required.

#### 5.3.5.2 Threats

When performing EAS discovery without authentication and authorization, a malicious application client may receive the list of services and gain insights on the topology structure the Edge Data Network from the EEC. The received information can reveal Edge Data Network's topology (e.g. number of Edge Application Servers, Application Server Functionalities, API type, protocols). A malicious application client may use this information to launch attacks on the Edge Data Network or use this information to gain competitive advantage.

#### 5.3.5.3 Potential security requirements

The Edge Enabler Client (EEC) should be able to provide mutual authentication with the Application Client over EDGE-5 interface.

The Edge Enabler Client (EEC) should be able to determine whether Application client is authorized to access EEL service offered by Edge Enabler Client (EEC).

NOTE: How to fulfil above security requirements is left to the UE implementation.

### 5.3.6 Key issue #2.6: New KI on authorization between EESes

#### 5.3.6.1 Key issue details

According to TR 23.558 [11], the EDGE-9 reference point enables interactions between the Edge Enabler Servers (EES).

EDGE-9 supports:

a) discovery of T-EAS information to support Application Context Relocation (ACR);

b) EEC context relocation procedures; and

c) transparent transfer of the application context during Edge Enabler layer Managed ACR.

In the situations such as UE mobility, overload control, or maintenance, different EESs can be more suitable for serving the ACs in the UE. Such mobility transitions result in replacing the source the EES (S-EES) with a target EES (T-EES). Replacing the S-EES with the T-EES requires a procedure named Application Context Relocation (ACR).

3GPP TS 33.558 [4] clause 5.1.2 states that "confidentiality, integrity, and replay protection shall be supported on the EDGE-1-4 and EDGE 6-9 interfaces". In addition, for the interfaces EDGE-3/6/9, "the EAS, EES and ECS shall support TLS and HTTPS". However, how these EESes authenticate and authorize each other was not clearly defined.

Therefore, it is proposed to study authenticate and authorization between two EESes.

#### 5.3.6.2 Threats

If the S-EES is not authenticated and authorized by the T-EES, then the services of the T-EES can be consumed by unauthorized entities.

If the T-EES is not authorized by the S-EES, then the EEC application context can be sent to an entity not authorized to receive the information.

If the T-EES is not authenticated by the S-EES, then EEC context and in the application context can be revealed to unauthorized entities. Also, disruption of the service can happen.

#### 5.3.6.3 Potential security requirements

The S-EES and T-EES should mutually authenticate each other. Also, T-EES should authorize the S-EES and the T‑EES should be authorized to receive the information from the S-EES.

### 5.3.7 Key issue #2.7: EEC provided information verification

#### 5.3.7.1 Key issue details

Clause 8.6.5 of 3GPP TS 23.558 [11] defines UE identifier API which is used by an EAS or EEC to obtain the identifier of the UE if the EAS or EEC does not have it (e.g. has not already cached). This identifier, called UE ID (could be the GPSI or the EEL-generated Edge UE ID, defined in clause 7.2.6 of 3GPP TS 23.558 [11]), is used by the EAS to invoke capability APIs specific to UEs over EDGE-3 and/or EDGE-7 depending on the UE ID type.

The EES uses user information (e.g. IP address) received in the UE Identifier API invocation and obtains the UE identifier by interacting with NEF as specified in clause 4.15.10 of 3GPP TS 23.502 [9]. The EES may utilize the Nnef\_UEId\_Get service (clause 4.15.10 of 3GPP TS 23.502 [9]) providing the user information provided by the EEC, i.e. private UE IP address.

Since the user information (i.e. private UE IP address) may be used to determine the UE ID, it is needed to ensure that the user information is trusted, and the EEC is authorized to use this user information as a parameter in the API invocation.

This key issue is to study the security and privacy aspects of usage of user information provided by the EEC in the UE ID API invocation.

#### 5.3.7.2 Threats

If user information (i.e. the private UE IP address) provided by the EEC is not verified and the EEC is not authorized to use this information, a malicious or compromised EEC or a malicious API consumer can try to execute IP address spoofing attacks to learn identifiers of other UEs, including those they are not authorized to access. In this case, the EAS obtains an incorrect UE identifier, when the EAS use this incorrect UE identifier to invoke capability APIs specific to UE over EDGE-7, unauthorized information (e.g. UE location) belonging to another UE is exposed to the EAS.

#### 5.3.7.3 Potential security requirements

The user information (i.e. private UE IP address) provided by the EEC should be verified and the EEC should be authorized to use this information.

# 6 Proposed solutions

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

| Solutions | Key Issues | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1.1 | 1.2 | 2.1 | 2.2 | 2.3 | 2.4 | 2.5 | 2.6 | 2.7 |
| Solution #1: Authentication and authorization between EEC hosted in the roaming UE and ECS |  |  | x |  |  |  |  |  |  |
| Solution #2: Authentication and authorization between EEC hosted in the roaming UE and EES |  |  | x |  |  |  |  |  |  |
| Solution #3: Authentication mechanism selection between EEC and ECS |  |  |  | x |  |  |  |  |  |
| Solution #4: Authentication mechanism selection between EEC and EE |  |  |  | x |  |  |  |  |  |
| Solution #5: 5GC-based authentication mechanism selection between EEC and ECS/EES |  |  |  | x |  |  |  |  |  |
| Solution #6: ECS/EES authentication method information provisioning |  |  |  | x |  |  |  |  |  |
| Solution #7: Negotiation procedure for the Authentication and Authorization |  |  |  | x |  |  |  |  |  |
| Solution #8: Authentication mechanisms selected by ECS/EES |  |  |  | x |  |  |  |  |  |
| Solution #9: Authentication mechanism selection procedure between EEC and ECS |  |  |  | x |  |  |  |  |  |
| Solution #10: Authentication mechanism selection procedure between EEC and EES |  |  |  | x |  |  |  |  |  |
| Solution #11: Authentication mechanism selection procedure among EEC, ECS, and EES |  |  |  | x |  |  |  |  |  |
| Solution #12: Authorization for PDU session supporting local traffic routing to access an EHE in the VPLMN | x |  |  |  |  |  |  |  |  |
| Solution #13: A solution for authentication of EEC/UE and GPSI verification by EES/ECS |  |  | x |  |  |  |  |  |  |
| Solution #14: A solution for authentication of UE and GPSI verification by EES/ECS |  |  | x |  |  |  |  |  |  |
| Solution #15: Authentication algorithm selection procedure between EEC and ECS |  |  |  | x |  |  |  |  |  |
| Solution #16: Authentication algorithm selection procedure between EEC and EES |  |  |  | x |  |  |  |  |  |
| Solution #17: Using existing AKMA/GBA negotiation mechanism |  |  |  | x |  |  |  |  |  |
| Solution #18: Authentication and Authorization between V-ECS and H-ECS |  |  |  |  | x |  |  |  |  |
| Solution #19: Authorization of V-ECS in roaming scenario |  |  |  |  | x |  |  |  |  |
| Solution #20: Transport security for the EDGE10 interface |  |  |  |  |  | x |  |  |  |
| Solution #21: Using local policy on authorization between EESes |  |  |  |  |  |  |  | x |  |
| Solution #22: Using existing TLS 1.3 to perform negotiation mechanism |  |  |  | x |  |  |  |  |  |
| Solution #23: EAS discovery procedure protection |  | x |  |  |  |  |  |  |  |
| Solution #24: Public key signature based ECS/EES authentication |  |  | x |  |  |  |  |  |  |
| Solution #25: Utilizing Token-Based Solutions for EEC authentication |  |  | x | x |  |  |  |  |  |
| Solution #26: Using local policy on authorization between EESes |  |  |  |  |  |  |  | x |  |
| Solution #27: Token-based solution for authorization between EESes |  |  |  |  |  |  |  | x |  |
| Solution #28: Usage of randomly generated ticket to verify EEC provided IP address |  |  |  |  |  |  |  |  | x |
| Solution #29: Authorizing the Service Consumer when Resolving an IP Address to a UE ID |  |  |  |  |  |  |  |  | x |
| Solution #30: Usage of existing public IP address to verify EEC provided IP address |  |  |  |  |  |  |  |  | x |
| Solution #31: AKMA/GBA based verification of EEC provided IP address |  |  |  |  |  |  |  |  | x |
| Solution #32: KDF based verification of EEC provided IP address |  |  |  |  |  |  |  |  | x |
| Solution #33: Verification of EEC provided IP address |  |  |  |  |  |  |  |  | x |
| Solution #34: Verification of EEC provided IP address using access token |  |  |  |  |  |  |  |  | x |

## 6.1 Solution #1: Authentication and authorization between EEC hosted in the roaming UE and ECS

### 6.1.1 Solution overview

This solution addresses the KI #2.1 of the present document, in which the solution re-uses the existing GBA to support the mutual authentication procedure.

In edge computing scenarios, one UE may have multiple EECs. Each EEC hosted in UE should be authenticated and authorized by the ECS.

Moreover, to authenticate the EEC via correct network functions, ECS needs to know if UE is roaming. Specifically, without the correct serving network name of EEC/UE, ECS cannot connect to the correct network functions related to the authentication procedure.

To address the challenge, authentication and authorization between EEC hosted in the roaming UE and ECS are proposed.

### 6.1.2 Solution details



Figure 6.1.2-1: Authentication and authorization between EEC hosted in the roaming UE and ECS

It is assumed that UE(EEC) and ECS have selected the GBA with TLS as the authentication mechanism.

Step 0. UE is registered in the home network. UE obtains B-TID from BSF in the home network during the GBA procedure. By regarding the ECS as the NAF, according to 3GPP TS 33.220 [6], UE can calculate Ks\_NAF, Ks\_int\_NAF, and Ks\_ext\_NAF based on NAF ID of the ECS. UE selects one of them as the KECS. And UE can derive KEEC-ECS based on KECS and EEC ID. KEEC-ECS can be derived using KDF that is defined in Annex B of 3GPP TS 33.220 [6], where EEC ID is served as the input parameter and KECS is served as key that is utilized to derive KEEC-ECS.

Step 1. EEC sends provisioning request to the ECS. The provisioning request includes B-TID, encrypted EEC ID, and key indicator, where EEC ID is encrypted by KECS. Key indicator is a string (e.g. 'Ks\_int\_NAF') that is utilized to indicate the key type that is served as the KECS. EEC may also send GPSI to ECS via the provisioning request. MAC-I is the Message Authentication Code that is employed to protect the integrity of B-TID, encrypted EEC ID, GPSI (if provided), and key indicator. MAC-I can be built on Annex D of 3GPP TS 33.501 [7], where KECS is served as the integrity key.

Step 2. Upon receiving the provisioning request, ECS detects the home network of the UE based on the B-TID according to 3GPP TS 33.220 [6]. ECS should obtain UE information, which include the PLMN identifier where the UE is currently located, the access types that are utilized by the UE, and RAT types that are utilized by the UE. According to subclause 6.1.3.18 of 3GPP TS 23.503 [16], AF can obtain UE information from PCF using the event report procedure. And ECS can verify if UE is roaming by comparing the home network identifier with the PLMN identifier that is sent by PCF. Specifically, UE is roaming if Mobile Country Code and Mobile network Code in home network identifier are not identical to these in PLMN identifier that is sent by PCF. If EEC is not hosted in the roaming UE, the non-roaming authentication and authorization mechanism among EEC and ECS can be employed. Otherwise, the procedure goes to step 3.

Step 3. In UE roaming scenarios, according to 3GPP TS 33.220 [6], ECS needs to request KECS (i.e. KAF corresponding to ECS) via Zn-Proxy if ECS is connected to the serving network of UE. The authentication request includes the B-TID, NAF ID of the ECS and key indicator. In roaming scenarios, the ECS directly request KECS from BSF in the home network of UE/ECS if ECS is connected to the home network of UE.

Step 4. Zn-Proxy sends the authentication request to the BSF in the home network of the UE. The authentication request includes the B-TID, NAF ID of the ECS and key indicator.

Step 5. BSF derive the KECS according to the B-TID, NAF ID of the ECS and key indicator. BSF sends the KECS and the corresponding expiration time to the Zn-Proxy. In roaming scenarios, the BSF directly sends KECS to ECS if ECS is connected to the home network of UE.

Step 6. Zn-Proxy sends the KECS and KECS expiration time to the ECS.

Step 7. If MAC-I is received, ECS leverages the KECS and MAC-I to verify the integrity of the provisioning request message. If the provisioning request message is modified, ECS terminates the provisioning request procedure. Otherwise, ECS decrypt the EEC ID. EEC checks if the EEC is authorized to do the provisioning request operation based on the pre-configured policy. If the EEC is authorized, the procedure goes to step 8. Otherwise, ECS terminates the provisioning request procedure.

Step 8. Upon receiving the KECS, ECS derives the KEEC-ECS based on the KECS and EEC ID. KEEC-ECS can be derived using KDF that is defined in Annex B of 3GPP TS 33.220 [6], where EEC ID is served as the input parameter and KECS is served as key that is utilized to derive KEEC-ECS.

Step 9. Mutual authentication and TLS connection is realized based on clause 5 of 3GPP TS 33.222 [10], where KEEC-ECS is served as NAF key. ECS can also verify the GPSI of UE via UE identifier API.

Step 10. ECS generates token for the EEC after the EEC is authenticated and TLS connection is established. The token is sent to UE through secure TLS connection. ECS authorize EEC based on the pre-configureed policies. Considering EEC and GPSI of UE are successfully authenticated by the ECS, the EES service tokens may include the ECS FQDN (issuer), EEC ID and GPSI (subject), expected EES service name(s) (Scope), EES FQDN (audience), expiration time (expiration), the digital signature generated by the ECS.

### 6.1.3 Solution evaluation

ECS can verify if EEC is hosted in a roaming UE based on B-TID and UE information that is obtained from PCF.

Mutual authentication between EEC and ECS can be realized based on KEEC-ECS.

ECS authorizes EEC based on the pre-configured policies.

The solution is realized based on GBA.

## 6.2 Solution #2: Authentication and authorization between EEC hosted in the roaming UE and EES

### 6.2.1 Solution overview

This solution addresses the KI #2.1 of the present document.

This solution reuses the existing GBA mechanism to support the mutual authentication procedure.

In edge computing scenarios, one UE may have multiple EECs. Each EEC hosted in UE should be authenticated and authorized by the EES.

Moreover, to authenticate the EEC via correct network functions, EES needs to know if UE is roaming. Specifically, without the correct serving network name of EEC/UE, ECS cannot connect to the correct network functions related to the authentication procedure.

Since EEC may authorized by ECS to request services from EES, EES needs to support verify the token that is generated by the ECS.

To address the challenge, authentication and authorization between EEC hosted in the roaming UE and EES are proposed.

### 6.2.2 Solution details



Figure 6.2.2-1: Authentication and authorization between the EEC and EES based on Zn-Proxy

It is assumed that EES is deployed in the 3GPP operator domain and trusted by the 3GPP operator.

It is assume that EES has obtained certificate or public key of ECS.

It is assumed that UE(EEC) and EES have selected the GBA with TLS as the authentication mechanism.Step 0. UE is registered in the home network. UE obtains B-TID from BSF in the home network during the GBA procedure. By regarding the ECS as the NAF, according to 3GPP TS 33.220 [6], UE can calculate Ks\_NAF, Ks\_int\_NAF, and Ks\_ext\_NAF based on NAF ID of the EES. UE selects one of them as the KEES. And UE can derive KEEC-EES based on KEES and EEC ID. KEEC-EES can be derived using KDF that is defined in Annex B of 3GPP TS 33.220 [6], where EEC ID is served as the input parameter and KEES is served as key that is utilized to derive KEEC-EES.

Step 1. EEC sends EEC registration request to the EES. The request includes B-TID, encrypted EEC ID, and key indicator, where EEC ID is encrypted by KEES. Key indicator is a string (e.g. 'Ks\_int\_NAF') that is utilized to indicate the key that is served as the KEES. EEC may also send GPSI to EES via the provisioning request. If ECS authorize EEC to access EES via the token, ECC will send the token to the EES via the provisioning request. MAC-I is the Message Authentication Code that is employed to protect the integrity of B-TID, encrypted EEC ID, GPSI (if provided), key indicator, and the token (if provided by ECS). MAC-I can be built on Annex D of 3GPP TS 33.501 [7], where KEES is served as the integrity key. The generation of MAC-I is optional.

Step 2. Upon receiving the provisioning request, EES detects the home network of the UE based on the B-TID according to 3GPP TS 33.220 [6]. ECS should obtain UE information, which include the PLMN identifier where the UE is currently located, the access types that are utilized by the UE, and RAT types that are utilized by the UE. According to subclause 6.1.3.18 of 3GPP TS 23.503 [16], EES can obtain UE information from PCF using the event report procedure. And EES can verify if UE is roaming by comparing the home network identifier with the PLMN identifier that is sent by PCF. Specifically, UE is roaming if Mobile Country Code and Mobile network Code in home network identifier are not identical to those in PLMN identifier that is sent by PCF. If EEC is not hosted in the roaming UE, the non-roaming authentication and authorization mechanism among EEC and EES can be employed. Otherwise, the procedure goes to step 3.

Step 3. In UE roaming scenarios, according to 3GPP TS 33.220 [6], EES needs to request KEES­ (i.e. KAF corresponding to EES) via Zn-Proxy if EES is connected to the serving network of UE. The authentication request includes the B-TID, NAF ID of the EES and key indicator. In roaming scenarios, the EES directly request KEES from BSF in the home network of UE/ECS if EES is connected to the home network of UE.

Step 4. Zn-Proxy sends the authentication request to the BSF in the home network of the UE. The authentication request includes the B-TID, NAF ID of the EES and key indicator.

Step 5. BSF derives the KEES according to the B-TID, NAF ID of the EES and key indicator. BSF sends the KEES and the corresponding expiration time to the Zn-Proxy. In roaming scenarios, the BSF directly sends KEES to EES if EES is connected to the home network of UE.

Step 6. Zn-Proxy sends the KEES and KEES expiration time to the EES.

Step 7. If MAC-I is received, EES leverages the KEES and MAC-I to verify the integrity of the provisioning request message. If the provisioning request message is modified, EES terminates the provisioning request procedure. Otherwise, EES decrypts the EEC ID.

Step 8. Upon receiving the KEES, EES derives the KEEC-EES based on the KEES and EEC ID. KEEC-EES can be derived using KDF that is defined in Annex B of 3GPP TS 33.220 [6], where EEC ID is served as the input parameter and KEES is served as key that is utilized to derive KEEC-EES.

Step 9. Mutual authentication and TLS connection can be realized based on KEEC-EES. Specifically, the mutual authentication and TLS connection is realized based on clause 5 of 3GPP TS 33.222 [10], where KEEC-EES is served as NAF key.

Step 10. EES authorizes EEC for the requested service. The EEC authorization is processed based on pre-configured policies or the token provided by the EEC. For the pre-configured policies based EEC authorization case, EES authorizes the EEC if the EEC registration request message matches the pre-configured policies. For the token-based EEC authorization case, the EES first checks if the token is expired. If the token is not expired, EES verifies the ECS digital signature in the token using the public key or certificate of ECS. Otherwise, EES rejects the request. If ECS digital signature in the token is successfully verified, EES checks against EEC ID, GPSI (if provided), and requested EES service name(s) against the token claims. If the information is matched, EES authorizes EEC to access the requested service. Otherwise, EES rejects the request.

Step 11. EES sends the authorization result via the EEC registration response message.

### 6.2.3 Solution evaluation

EES can verify if EEC is hosted in a roaming UE based on B-TID and UE information that is obtained from PCF.

Mutual authentication between EEC and EES can be realized based on KEEC-EES.

EES authorizes EEC based on the pre-configured policies or tokens that are generated by EEC.

The solution is realized based on GBA.

## 6.3 Solution #3: Authentication mechanism selection between EEC and ECS

### 6.3.1 Solution overview

This solution proposes a mechanism to select one of the authentication method(s) supported by Home network and indicate the same to the EEC addressing the security requirements of key issue#2.2.

### 6.3.2 Solution details

#### 6.3.2.0 Authentication mechanism selection between EEC and ECS



Figure 6.3.2-1: Authentication mechanism selection between EEC and ECS

Step 1. The 3GPP network provides the ECS configuration information to the EEC as specified in 3GPP TS 23.558 [11]. The ECS configuration information includes the ECS address, ECS provider identifier and authentication method(s) selected by HN and SN.

Step 2. The UE determines the authentication method based on the information received in ECS configuration information. The selection of the authentication method by the UE, EEC, 3GPP network and the ECS can be as follows:

- If more than one authentication methods are supported, the authentication method selected by EEC, HN and SN based on the operator or local policy is selected.

- If one authentication method is selected and indicated then the same should be used by the UE, EEC, HN and SN.

- If no supported authentication method in common, then a default authentication method has to be selected. Defining default authentication method is based on operator policy.

Step 3. The UE sends the initial provisioning request to the ECS. The initial provisioning request includes the relevant parameter (e.g. A-KID or B-TID or OAuth Token) based on the selected authentication method.

Step 4. The UE and the ECS performs the authentication using the selected authentication method.

#### 6.3.2.1 ECS configuration

Table 6.3.2.1-1 describes the information elements of ECS configuration information as specified in clause 8.3.2.1, table 8.3.2.1-1 of 3GPP TS 23.558 [11], with an additional IE to indicate selected authentication method.

Table 6.3.2.1-1: ECS configuration information per ECS

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| ECS address | M | Endpoint information of ECS (e.g. URI, FQDN, IP address) |
| ECSP Identifier | O | The identifier of the ECSP (e.g. the MNO or a 3rd party service provider) that provides the ECS |
| Spatial Validity Conditions | O | Spatial validity condition, as described in 3GPP TS 23.548 [15] |
| Authentication Method | M | Selected authentication method (for example, TLS with client-server certificate-based, AKMA, GBA) |
| NOTE: This IE shall be included when the ECS configuration information is provisioned by the MNO through the 5GC procedure. | | |

### 6.3.3 Solution evaluation

This solution addresses the security requirement from Key issue#2.2 i.e. selection of authentication mechanism for authentication procedures between EEC and ECS.

In this solution the decision or selection of the authentication method is determined based on the UE, EEC, home network and serving network capability. The selected authentication is indicated to the EEC in ECS configuration information provisioned per ECS. The solution requires a mechanism to provision the HPLMN capability to the UE.

## 6.4 Solution #4: Authentication mechanism selection between EEC and EES

### 6.4.1 Solution overview

This solution proposes a mechanism to select one of the authentication methods supported by Home network and indicate the same to the EEC addressing the security requirements of key issue#2.2.

### 6.4.2 Solution details

#### 6.4.2.0 EES registration



Figure 6.4.2-1: EES indicates the supported authentication method in  
EES profile during the EES registration

Step 1. The EES sends the EES registration request to the ECS. The request from the EES includes the EES profile, EES security credentials and the supported authentication method(s) by the EES.

Step 2. Upon receiving the request from the EES, the ECS verifies the security credentials of the EES and stores the EES registration information obtained in step 1.

Step 3. The ECS sends an EES registration response indicating success or failure of the registration operation.

During service provisioning, the ECS responds to the EEC's request with a service provisioning response which includes a list of EDN configuration information, e.g. identification of the EDN, EDN service area, the required information (e.g. URI, IP address) for establishing a connection to the EES and authentication method selected. ECS selects the authentication method between the EEC and EES based on the authentication method(s) supported by the UE, EEC, EES, HN and SN. ECS gets the information on the home network and serving network supported authentication method(s) from the core network. The NEF exposes the network supported authentication method.

#### 6.4.2.1 EES profile

Table 6.4.2.1-1 describes the information elements of EES profile as specified in clause 8.2.6, table 8.2.6-1 of 3GPP TS 23.558 [11], with additional IE to indicate selected authentication method.

Table 6.4.2.1-1: EES Profile

|  |  |  |
| --- | --- | --- |
| Information element | Status | Description |
| EESID | M | The identifier of the EES. |
| EES Endpoint | M | Endpoint information (e.g. URI, FQDN, IP address) used to communicate with the EES. This information is provided to the EEC to connect to the EES. |
| EASIDs | M | List of EASIDs registered with the EES. |
| EEC registration configuration | M | Indicates whether the EEC is required to register on the EES to use edge services or not. |
| EES Provider Identifier | O | The identifier of the ECSP that provides the EES Provider. |
| EES Topological Service Area | O | The EES serves Ues that are connected to the Core Network from one of the cells included in this service area. EECs in Ues that are located outside this area shall not be served. See possible formats in table 8.2.7-1 of TS 23.558 [11]. |
| EES Geographical Service Area | O | The area being served by the EES in Geographical values (as specified in clause 7.3.3.3 of TS 23.558 [11]). |
| List of EES DNAI(s) | O | DNAI(s) associated with the EES. This IE is used as Potential Locations of Applications in clause 5.6.7 of 3GPP TS 23.501 [2].  It is a subset of the DNAI(s) associated with the EDN, where the EES resides. |
| EES Service continuity support | O | Indicates if the EES supports service continuity or not. This IE also indicates which ACR scenarios are supported by the EES. |
| Authentication Method | M | Supported Authentication method (for example, client-server certificate-based, AKMA & GBA). |

### 6.4.3 Solution evaluation

This solution addresses the security requirement from Key issue#2.2, i.e. selection of authentication mechanism for authentication procedures between EEC and EES.

In this solution the decision or selection of the authentication method is determined based on the UE, EEC, home network and serving network. EES indicates the supported authentication method(s) to the ECS in the EES profile. The NEF exposes the authentication method supported by the network. The solution requires a new service provided by the NEF. The ECS then selects the authentication method based on UE, EEC, EES, HN and SN and then indicates the selected authentication method to the EEC in the service provisioning response.

## 6.5 Solution #5: 5GC-based authentication mechanism selection between EEC and ECS/EES

### 6.5.1 Solution overview

This solution addresses KI 2.2 of the present document.

To select TLS with GBA/AKMA based authentication methods, EES/ECS needs to support GBA/AKMA protocol. However, in some cases, EES/ECS cannot select TLS with GBA/AKMA based authentication methods even if EEC/ECS can support GBA/AKMA protocol.

Specifically, in TLS with GBA/AKMA based authentication methods, EES/ECS takes the role of NAF or AF. To do the mutual authentication between EES/ECS and ECC, EES/ECS needs to obtain keys (e.g. KAF in AKMA scenarios) from 5GC. However, EES/ECS may fail to obtain keys from 5GC. For instance, according to subclause 6.2.1 of 3GPP TS 33.535 [8], it is stated that "*The AanF shall check whether the AanF can provide the service to the AF based on the configured local policy or based on the authorization information or policy provided by the NRF using the AF\_ID. If it succeeds, the following procedures are executed. Otherwise, the AanF shall reject the procedure.* ". According to clause J.2 of 3GPP TS 33.220 [6], it is stated that "*In any case, the GAA based security setup will fail between the UE and the NAF since the NAF did not get the NAF specific shared key(s)*". And EES/ECS without keys cannot support TLS with GBA/AKMA based authentication methods.

Therefore, ECS/EES needs to ensure it can obtain keys from 5GC during the selection of the authentication method between EEC and ECS/EES.

To address the problem, the 5GC-based authentication mechanism selection between EEC and ECS/EES is proposed.

### 6.5.2 Solution details



Figure-6.5.2.1: Authentication method selection between EEC and ECS/EES

It is assumed that the negotiation messages between EEC and ECS/EES are protected by TLS 1.3.

Step 1. The EEC sends the authentication method selection request to the ECS/EES. EEC sends the authentication method identifiers (e.g. TLS with AKMA , TLS with GBA) and the types of key(e.g. Ks\_int\_NAF) that it supports in this message, EEC may send A-KID or B-TID to ECS/EES in the authentication method selection request message.

Step 2. Upon receiving authentication method selection request, ECS/EES choose an authentication method based on the authentication methods that the EEC supports and its pre-configured policies. The policies may contain the priority of the network supported authentication methods configured by 3GPP operators or ECS/EES providers. The ECS/EES may select the authentication method based on the priority of the network supported authentication methods.

Step 3a. If ECS/EES selects AKMA or GBA based authentication method, ECS/EES needs to request authentication key from AANF or BSF in the home network of UE/EEC. Otherwise, the procedure goes to step 3b. ECS/EES identifies the home network of the UE/EEC based on the A-KID/B-TID. The authentication key is KAF of EEC/EES when ECS/EES chooses AKMA-based authentication method. The authentication key is NAF key of EEC/EES when ECS/EES chooses GBA-based authentication method. Details about the authentication key request procedure depend on the selected authentication method. If ECS/EES can obtain authentication key corresponding to the selected authentication method, ECS/EES can determine to use the selected method to do the authentication. For the case that ECS/EES chooses AKMA or GBA based authentication method, ECS/EES needs to exclude the selected method and re-select the authentication method if ECS/EES cannot obtain the authentication key. To re-select the authentication method, the procedure goes to step 2. And ECS/EES needs to skip the authentication method that it excludes in step 3a during the re-select procedure.

Step 3b. ECS/EES sends the selected authentication method to the UE/EEC via the authentication mechanism selection response message. ECS/EES needs to send the error code to the UE/EEC when ECS/EES cannot support any authentication methods provided by the UE/EEC.

### 6.5.3 Solution evaluation

In this solution, ECS/EES can re-select authentication mechanism when ECS/EES cannot obtain keys related to the selected authentication method from 5GC.

Before choosing authentication mechanism related to AKMA/GBA, ECS/EES needs to obtain key related to AKMA/GBA from 5GC. The obtaining of keys related to AKMA/GBA from 5GC implicitly indicates the security capability of 5GC.

## 6.6 Solution #6: ECS/EES authentication method information provisioning

### 6.6.1 Solution overview

This solution addresses KI#2.2: Authentication mechanism selection between EEC and ECS/EES.

During the PDU session establishment procedure, UE that hosts EEC(s) receives ECS/EES authentication method information (e.g. via PCO) and determines which to use.

### 6.6.2 Solution details

If the UE hosts an EEC and supports transferring the ECS/EES authentication method information from the 5GC to the EEC, the UE indicates in the PCO at PDU Session establishment that it supports the ability to receive ECS address(es) via NAS and to transfer the ECS Address(es) to the EEC(s) (see 3GPP TS 23.502 [9]). As described in 3GPP TS 23.502 [9], if the UE supports the ability to receive ECS/EES authentication method information via NAS and to transfer the ECS/EES authentication method information to the EEC(s), the UE may receive ECS/EES authentication method information from the SMF via PCO during PDU Session Establishment and/or during PDU Session Modification procedures.

The SMF may receive ECS/EES authentication method information from the UDM together with SM subscription information. The UDM in the HPLMN may provide the SMF with ECS/EES authentication method information. Or the ECS/EES authentication method information is preconfigured in the SMF, for example, in H-SMF for HR case or V-SMF for LBO cases.

The SMF determines the ECS/EES authentication method information to be sent to the UE based on UE subscription information received from UDM (as described in clause 4.15.6.3d-2 of 3GPP TS 23.502 [9]).

According to the ECS/EES authentication method information received from SMF (via PCO), UE selects TLS authentication methods both supported by EEC and ECS/EES. If there is no authentication methods supported by both sides, it returns failure.

If the UE has already done an edge computing service in the home network, the UE stores the selected TLS authentication method. While roaming, after receiving the ECS/EES authentication method information from SMF (via PCO), the UE checks if the selected TLS authentication method is supported by ECS/EES. If the selected TLS authentication method is not supported, it returns failure.

### 6.6.3 Solution evaluation

This solution has the following impacts:

- UE: UE that hosts EEC(s) use the indicator (e.g. PCO) to indicate that it supports the ability to receive ECS/EES authentication information. According to the received ECS/EES authentication information, UE selects TLS authentication methods supported by both sides. UE that hosts EEC(s) stores the TLS authentication method used in the home network.

- SMF: The ECS/EES authentication method information may be preconfigured in the SMF. SMF provides ECS/EES authentication information to UE.

NOTE: This solution requires a method to provision an ordered list for authentication mechanism supported by HPLMN to the UE (EEC).

## 6.7 Solution #7: Negotiation procedure for the Authentication and Authorization

### 6.7.1 Solution overview

This contribution addresses key issue #2.2 "Authentication mechanism selection between EEC and ECS/EES".

### 6.7.2 Solution details

The negotiation procedure is as follows in figure 6.7.2-1.

Graphical user interface, text, application

Description automatically generated

Figure 6.7.2-1: Negotiation Procedure for the Authentication and  
Authorization between EEC and ECS

Step 0. Primary authentication is performed as defined in 3GPP TS 33.501 [7]. After this step, UE is successfully registered into the 5GS network.

Step 1. UE sends the EEC Registration Request message as defined in 3GPP TS 23.558 [11], which includes the list of UE supporting authentication mechanisms. The potential authentication mechanisms list includes TLS with AKMA, TLS with GBA, TLS with certificate, or other mechanisms if any. The order in the list indicates the priority of the UE preference.

When UE supports AKMA or GBA, UE shall include the corresponding Key ID (A-KID or B-TID) in the EEC registration request, which could implicitly indicate HPLMN supports AKMA and UE has subscribed with AKMA service.

Step 2. ECS selects one authentication method from the list of UE supporting authentication mechanisms based on local policy. If there is no shared authentication mechanisms between EEC and network, the network could cease the authentication, and the following steps from step 3 will not take place.

Step 3. If there is shared authentication mechanism, and ECS successfully chose one in Step 2, then ECS sends the EEC registration response including the chosen authentication mechanism to UE.

Step 4.1. After receiving the response from ECS in step 3, UE prepares for the authentication procedure according to the chosen authentication mechanism. E.g. generating AKMA/GBA keys or key for other mechanisms. The procedures to derive the credentials follow the 3GPP TS 33.535 [8] for AKMA, 3GPP TS 33.220 [6] for GBA, IETF RFC 8446 [12] for TLS 1.3.

Step 4.2. After sending the response to UE in step 3, network prepares for the authentication procedure according to the chosen authentication mechanism. E.g. generating AKMA/GBA keys or generating certificates. The procedures follow the 3GPP TS 33.535 [8] for AKMA, 3GPP TS 33.220 [6] for GBA, IETF RFC 8446 [12] for TLS 1.3.

### 6.7.3 Solution evaluation

This solution is not evaluated.

## 6.8 Solution #8: Authentication mechanisms selected by ECS/EES

### 6.8.1 Solution overview

This solution addresses the Key Issue #2.2.

### 6.8.2 Solution details

#### 6.8.2.0 General

The selection of the authentication methods between EEC and ECS/EES is under the control of the entities operating ECS/EES.

#### 6.8.2.1 Authentication between EEC and ECS

The authentication between EEC and ECS is performs thanks to the execution of TLS handshake protocol with authentication method selected by the ECS. The authentication method selected by the ECS for TLS handshake is configured in the EEC or sent to the EEC.

At the end of the procedure for authentication and authorization between the EEC and the ECS, the ECS sends to the EEC the service response that includes EES authentication capability for authentication between the EEC and the EES. The EES authentication capability for authentication indicates the authentication method selected by the EES for the TLS handshake.

NOTE: How to consider security capabilities of Ues and PLMNs in the negotiation is not addressed in the present document.

#### 6.8.2.2 Authentication between EEC and EES

The authentication between EEC and EES is performed thanks to the execution of TLS handshake protocol with authentication method indicated in EES authentication capability, which was sent at the end of the authentication and authorization procedure between the EEC and the ECS.

NOTE: How to consider security capabilities of Ues and PLMNs in the negotiation is not addressed in the present document.

### 6.8.3 Solution evaluation

This solution is not evaluated.

## 6.9 Solution #9: Authentication mechanism selection procedure between EEC and ECS

### 6.9.1 Solution overview

This solution addresses security requirement for authentication mechanism selection between EEC and ECS in key issue #2.2.

### 6.9.2 Solution details

For authentication between EEC and ECS, EEC and ECS should support TLS with certificates by default, and optionally support, TLS with AKMA as specified in 3GPP TS 33.535 [8], TLS with GBA as specified in 3GPP TS 33.222 [10]. And the detail of TLS authentication method selection needs to be addressed.

To support authentication between the EEC and ECS, the EEC and the ECS should be configured with the security capability according to the local configuration (TLS with certificates by default, TLS with AKMA [8], and TLS with GBA [6], optionally supported).

Before the authentication mechanism selection procedure between EEC and ECS, the EEC should be pre-configured with or have discovered the address (e.g. URI) of the ECS as specified in clause 8.3.2 of 3GPP TS 23.558[11]. There is a list for authentication mechanism supported by HPLMN, which is ordered according to a priority based on operator's security policy. The EEC obtains the HPLMN supported mechanism list during registration, and chooses the authentication mechanism with highest priority based on HPLMN supported mechanism list and its security capability. The shared key-based authentication with certificate-based AF authentication or shared key-based mutual authentication using TLS between UE and AF as specified in Annex B of 3GPP TS 33.535[8] or clauses 5.3 and 5.4 of 3GPP TS 33.222[10] is used for the authentication mechanism selection. In this case, EEC takes the role of UE and ECS takes the role of AF respectively.

### 6.9.3 Solution evaluation

This solution addresses KI#2.2 by authentication mechanism selection between EEC and ECS.

This solution based on TLS authentication protocols introduces no impact to network entities and existing procedures.

This solution requires a method to provision an ordered list for authentication mechanism supported by HPLMN to the UE (EEC).

In this solution, TLS with certificates is adopted as the default authentication for EEC and ECS.

## 6.10 Solution #10: Authentication mechanism selection procedure between EEC and EES

### 6.10.1 Solution overview

This solution addresses security requirement for authentication mechanism selection between EEC and EES in key issue #2.2.

### 6.10.2 Solution details

For authentication between EEC and EES, should support TLS with certificates by default, and optionally support TLS with AKMA as specified in 3GPP TS 33.535 [8], TLS with GBA as specified in 3GPP TS 33.222 [10]. And the detail of TLS authentication method selection needs to be addressed.

To support authentication between the EEC and EES, the EEC and the EES should be set with the security capability according to the local configuration (TLS with certificates by default, TLS with AKMA [6], TLS with GBA [8] and, or other TLS authentication methods optionally supported).

Before the authentication mechanism selection procedure between EEC and EES, the EEC should be configured with the address (e.g. URI) of the EES by the ECS as defined in clause 8.3.3 of 3GPP TS 23.558[11]. There is a list for authentication mechanism supported by HPLMN, which is ordered according to a priority based on the operator's security policy. The EEC obtains the HPLMN supported mechanism list during registration, and chooses the authentication mechanism with highest priority based on HPLMN supported mechanism list and its security capability. The shared key-based authentication with certificate-based AF authentication or shared key-based mutual authentication using TLS between UE and AF as specified in Annex B of 3GPPTS 33.535[8] or clauses 5.3 and 5.4 of 3GPPTS 33.222[10] is used for the authentication mechanism selection. In this case, EEC takes the role of UE and EES takes the role of AF respectively.

### 6.10.3 Solution evaluation

This solution addresses KI#2.2 by authentication mechanism selection between EEC and EES.

This solution based on TLS authentication protocols introduces no impact to network entities and existing procedures.

This solution requires a method to provision an ordered list for authentication mechanism supported by HPLMN to the UE (EEC).

In this solution, TLS with certificates is adopted as the default authentication for EEC and EES.

## 6.11 Solution #11: Authentication mechanism selection procedure among EEC, ECS, and EES

### 6.11.1 Solution overview

This solution addresses security requirement for authentication mechanism selection between EEC and ECS, EEC and EES in key issue #2.2.

### 6.11.2 Solution details

The EEC should be configured with the security capability according to the local configuration. The EEC should support TLS with certificates by default, and should optionally support TLS with AKMA [6] and, TLS with GBA [8]). The ECS and EES should be separately configured via network management with mechanisms that are are allowed the ECS and EES should support TLS with certificates by default and optionally support TLS with AKMA [6] and TLS with GBA [8].

The EES provides the supported authentication mechanism(s) to the ECS during the EES registration procedure in clause 8.4.4.2.2 in 3GPP TS 23.558[11], and the ECS stores the security capability of the registered EES.

The ECS provisions the Edge configuration information to the EEC which contains the information for establishing a connection with EESs (such as URI), in the Service provisioning procedure as specified in clause 8.3.3 of 3GPP TS 23.558[11]. ECS helps the authentication mechanism selection between EEC and EES, and contains the selection result in the Edge configuration information, to establish the security connection between EEC and EES.



Figure 6.11.2-1: Procedure for authentication mechanism selection among EEC, EES, and ECS

Step 0a: There is a list for authentication mechanism supported by HPLMN, which is ordered according to a priority based on operator's security policy. The edge enabled UE (EEC) obtains the HPLMN supported mechanism list during registration.

Step 0b: The EEC is pre-configured with or has discovered the address (e.g. URI) of the ECS.

Step 1. The EEC chooses an authentication mechanism with the highest priority based on the HPLMN supported mechanism list and its security capability, and sends an Authentication Mechanism Selection Request message to the ECS, including EEC security capability, the chosen authentication mechanism, and may include the UE identifier such as GPSI, connectivity information, UE location and AC profile(s) information. Step 2a. The ECS stores the security capability of EEC, and checks if it supports the authentication mechanism chosen by EEC.

Step 2b. The ECS may utilize the capabilities (e.g. UE location) of the 3GPP core network or the profile(s) provided by the EEC, to identify the EES as specified in clause 8.3.3.2 of 3GPP TS 23.558[11]. With the security capability of the identified EES stored in EES registration, and the receiving security capability of the EEC in step 1, the ECS checks if the identified EES supports the authentication mechanism chosen by EEC.

Step3. The ECS sends the Authentication Mechanism Selection Request message to the identified EES, including EEC security capability, and the authentication mechanism chosen by EEC. If not, the step 6 and step 7 can be skipped.

Step4. If ECS supports any mechanism in EEC's security capability, ECS may use the authentication mechanism EEC chooses or another mechanism in EEC's security capability (e.g. based on local policy), ECS should sends EEC the Authentication Mechanism Selection completes message including the selection result. Otherwise the ECS should reply with a failure indication.

ECS helps the identified EES to select the authentication mechanism based on the security capability of EEC and EES, and authentication mechanism chosen by EEC and HPLMN., and the selection result of ECS should be contained in the Edge configuration information, and provide to the EEC in the Service provisioning procedure as specified in clause 8.3.2.2 of 3GPP TS 23.558 [11], for the EEC to establish security connection with the EES. If the EES could not support any mechanism in EEC's security capability, ECS sends a failure indication to EEC.

Step5. Upon receiving the Authentication Mechanism Selection Complete message from ECS with the selection result, EEC starts using the mechanism indicated in selection result to authenticate and establish TLS connection with ECS. Otherwise the authentication mechanism selection failed between EEC and ECS.

Step6. After the authentication and TLS connection establishment between EEC and ECS, the ECS sends back EEC's security capability and chosen mechanism to the EEC, and this message can be security protected by the TLS context. Thus, the EEC can verify the message had not been tampered with. The EES stores the security capability of EEC, and checks if it supports the authentication mechanism chosen by EEC.

Step 7. If EES supports any mechanism in EEC's security capability, EES uses the authentication mechanism EEC chooses or another mechanism in EEC's security capability (e.g. based on local policy), EES sends EEC the Authentication Mechanism Selection Response message including the selection result. If EES does not support any of the authentication mechanisms as indicated by EEC's security capability, the ECS replies with a failure indication.

### 6.11.3 Solution evaluation

This solution addresses the security requirement of KI #2.2 i.e. selection of authentication mechanism for authentication procedures between EEC and ECS/EES.

This solution reuses the existing signalling and processes (i.e. EES registration and ECS service provisioning as specified in clause 8.4.4 and clause 8.3.3 of 3GPP TS 23.558 [11]) in ECS helping the authentication mechanism selection between EEC and EES. Specifically, The EES provides the supporting mechanism to the ECS during the EES registration. After receiving the authentication mechanism chosen by EEC and EEC's security capability, the ECS can choose the authentication mechanism supported by EEC and EES, then provide the selection result as Edge configuration information to the EEC. Therefore, this solution can reduce signalling overhead comparing with separately negotiation method.

This solution requires a method to provision an ordered list for authentication mechanism supported by HPLMN to the UE (EEC).

In this solution, TLS with certificates is adopted as the default authentication for EEC, ECS and EES.

## 6.12 Solution #12: Authorization for PDU session supporting local traffic routing to access an EHE in the VPLMN

### 6.12.1 Introduction

The following solution addresses the security requirement for the key issue #1.1 How to authorize PDU session to support local traffic routing to access an EHE in the VPLMN.

### 6.12.2 Solution details

Two scenarios have been defined in 3GPP TR 23.700-48 [2]: accessing EHE via LBO PDU Session or via HR PDU Session.

According to the current PDU establishment procedure, the secondary authentication can be used for PDU session authorization irrespective of whether it is an LBO or HR PDU session. Hence, it is suggested to reuse the secondary authentication for key issue #1.1.

For the first scenario, the existing mechanism defined in 3GPP TS 33.501 [7] that uses the subscription data for the authorization and secondary authentication if necessary can be reused for the PDU session authorization.

For the second scenario, enhanced authorization on whether to support local traffic routing to access EHE is required according to the subscription data besides the existing mechanism defined in 3GPP TS 33.501 [7] for the first scenario.

NOTE: The authorization on whether to support local traffic routing to access EHE in the HR PDU session can be left to the agreement in 3GPP TR 23.700-48 [2].

### 6.12.3 Solution evaluation

The proposed solution meets all the requirements of key issue #1.1. The solution reuses the already specified secondary authentication for authorization between UE and Edge Data Network, and the potential authorization enhancement based on subscription in 3GPP TR 23.700-48 [2]. Hence, there is no impact of the existing security procedures.

## 6.13 Solution #13: A solution for authentication of EEC/UE and GPSI verification by EES/ECS

### 6.13.1 Solution overview

This solution addresses the key issue #2.1 where it is stated that EEC/UE authentication is required considering both the roaming and non-roaming cases. EEC authentication means verification of the EEC ID sent from the EEC to the ECS/EES while UE authentication means verification of the GPSI of the UE that hosts the EEC communicating with the ECS/EES.

The solution proposes usage of AKMA for UE and EEC authentication by the ECS/EES. In addition to the AKMA usage for UE authentication, this solution uses AF Specific UE ID retrieval API as an optional solution to authenticate the UE, i.e. to verify the GPSI.

### 6.13.2 Solution details

The procedure flow of the solution is depicted in figure 6.13.2-1 and the steps are explained below. The solution assumes that there is a mechanism in the UE to authenticate the EEC.



Figure 6.13.2-1: Authentication of EEC and UE by ECS/EES

Step 0. UE and HPLMN run primary authentication and derive KAKMA. UE learns the A-KID and KAKMA.

Step 1. KAF is derived as defined in AKMA procedure. KEEC is derived from KAF and EEC-ID as KEEC = KDF(KAF, EEC-ID). KEEC and E(KAF, EEC-ID) are revealed to the EEC where E(KAF, EEC-ID) is the encryption of EEC-ID under the key KAF.

The EEC ID is authenticated in the UE with a method out of the scope of this solution, e.g. by the operating system running in the UE. Since the KEEC derived from the EEC ID is revealed only to the authenticated EEC having the EEC ID, the EES/ECS will ensure that the EEC is the client having the EEC ID after driving the KEEC from the EEC ID.

If the EEC ID is sent over a secure channel between EEC and EES/ECS, then no additional encryption for it is necessary.

Step 2. The EEC sends a session establishment request to the ECS/EES, including the parameters A-KID, E(KAF, EEC-ID).

Step 3. The EES/ECS request KAF from the network. In this request, ECS/EES sends A-KID and ECS-ID/EES-ID.

Step 4. The network executes the authentication and authorization for the ECS/EES as defined in the AKMA procedure and if the result is successful then derives the KAF such that KAF = KDF (KAKMA, ECS-ID/EES-ID).

Step 5. The network sends KAF, expire time for the key and and optionally GPSI to the ECS/EES.

Step 6. Using the KAF key, the ECS/EES decrypts the encrypted EEC-ID and also derives KEEC such that KEEC = KDF(KAF, EEC-ID).

Step 7. The EEC and the ECS/EES use KEEC in Ua\* protocol, instead of KAF.

If the EEC sends GPSI to the ECS/EES, then the ECS/EES verifies the received GPSI using the GPSI received from the network via AKMA or via UE ID API.

### 6.13.3 Solution evaluation

This solution addresses key issue #2.1 by proposing a mechanism for authentication of both the EEC and UE by the ECS/EES. The authentication of the EEC by the ECS/EES relies on the authentication of the EEC by the UE with a method out of the scope of this solution.

This solution doesn't have any impact on the existing AKMA mechanism.

This solution also proposes two alternative methods for validation of the GPSI, by the ECS/EES, which is optionally sent by the EEC to the ECS/EES. These methods are re-using the existing AKMA and UE ID retrieval API.

## 6.14 Solution #14: A solution for authentication of UE and GPSI verification by EES/ECS

### 6.14.1 Solution overview

This solution addresses the key issue #2.1 where it is stated that UE authentication is required considering both the roaming and non-roaming cases. UE authentication means verification of the GPSI of the UE that hosts the EEC communicating with the ECS/EES.

The solution proposes usage of AKMA for UE authentication by the ECS/EES. In addition to the AKMA usage for UE authentication, this solution uses AF Specific UE ID retrieval API as an optional solution to authenticate the UE, i.e. to verify the GPSI.

### 6.14.2 Solution details

The procedure flow of the solution is depicted in figure 6.14.2-1 and the steps are explained below.



Figure 6.14.2-1: Authentication of EEC and UE by ECS/EES

Step 0. UE and HPLMN run primary authentication and derive KAKMA. UE learns the A-KID and KAKMA.

Step 1. KAF is derived as defined in AKMA procedure and revealed to the EEC.

Step 2. The EEC sends a session establishment request to the ECS/EES, including the parameter A-KID.

Step 3. The EES/ECS request KAF from the network. In this request, ECS/EES sends A-KID and ECS-ID/EES-ID.

Step 4. The network executes the authentication and authorization for the ECS/EES as defined in the AKMA procedure and if the result is successful then derives the KAF such that KAF = KDF (KAKMA, ECS-ID/EES-ID).

Step 5. The network sends KAF, expire time for the key and and optionally GPSI to the ECS/EES.

Step 6. The EEC and the ECS/EES use KAF in Ua\* protocol.

If the EEC sends GPSI to the ECS/EES, then the ECS/EES verifies the received GPSI using the GPSI received from the network via AKMA or via UE ID API.

### 6.14.3 Solution evaluation

This solution addresses key issue #2.1 by proposing to re-use existing AKMA mechanism for authentication the UE by the ECS/EES. It does not have any impact on the existing AKMA mechanism.

This solution also proposes two alternative methods for validation of the GPSI, by the ECS/EES, which is optionally sent by the EEC to the ECS/EES. These methods are re-using the existing AKMA and UE ID retrieval API.

## 6.15 Solution #15: Authentication algorithm selection procedure between EEC and ECS

### 6.15.1 Solution overview

This solution addresses security requirement for authentication algorithm selection between EEC and ECS in key issue #2.2.

In this solution, the UE first retrieves the supported Authentication mechanism (s) of the network during registration, and optionally get the ECS Authentication mechanism capability. When the EEC intend to connect to ECS, the EEC determines the used authentication mechanism or candidate authentication mechanism.

### 6.15.2 Solution details

This solution assumes that:

- Home network and/or Serving network, UE (EEC), ECS (as NAF in GBA, or AF in AKMA) may support one or multiple mechanisms (e.g. TLS with AKMA, TLS with GBA).

- EEC and ECS shall support TLS with certificates by default.

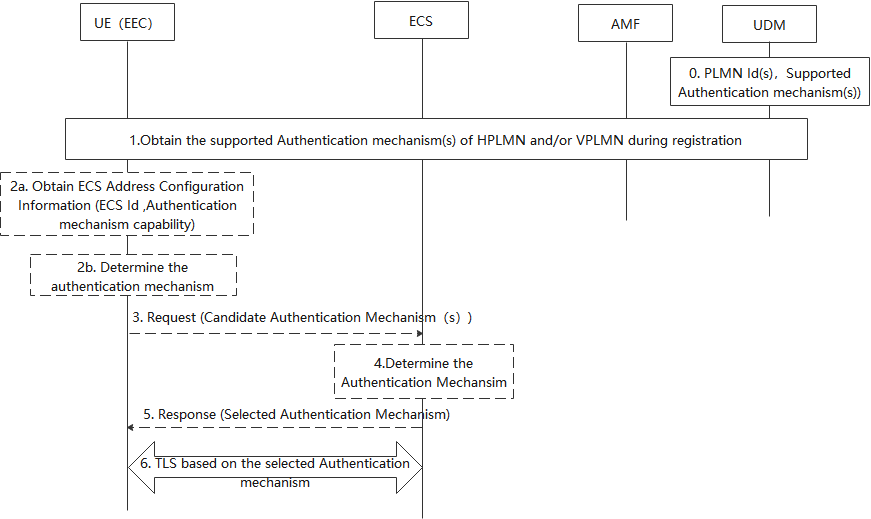
T

Figure 6.15.2-1: Authentication mechanism selection between the EEC and ECS

Step 0. Supported Authentication method(s) per network (e.g. GBA, AKMA) of PLMN(s) is stored in UDM.

Step 1. During the registration procedure, the UDM obtains the supported Authentication method(s) based on the PLMN Id provided by AMF. In non-roaming case, the UDM obtains the supported Authentication method(s) of UE HPLMN, if the UE is in roaming case, the UDM also obtains the supported authentication mechanism (s) of the UE's VPLMN. The UDM provides to UE via AMF using UCU procedure or registration response.

Step 2a. [Optional] During PDU Session Establishment, the SMF may provide ECS Address Configuration Information (ECS ID (e.g. FQDN or IP address(es) of ECS), [Authentication mechanism capability]) to the UE. The Authentication mechanism capability indicates the authentication mechanism the ECS support. When the UE would like to connect with ECS, if the Authentication mechanism capability received, performs step 2b, skip steps 3 to 5. Otherwise, performs steps 3 to 5 and skip step 2b.

Step 2b. [Conditional] The UE determines the available network authentication mechanism based on the received supported authentication mechanism (s) and the PLMN Id of network the ECS located. Then the EEC determines the target authentication mechanism based on EEC authentication capability, authentication mechanism capability and the available network authentication mechanism.

Step 3. [Conditional] The UE determines the available network authentication method based on the received supported authentication mechanism (s) and the PLMN Id of network the ECS located. Then the EEC determines the candidate authentication mechanism (s) based on EEC authentication capability and the available network authentication mechanism. The UE sends request to ECS with candidate authentication mechanism (s).

Step 4. The ECS determines selected authentication mechanism based on the received candidate authentication mechanism and the configured local policy.

Step 5. The ECS sends response with selected authentication mechanism to EEC.

Step 6. EEC and ECS establish the TLS based on the selected authentication mechanism.

After the TLS established, the ECS sends the received candidate authentication mechanism(s) to the UE via the service provisioning response during the service provisioning procedure as specified in clause 8.3.3.2.2 of 3GPP TS23.558 [11]. The EEC checks candidate authentication mechanism(s) sent by the ECS match the ones stored in the EEC to ensure that these were not modified by an attacker.

### 6.15.3 Solution evaluation

This solution proposes the 5GC to provide the UE supported authentication methods of UE SN and/or HN during the the registration procedure. And the ECS Authentication mechanism capability is preconfigured as part of ECS Address Configuration Information. Then the EEC can determine the candidate authentication mechanism(s) which is supported by UE, EEC and SN/HN and send the candidate mechanism(s) to the ECS, and the ECS determines the used authentication based on received candidate authentication mechanism(s). The solution also extends the service provisioning procedure to send the replayed candidate authentication mechanism for preventing binding down attack because the negotiation procedure is not protected.

## 6.16 Solution #16: Authentication algorithm selection procedure between EEC and EES

### 6.16.1 Solution overview

This solution addresses security requirement for authentication algorithm selection between EEC and EES in key issue #2.2.

In this solution, the UE first retrieves the supported Authentication mechanism (s) of the network during registration, and optionally get the EES Authentication mechanism capability from ECS. When the EEC intend to connect to EES, the EEC determines the used authentication mechanism or candidate authentication mechanism.

### 6.16.2 Solution details

This solution assumes that:

- Home network and/or Serving network, UE(EEC), EES (as NAF in GBA, or AF in AKMA) may support one or multiple mechanisms (e.g. TLS with AKMA, TLS with GBA).

- EEC and EES shall support TLS with certificates by default.

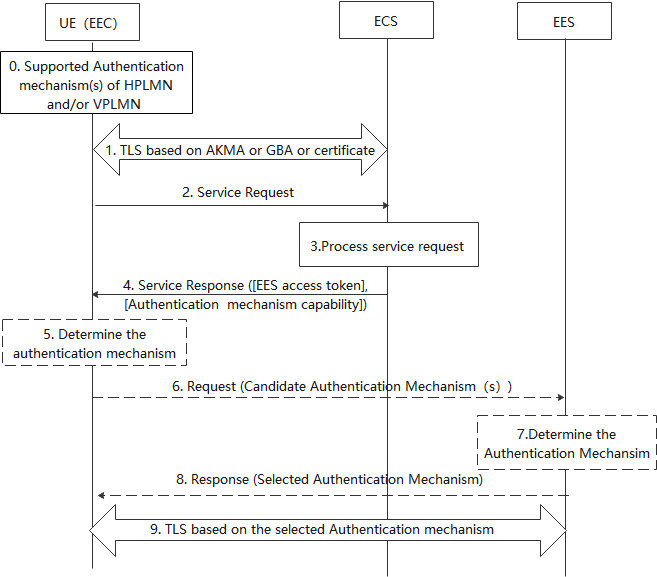


Figure 6.16.2-1: Authentication mechanism selection between the EEC and EES

Step 0. During the registration procedure, the UDM obtains the supported Authentication method(s) based on the PLMN Id provided by AMF. In non-roaming case, the UDM obtains the supported Authentication method(s) of UE HPLMN, if the UE is in roaming case, the UDM also obtains the supported authentication mechanism (s) of the UE's VPLMN. The UDM provides to UE via AMF using UCU procedure or registration response.

Step 1. EEC establishes TLS connection with ECS based on the AKMA or GBA or certificate.

Step 2. The EEC sends the service request to the ECS.

Step 3. The ECS should authorize the EEC by its local authorization policy, if the authentication and authorization is successful, then the ECS processes the request.

Step 4. The ECS decides whether access tokens are required for the candidate EESes using the configuration information and issues separate EES access tokens to be used for each candidate EESes that use token-based authorization. The ECS sends the EES access tokens to the EEC. Optionally, the Authentication mechanism capability is included. The Authentication mechanism capability indicates the authentication mechanism the EES support.

When the EEC would like to connect with EES, if the Authentication mechanism capability received, performs step 5, skip steps 6 to 8. Otherwise, performs steps 6 to 8 and skip step 5.

Step 5. [Conditional]The UE determines the available network authentication mechanism based on the received supported authentication mechanism (s) and the PLMN Id of network the EES located. Then the EEC determines the target authentication mechanism based on EEC authentication capability, authentication mechanism capability and the available network authentication mechanism.

Step 6. [Conditional] The UE determines the available network authentication method based on the received supported authentication mechanism (s) and the PLMN Id of network the EES located. Then the EEC determines the candidate authentication mechanism (s) based on EEC authentication capability and the available network authentication mechanism. The EEC sends request to EES with candidate authentication mechanism (s).

Step 7. [Conditional]The EES determines selected authentication mechanism based on the received candidate authentication mechanism and the configured local policy.

Step 8. [Conditional]The EES sends response with selected authentication mechanism to EEC.

Step 9. EEC and ECS establish the TLS based on the selected authentication mechanism.

After the TLS established, the EES sends the received candidate authentication mechanism(s) to the UE via the EAS discovery response during the EAS Discovery procedure as specified in clause 8.5.2.2 of 3GPP TS23.558 [11]. The EEC checks candidate authentication mechanism(s) sent by the EES match the ones stored in the EEC to ensure that these were not modified by an attacker.

### 6.16.3 Solution evaluation

This solution proposes the 5GC to provide supported authentication methods of UE SN and/or HN to UE during the the registration procedure and the ECS to provide the EES's security authentication mechanism capability during the EES discovery procedure (e.g. service provisioning procedure), then the EEC can determine the used authentication mechanism(s) which is supported by UE, EEC, EES and SN/HN. In addition, if the ECS does not provide the EES's security authentication mechanism capability, the EEC can determine the candidate authentication mechanism(s) which is supported by UE, EEC and SN/HN and send the candidate mechanism(s) to the EES, and the EES determines the used authentication based on received candidate authentication mechanism(s). In this case, the EES need to extends the EAS discovery procedure to send the replayed candidate authentication mechanism for preventing binding down attack because the negotiation procedure is not protected.

## 6.17 Solution #17: Using existing AKMA/GBA negotiation mechanism

### 6.17.1 Solution overview

This solution addresses key issue #2.2 that focuses on authentication method negotiation for the case that there is more than one authentication method for the authentication of EEC/UE. This contribution proposes a solution that re-uses existing negotiation mechanism for AKMA/GBA.

### 6.17.2 Solution details

#### 6.17.2.0 General

This solution proposes a mechanism for shared key based EEC/UE authentication and certificate based ECS/EES authentication in clause 6.17.2.1 and a mechanism for shared key based mutual authentication in clause 6.17.2.2.

#### 6.17.2.1 Shared key based EEC/UE authentication and certificate based ECS/EES authentication

It is assumed that the ECS/EES is preconfigured with the information indicating which feature (AKMA or GBA) is supported by the HPLMN. The steps of the negotiation procedure are described below.

If it is not possible to configure the information about the authentication method support of HPLMN in the ECS/EES, then it can be assumed that the UE/EEC is preconfigured with that information. In this case, in step 2 the UE/EEC sends supported PSK hints to the ECS/EES:

1) The UE/EEC and ECS/EES establish TLS connection using TLS server certificate.

2) The UE/EEC sends all possible PSK hints ("3GPP-AKMA", "3GPP-bootstrapping", "3GPP-bootstrapping-uicc", "3GPP-bootstrapping-digest") and the HPLMN identifier to the server (ECS/EES).

3) The server indicates the PSK identity hints considering the support of the HPLMN, and the existence of the agreement between the server and the HPLMN about the usage of AKMA/GBAin the HTTP response.

4) Remaining steps in clause 5.3 in TS 33.222 [10] with the enhancements specified in Annex B.1.2 of 3GPP TS 33.535 [8] are executed.

NOTE: Using of HPLMN identifier is not addressed in the present document.

#### 6.17.2.2 Shared key based mutual authentication

##### 6.17.2.2.1 Shared key based mutual authentication in TLS 1.2

It is assumed that the ECS/EES is preconfigured with the information indicating which feature (AKMA or GBA) is supported by the HPLMN. The steps of the negotiation procedure are described below.

If it is not possible to configure the information about the authentication method support of HPLMN in the ECS/EES, then it can be assumed that the UE/EEC is preconfigured with that information. In this case, in step 2 the ECS/EES doesn't need to consider the authentication method support of the HPLMN and includes possible PSK identity hints considering the existence of the agreement between the server and the HPLMN about the usage of AKMA/GBA, in step 3 the UE/EEC selects the PSK identity hint considering the HPLMN support and UE/EEC capability:

1) The UE/EEC sends ClientHello message including the HPLMN identifier to the server (ECS/EES).

2) The server sends ServerHello and ServerKeyExchange message to the UE/EEC. In the ServerKeyExchange message, the server includes the PSK identity hints considering the support of the HPLMN, i.e. "3GPP-AKMA" or "3GPP-bootstrapping", "3GPP-bootstrapping-uicc", "3GPP-bootstrapping-digest".

The UE/EEC can store the feature support information to use it in further interactions between the EEC and ECS/EES.

3) The UE/EEC runs AKMA or GBA procedures and sends the PSK hint and A-KID or B-TID in the ClientKeyExchange message to the server.

##### 6.17.2.2.2 Shared key based mutual authentication in TLS 1.3

It is assumed that the ECS/EES is preconfigured with the information indicating which feature (AKMA or GBA) is supported by the HPLMN. The steps of the negotiation procedure are described below.

If it is not possible to configure the information about the authentication method support of HPLMN in the ECS/EES, then it can be assumed that the UE/EEC is preconfigured with that information. In this case, in step 1 the UE/EEC generates A-KID or B-TID depending on the HPLMN support, in step 2, the UE/EEC sends A-KID or B-TID depending on the HPLMN support and includes related PSK identity hints depending on the HPLMN support, in step 3 the ECS/EES doesn't need to consider the authentication method support of the HPLMN, step 4 is not executed if the UE/EEC has already performed the GBA bootstrapping procedure:

1) The UE/EEC sends ClientHello message including all possible PSK identity hints (i.e. "3GPP-AKMA", "3GPP-bootstrapping", "3GPP-bootstrapping-uicc" and "3GPP-bootstrapping-digest") and A-KID/B-TID (if available) to the server.

If none of A-KID or B-TID is available, then the UE/EEC includes the HPLMN identifier in the ClientHello message.

2) The server extracts the HPLMN id from the A-KID or the B-TID (if included) and checks the configured HPLMN support information. Then the server sends the ServerHello message including the appropriate PSK hint ("3GPP-AKMA" if HPLMN supports AKMA or "3GPP-bootstrapping", "3GPP-bootstrapping-uicc", "3GPP-bootstrapping-digest" if HPLMN supports GBA). If the PSK hint indicates a GBA type of method and the ClientHello message includes a dummy B-TID then the server requests the UE to run a new GBA bootstrapping as specified in 3GPP TS 33.222 [10], 5.4.0.2, step 2.

3) Step 4. The UE/EEC executes the GBA bootstrapping procedure if the PSK hint from the server indicates that GBA should be run.

The UE/EEC can store the feature support information to use it in further interactions between the EEC and ECS/EES.

#### 6.17.2.3 Handling EEC authentication negotiation failure

In case of authentication negotiation failure, whether the server provides services is up to implementation.

#### 6.17.2.4 GPSI verification

If the EEC sends the GPSI to the server, the server needs to verify the GPSI to ensure that the GPSI belongs to the GPSI of the UE where the EEC is running. There are two alternatives for this verification: AKMA and AF Specific UE ID Retrieval API. Since the decision is done by the server itself, there is no need to have a negotiation mechanism for this check. The server decides on the method considering existence of AKMA usage agreement with the HPLMN. How this decision is done is left to implementation.

### 6.17.3 Solution evaluation

The solution uses existing AKMA/GBA negotiation mechanism that utilizes TLS negotiation method as much as possible. To handle the negotiation failure case, the solution leaves the decision to the implementation considering possible future services that can be provided by the servers, where some of them can be more critical in terms of security and privacy.

## 6.18 Solution #18: Authentication and Authorization between V-ECS and H-ECS

### 6.18.1 Solution overview

This solution addresses the security requirement for authentication and authorization between V-ECS and H-ECS in key issue #2.3.

### 6.18.2 Solution details

Pre-requisite:

- The V-ECS and H-ECS are preconfigured with credentials (e.g. certificate, shared keys/secrets) for mutual authentication.

The mutual authentication between V-ECS and H-ECS can be done based on the preconfigured credentials.

The H-ECS can authorize the V-ECS based on preconfigured local authorization policy.

6.18.3 Solution evaluation

The solution addresses the key issue #2.3.

Preconfigured credentials could be used for mutual authentication between V-ECS and H-ECS, and local policy could be used for v-ECS authorization by H-ECS. No further impact is identified on ECSes.

## 6.19 Solution #19: Authorization of V-ECS in roaming scenario

### 6.19.1 Solution overview

This contribution propose new solution for key issue#2.3. In roaming scenario, if the service provisioning request contains the serving PLMN ID, it is proposed that the H-ECS requests the 3GPP core network the list of VPLMN IDs UE is authorized to roam in and check against the received PLMN ID to authorize the V-ECS.

### 6.19.2 Solution details

In this solution, it is assumed that the HPLMN (ECSP1) and VPLMN (ECSP2) have a service level agreement to share edge services. If the H-ECS cannot discover a suitable EES to serve the UE at the current location (e.g. all the EESs registered on the H-ECS do not cover the given UE location), the H-ECS discovers another V-ECS which may have suitable EES and discovers the EES via the V-ECS.

For roaming scenario, if the service provisioning request from the EEC from the EEC does not contain the serving PLMN ID, the H-ECS requests the UDM the list of VPLMN IDs or ECS provider identifier allowed for the UE. If the PLMN ID is sent or included in the service provisioning request by the EEC, then the H-ECS checks with the pre-configured roaming information or the H-ECS reaches out to the UDM to check if the provided PLMN ID is the PLMN that the UE is allowed to access and is authorized to avail the Edge services.



Figure 6.19.2-1: Authorization of V-ECS by H-ECS

Step 1. The EEC sends a service provisioning request to the H-ECS. The request may include the UE location. For roaming scenario, the request may also include serving PLMN ID of the UE hosting the EEC.

Step 2. If the request does not contain the UE location information, the H-ECS interacts with 3GPP core network to retrieve the UE location. If the H-ECS cannot discover a suitable EES-2 to serve the UE at the received or retrieved UE location based on the received information (e.g. all the EESs registered on the H-ECS do not cover the given UE location), the H-ECS discovers another V-ECS which may have suitable EES based on the information such as the UE location.

Step 3. For roaming scenario, if the request does not contain the serving PLMN ID, the H-ECS requests the core network to retrieve the list of VPLMNs supporting EDGE. The H-ECS sends roaming information request message to the NEF.

Steps 4-5. The NEF retrieves the roaming information from the UDM. The roaming information includes the list of VPLMNs supporting EDGE and/or preferred ECSPs in VPLMN and/or EES or ECS provider identifier.

Step 6. The H-ECS can check if the edge computing service for the EEC can be supported in the VPLMN based on the received roaming information on edge computing services between PLMNs or ECSPs. The H‑ECS discovers the V-ECS which have suitable EES based on the roaming information.

NOTE: Whether local configuration in the ECS is enough or ECS needs to learn the list from the UDM is not addressed in the present document.

### 6.19.3 Solution evaluation

This solution is not evaluated.

## 6.20 Solution #20: Transport security for the EDGE10 interface

### 6.20.1 Solution overview

This solution addresses security requirement for transport security for the EDGE10 interface in key issue #2.4.

### 6.20.2 Solution details

Since the EDGE10 interface is SBI based, it is proposed to reuse the same security mechanisms specified in 3GPP TS 33.558 [4] as for EDGE6/9.

### 6.20.3 Solution evaluation

This solution addresses the transport security for the EDGE10 in the key issue #2.4. The solution is based on reusing existing mechanisms and hence has no standard impact.

## 6.21 Solution #21: Using local policy on authorization between EESes

### 6.21.1 Solution overview

This solution addresses KI#2.6 on the authorization between EESes.

### 6.21.2 Solution details

For the EDGE-9 interface between EESes, it is proposed to base authorization on local policies described in 3GPP TS 33.501 [7] clause 13.3.0.

### 6.21.3 Solution evaluation

This solution addresses the requirements of KI#2.6 on the authorization between EESes.

Local policy could be reused here for the authorization between EESes. No further impact is identified on the EES.

6.22 Solution #22: Using existing TLS 1.3 to perform negotiation mechanism

6.22.1 Solution overview

This solution addresses key issue #2.2 by providing a secure way to negotiate the authentication method used between the EEC and ECS/EES using existing procedures.

6.22.2 Solution details

There are multiple methods that the EEC could use to authenticate to the ECS/EES with the main ones as follows.

NOTE 1: This solution is not taking a stance on the viability of these solutions. It is focusing on providing a method for negotiating between the possible methods.

The solution use TLS 1.3 with the any of the following included in the ClientHello based on the authentication methods that the EEC can use:

- AKMA: AKID and symmetric key ciphersuite(s);

- GBA: B-TID and symmetric key ciphersuite(s);

- Digest/Token methods: Ciphersuite(s) supporting server side certificates only; and

- Client certificates: Ciphersuites supporting both client and server side certificates.

From this information, the ECS/ESS can determine which are possible authentication methods. If the UE and ECS/EES do not support a common method, the TLS handshake will fail.

For example, in case A-KID/B-TID are sent along with other methods supported by the UE, the ECS/EES can easily determine if an AKMA/GBA key is available for that UE. This is done by first using the A-KID (or B-TID) received in the ClientHello to determine the HPLMN of the UE and further determine if the ECS/EES supports AKMA (or GBA) with that HPLMN. The ECS/EES can then request an AKMA (GBA) key using related interfaces. If these steps succeed then the ECS/EES can use AKMA (GBA) with the UE to establish the TLS connection. If any of these steps fails, the ECS/EES can respond to the ClientHello and try any of the other methods supported by the EEC, and complete the TLS handshake appropriately.

The TLS handshake protects the method from bidding down.

The solution requires no new functionality to be supported.

NOTE 2: For client authentication methods that happen in the TLS tunnel, the Digest realm parameter can be used as a hint of which digest credentials might work with the ECS/ESS. For token methods, information in or related to the token is used to decide if the token can be used with ECS/ESS.

6.22.3 Solution evaluation

his solution is not evaluated.

## 6.23 Solution #23: EAS discovery procedure protection

### 6.23.1 Solution overview

The key issue #1.2 is proposed to protect EAS discovery procedure via V-EASDF. In an edge computing environment, DNS message is needed to query the Edge application Server's address. If the DNS destination address is modified by the attacker, then the wrong Edge Application 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.

3GPP TS 33.501 [7] has an informative annex P.2 describing security aspects on DNS for 5G, and it is proposed to reuse the DNS over (D)TLS in the MEC system.

### 6.23.2 Solution details

According to the specification in 3GPP TS23.548 [15], V-EASDF is used as DNS server for EAS discovery. Therefore, V-EASDF should support DNS over (D)TLS, as specified in IETF RFC 7858 [17] and IETF RFC 8310 [18]. The V-EASDF that are deployed within the 3GPP network can enforce the use of DNS over (D)TLS. The core network configures the V-EASDF security information to the UE as follows: the V-SMF can be preconfigured with the V-EASDF security information, or fetch the information from the V-EASDF. And then V-SMF provides the V-EASDF security information to UE directly (i.e. LBO case), or via H-SMF (i.e. case where HR SBO is authorized by HPLMN), during the PDU session establishment or during modification procedure when the V-SMF determines to use a new V-EASDF for EAS discovery.

If the core network is used for V-EASDF security information provisioning, the V-SMF provides the V-EASDF security information to UE directly (i.e. LBO case) or via H-SMF (i.e. LBO case) during the PDU session establishment or modification procedure when the V-SMF determines to use V-EASDF for EAS discovery.

### 6.23.3 Solution evaluation

This solution reuses the security recommendations from 3GPP TS 33.501 [7].

This solution restricts to the provisioning from the v-SMF to the UE in the visited network, which means that it does not impact the provision from the HPLMN to the UE.

In addition, it requires UE and V-EASDF to support DNS over (D)TLS, if the core network is used for V-EASDF security information provisioning, the V-SMF is responsible for provide the security information of V-EASDF.

## 6.24 Solution #24: Public key signature based ECS/EES authentication

### 6.24.1 Solution overview

This solution proposes a mechanism to set and select the public key signature based ECS/EES authentication using server certificate or raw public key based TLS as default authentication mechanism, when there is no support for common method between UE and ECS/EES. This solution partially addresses the security requirements of key issue#2.1, as only authenticity of the server is verified.

### 6.24.2 Solution details

The public key signature based ECS/EES authentication using server certificate or raw public key based TLS is used as default authentication mechanism, when UE/EEC, HN, SN and ECS/EES fails to negotiate a common method and/or based on operators choice. It is mandatory to support the public key signature based ECS/EES authentication using certificate or raw public key based TLS in the ECS, EES and UE and to be used only when there is no common mutual authentication method supported.

The root certificate (for ECS/EES certificate verification) or the public key is provisioned to the UE/EEC as part of ECS configuration information during service provisioning.

As there is no client/UE side authentication and authorization performed, the UE is provided with no privileged services and not provided with UE specific information, but provided only with generic information i.e. the ECS/EES and the network is not allowed to expose any UE specific information for example, UE ID, location information like so, as this may lead to privacy issue (exposing UE specific information to an unauthenticated UE).

### 6.24.3 Solution evaluation

This solution partially addresses the security requirement from Key issue#2.1, as only server side authentication is performed, not the mutual authentication. The solution has impact on provisioning of root certificate or the public key. However, at least server side authentication is required for the scenarios where there is no common mutual authentication method supported by the UE, HN, SN and ECS/EES in order to provide EDGE service to the UE.

## 6.25 Solution #25: Utilizing Token-Based Solutions for EEC authentication

### 6.25.1 Solution overview

The methods for authentication of EEC by the ECS/EES has been left as out of scope for Rel-17 in 3GPP TS 33.558 [4]. In the present document, possible methods and negotiation mechanisms have been studied under key issue #2.1 and #2.2, respectively.

Possible options proposed so far include AKMA, GBA and TLS client certificate. Also, how to handle negotiation failure cases are under discussion. To prevent negotiation failures, there can be two alternatives:

1) the UE side or PLMN side has to support all the methods;

2) at least one mandatory method should be specified.

If none of the alternatives cannot be agreeable by SA3 working group, then it is possible to have negotiation failures in run time.

To handle the negotiation failures, two approaches have been proposed so far in the discussions:

1) no client authentication;

2) TLS client certificates usage.

It should be noted that TLS client certificates are not feasible in practice because it is not appropriate to use Internet PKI for many instances of applications running different Ues and to handle private PKIs for the setting that there are different players and providers. Thus, the only alternative becomes no client authentication. However, if no client authentication is specified as one option, then having other methods will not bring any security value because the malicious client will find a way to use no client authentication method.

To look to the problem from a different perspective, commonly used methods in the ecosystem should be considered for client authentications in UEs. One of the methods commonly used in the ecosystem is the methods based on token usage. There can be different methods how and where the client can receive a token. One example can be the utilization of Service Entitlement Configuration mechanisms documented by GSMA in [14] where the Entitlement Configuration Server provides a token to the client to be used towards to the servers for related services.

This contribution proposes a high-level solution for EEC authentication using token-based mechanisms.

### 6.25.2 Solution details

The EEC authentication is executed by a mechanism out of scope of this solution. Such a mechanism can be Service Entitlement Configuration specified in [14] where the Entitlement Configuration Server issues a token for the client. After the authentication, the EEC receives a token to be used towards to the Edge Configuration Server (ECS) / Edge Enabler Server (EES).

Utilization of such a token-based mechanism can be embedded to the authentication between the EEC and the ECS/EES mechanism as follows considering the Service Entitlement Configuration specified in [14] as an example.

1) The EEC requests a token from the Entitlement Configuration Server. This request can be executed via the Entitlement Client specified in [14] or the EEC can have functionality of the Entitlement Client. The Entitlement Configuration Server authenticates the EEC/UE using one of the methods specified in [14] and then issues a token with the claims of the Entitlement Configuration Server FQDN, EEC ID, optionally GPSI, ECS/EES FQDN, and expire time.

2) For the ECS/EES authentication by the EEC, TLS server certificate is used. For EEC authentication by the ECS/EES, the EEC provides the token to the ECS/EES so that the ECS/EES accepts the request coming from the EEC. The ECS/EES validates the claims in the token and verifies the token by communicating with the Entitlement Configuration Server or by using the certificate of the Entitlement Configuration Server.

The communication between Entitlement Configuration Server and ECS/EES is not in the scope of this solution (i.e. it is in the scope of [14]). This solution requires that this communication is security protected to prevent token interception by unauthorized entities. The security credential and the authentication of the EEC by the Entitlement Configuration Server is out of scope of this solution (i.e. it is in the scope of [14]).

### 6.25.3 Solution evaluation

This solution introduces another authentication method option, token-based approach, which is a method widely used in the ecosystem. The details of the token-based solution are not specified but an example is presented to skect how this method can be used.

## 6.26 Solution #26: Using authorization token on authorization between EESes

### 6.26.1 Solution overview

This solution addresses KI#2.6 on the authorization between EESes.

### 6.26.2 Solution details - Target EES Decided ACR

For the EDGE-9 interface between EESes, it is proposed to use the authorization token for application context transfer authorization between the S-EES and the T-EES.

Figure 6.26.2-1 illustrates an example procedure for EEC Authorization of EEC Context transfer in a scenario where an ACR procedure IS initiated by the EEC and the procedure requires that EEC Context be PUSHED from the S-EES to the T-EES.



Figure 6.26.2-1: Application Context Transfer with ACT authorization tokens

Figure 6.26.2-1 shows the procedure of application context transfer from S-EES to T-EES steps with the following:

Step 1. The EEC established a secure connection with the source ECS which is optionally based on TLS setup with AKMA or GBA pre-shared key using the procedure specified in 3GPP TS 33.558 [4]. Depending on configuration, a reauthentication or AKMA/GBA may be needed when AC receives the ACR Selection message.

Step 2. The AC receives the ACR Selection message and this message triggers the EEC to start ACT. The AC decides to initiate the transfer of application context from the S-EES to the T-EES. In addition to request the authorization token for EES and EAS access, the EEC also request tokens for application context transfer authorization from the S-EES to T-EES (ACT authorization tokens). Alternatively, the tokens may have been received in the ACR Selection message.

Step 3. ECS processes the request and generates the requested tokens after authorization of EEC. The ACT authorization token may include but not limited to AC ID, S-EES ID, T-EES ID, ECS ID, token validity time, action authorized, claims, scope, etc.

Since the EEC is the owner of the application context stored in EES and the context contains sensitive information such as UE ID, UE location, and etc, the relocation of the application context from the source EES to the target EES. Therefore, in this step, the EEC agree the application context transfer and request a token from the ECS that the T-EES and S-EES can use as the approval that the application context transfer is authorized by the EEC. In this case, the ECS serves as the Authorization Server, the same role when the ECS issues authorization token used by the EEC to access the EES.

Step 4. The ECS sends the tokens and ACT authorization tokens to the AC/EEC.

Step 5. The AC/EEC establishes TLS with the target ECS if the ECS changes during ACR and it receives tokens of authorization to access T-EES, and setup TLS with T-EES.

The AC/EEC sends an Application Context Transfer request to the T-EES and the request included T-EES access authorization tokens and ACT Authorization tokens.

Step 6. Optionally, the T-EES and S-EES setup the security connection (e.g. TLS connection) if there is a need.

Step 7. The T-EES authorizes the AC with EES access token, and then send the application context transfer request along with the ACT Authorization token to the S-EES.

Step 8. Upon receiving the ACT request from the T-EES, the S-EES validates the received authorization token.

Step 9. The S-EES transfer the AC application context to the T-EES if the token validation is successful.

Step 10. The T-EES sends the ACT complete message to the AC/EEC.

### 6.26.3 Solution details: Source EAS decided ACR

Figure 6.26.3-1 illustrates an example procedure for EEC Authorization of EEC Context transfer in a scenario where an ACR procedure IS NOTinitiated by the EEC and the procedure requires that EEC Context be PUSHED from the S-EES to the T-EES.

In this scenario, the S-EAS may detect the need of ACR locally or is notified by the S-EES via ACR management notifications or UE location notifications.In the same time, the EEC has also subscribed to receive ACR information notifications for target information notification events.

When the notification is received by the EEC from the S-EES, the EEC responds to the EES with the authorization token to authorize the ACR to be used for the application context transfer from the S-EES and T-EES. The S-EAS make the decision about whether to perform the ACR, and starts the ACR at a proper time.



Figure 6.26.3-1: S-EAS decided ACR

Phase 0: EEC Configuration and Provision:

0. Same as steps 1-4 in the figure 6.26.2-1. The EEC received the ACR authorization token from the ECS as the results.

Phase I: ACR Detection:

1. The S-EAS either receives ACR management notifications from source Edge Enabler Sever indicating that ACR may be required ("ACR monitoring" event), or self detects the need for ACR (e.g. upon receipt of a "user plane path change" event or UE location notification.

Phase II: ACR Decision:

2. The S-EAS makes the decision to perform the ACR.

Phase III: ACR Execution:

3. The S-EAS discovers the T-EAS.

4. The S-EAS sends selected T-EAS declaration message to S-EES, to inform S-EES the determined. The S-EAS may send the ACID and Predicted/Expected UE location or Expected AC Geographical Service Area to the EES. When the EES receives the predicted/expected UE location or Expected AC Geographical Service Area from the EAS, then the EES will determine to monitor the UE mobility.

5. Based on the T-EAS selection information received from the S-EAS, the S-EES sends the target information notification to the EEC as described in clause 8.8.3.5.3 of 3GPP TR 33.839 [5]. The selected T-EES may be included in the target information and the ACID which corresponds to the selected target EAS is included in the notification sent to the EEC as described in clause 8.8.3.5.3 of 3GPP TR 33.839 [5].

Alternative to step 0, if authorization token is based on the EES instance, the EEC can request the authorization token from the ECS before send the request in the next step.

6. When the EEC receives the ACR information and authorizes the application context relocation, it responds to the S-EES with the authorization token.

7. If the T-EES is different than the S-EES and the EEC Context at the S-EES is not stale, the S-EES initiates EEC Context Push relocation with the T-EES with the authorization token received from the EEC. Otherwise, if the T-EES is the same as the S-EES, EEC Context Push relocation is skipped.

The EES context transfer procedure is the same as in the steps 6-9 in the figure 6.26.2-1 and therefore they are not repeated here.

### 6.26.4 Solution details: S-EES executed ACR

Figure 6.26.4-1 illustrates an example procedure for EEC Authorization of EEC Context transfer in a scenario where an ACR procedure IS initiated by the EEC and the procedure requires that EEC Context be PULLED from the S-EES to the T-EES.

In the case of S-EES executed ACR, the EEC has subscribed to receive ACR information notifications for target information notification events.

When the notification is received from the S-EES, the EEC responds to the EES with the authorization token to authorize the ACR to be used for the application context transfer from the S-EES and T-EES.



Figure 6.26.4-1: S-EES executed ACR

Phase 0: EEC Configuration and Provision:

0. Same as steps 1-4 in the figure 6.26.2-1 of the clause 6.26.2. The EEC received the ACR authorization token from the ECS as the results.

1. The S-EAS may initiate EELManagedACR with S-EES. In this step, the S-EAS and S-EES negotiate an address of the Application Context storage to S-EES.

Phase I: ACR Detection:

2. Detection entities (S-EAS, S-EES, EEC) detect that ACR may be required and identify the ACID and Predicted/Expected UE location or Expected AC Geographical Service Area. The detection by the S-EES may be triggered by the User Plane path change notification received from the 3GPP Core Network due to S-EAS request for "ACR facilitation" event.

Phase II: ACR Decision:

3. The detection entity performs ACR launching procedure with the ACR action indicating ACR determination and the corresponding ACR determination data. If the EEC or S-EAS detect the ACR event, the EEC or S-EAS may inform S-EES with ACID, and predicted/expected UE location or Expected AC Geographical Service Area in the ACR launching procedure.

4. The S-EES authorizes the message if received. The S-EES decides to execute ACR based on the information received or local detection, and the information of EEC context or EAS profile, and then proceed the below steps. When the EES receives the predicted/expected UE location or Expected AC Geographical Service Area from the EEC or the EAS in ACR determination, or the EES received service continuity planning from EAS in ACR facilitation event subscription, then the EES will determine to monitor the UE mobility.

Phase III: ACR Execution:

5a. The S-EES determines T-EES and T-EAS via the Discover T-EAS procedure.

5b. If required, the S-EES performs ACR parameter information procedure by sending the ACR parameter information request to the T-EES.

6. The S-EES sends the target information notification to the EEC.

Alternative to step 0, if authorization token is based on the EES instance, the EEC can request the authorization token from the ECS before send the request in the next step.

7. As the results of receiving the notification, the EEC responds to the EES with the authorization token to authorize the ACR.

8. If the T-EES is different than the S-EES and the EEC Context at the S-EES is not stale, the S-EES initiates EEC Context Push relocation with the T-EES along with the authorization token received from the EEC in step 7. Otherwise, if the T-EES is the same as the S-EES, EEC Context Push relocation is skipped.

The EES context transfer procedure is the same as in the steps 6-9 in the figure 6.26.2-1 in clause 6.26.2 and therefore they are not repeated here.

9. The S-EES may apply the AF traffic influence with the N6 routing information of the T-EAS in the 3GPP Core Network (if applicable).

10. The S-EES sends the ACR management notification to the S-EAS to initiate ACT between the S-EAS and the T-EAS.

### 6.26.5 Solution evaluation

This solution addresses the requirements of KI#2.6 on the authorization between EESes.

Authorization token is used here for the authorization between EESes dynamically and authorized by the application user. No further impact is identified on the EES.

When the EEC Context contans sensitive information on the AC and the EEC is the information owner, the ACR should be authorized by the AC/EEC. Authorization using the token can fulfil such need and provides more flexible and dynamic authorization mechanism when the application context contains sensitive AC/EEC information and needs to get the permission from the information owner.

NOTE: How to get the target EES's ID in the authorization token is not addressed in the present document.

## 6.27 Solution #27: Token-based solution for authorization between EESes

### 6.27.1 Solution overview

This solution addresses KI#2.6 on the authorization between EESes.

### 6.27.2 Solution details

For the EDGE-9 interface between EESes, it is proposed to use the authorization token similar to the token-based solution for EEC authorization by the EES, specified in clause 6.2 of 3GPP TS 33.558 [4]. For token-based solution, OAuth 2.0 framework is used with client credentials grant type where the ECS assumes the role of authorization server. The token includes the T-EES FQDN, the S-EES FQDN, the ECS FQDN and optionally the EEC ID in the token claims.

For the case that the two EESes are registered to different ECSes, the following procedure similar to the procedure of multiple NRF deployment case defined in clause 13.4.1.1.3 of 3GPP TS 33.501 [7] is applied. An EES sends its access token requests to the ECS where it is registered as OAuth 2.0 client. The ECS authenticates the EES and can verify the input parameters in the access token request. After successful authentication and verification of the input parameters, the ECS can forward the access token request to another ECS. If an ECS receives an access token request for an EES that is not registered at this ECS, the ECS determines the target ECS where the EES is registered and forwards the access token request to the target ECS.

### 6.27.3 Solution evaluation

This solution addresses the requirements of KI#2.6 on the authorization between EESes.

Since the ECS has the knowledge of source and target EES and also already assumes the role of authorization server for the token-based solution for EEC authorization by the EES, it can be stated that this solution re-uses existing mechanism.

Regarding the resource server role, since the EES implements the role of resource server for the EEC authorization case specified in clause 6.3 of 3GPP TS 33.558 [4], there is no additional impact on the EES.

Regarding the client role, the EES needs to implement the client role functionality.

The solution also addresses the case that the two EESes are registered to different ECSes, by using a mechanism similar to the procedure defined in clause 13.4.1.1.3 of 3GPP TS 33.501 [7].

## 6.28 Solution #28: Usage of randomly generated ticket to verify EEC provided IP address

### 6.28.1 Solution overview

This solution is for the key issue on EEC provided IP address verification.

Since the core network assigned IP addresses are guessable values, a compromised EEC can spoof the IP address to learn the identifier of another UE. To prevent such attacks, this solution proposes to use a non-guessable parameter called ticket or nonce provided by the core network to the EEC and to check the mapping between the IP address and the ticket value in the UE ID API invocation.

### 6.28.2 Solution details

High-level overview of the solution is presented in figure 6.28.2-1 and steps are explained in detail below.



Figure 6.28.2-1: EEC provided IP address verification

Step 1: In the PDU session establishment, the SMF/UPF generates a random ticket value during UE IP address allocation procedure. The ticket value in addition to the private IP address is sent to the UE by SMF.

Step 2: The ticket value is sent to the PCF.

Step 3: The ticket value is sent to and stored in the BSF as part of the PDU session binding information.

Step 4: The EEC in the UE sends the ticket value and the IP address to the EES.

Step 5: The EES invokes the Nnef\_UEId GET service operation using the ticket value and the IP address.

Step 6: The NEF sends the received ticket value to the BSF (Binding Support Function specified in TS 23.501) in Nbsf\_Management\_Discovery service operation.

Step 7: The BSF performs the verification by checking the mapping between the ticket value and the IP address.

NOTE: If the BSF cannot find a binding information having both requested IP address and ticket, it implies that the verification fails.

Step 8: The BSF sends the verification result to the NEF.

Step 9: If the verification is successful, then the NEF provides the AF specific GPSI to the EES.

Step 10: The EES sends the response to the EEC.

### 6.28.3 Solution evaluation

This solution addresses the potential security requirements with less impact on the network functions. The SMF will only need to generate a random ticket and send it to the UE and BSF, without needing to store any parameter.

This solution works under the assumption that the EEC can obtain 3GPP core network allocated IP address from lower layer.

This solution has an impact on the BSF for receiving and checking the ticket, impact on SMF for generating the ticket, and impact on PCF for forwarding the ticket to the BSF.

NOTE: More evaluation is needed, especially the impact on the various entities involved.

## 6.29 Solution #29: Authorizing the Service Consumer when Resolving an IP Address to a UE ID

### 6.29.1 Solution overview

The Nbsf\_Management\_Discovery service is used to resolve a UE IP Address to a SUPI. The solution describes how to enhance the service so that the BSF can verify that the consumer is authorized to obtain the UE ID.

### 6.29.2 Solution details

This solution supports the 5G System to verify the IP address in the request to obtain a UE Identifier. In the proposed procedure, both the EEC and BSF perform a hash calculation. The UE's IP Address is an input to the hash calculation. Some additional inputs to the hash calculation are values that are known to the UE that hosts the EEC and the BSF, whch is not easily known when combined, or determined, by functions other than the UE that hosts the EEC (e.g. the SUPI of the UE). When the BSF is requested to provide information about the UE (e.g. the SUPI of the UE), the BSF may compare the result of the BSF's calculation and the hash value that was provided by the EEC of the UE. If the result of the BSF's calculation and the hash value that was provided by the EEC of the UE are the same, then the BSF can support the request. If the result of the BSF's calculation and the hash value that was provided by the EEC of the UE are not the same, then the BSF may not authorize the request.

### 6.29.3 Solution evaluation

This solution is not evaluated.



Figure 6.29.3-1: IP Address Verification Using Hash

Step 1. The EEC performs the authentication and authorization procedures with EES. Thereafter, the secured communication is established between the EEC and the EES.

Step 2. The EES generate a nonce such as a time stamp, and other related parameters.

Step 3. The nonce is sent to the EEC that will derive the shared credential with the same inputs as the network side, to be used for future use such as the API invocation between the EEC and the EES.

Step 4. When the EEC is triggered by the AC to get the UE ID, the EEC invokes the API Nnef\_UEId\_Get to get the UE ID from EES. The request from the EEC includes the IP address and credential along with other parameters specified in 3GPP TS 23.558 [11]. The request can include an IP Address and the request can be to retrieve a UE ID that is associated with the IP Address.

In addition, the request includes a hash value. The EEC may determine the hash value using the following parameters as inputs:

- the private IP Address of the UE;

- the SUPI of the UE;

- the DNN and/or S-NSSAI of the PDU Session that the IP Address is associated with;

- the credential that is shared between the EEC and BSF.

Step 5. The EES may receive the request from the EEC. The EES may then act as an AF and invoke Nnef\_UEId\_Get request service of the NEF. The EES includes the IP Address that was provided by the EES as an input to the Nnef\_UEId\_Get request service invocation along with the nonce generated in the step 2.

Step 6. The NEF authorizes the AF request. If the authorization is not granted, the NEF replies to the EES with a Result value indicating authorization failure; otherwise the NEF proceeds with the following steps. The NEF determines corresponding DNN and/or S-NSSAI information: this may have been provided by the EES or is determined by the NEF based on the requesting EES Identifier and EES Provider Information.

If the NEF has received a Port Number in step 5, based on configuration, the NEF may recognize the address received is an IP address which is different from the actual private UE IP address assigned by 5GC, i.e. the UE is behind a NAT. If so, the NEF performs steps 7 to 10. Otherwise, steps 7 to 10 are skipped.

Step 7. The NEF uses the Nnrf\_NFDiscovery service operation to obtain the address of the UPF implementing NAT functionality for the UE (public) IP address. The request includes the UE (public) IP address. The NEF may also include the DNN and S-NSSAI associated with the AF ID, as well as the IP domain.

Step 8. The NRF responds with a Nnrf\_NFDiscovery response message including the UPF address of the UPF implementing NAT functionality for the UE (public) IP address.

Step 9. The NEF uses the Nupf\_GetPrivateUEIP\_Get service operation to request UE's (private) IP address from the UPF. The request includes the UE (public) IP address and Port Number, and optionally IP domain, DNN and S-NSSAI associated with the AF ID.

Step 10. The UPF responds with the Nupf\_GetPrivateUEIP\_Get response message including UE's IP address and optionally, the IP domain. If the UPF has applied a NAT functionality, the UE's IP address returned by the UPF is the private UE IP address.

Step 11. When the NEF invokes the Nbsf\_Management\_Discovery service operation, the NEF provides the hash value and the nonce to the BSF.

Step 12. The BSF will determine the SUPI that is associated with IP Address, derive the credential using the same inputs as the EEC, and calculate the expected hash value. The calculation that is used to determine the expected hash value will be the same as the calculation that the EEC performed in step 4.

The BSF will compare the expected hash value and the hash value that was received.

Step 13. If the received hash value and the expected hash value are the same, then the BSF will respond to the NEF with a SUPI.

In step 13 if the received hash value and the expected hash value are different, then the BSF will respond to the NEF with an indication that request is denied because the IP Address is not associated with the UE that made the request.

Step 14. The NEF will then use the SUPI to query the UDM and receive the UE ID from the UDM. The NEF interacts with UDM to retrieve the AF specific UE Identifier via the Nudm\_SDM\_Get service operation. The request message includes SUPI and at least one of Application Port ID, MTC Provider Information or AF Identifier.

Step 15. The UDM responds to the NEF with an AF specific UE Identifier represented as an External Identifier for the UE which is uniquely associated with the Application Port ID, MTC provider Information and/or AF Identifier.

Step 16. The NEF will send the UE ID to the EES.

Step 17. The EES will send the UE ID to the EEC.

## 6.30 Solution #30: Usage of existing public IP address to verify EEC provided IP address

### 6.30.1 Solution overview

This solution is for the key issue 2.7 on EEC provided IP address verification.

The EEC can spoof the IP address because the source IP address (i.e. UE private IP address) of the message is concealed by UPF via NAT, the EES only know the public IP address which can be used by different UEs. In NAT case, to differentiate different UEs using the same public IP address, the UPF will allocate a unique port number for each UE and the UPF stores the mapping between private IP address, public IP address and port number, the IP information knowed in each node in NAT case is showed in the following figure 6.30.1-1.

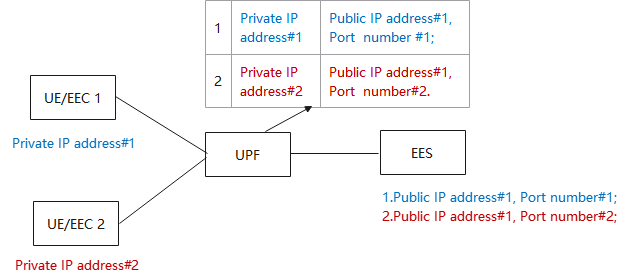


Figure 6.30.1-1: NAT procedure

Therefore, to verify the EEC provided IP address, this solution proposes to use the mapping between private IP address, public IP address and port number in the UPF to verify the mapping EEC provided IP address, EES obtained public IP address and port number based on the source IP address and port number of received UE ID API message.

### 6.30.2 Solution details

The procedure of the solution is presented in figure 6.30.2-1 and steps are explained in detail below.

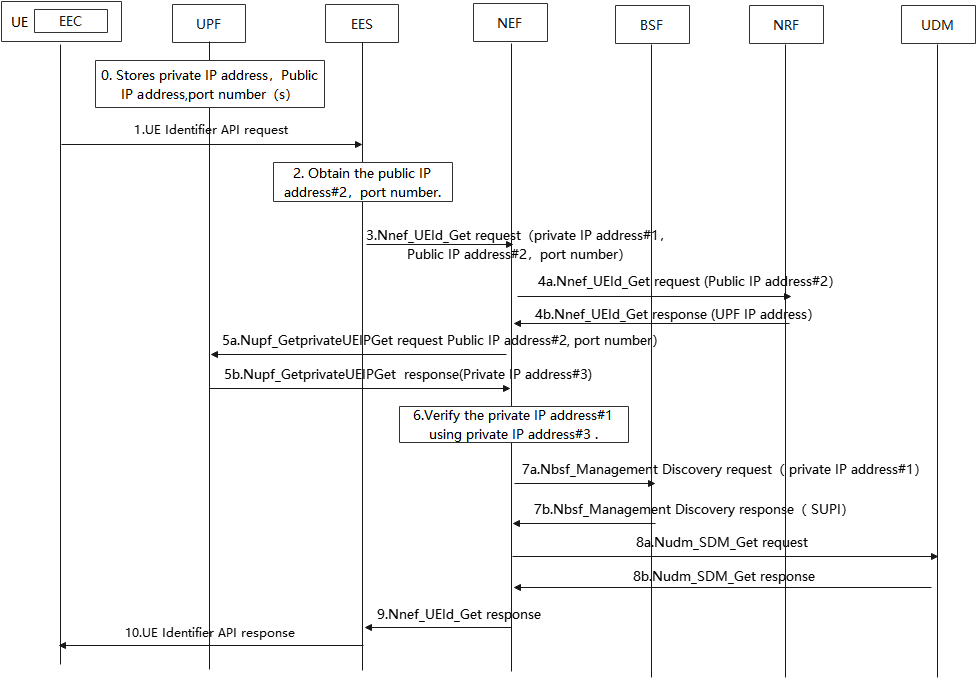


Figure 6.30.2-1 EEC provided IP address verification via existing public IP address and port number

Step 0. If NAT is used, the UPF stores the mapping between private IP address, public IP address, port number.

Step 1. The EEC in the UE sends UE Identifier API request with the private IP address#1 to the EES as clause 8.6.5 of 3GPP TS23.558 [11].

Step 2. EES obtains the UE public IP address#2, port number based on the sourse IP address and sourse port number of the IP data from UPF which include the UE Idenfifier API request.

Step 3. EES requests to retrieve UE ID via the Nnef\_UEId\_Get service operation. The request message includes private IP address #1, public IP address#2, port number associated with the public IP address#2.

Steps 4-5. NEF obtains the private IP address#3 from UPF via existing procedure specified in clause 4.15.10 (from step 3 to step 6) of 3GPP TS23.502 [9].

Step 6. NEF verify if the private IP address#3 is equal to EEC provided IP address#1, if verification is successful, the NEF continues to obtain the AF specific GPSI via step 7 and step 8.

Steps 7-8. NEF obtains AF specific GPSI via existing procedure specified in clause 4.15.10 (from step 7 to step 10) of 3GPP TS23.502 [9].

Steps 9-10. NEF sends Nnef\_UEId\_Get response with AF specific GPSI to EES, and the EES send UE Identifier API request with AF specific GPSI to EEC.

### 6.30.3 Solution evaluation

This solution is not evaluated.

## 6.31 Solution #31: AKMA/GBA based verification of EEC provided IP address

### 6.31.1 Solution overview

This solution leverages the BSF to address key issue #2.7.

In specific, according to clause 4.15.10 and clause 5.2.13 of 3GPP TS 23.502 [9], the BSF maintains the mapping relationship between the IP address and SUPI of the UE.According to clause 4.5.2 of 3GPP TS 33.220 [6], the UE can obtain a random number from the BSF if it needs to do GBA based authentication mechanism.

Refering to clause 6.1 of 3GPP TS 33.535 [8], the AAnF maintans the mapping relationship between the A-KID and the SUPI of the UE.

Therefore, in this solution, A-KID and the random number in GBA scenarios are used as the verification information to enable the BSF to detect IP address spoofing attack.

### 6.31.2 Solution details



Figure 6.31.2-1: IP address verification mechanism for edge computing scenarios

Step 1. EES receives the UE's IP address and the verification information from the EAS/UE/EEC. The verification information is the random number in GBA scenarios or A-KID in AKMA scenarios.

Step 2. EAS/EES sends the UE's IP address and the verification information to the BSF.

Step 3. If A-KID is provided, the NEF gets SUPI of the UE from the AAnF. Otherwise, step 3 can be skipped.

Step 4. The NEF provides the UE's IP address, the random number, or SUPI of the UE to the BSF.

Step 5. The BSF locates the IP address allocated to the UE by the network based on the received SUPI.

- In specific, with the verification information of the random number, the BSF first locates the UE's IMPI based on the random number.

- Then the BSF identifies the UE's SUPI based on the IMPI.

- The BSF compares the IP address allocated by the network with the received one.

Step 6. If the IP addresses are not identical, the BSF sends the error message to the NEF. Otherwise, the BSF sends SUPI of the UE to the NEF.

Step 7. If the NEF receives the SUPI from the BSF, the NEF gets an AF-specific UE ID from the UDM. Otherwise, step 7 can be skipped.

Step 8. If the NEF receives an error message from the BSF, the NEF forwards the error information to the EAS/EES in the response message. Otherwise, the NEF sends the response message containing the AF‑specific UE ID to the EAS/EES.

### 6.31.3 Solution evaluation

This solution is not evaluated.

## 6.32 Solution #32: KDF based verification of EEC provided IP address

### 6.32.1 Solution overview

This solution leverages the BSF to address key issue #2.7.

In specific, according to clause 4.15.10 and clause 5.2.13 of 3GPP TS 23.502 [9], BSF maintains the mapping relationship between the IP address and the SUPI. To generate verification information, the IP address and the SUPI are set as the inputs of the KDF. The output of the KDF is set as the verification information that enables BSF to detect IP address spoofing attack.

### 6.32.2 Solution details

It is assumed that the BSF generates the network side verification information based on the locally stored IP address and SUPI of the UE.

Step 1. EEC/UE sends the UE's IP address and the verification information to the EES directly or via the EAS. The verification information is generated based on the IP address and the SUPI of the UE. In specific, the IP address and the SUPI of the UE are set as the input of the KDF. And the output of the KDF is set as the verification information.

Step 2. EES sends the UE's IP address and the verification information to the BSF via the NEF.

Step 3. For the BSF side, if the network side verification information is not identical to the one provided by the EEC/UE, BSF sends the error message to EES to indicate the IP address spoofing attack.

### 6.32.3 Solution evaluation

This solution is not evaluated.

## 6.33 Solution #33: Verification of EEC provided IP address

### 6.33.1 Solution overview

This solution addresses the security requirement of key issue#2.7 on EEC provided IP address verification.

This solution proposes to use a PDU session ID for verifying the authenticity of assigned IP address.

### 6.33.2 Solution details



Figure 6.33.2-1: EEC provided IP address verification

Step 1: The UE/EEC invokes UE Identifier API exposed by the EES. The request includes the CN assigned private IP address of the UE and the PDU session ID.

Step 2: On receiving the UE Identifier API request, the EES invokes Nnef\_UEId\_Get service operation for translating the UE's Private IP address to its UE ID. EES includes the received IP Address and PDU Session ID in the request message.

Step 3: The NEF invokes the Nudm\_SDM\_Get request and sends the corresponding SUPI in the request.

Step 4: In Nudm\_SDM\_Get response the UDM sends the AF specific UE identifier and the PDU session ID(s) of the SUPI.

Step 5: The NEF verifies whether the received PDU Session ID from EES is present in the list of PDU session ID(s) from the UDM.

Step 6-7: If the verification is successful, then the NEF provides the AF specific UE Identifier to the EES in Nnef\_UEId\_Ger response. Then the EES forwards the AF specific UE Identifier to the UE/EEC.

### 6.33.3 Solution evaluation

This solution is not evaluated.

## 6.34 Solution #34: Verification of EEC provided IP address using access token

### 6.34.1 Solution overview

This solution addresses the security requirement of key issue#2.7 on EEC provided IP address verification.

This solution proposes to use an access token for mapping with the assigned IP address. This access token is provided by the ECS as specified in 3GPP TS 33.558 [4].

### 6.34.2 Solution details



Figure 6.34.2-1: EEC provided IP address verification

Step 1: The UE/EEC invokes UE Identifier API exposed by the EES. The request includes the CN assigned private IP address of the UE and the access token.

Step 2: On receiving the UE Identifier API request, the EES verifies the access token and then invokes Nnef\_UEId\_Get service operation for translating the UE's Private IP address to its UE ID. EES includes the received IP Address in the request message.

Step 3: The NEF invokes the Nudm\_SDM\_Get request and sends the corresponding SUPI in the request.

Step 4-5: In Nudm\_SDM\_Get response the UDM sends the AF specific UE identifier and UE IDs of the received SUPI. The NEF provides the AF specific UE Identifier and UE IDs to the EES in Nnef\_UEId\_Get response.

Step 6: The EES then verifies whether the UE ID received in the access token from EEC and from the NEF are the same.

Step 7: If the verification is successful, then the EES provides the AF specific UE Identifier to the EEC in UE Identifier API response.

### 6.34.3 Solution evaluation

This solution is not evaluated.

# 7 Conclusions

## 7.1 Conclusions for Key Issue #2.4

Solution #20 that proposes to reuse the TLS to solve key issue #2.4 is endorsed for conclusion.

## 7.2 Conclusions for Key Issue #2.3

Solution#18 is endorsed for normative phase for the mutual TLS authentication, and authorization based on local policy between V-ECS and H-ECS.

## 7.3 Conclusions for Key Issue #2.5

Key issue #2.5 requires that the Edge Enabler Client (EEC) should be able to provide mutual authentication with the Application Client over EDGE-5 interface, and the EEC should be able to determine whether Application client is authorized to access EEL service offered by EEC.

It is concluded that UE could handle the Authentication and Authorization between AC and EEC base on local policy, security mechanisms for authentication and authorization between AC and EES are left to implementation.

## 7.4 Conclusions for Key Issue #1.1

It is agreed in 3GPP TR 23.700-48 [2] to support authorizing the HR-local traffic routing to access EHE in the PDU session. Solution #12 that proposes to reuse secondary authentication to solve key issue #1.1 is endorsed for conclusion. Hence, no normative work is required on Key issue #1.1.

## 7.5 Conclusions for Key Issue #2.1

It is concluded to reuse authentication and authorization mechanism specified in 3GPP TS 33.558 [4] to realize authorization and mutual authentication between UE and ECS/EES.

Server side certificate-based TLS authentication is mandatory supported.

It is concluded to clarify in the normative work that ECS/EES can retrieve the GPSI from the core network if necessary and the ECS/EES should not trust the GPSI received from the EEC/UE.

NOTE 1: If only Server side certificate-based TLS authentication is performed, it is left to implementation on which services will be provided by the ECS/EES.

NOTE 2: Token-based solutions (e.g. Solution #25 for EEC/UE authentication by the ECS/EES) are left to implementation.

## 7.6 Conclusions for Key Issue#2.2

It is concluded that the negotiation mechanism will re-use existing TLS v1.3. If the UE has information about the capability (authentication method) of the server in the ECS/EES configuration information, then the EEC/UE can use this information in the negotiation. The ECS configuration information with the information on the authentication method can be received as specified in 3GPP TS 23.558 [11]. The EES configuration information with the information on the authentication method can be received from the ECS. Further optimization regarding having knowledge about the capability, such as UE storing the selected algorithm from past negotiation results, can be left to EEC/UE implementation.

## 7.7 Conclusions for Key Issue #2.6

Solution #21 that proposes to use local policy for authorization as described in 3GPP TS 33.501 [7] clause 13.3.0 between EESes is endorsed for conclusion. Hence, no new mechanism is required.

## 7.8 Conclusions for Key Issue #1.2

It is proposed to reuse the DNS over (D)TLS specified in Annex P of 3GPP TS33.501 [7] to protect the discovery message between UE and V-EASDF.

Hence, it is required to clarify in Annex T of 3GPP TS33.501 [7] that the UE and V-EASDF need to support DNS over (D)TLS, and if the core network is used to configure the security information used for (D)TLS protection to the UE as specified in Annex P of 3GPP TS33.501 [7], the V-SMF as the specific NF of the core network is used to provide the security information of V-EASDF to the UE directly (i.e. LBO case), or via H-SMF (i.e. case where HR SBO is authorized by HPLMN), during the PDU session establishment or during modification procedure when the V-SMF determines to use a new V-EASDF for EAS discovery. The V-SMF can be preconfigured with the V-EASDF security information, or fetch the information from the V-EASDF.

NOTE: The security information of V-EASDF provided to the UE is only related with the VPLMN parameter.

## 7.9 Conclusions for Key Issue #2.7

There is no agreement for this key issue in the present document.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | | |
| Date | Meeting | Tdoc | CR | Rev | Cat | Subject/Comment | New version |
| 2023-09 | SA#101 | SP-230869 |  |  |  | Presented for information and approval | 1.0.0 |
| 2023-09 | SA#101 |  |  |  |  | EditHelp review and upgrade to change control version | 18.0.0 |
| 2023-12 | SA#102 | SP-231327 | 0001 | 1 | F | CR of fixing references | 18.1.0 |
| 2023-12 | SA#102 | SP-231327 | 0002 |  | F | CR of terms, abbreviations and symbols | 18.1.0 |