|  |
| --- |
| 3GPP TR 33.749 V0.5.0 (2024-11) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of enhancement of support foredge computing in the 5G Core (5GC) phase 3 (Release 19) |
|   |
|  |  |
| 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.© 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 8

3.3 Abbreviations 8

4 Overview 8

5 Key issues 8

5.1 General 8

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

5.2.1 Key Issue #1.1: Security aspects related to enhancements of EAS and local UPF (re)selection. 9

5.2.1.1 Key issue details 9

5.2.1.2 Security threats 9

5.2.1.3 Potential security requirements 9

5.3 Key issues related with enhanced architecture for enabling Edge Applications 9

5.3.1 Key Issue #2.1: Secure retrieval of 5G system UE Ids and privacy related information. 9

5.3.1.1 Key issue details 9

5.3.1.2 Security threats 10

5.3.1.2.1 Threats posed by a malicious EEC 10

5.3.1.2.2 Threats posed by malicious EAS/EES outside of the operator domain 10

5.3.1.3 Potential security requirements 10

5.3.1.3.1 Verification of the user information provided by the EEC 10

5.3.1.3.2 Protection of the UE privacy 10

6 Solutions 10

6.1 Solution #1: Usage of existing public IP address to verify EEC provided IP address 11

6.1.1 Solution overview 11

6.1.2 Solution details 12

6.1.3 Solution evaluation 12

6.2 Solution #2: Authorizing AF to retrieve UE ID 13

6.2.1 Solution overview 13

6.2.2 Solution details 13

6.2.3 Evaluation 14

6.3 Solution #3: Secure retrieval of 5G UE Id and privacy related information 15

6.3.1 Introduction 15

6.3.2 Solution details 15

6.3.3 Evaluation 16

6.4 Solution #4: Secure retrieval of 5G UE privacy related information based on AKMA 16

6.4.1 Introduction 16

6.4.2 Solution details 16

6.4.3 Evaluation 17

6.5 Solution #5: EEC proviced information verification 18

6.5.1 Introduction 18

6.5.2 Details 18

6.5.3 Evaluation 19

6.6 Solution #6: UE ID token 19

6.6.1 Solution overview 19

6.6.2 Solution details 19

6.6.3 Solution evaluation 20

6.7 Solution #7: Verification of EEC provided IP address 20

6.7.1 Solution overview 20

6.7.2 Solution details 21

6.7.3 Solution evaluation 22

6.8 Solution #8: Verification of EEC provided IP address using access token 22

6.8.1 Solution overview 22

6.8.2 Solution details 22

6.8.3 Solution evaluation 23

6.9 Solution #9: Simplified UE ID token based solution 23

6.9.1 Solution overview 23

6.9.2 Solution details 23

6.9.3 Solution evaluation 25

6.10 Solution #10: Reuse NDS/IP to protect N6 delay measurement message 26

6.10.1 Introduction 26

6.10.2 Solution details 26

6.10.3 Evaluation 26

7 Conclusions 26

7.1 KI#1.1: Security aspects related to enhancements of EAS and local UPF (re)selection. 26

7.2 KI#2.1: Secure retrieval of 5G system UE Ids and privacy related information 26

Annex <X> (informative): Change history 28

# 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 enhancements on the support for Edge Computing in the 5G Core network defined in TR 23.700-49 [2], and enhanced architecture for enabling Edge Applications defined in TS 23.558 [3]. Specifically, the present document focuses on the following:

1. Study the security aspects on the enhancements for EAS (re)discovery and UPF (re)selection with reducing impact on central 5GC NFs, enhancement of EAS and local UPF (re)selection, and EC Traffic Routing between local part of DN and central part of DN the Edge Hosting Environment information management.
2. Study the security on the enhancements to Edge Enabler layer (EEL) to support additional scenarios for edge services.
3. Study the authorization between EESes for both Application Context Relocation (ACR) and Edge Node Sharing (ENS) scenarios.
4. Study the secure retrieval of 5G system UE Ids and privacy related information in the EDGE.

The study is based on the work done in the 3GPP TS 33.558 [4], 3GPP TR 33.839 [5], 3GPP TR 33.739 [6].

# 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 23.700-49: "Study on Enhancement of support for Edge Computing in 5G Core network - Phase 3".

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

[4] 3GPP TS 33.558: "Security aspects of enhancement of support for enabling edge applications; Stage 2".

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

[6] 3GPP TR 33.739: "Study on security enhancement of support for edge computing phase 2".

[7] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

[8] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[9] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)"

[10] IETF RFC 4656: "A One-way Active Measurement Protocol (OWAMP)".

[11] IETF RFC 5357: "A Two-Way Active Measurement Protocol (TWAMP)".

[12] IETF RFC 8762: "Simple Two-Way Active Measurement Protocol".

[13] IETF RFC 2681: "A Round-trip Delay Metric for IPPM".

[14] IETF RFC 792: “INTERNET CONTROL MESSAGE PROTOCOL”.

[15] [USENIX](https://en.wikipedia.org/wiki/USENIX%22%20%5Co%20%22USENIX) Association: ["Password Protection for Modern Operating Systems"](https://www.usenix.org/system/files/login/articles/1103-alexander.pdf).

[16] 3GPP TS 23.003: " Technical Specification Group Core Network and Terminals; Numbering, addressing and identification”.

[17] 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].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

EAS Edge Application Server

EEC Edge Enabler Client

EES Edge Enabler Server

IPPM IP Performanace Metrics

OWAMP One-way Active Measurement Protocol

TWAMP Two-Way Active Measurement Protocol

# 4 Overview

The present document studies the security enhancements on the support for Edge Computing in the 5G Core network defined in 3GPP TS 23.548 [7], and application architecture for enabling Edge Applications defined in 3GPP TS 23.558 [3]. For the architecture and procedure of EC supported in 5GC, refer to 3GPP TS 23.548 [7]. For more details on enabling Edge Applications, it is proposed to refer to 3GPP TS 23.558 [3].

# 5 Key issues

## 5.1 General

Clause 5 describes the security key issues related with 5G System Enhancements for Edge Computing of 3GPP TR 23.700‑49 [2] in clause 5.2, and Enhanced Architecture for Enabling Edge Applications of 3GPP TS 23.558 [3] in clause 5.3.

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

### 5.2.1 Key Issue #1.1: Security aspects related to enhancements of EAS and local UPF (re)selection.

#### 5.2.1.1 Key issue details

Several enhancements in the procedures for EAS and local UPF (re)selection have been proposed in TR 23.700-49 [2]. It has been concluded that N6 delay measurement is a factor of decision in those procedures. The N6 delay measurement between the termination points, i.e., UPF and EAS, is to be performed using existing IETF standard protocols (e.g., ICMP, TWAMP, OWAMP, etc.). The 5G network and the EDGE negotiate and exchange information about the termination points, protocols and parameters to be used, and then the SMF (“controller”) configures the UPF(s) to conduct the measurements as “senders” to the network devices/compute nodes/EAS(s) acting as “reflectors/receiver”. The UPF(s) will report the results to SMF.

The IETF RFCs corresponding to the IP Performanace Metrics (IPPM) defined protocols, such as RFC 4656 [10], RFC 5357 [11], RFC 8762 [12], etc., include security considerations to be taken into account when those protocols are in use. RFC 2681 [13] refers to two types of security concerns in these metrics: the potential harm caused by measurements, and the potential harm to the measurements.

The security risks associated with each protocol need to be tackled in the context of EAS and local UPF (re)selection, assuming that EDGE servers, such as the EAS, are placed outside the operator domain.

#### 5.2.1.2 Security threats

Denial of Service: Potential attackers can exploit the capabilities of protocols like ICMP to overwhelm targeted servers like EAS (e.g., ping flood, smurf attacks, etc.).

Spoofing and Theft of service: Without authentication between, the termination points, the client may fake the source address of other device and use the measurement services produced by the server/reflector/receiver.

Tampering: The measurement traffic can be compromised by for example a man-in-the-middle entity, which can inject fake measurement traffic, or give to that a different priority, etc. Consequently, the selection of the server (UPF or EAS) could be biased by the attacker to their interest, leading in the worst-case scenario to the selection of a UPF or EAS already compromised and/or under their control.

#### 5.2.1.3 Potential security requirements

5G system should provide capability to enable security mechanism, e.g., integrity, anti-replay protection, authentication, optionally confidentiality protection, provided by N6 delay measurement protocol(s).

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

### 5.3.1 Key Issue #2.1: Secure retrieval of 5G system UE Ids and privacy related information.

#### 5.3.1.1 Key issue details

This Key issue addresses the security and privacy aspects related to the retrieval of 5G system UE Ids and privacy related information (e.g., UE location) by an Edge Application Server (EAS), Edge Enabler Server (EES) and/or Edge Enabler Client (EEC).

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

The EES uses user information (e.g. IP address) received in the *UE Identifier API* invocation and obtains the UE identifier by interacting with NEF as specified in clause 4.15.10 of 3GPP TS 23.502 [8]. The EES may utilize the Nnef\_UEId\_Get service (clause 4.15.10 of 3GPP TS 23.502 [8]) providing the user information provided by the EEC. Without proper security mechanisms in place, *Nnef\_UEId API* services can be abused, so that UE Id may be disclosed to un-authorized entities, enabling them for example to track UEs.

Since user information may be used to determine the 5G system UE Id and consequently privacy related information (e.g., identity, location, etc.), it is needed to ensure that this user information being used in the APIs (*UE Identifier API* and *Nnef\_UEId* ) is trusted, and that the AFs (EAS, EES, ECS) and EEC are authorized to use this user information as parameter(s) in their API invocations.

Following the security principle of sharing information on a need-to-know principle, it should be analysed whether and how (i.e. under which circumstances) EAS needs to know the 5G UE Id when requesting a service on the UE’s behalf.

The related security and privacy aspects in the use of the *UE Identifier API* and *Nnef\_UEId API* concern the information provided by the EEC, as well as the behaviour of EDGE Application Functions (AFs), namely EAS and EES. The security threats and corresponding requirements have been split to cover both aspects.

#### 5.3.1.2 Security threats

##### 5.3.1.2.1 Threats posed by a malicious EEC

If the User information provided by the EEC is not verified and the EEC is not authorized to use them, a malicious or compromised EEC or a malicious API consumer can try to execute spoofing attacks to learn identifiers of other UEs.

##### 5.3.1.2.2 Threats posed by malicious EAS/EES outside of the operator domain

If the User information provided by the EEC do not ensure the privacy of the UE, EAS/EES can abuse the *UE Identifier API* and/or *Nnef\_UEId* APIs to break UE privacy (e.g., UE identity, location, etc.).

Editor’s note: Whether the abuse of the UE Identifier API and/or Nnef\_UEId APIs can be used to know the network topology is ffs.

#### 5.3.1.3 Potential security requirements

##### 5.3.1.3.1 Verification of the user information provided by the EEC

5G system should support a mechanism to verify the user information provided by EEC.

##### 5.3.1.3.2 Protection of the UE privacy

5G system should verify that the EDGE application functions are authorized to retrieve the 5G system UE Id and that the procedures of calling *UE identifier API* and *Nnef\_UEId API* do not compromise the privacy related information.

# 6 Solutions

Table 6.0-1: Mapping of Solutions to Key Issues

| Solutions | Key Issues |
| --- | --- |
| KI#1.1 | KI #2.1 |
| Solution #1: Usage of existing public IP address to verify EEC provided IP address |  | X |
| Solution #2: Authorizing AF to retrieve UE ID |  | X |
| Solution #3: Secure retrieval of 5G UE Id and privacy related information |  | X |
| Solution #4: Secure retrieval of 5G UE privacy related information based on AKMA |  | X |
| Solution #5: EEC proviced information verification |  | X |
| Solution #6: UE ID token |  | X |
| Solution #7: Verification of EEC provided IP address |  | X |
| Solution #8: Verification of EEC provided IP address using access token |  | X |
| Solution #9: Simplified UE ID token based solution |  | X |
| Solution #10: Reuse NDS/IP to protect N6 delay measurement message | X |  |

## 6.1 Solution #1: Usage of existing public IP address to verify EEC provided IP address

### 6.1.1 Solution overview

This solution is for the key issue # 2.1 on secure retrieval of 5G system UE Ids and privacy related information.

In NAT case, to differentiate different UEs using the same public IP address, the UPF will allocate a unique port number for each UE and the UPF stores the mapping between private IP address, public IP address and port number, the IP information knowed in each node in NAT case is showed in the following figure 6.1.1-1.



Figure 6.1.1-1: NAT procedure

Therefore, to verify the EEC provided IP address, this solution proposes to use the mapping between private IP address, public IP address and port number in the UPF to verify the mapping EEC provided IP address, EES obtained public IP address and port number based on the source IP address and port number of received UE ID API message.This solution can be applied in the case where NAT is embedded in the UPF and no matter which NAT mode is used by UPF.

Editor’s notes: it is FFS for the potential risk of exposing the private and public IP addresses of EEC to an entity as EES.

### 6.1.2 Solution details

The procedure of the solution is presented in figure 6.1.2-1 and steps are explained in detail below.



Figure 6.1.2-1 EEC provided IP address verification via existing public IP address and port number

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

Step 1. The EEC in the UE sends UE Identifier API request with the private IP address#1 to the EES as clause 8.6.5 of 3GPP TS 23.558 [3].

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

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

Steps 4-5. NEF obtains the private IP address#3 from UPF via existing procedure specified in clause 4.15.10 (from step 3 to step 6) of 3GPP TS 23.502 [8].

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

Steps 7-8. NEF obtains AF specific GPSI via existing procedure specified in clause 4.15.10 (from step 7 to step 10) of 3GPP TS 23.502 [8].

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

### 6.1.3 Solution evaluation

This solution addresses the requirements of KI#2.1 on the user information verification.

The EEC provided IP address, public IP address and port number are all provided to NEF, then the NEF retrieves the private IP address corresponding to the public IP address and port number via the exising procedure and performs the EEC provided IP address verification. There is no additional impact to other network functions.

The verification may not be required when the UPF has the mapping table between public IP address and private IP address.

The solution assumes that NAT is embedded in the UPF, and the NAT mapping table can be exposed to EDGE application.

The solution is limited to the verification of the provided private IP address by the EEC to the EES, and used by the EES to invoke NEF API.

## 6.2 Solution #2: Authorizing AF to retrieve UE ID

### 6.2.1 Solution overview

This solution is for KI#2.1 on the secure retrieval of 5G system UE IDs. Since the AF may request for the UE ID without UE authorization, the solution proposes to use fresh hash value with count, which is a changeable value shared between the UE and the 5GC, to authorize the AF to retrieve the UE ID. It can also prevent replay attacks from the malicious entity (e.g., malicious UE or AF).

### 6.2.2 Solution details

This solution supports the 5GC to verify whether the AF is authorized by the UE to retrieve the UE ID based on the IP address, and verify whether the parameters used for verification is replayed by the adversary. Specifically, when the UE receives the UE ID request, it generates a hash value based on the count, salt, SUPI and IP address, and then sends the generated hash value and count to the AF, which uses the IP address to request for the UE ID from the NEF. The NEF then requests BSF to provide information of the UE (i.e., SUPI). Before providing the SUPI of UE, the BSF shall also generate a hash' based on the shared count, salt, SUPI and IP address, and then compare the hash' value with the received hash value. If the hash value is equal to the hash' value, the BSF can provide the SUPI to the NEF. Otherwise, the BSF will provide a failure indication to the NEF.



Figure 6.2.2-1: Authorization of AF and verification of AF provided IP address

Step 0. During the PDU session establishment procedure, SMF generates the salt, which is a random value, and then sends the salt to both UE and BSF. SMF can send the salt to the BSF along with SM policy Association Establishment or SM policy Association Modification message in clauses 4.16.4 or 4.16.5 of TS 23.502 [8]. If the SM policy Association Establishment and SM policy Association Modification procedures are not performed, SMF will not send the salt to the UE.

Step 1. UE receives the UE ID request.

Step 2. The UE generates a hash value based on the SUPI, IP address, salt, and count, and other values that is only known to both the EEC and BSF (e.g., DNN of the PDU Session, and S-NSSAI of the PDU Session). After that, the UE increases the count by 1, which is used for the next hash value generation procedure. Note that the count can be configured to start from 0 in each PDU session.

 Note1: In order to mitigate the rainbow table attack, the following solutions should be adopted:

 (1) using strong hash algorithms, e.g., SHA-256.

 (2) increasing the length of the hash algorithm's input.

* The length of the salt can be set as 128bits to make the rainbow table attack infeasible [15].
* The input space of the SUPI is large enough to mitigate the rainbow table attack, considering that the length of IMSI is 15-16 digits, and NAI is 1-759 bits, as specified in TS 23.003 [16].
* Other inputs, including DNN of the PDU Session, and S-NSSAI of the PDU Session, can also help defend against the rainbow table attack.

 (3) key stretching. The inputs can be run through the hash function multiple times to increase the time to build a precomputed rainbow table.

 Note2: The UE can send the hash value and the count together to avoid the out-of-synchronization between the UE and BSF.

Step 3. The UE sends the generated hash value and count to the AF.

Step 4. The AF invokes the Nnef\_UEId\_Get request with the parameter of hash value, count, and IP address to get the UE ID.

NOTE 1: If private IP address is sent in step 3, then the same private IP address will be sent in step 4.

Steps 5-8. This solution reuses Steps 3-6 in Clause 4.15.10, TS 23.502 [8].

NOTE 2: Steps 5-8 are workable only if NAT is in the UPF.

Step 9. When the NEF invokes the Nbsf\_Management\_Discovery service operation, the NEF provides the hash value and IP address to the BSF.

Step 10. The BSF determines the SUPI, salt and count based on the IP address. The BSF then generates the hash' value, and then compares the hash' value with the received hash value.

Step 11. If the hash' value is equal to the received hash value, the BSF will respond to the NEF with a SUPI. Otherwise, the BSF will respond to the NEF with an indication that request is denied with the reason that the IP address is not associated with the UE.

Steps 12-14. This solution reuse Steps 9-11 in Clause 4.15.10, TS 23.502 [8].

### 6.2.3 Evaluation

The solution addresses the requirement of KI#2.1 related to the authorization of AF to retrieve UE ID. The solution proposes to use the hash value to authorize the AF to retrieve the UE ID based on the SUPI, IP address, count, salt and other values that is known to both the EEC and BSF.

If private IP address is conveyed in step 3, there is a privacy issue as the AF can abuse this information to compromise the privacy of the user.

NOTE: Optional flows (5-8) in Figure 6.2.2-1 are not needed in case UE is allocated with a public IP address.

The solution has the following impacts on the entities/NFs:

1. UE needs to generate hash value based on the SUPI, IP address, count, salt and other values that is known to both the EEC and BSF. UE also needs to update the count.

2. The SMF needs to generate the salt, and forward the salt to the BSF along with SM policy Association Establishment or SM policy Association Modofication message..

3. BSF needs to determine the SUPI, count and salt associated with IP address. BSF also needs to validate the hash value by generating hash' based on the SUPI, count, salt and IP address.

4. The UE and operating system running on the need to support the delivery of the parameters to the EEC.

## 6.3 Solution #3: Secure retrieval of 5G UE Id and privacy related information

### 6.3.1 Introduction

This solution addresses the security requirements exposed in key issue #2.1 related to the secure retrieval of 5G system UE Id and privacy related information, i.e., the verification of the user information provided by the EEC, and the protection of the UE privacy.

The main design principle of the solution is based on the utilization of a temporary identifier (ID) as UE identity to fetch the Application Function (AF) specific UE Id from Nnef\_UEId service. The temporary ID is generated by the 5G Core (e.g., UDM), it includes a randomly generated value, and it is associated to the PDU session (eventually to the AF ID).

### 6.3.2 Solution details

Figure 6.3.2-1 illustrates the procedure to fetch the 5G system UE Id and privacy related information.



Figure 6.3.2-1: Procedure to fetch the 5G system UE Id and privacy related information

Precondition:

Step 0. The EEC requests a Temporary ID to UE through interface provided by UE module.

1. PDU session establishment / modification request is sent from the UE to the 5G system.

2. The 5G Core (e.g., UDM) generates (per UE) an internal temporary ID (with a ramdomly generated part) for PDU session.

NOTE 1: The UE could request multiple temporary IDs during the same PDU session (PDU Session modification). The UE can use this to invalidate previous IDs which might have been compromised and/or at fix intervals without initializing another PDU session establishment/modification.

NOTE 2: The Temporary ID consists of a random part and an identifier of the UDM (UDM group ID) that generated the Temporary ID.

NOTE 3: The Temporary ID could also be generated from SMF and sent to UDM/UDR for storage.

3. The 5G Core returns the internal temporary ID to the UE as part of the NAS PDU session establishment/modification response.

4. The EEC uses the allocated temporary ID, received from the UE, inside the Edge application layer communication with the application function AF (e.g., EAS).

5. The AF uses the received temporary ID to invoke the Nnef\_UEId API intended to fetch the 5G system UE identifier, i.e., AF specific UE Id, as per the procedure described in TS 23.502 figure 4.15.10-1 [8].

6. The NEF verifies the temporary ID, authorizes the request coming from the AF and accordingly retrieves from the 5G Core the AF specific UE Id corresponding to the temporary ID.

NOTE 4: NEF retrieves the correct UDM instance from the UDM identifier in the Temporary ID, and NEF queries UDM to obtain the UE ID from the temporary ID.

7. The NEF replies to the AF with the corresponding AF specific UE Id.

8-9 (Optional). Assuming the application logic requires to fetch the UE location, a location request is sent to the NEF using the AF specific UE Id, and the corresponding information is provided by the 5G system through the NEF.

10. The AF responds to the UE (EEC).

### 6.3.3 Evaluation

The solution requires the generation of a new temporary ID identifier by the 5G Core, e.g. UDM or SMF, that needs to be used in the invocation of Nnef\_UEId API services.

The solution requires UE module to support Temporary ID request from application layer.

The solution avoids the mapping of potentially long-term and easily inferred identifiers, with the 5GS UE Id, to block malicious applications from performing UE tracking type of attacks.

The solution solves the issue of verification of the user information provided by the EEC through the generation of a temporary ID in 5G Core per UE and PDU session, that is verified in the NEF when Nnef\_UEId or other APIs (e.g., location) are invoked by the AF(s). The solution also solves the potential privacy concerns during the retrieval process of 5G system UE Id by avoiding the use of permanent or semi-permanent identifiers.

Editor’s Note: Further evaluation is to be defined.

## 6.4 Solution #4: Secure retrieval of 5G UE privacy related information based on AKMA

### 6.4.1 Introduction

This solution addresses the security requirements exposed in key issue #2.1 related to the secure retrieval of 5G system UE privacy related information, i.e., the verification of the user information provided by the EEC, and the protection of the UE privacy.

The main design principle of the solution is based on AKMA feature, more specifically on the A-KID, an application specific ID derived from the long term symmetric pre-shared key K between the UE and the network. The EDGE application server (EAS) and/or enabler server (EES), use the AKMA protocol to retrieve the 5G UE privacy related information.

The solution assumes that AF (EES/EAS) communicates with 5GC through NEF.

### 6.4.2 Solution details

Figure 6.4.2-1 illustrates the procedure to fetch the 5G system UE privacy related information.



Figure 6.4.2-1: Procedure to fetch the 5G system UE Id and privacy related information

Preliminary steps:

- Primary authentication

- AKMA Key derivation (A-KID) as per procedure in TS 33.535 [9].

- Creation of AKMA context in AAnF (SUPI, KAKMA, A-KID) as per procedure in [9].

1. The application client in the UE (EEC) requests a service to the AF, i.e., EDGE application server (EAS, EES), including the A-KID (AKMA Key Identifier) in the request.

2-5. AKMA procedure intended to provide KAF to the AF from the AAnF via NEF as specified in clause 6.3 of [9].

NOTE: AF specific UE Id does not need to be part of the of the incoming request (step 2), since the NEF will provide the GPSI (external ID) to AF.

6. The AF requires to know privacy information of the UE available in the 5G Core, such as the the location of UE, and makes the request to the 5G Core via NEF, using the given GPSI as UE identifier.

7. The NEF checks the GPSI and if the request is authorized, the corresponding information, in this example location of the UE, is provided to the AF.

8. The AF responds to the UE (EEC).

### 6.4.3 Evaluation

The main impact and assumption of the solution is that it requires the support of AKMA feature in the 5G system. AKMA feature itself, implicitly addresses the first and second requirements (clauses 5.3.1.3.1 and 5.3.1.3.2) simply by reusing the A-KID.

The 5G UE Id is not required to be fetched by the AF, since 5G Core through AKMA feature provides already the authentication service, and the trust between UE, 5G Core and AF. Therefore, the privacy of the UE is implicitly preserved.

The solution avoids the need to retrieve a 5G system UE Id to be used in the invocations of the NEF APIs. AKMA itself ensures the reliability of A-KID, that it is being reused in the AF invocation towards the NEF, instead of using any other identifier provided by the EEC to be further verified in the procedure.

## 6.5 Solution #5: EEC proviced information verification

### 6.5.1 Introduction

This solution addresses key issue #2.1: "5G system should support a mechanism to verify the user information provided by EEC".

Clause 8.6.5 of 3GPP TS 23.558 [3] defines *UE identifier API* which is used by an EAS or EEC to obtain the identifier of the UE if the EAS or EEC does not have it (e.g. it has not already cached).

When EEC invokes the API, if available, this IE contains both UE’s private IPv6 address (due to the existence of NAT66) and UE’s private IPv4 address. According to TS 33.558, EEC authentication is not mandatory, there might be cases that EEC is not authenticated. When EEC is not authenticated, there is risk that the information provided by EEC is not owned by this EEC, leading to the result that the UE indentifier API is abused and other UE information is leaked.

This solution proposed to add the varification method when EEC authentication is not performed.

### 6.5.2 Details

Preassumption: the authenticated EEC will not provide untrusted user information.

Following the procedure in TS 23.558 on EEC requesting UE identifier, it shall provide the security credentials. It is proposed in this solution, that the security credential in the UE Identifier API request can be a certificate to EES to verify, when the EEC doesn’t support any other authentication methods defined in TS 33.558.

 

Step 1. EEC sends the UE Identifier API request, including the User Information (i.e.UE address), EEC signs the User Information using its private key. EEC also includes the Cert information as the security credential field as defined in TS 23.558[3].

Step 2. EES verifies the certificate. If the verification is successful, EES verifies the signature of the User information using the public key.

Step 3-6. Following the TS 23.558 clause 8.6.5.2 step 2-4, EES retrieves UE ID fro NEF and sends it back to EEC.

Editor’s Note: how to address the certificate management issue is FFS.

NOTE: the trustworthiness of EEC provided information is relying on PKI.

### 6.5.3 Evaluation

TBD

Editor’s note: The evaluation should state the applicability of the solution, i.e. what is the solution solving and what are the assumptions.

## 6.6 Solution #6: UE ID token

### 6.6.1 Solution overview

This solution proposes usage of UE ID token to address the security requirements key issue #2.1. With the usage of UE ID token, there will be no need to share private IP address with EEC and other entities in the EC architecture.

### 6.6.2 Solution details

High-level overview of the solution is presented in figure 6.6.2-1 and steps are explained in detail below.



Figure 6.6.2-1: UE ID token based solution

Step 1: The EEC obtains a UE ID token from the UE ID server which is located inside the operator domain. UE ID server can identify the UE by using the private IP address of the PDU session. The UE ID Server can fetch the IP address from the IP packets received from the EEC. The UE ID Server can use the Nbsf\_Management\_Discovery service operation with UE address and IP domain to retrieve the session binding information of the UE. For the UE ID Server service consumption by the EEC, the UE where the EEC is running on needs to execute the primary authentication successfully and have a PDU session. The EEC can authenticate the UE ID Server by using server certificate. The EEC needs to be configured with the root certificate or certificate of the UE ID Server, or the Internet (public) PKI mechanism can be used. The EEC does not need to authenticate with the server since the server issues the UE ID token, which does not include cleartext sensitive information, to the EEC running on the UE who has already executed the primary authentication.

NOTE: Since the issuer and resolver of the UE ID token is the UE ID Server, the details of the UE ID token (e.g., whether it is a signed token or a random number) can be left to implementation.

Step 2: The EEC sends the token to the EES to learn edge specific UE ID.

Step 3: The EES invokes the NEF IP by sending the UE ID token.

Step 4: The NEF interacts with the UE ID server to identify the UE.

Step 5: The NEF sends the UE ID to the EES.

Step 6: The EES sends the response to the EEC.

The UE ID Server is an AF function located inside the HPLMN trust domain and before the execution of NAT. In step 1, the UE ID server uses the UE IP address to identify the UE. For the execution of step 4, the NEF needs to be able to consume the UE ID Server service to obtain the UE ID by providing the UE ID token.

### 6.6.3 Solution evaluation

Solution applicability evaluation:

- The solution addresses both the privacy and prevention against spoofing attacks requirements of key issue #2.1.

- The solution works also for the case that the NAT operation is performed after the UPF.

Solution impact evaluation:

- The solution does not have any impact on the core network functions except the NEF UE ID API.

- The solution does not have any impact on the ME and the USIM. There is impact on the EEC such that the EEC needs to be able to access the UE ID Server, obtain the UE ID token and provide the token to the EES.

- The procedure in TS 23.558 clause 8.6.5.2 needs minor update to allow the EEC to use the UE ID token instead of UE IP address.

- A new AF (UE ID Server) needs to be introduced.

- A new interface between the UE ID Server and the NEF for the NEF to be able to consume the UE ID Server service is required.

- EES Eees\_UEIdentifier API and NEF's Nnef\_UEId API needs minor update to allow the use of UE ID token as an input parameter.

## 6.7 Solution #7: Verification of EEC provided IP address

### 6.7.1 Solution overview

This solution addresses the security requirement of key issue#2.1 on EEC provided IP address verification.

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

### 6.7.2 Solution details



Figure 6.7.2-1: EEC provided IP address verification

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

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

NOTE: With SUPI, the NEF fetches the PDU session ID to be sent in step 4. As per clause 5.2.3.3 in TS 23.502 [8], SUPI is sent as the “key for subscription data type” in the request message for subscription data type “UE context in SMF data” (Step 3). The required output includes the requested subscription data i.e., PDU session ID(s) for the UE also in Step 4.

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

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

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

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

Editor’s Note: Whether there is a privacy on usage of PDU session ID and whether usage of PDU session ID as secret information is enough to prevent spoofing attacks are FFS.

### 6.7.3 Solution evaluation

This solution addresses the potential security requirements. The existing parameter, PDU session ID (already available in the UDM (TS 23.502 [8])) is used for IP address authenticity verification and the impact is including the PDU Session ID in the Nudm\_SDM\_Get response and check to be performed by the NEF.

Editor’s Note: Additional evaluation is FFS.

## 6.8 Solution #8: Verification of EEC provided IP address using access token

### 6.8.1 Solution overview

This solution addresses the security requirement of key issue#2.1 on EEC provided IP address verification.

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

### 6.8.2 Solution details



Figure 6.8.2-1: EEC provided IP address verification

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

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

Editor’s note: How NEF gets the SUPI for the IP address is FFS.

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

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

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

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

### 6.8.3 Solution evaluation

This solution addresses the potential security requirements of key issue#2.1. The UE ID in the access token (as specified TS 33.558 [4], clause 6.3) assigned by the ECS is used for the IP address authenticity verification.

Editor’s note: Applicability of the solution and additional evaluation is FFS.

## 6.9 Solution #9: Simplified UE ID token based solution

### 6.9.1 Solution overview

This solution proposes usage of UE ID token to address the security requirements of key issue #2.1. With the usage of UE ID token, there will be no need to share private IP address with EEC and other entities in the EC architecture. In section 6.9.2, the generic view of the solution is presented and how the solution can work for the following special cases of NEF API invocation by the EAS, NEF API invocation by the EES, and EES API invocation by the EAS is explained.

### 6.9.2 Solution details

Generic representation of the solution is presented in Figure 6.9.2-1.



Figure 6.9.2-1: Generic view of UE ID token based solution

Step 1: The client obtains a UE ID token from the UE ID server which is located inside the operator domain. UE ID server can identify the UE by using the private IP address of the PDU session. The UE ID Server can fetch the IP address from the IP packets received from the Client. The UE ID Server can use the Nbsf\_Management\_Discovery service operation with UE address and IP domain to retrieve the session binding information of the UE. For the UE ID Server service consumption by the client, the UE where the client is running on needs to execute the primary authentication successfully and have a PDU session. The client can authenticate the UE ID Server by using server certificate. The Client needs to be configured with the root certificate or certificate of the UE ID Server, or the Internet (public) PKI mechanism can be used. The client does not need to authenticate with the server since the server issues the UE ID token, which does not include cleartext sensitive information, to the client running on the UE who has already executed the primary authentication.

NOTE: Since the issuer and resolver of the UE ID token is the UE ID Server, the details of the UE ID token (e.g., whether it is a signed token or a random number) can be left to implementation.

Step 2: The client forwards the token to the AF.

Step 3: The AF invokes a NEF service and use the UE ID token as UE identifier.

Step 4: The NEF interacts with the UE ID server to resolve the UE ID token into UE information (e.g., private IP address, MSISDN, SUPI) needed for the operation.

Step 5: The UE ID server returns the requested information.

Step 6: The NEF interacts with other NFs as per existing NEF service procedures as per TS 23.502.

Step 7: The NEF returns the result of the NEF service execution.

Note that if the AF is a trusted AF, it can directly interact with the UE ID Server to identify the UE and the obtain required information such as IP address, and then invoke the NF/NEF directly with the required inputs.

Application of the solution to the case of NEF API invocation by the EAS/EES is presented in Figure 6.9.2-2.



Figure 6.9.2-2: The EAS/EES invokes NEF API

Step 1: The AC/EEC obtains a UE ID token from the UE ID server.

Step 2: The AC or the EEC respectively forward the token to the EAS or the EES.

Step 3: The EAS/EES invokes a NEF service and use the UE ID token as UE identifier.

Step 4: The NEF interacts with the UE ID server to resolve the UE ID token into UE information (e.g., private IP address, MSISDN, SUPI) needed for the operation.

Step 5: The UE ID server returns the requested information.

Step 6: The NEF interacts with other NFs as per existing NEF service procedures as per TS 23.502.

Step 7: The NEF returns the result of the NEF service execution.

Application of the solution to the case of EES API invocation by the EAS is presented in Figure 6.9.2-3.



Figure 6.9.2-3: The EAS invokes the EES API

Step 1: The AC obtains a UE ID token from the UE ID server.

Step 2: The AC forwards the token to the EAS.

Step 3: The EAS invokes a EES service and use the UE ID token as UE identifier.

Step 4: The EES invokes the NEF API by sending the UE ID token.

Step 5: The NEF interacts with the UE ID server to resolve the UE ID token into UE information (e.g., private IP address, MSISDN, SUPI) needed for the operation.

Step 6: The UE ID server returns the requested information.

Step 7: The NEF sends the UE ID to the EES.

Step 8: The EES returns the result of the EES service execution.

### 6.9.3 Solution evaluation

Solution applicability evaluation:

- The solution addresses both the privacy and prevention against spoofing attacks requirements of key issue #2.1.

- The solution works also for the case that the NAT operation is performed after the UPF.

- The solution does not require interaction between AC and EEC.

- The EAS only learns the UE ID token, so there is no need to assign AF specific GPSI for the EAS.

Solution impact evaluation:

- The solution does not have any impact on the ME and the USIM. There is impact on the Client (the EEC and the AC) such that the Client needs to be able to access the UE ID Server, obtain the UE ID token and provide the token to the EAS/EES.

- The solution has impact on NEF services. To reduce the impact the UE ID token can be provided as input in any NEF Service that takes GPSI as input (as NAI/External Id format).

- The procedure in TS 23.558 clause 8.6.5.2 needs minor update to allow the EEC to use the UE ID token instead of UE IP address.

- A new AF (UE ID Server) needs to be introduced.

- A new interface between the UE ID Server and the NEF for the NEF to be able to consume the UE ID Server service is required.

- EES Eees\_UEIdentifier API and NEF's Nnef\_UEId API needs minor update to allow the use of UE ID token as an input parameter.

## 6.10 Solution #10: Reuse NDS/IP to protect N6 delay measurement message

### 6.10.1 Introduction

This solution is for the key issue # 1.1 on Security aspects related to enhancements of EAS and local UPF (re)selection.

This solution propose to reuse the NDS/IP as specified in TS 33.210 [17].

### 6.10.2 Solution details

For the N6 delay measurement protocol works on the transport layer, traffic can be both integrity and confidentiality protected at network layer according to NDS/IP as specified in TS 33.210 [17].

### 6.10.3 Evaluation

The NDS/IP may introduce operational complexity, overload the communication. Due to known vulnerability of some unsecure IP measurement protocol (e.g. ICMP), it can be filtered by firewall or security gateway of data network.

# 7 Conclusions

## 7.1 KI#1.1: Security aspects related to enhancements of EAS and local UPF (re)selection.

In conclusion of KI#2 of TR 23.700-49 (see 8.2 of [2]):

- N6 delay between 5GC N6 termination point (i.e. UPF) and the measurement endpoint at application side (i.e. EAS IP address(es)/Designated IP (range)) is measured by leveraging existing mechanisms (e.g. ICMP, TWAMP, OWAMP or other protocols defined by IETF).

The following guidelines from the security point of view for the N6 delay measurement between UPF PSA and EAS will be documented:

- It is recommended to use of the measurement protocols supporting authentication, integrity, and anti-replay protection.

- It is recommended not to use a delay measurement mechanism that requires sensitive information exchange but does not support confidentiality by the measurement protocols.

- It is not recommended to use a measurement protocol without authentication, integrity and anti-replay protection in place.

- It is not recommended to use a measurement protocol with disclosed vulnerabilities which may be exploited for attack or blocked by the operators.

NOTE: The enablement of the security mechanisms available in the selected measurement protocol, i.e., the configuration and provision of corresponding security parameters, makes use of existing procedures to enable N6 delay measurement defined in TS 23.548 [7] and TS 23.502 [8].

## 7.2 KI#2.1: Secure retrieval of 5G system UE Ids and privacy related information

The following solution design principles are to be followed in normative phase:

- The information used in Nnef\_UEId API call invocation and UE Identifier API call invocation needs to prevent the use of permanent or semi-permanent UE identifiers subject to be abused/compromised by malicious applications.

- The entity responsible for the generation of the information needs to be part of the 5G system in HPLMN, and needs to be verified by the 5G system in HPLMN. Alternatively, the information can be generated by both the UE and the 5G system.

- The information may be used by the AF invoking the NEF APIs, so that the NEF APIs can identify the UE by using the information.

NOTE 1: The API invoker does not need to obtain the permanent 5G UE ID, which improves the privacy.

Alternative solutions having the design principles above will be captured in an informative annex in the normative work.

NOTE 2: The principles above will not prevent usage of existing mechanisms of Nnef\_UEId API and UE Identifier API.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-04 | SA3#115 Adhoc-e | S3-241217 |  |  |  | Skeleton of TR33.749 | 0.0.0 |
| 2024-04 | SA3#115 Adhoc-e | S3-241569 |  |  |  | Included changes from S3-241564 and S3-241216 | 0.1.0 |
| 2024-05 | SA3#116 | S3-242604 |  |  |  | Included changes from S3-242567 and S3-242661 | 0.2.0 |
| 2024-08 | SA3#117 | S3-243721 |  |  |  | Included changes from S3-243627, S3-243628, S3-243629, S3-243630, S3-243631, S3-243632, S3-243633, S3-243634, S3-243635 and S3-243665  | 0.3.0 |
| 2024-10 | SA3#118 | S3-243833 |  |  |  | Included changes from S3-244050, S3-244286, S3-244428, S3-244429, S3-244430, S3-244431, S3-244432, S3-244434, S3-244435, S3-244437, S3-244501, S3-244502 | 0.4.0 |
| 2024-11 | SA3#119 | S3-245198 |  |  |  | Included changes from S3-245272, S3-245273, S3-245274, S3-245348 and S3-245349 | 0.5.0 |