|  |
| --- |
| 3GPP TR 33.739 V0.4.0 (2022-11) |
| Technical Specification|Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System AspectsStudy 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2021, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 9

3.3 Abbreviations 9

4 Overview of Edge Computing — Phase 2 9

5 Key issues 9

5.1 General 9

5.2 Key issues related with 5G System Enhancements for Edge Computing of SA WG2 9

5.2.1 Key issue #1.1: How to authorize PDU session to support local traffic routing to access an EHE in the VPLMN 9

5.2.1.1 Key issue details 9

5.2.1.2 Threats 9

5.2.1.3 Potential security requirements 9

5.3 Key issues related with enhanced architecture for enabling Edge Applications of SA WG6 10

5.3.1 Key Issue #2.1: Authentication and authorization of the EEC/UE by the ECS/EES 10

5.3.1.1 Key issue details 10

5.3.1.2 Security threats 10

5.3.1.3 Potential security requirements 10

5.3.2 Key issue #2.2: Authentication mechanism selection between EEC and ECS/EES 10

5.3.2.1 Key issue details 10

5.3.2.2 Security threats 11

5.3.2.3 Potential security requirement 11

5.3.3 Key issue #2.3: Authentication and Authorization between V-ECS and H-ECS 11

5.3.3.1 Key issue details 11

5.3.3.2 Threats 11

5.3.3.3 Potential security requirements 11

5.3.4 Key issue #2.4: Transport security for the EDGE10 interface 11

5.3.4.1 Key issue details 11

5.3.4.2 Threats 11

5.3.4.3 Potential security requirements 12

5.3.5 Key issue #2.5: Authentication and Authorization between AC and EEC 12

5.3.5.1 Key issue details 12

5.3.5.2 Threats 12

5.3.5.3 Potential security requirements 12

5.3.6 Key issue #2.6: New KI on authorization between EESes 12

5.3.6.1 Key issue details 12

5.3.6.2 Threats 13

5.3.6.3 Potential security requirements 13

6 Proposed solutions 13

6.0 Mapping of Solutions to Key Issues 13

6.1 Solution #1: Authentication and authorization between EEC hosted in the roaming UE and ECS 14

6.1.1 Solution overview 14

6.1.2 Solution details 15

6.1.3 Solution evaluation 16

6.2 Solution #2: Authentication and authorization between EEC hosted in the roaming UE and EES 16

6.2.1 Solution overview 16

6.2.2 Solution details 17

6.2.3 Solution evaluation 18

6.3 Solution #3: Authentication mechanism selection between EEC and ECS 18

6.3.1 Solution overview 18

6.3.2 Solution details 19

6.3.2.1 ECS configuration 19

6.3.3 Solution evaluation 20

6.4 Solution #4: Authentication mechanism selection between EEC and EES 20

6.4.1 Solution overview 20

6.4.2 Solution details 20

6.4.2.1 EES profile 21

6.4.3 Solution evaluation 21

6.5 Solution #5: 5GC-based authentication mechanism selection between EEC and ECS/EES 22

6.5.1 Solution overview 22

6.5.2 Solution details 22

6.5.3 Solution evaluation 23

6.6 Solution #6: ECS/EES authentication method information provisioning 23

6.6.1 Solution overview 23

6.6.2 Solution details 23

6.6.3 Solution evaluation 24

6.7 Solution #7: Negotiation procedure for the Authentication and Authorization 24

6.7.1 Solution overview 24

6.7.2 Solution details 24

6.7.3 Solution evaluation 25

6.8 Solution #8: Authentication mechanisms selected by ECS/EES 25

6.8.1 Solution overview 25

6.8.2 Solution details 25

6.8.2.1 Authentication between EEC and ECS 25

6.8.2.2 Authentication between EEC and EES 25

6.8.3 Solution evaluation 25

6.12 Solution #12: Authorization for PDU session supporting local traffic routing to access an EHE in the VPLMN 28

6.12.1 Introduction 28

6.12.2 Solution details 28

6.12.3 Solution evaluation 28

6.13 Solution #13: A solution for authentication of EEC/UE and GPSI verification by EES/ECS 29

6.13.1 Solution overview 29

6.13.2 Solution details 29

6.13.3 Solution evaluation 30

6.14 Solution #14: A solution for authentication of UE and GPSI verification by EES/ECS 30

6.14.1 Solution overview 30

6.14.2 Solution details 30

6.14.3 Solution evaluation 31

6.15 Solution #15: Authentication algorithm selection procedure between EEC and ECS 32

6.15.1 Solution overview 32

6.15.2 Solution details 32

6.15.3 Solution evaluation 33

6.16 Solution #16: Authentication algorithm selection procedure between EEC and EES 33

6.16.1 Solution overview 33

6.16.2 Solution details 33

6.16.3 Solution evaluation 35

6.17 Solution #17: Using existing AKMA/GBA negotiation mechanism 35

6.17.1 Solution overview 35

6.17.2 Solution details 35

6.17.3 Solution evaluation 35

6.18 Solution #18: Authentication and Authorization between V-ECS and H-ECS 35

6.18.1 Solution overview 35

6.18.2 Solution details 35

6.19 Solution #19: Authorization of V-ECS in roaming scenario 36

6.19.1 Solution overview 36

6.19.2 Solution details 36

6.19.3 Solution evaluation 37

6.20 Solution #20: Transport security for the EDGE10 interface 37

6.20.1 Solution overview 37

6.20.2 Solution details 37

6.20.3 Solution evaluation 37

6.21 Solution #21: Using local policy on authorization between EESes 37

6.21.1 Solution overview 37

6.21.2 Solution details 37

6.21.3 Solution evaluation 37

7 Conclusions 38

7.1 Conclusions for Key Issue #2.4 38

7.2 Conclusions for Key Issue #2.3 38

7.3 Conclusions for Key Issue #2.5 39

7.4 Conclusions for Key Issue #1.1 39

Annex <A>: <Informative annex title for a Technical Report> 40

Annex <X> (informative): Change history 41

# 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, a.k.a. phase 2, i.e. 5G System Enhancements for Edge Computing in TR 23.700-48 [2], and enhanced architecture for enabling Edge Applications in TR 23.700-98 [3]. The study bases on the work done in the TS 33.558 [4] and 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 TS 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: "3G security; Network Domain Security (NDS); IP network layer security".

# 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].

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

## 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].

# 4 Overview of Edge Computing — Phase 2

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

# 5 Key issues

## 5.1 General

Clause 5 describes the security key issues related with 5G System Enhancements for Edge Computing of SA WG2 in Clause 5.1, and Enhanced Architecture for Enabling Edge Applications of SA WG6 in Clause 5.2.

## 5.2 Key issues related with 5G System Enhancements for Edge Computing of SA WG2

### 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 the 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.

Editor’s Note: SA3 work PDU session to support local traffic routing to access an EHE in the VPLMN depends on SA2 conclusions.

## 5.3 Key issues related with enhanced architecture for enabling Edge Applications of SA WG6

### 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, 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 TS 23.700-98 v.0.6.0 [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 authorisation 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 TS 33.558[4], Clause 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 TS 33.535 [8], TLS with GBA as specified in 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 current 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 authorised 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 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).

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.

# 6 Proposed solutions

Editor’s Note: This clause will contain the proposed solutions

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |
| --- | --- |
| Solutions | Key Issues |
| 1.1 | 2.1 | 2.2 | 2.3 | 2.4 | 2.5 | 2.6 |
| 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 |  |  |  |  |
| #X: <Key issue name> |  |  |  |  |  |  |  |

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

## 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 this 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 [X], 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 sub clause 6.1.3.18 of 3GPP TS 23.503 [2], 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. 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.

Editor’s note: The way of sending EEC ID is FFS.

### 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 this 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 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 TS 33.220, 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 TS 33.501 [7], where KEES is served as the integrity key.

Step 2. Upon receiving the provisioning request, EES detects the home network of the UE based on the B-TID according to 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 sub clause 6.1.3.18 of 3GPP TS 23.503 [c], 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. 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 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 TS 33.222 [4], 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.

Editor’s note: The way of sending EEC ID is FFS.

### 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



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

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

1. The UE sends the initial provisioning request to the ECS. The initial provisioning request includes the relevant parameter (for example, A-KID or B-TID or OAuth Token) based on the selected authentication method.
2. The UE and the ECS performs the authentication using the selected authentication method.

#### 6.3.2.1 ECS configuration

Table 6.1.2,1-1 describes the information elements of ECS configuration information as specified in clause 8.3.2.1, Table 8.3.2.1-1 of TS 23.558 [11], with an additional IE to indicate selected authentication method.

Table 6.1.2.1-1: 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 [20] |
| 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.

Editor's note: Further evaluation is FFS.

## 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



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

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.
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.
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 core network is aware of the authentication method(s) supported by its roaming partners.

Editor’s Note: Which core network NF stores the supported authentication method details is FFS.

#### 6.4.2.1 EES profile

Table 6.2.2.1-1 describes the information elements of EES profile as specified in clause 8.2.6, Table 8.2.6-1 of TS 23.558 [11], with additional IE to indicate selected authentication method.

Table 6.2.2.1-1: 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. |
| EES Geographical Service Area | O | The area being served by the EES in Geographical values (as specified in clause 7.3.3.3) |
| 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 ECS selects the authentication method based on UE, EEC, EES, HN and SN and then indicated the selected authentication method to the EEC in the service provisioning response.

Editor's Note: Further evaluation is FFS.

## 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 this 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 sub clause 6.2.1 of 3GPP TS 33.535 [x], 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 Annex J.2 of TS 33.220 [y], 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

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 3. If ECS/EES receives A-KID or B-TID from UE/EEC in step 1, then step 3 to step 4 can be skipped. ECS/EES request authentication material from EEC. The authentication request message contains the identifier of the selected authentication method. Details about the requested authentication material depend on the selected authentication method. ECS/EES may request A-KID as the authentication material when ECS/EES chooses the AKMA-based authentication method. ECS/EES may request B-TID as the authentication material when ECS/EES chooses GBA-based authentication method.

Step 4. EEC sends the requested authentication material to the ECS/EEC.

Step 5a. 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 5b. 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 5a during the re-select procedure.

Step 5b. 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.

Editor’s Note: The negotiation messages between EEC and EES/ECS are not security protected, and therefore negotiation messages can be attacked. How to protect negotiation messages is FFS.

Editor’s Note: Consideration of UE security capability is FFS.

### 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.

## 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 TS 23.502 [9]). As described in 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 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.

### 6.6.3 Solution evaluation

Editor’s Note: Evaluation is FFS.

## 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 following:



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 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 TS 23.558, 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.

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 mechanis, 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 TS 33.535 [8] for AKMA, TS 33.220 [6] for GBA, RFC 8446 [xx] 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 TS 33.535 [8] for AKMA, TS 33.220 [6] for GBA, RFC 8446 [xx] for TLS 1.3.

Editor’s Note: It is FFS how to consider the HPLMN’s capability during the negotiation procedure.

Editor’s Note: Whether and what should be a default mechanism between UE and network is FFS.

### 6.7.3 Solution evaluation

TBA

## 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

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.

Editor's Note: How to consider security capabilities of UEs and PLMNs in the negotiation is FFS.

#### 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.

Editor's Note: How to consider security capabilities of UEs and PLMNs in the negotiation is FFS.

### 6.8.3 Solution evaluation

TBD.

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, TLS authentication methods (e.g., TLS with AKMA as specified in TS 33.535 [2], TLS with GBA as specified in TS 33.222 [3], other TLS authentication methods that uses other than 3GPP subscription credential(s) which is out of 3GPP) should be used. 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 (e.g., TLS with AKMA [2], TLS with GBA [3], or other TLS authentication methods).

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 TS 23.558[4]. 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 TS 33.535[2] or clause 5.3 and 5.4 of TS 33.222[3] 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.

Editor's Note: How to consider security capabilities of UEs and PLMNs in the negotiation is FFS.

Editor’s Note: it is FFS how to solve the authentication selection failure case if there do not exist the same authentication mechanisms between 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, TLS authentication methods (e.g., TLS with AKMA as specified in TS 33.535 [2], TLS with GBA as specified in TS 33.222 [3], other TLS authentication methods that uses other than 3GPP subscription credential(s) which is out of 3GPP) should be used. 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 (e.g., TLS with AKMA [2], TLS with GBA [3], or other TLS authentication methods).

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 TS 23.558[4]. 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 TS 33.535[2] or clause 5.3 and 5.4 of TS 33.222[3] 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.

Editor's Note: How to consider security capabilities of UEs and PLMNs in the negotiation is FFS.

Editor’s Note: it is FFS how to solve the authentication selection failure case if there do not exist the same authentication mechanisms between 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 (e.g., TLS with AKMA [3], TLS with GBA [4], or other TLS authentication methods). The ECS and EES should be separately configured via network management with mechanisms that are are allowed.

The EES provides the supported authentication mechanism(s) to the ECS during the EES registration procedure in clause 8.4.4.2.2 in TS 23.558[1], 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 TS 23.558[1]. 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 6.3.11.2-1: Procedure for authentication mechanism selection among EEC, EES, and ECS

Step 0: 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, 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 TS 23.558[1]. 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.

Editor’s Note: whether ECS should send the EEC’s security capability and EEC chosen method to EES is FFS

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 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 TS 23.5558[1], 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. Otherwise the authentication mechanism selection failed between EEC and ECS.

6.11.3 Solution evaluation

TBD

Editor's Note: How to consider security capabilities of UEs and PLMNs in the negotiation is FFS.

Editor’s Note: it is FFS how to solve the authentication selection failure case if there do not exist the same authentication mechanisms.

Editor’s Note: It if FFS to consider the security protection of selection messages between EEC and ECS.

## 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 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 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 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 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 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. The ECS/EES can also send an indication for receiving the GPSI of the UE if the ECS/EES prefers to use AKMA for GPSI authentication. Otherwise, the ECS/EES can invoke the AF specific UE ID API for GPSI retrieval (steps 3.a and 3.b).

Editor’s Note: It is FFS whether steps 3.a and 3.b are necessary.

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.

Editor’s Note: Further evaluation is FFS.

## 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. The ECS/EES can also send an indication for receiving the GPSI of the UE if the ECS/EES prefers to use AKMA for GPSI authentication. Otherwise, the ECS/EES can invoke the AF specific UE ID API for GPSI retrieval (steps 3.a and 3.b).

Editor’s Note: It is FFS whether steps 3.a and 3.b are necessary.

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.

Editor’s Note: Further evaluation is FFS.

## 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.



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

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

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.

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.

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.

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 authention mechanism. The UE sends request to ECS with candidate authentication mechanism (s).

Editor’s Note: The negotiation messages between EEC and ECS are not security protected, and therefore negotiation messages can be attacked. Whether and how to protect the negotiation messages is FFS.

4. The ECS determines selected authentication mechanism based on the received candidate authentication mechanism.

Editor’s Note: It is FFS whether ECS needs to check if it can obtain AKMA/GBA keys from network during the authentication mechanism selection procedure.

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

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

### 6.15.3 Solution evaluation

*TBD*

## 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 2 Authentication mechanism selection between the EEC and EES

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.
2. EEC establishes TLS connection with ECS based on the AKMA or GBA or certificate.
3. The EEC sends the service request to the ECS.
4. The ECS should authorize the EEC by its local authorization policy, if the authentication and authorization is successful, then the ECS processes the request.
5. 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.

1. [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.
2. [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).

Editor’s Note: The negotiation messages between EEC and EES are not security protected, and therefore negotiation messages can be attacked. Whether and how to protect the negotiation messages is FFS.

1. [Conditional]The EES determines selected authentication mechanism based on the received candidate authentication mechanism.

Editor’s Note: It is FFS whether EES needs to check if it can obtain AKMA/GBA keys from network during the authentication mechanism selection procedure.

1. [Conditional]The EES sends response with selected authentication mechanism to EEC.
2. EEC and ECS establish the TLS base on the selected authentication mechanism.

### 6.16.3 Solution evaluation

*TBD*

## 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

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.

Editor’s Note: Preconfiguration of HPLMN authentication method support in the ECS/EES is FFS.

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 i.e., “3GPP-AKMA” or “3GPP-bootstrapping”, “3GPP-bootstrapping-uicc”, “3GPP-bootstrapping-digest” in 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 TS 33.535 [8] are executed.

Editor’s Note: Using of HPLMN identifier is FFS.

Editor’s Note: It is FFS to exclude shared key-based mutual authentication between UE/EEC and ECS/EES.

Editor’s Note: It is FFS whether ECS/EES needs to check if it can obtain AKMA/GBA keys from network during the authentication mechanism selection procedure.

### 6.17.3 Solution evaluation

## 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 EECdoes 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

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.

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.

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.

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.

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.

Editor’s Note: Whether local configuration in the ECS is enough or ECS needs to learn the list from the UDM.is FFS.

### 6.19.3 Solution evaluation

Editor’s Note: The evaluation of this solution is FFS.

## 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 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

## 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 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, 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) 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 try other methods, and complete the TLS handshake appropriately.

Editor’s note: Clarification on the other methods is FFS.

The TLS handshake protects the method from bidding down.

The solution requires no new functionality to be supported.

Editor's note: Details how different method hints are carried over negotiation, e.g. digest/token is FFS.

6.22.3 Solution evaluation

TBD

# 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.

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

## 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.

Editor’s Note: Further conclusion is FFS.

## 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 TR 23.700-48 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.

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

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022.05 | SA3 #107e | S3-221095 |  |  |  | TR Skeleton | 0.0.0 |
| 2022.05 | SA3 #107e | S3-221235 |  |  |  | Implemented S3-221094, S3-221095, S3-221186, and S3-221191. | 0.1.0 |
| 2022.06 | SA3 #107e-adhoc | S3-221685 |  |  |  | Implemented S3-221412, S3-221477, S3-221599, S3-221600, S3-221611, S3-221613, S3-221614, S3-221654, S3-221673, S3-221678, S3-221683, S3-221704, S3-221694, S3-221695. | 0.2.0 |
| 2022.10 | SA3 #108e-adhoc | S3-222952 |  |  |  | Implemented S3-222530, [S3-223047](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_108e-AdHoc/Docs/S3-223047.zip), [S3-223050](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_108e-AdHoc/Docs/S3-223050.zip), [S3-222](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_108e-AdHoc/Docs/S3-222888.zip)888, S3-222501, [S3-222508](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_108e-AdHoc/Docs/S3-222508.zip), [S3-222658](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_108e-AdHoc/Docs/S3-222658.zip), S3222984, S3-223046, S3-223061, S3-223062, S3-223102, S3-223063, [S3-222503](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_108e-AdHoc/Docs/S3-222503.zip), [S3-222531](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_108e-AdHoc/Docs/S3-222531.zip), S3-223104, S3-222951 | 0.3.0 |
| 2022.11 | SA3 #109 | S3-224024 |  |  |  | Implemented S3-223545, S3-223587, S3-224023, S3-224025, S3-224026, S3-224027, S3-224028, and S3-223940. | 0.4.0 |

Change history of this template:

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