|  |  |
| --- | --- |
| 3GPP TR 33.749 V0.2.0 (2024-05) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on security aspects of enhancement of support for  edge computing in 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 address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 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 members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 7

3.3 Abbreviations 7

4 Overview 7

5 Key issues 7

5.1 General 7

5.2 Key issues related with 5G System Enhancements for Edge Computing 8

5.2.X Key Issue #X: <Key Issue Name> 8

5.2.X.1 Key issue details 8

5.2.X.2 Threats 8

5.2.X.3 Potential security requirements 8

5.3 Key issues related with enhanced architecture for enabling Edge Applications 8

5.3.1 Key Issue #2.1: Secure retrieval of 5G system UE Ids and privacy related information. 8

5.3.1.1 Key issue details 8

5.3.1.2 Security threats 8

5.3.1.2.1 Threats posed by a malicious EEC 8

5.3.1.2.2 Threats posed by malicious EAS/EES outside of the operator domain 8

5.3.1.3 Potential security requirements 8

5.3.1.3.1 Verification of the user information provided by the EEC 8

5.3.1.3.2 Protection of the UE privacy 8

5.3.X Key Issue #X: <Key Issue Name> 8

5.3.X.1 Key issue details 8

5.3.X.2 Security threats 8

5.3.X.3 Potential security requirements 8

6 Solutions 8

6.1 Solution #1: Usage of existing public IP address to verify EEC provided IP address 8

6.1.1 Solution overview 8

6.1.2 Solution details 8

6.1.3 Solution evaluation 8

6.Y Solution #Y: <Solution Name> 8

6.Y.1 Introduction 8

6.Y.2 Solution details 8

6.Y.3 Evaluation 8

7 Conclusions 8

Annex <X> (informative): Change history 9

# 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)".

# 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].

<ABBREVIATION> <Expansion>

# 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

Editor’s Note: This clause contains all the key issues identified during the study.

## 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.X Key Issue #X: <Key Issue Name>

#### 5.2.X.1 Key issue details

#### 5.2.X.2 Threats

#### 5.2.X.3 Potential security requirements

## 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.

### 5.3.X Key Issue #X: <Key Issue Name>

#### 5.3.X.1 Key issue details

#### 5.3.X.2 Security threats

#### 5.3.X.3 Potential security requirements

# 6 Solutions

Table 6.0-1: Mapping of Solutions to Key Issues

| Solutions | Key Issues |
| --- | --- |
| KI #2.1 |
| Solution #1: Usage of existing public IP address to verify EEC provided IP address | 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.

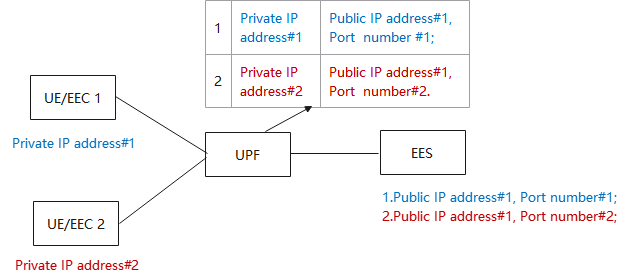


Figure 6.1.1-1: NAT procedure

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.

Editor’s notes: it is FFS if the NAT is not embedded in the UPF.

Editor’s notes: it is FFS if the verification is required when the UPF has the mapping table between public IP address and private IP address.

Editor’s notes: it is FFS for all the NAT cases, such as PBA (Port based allocation) or deterministic NAT.

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.

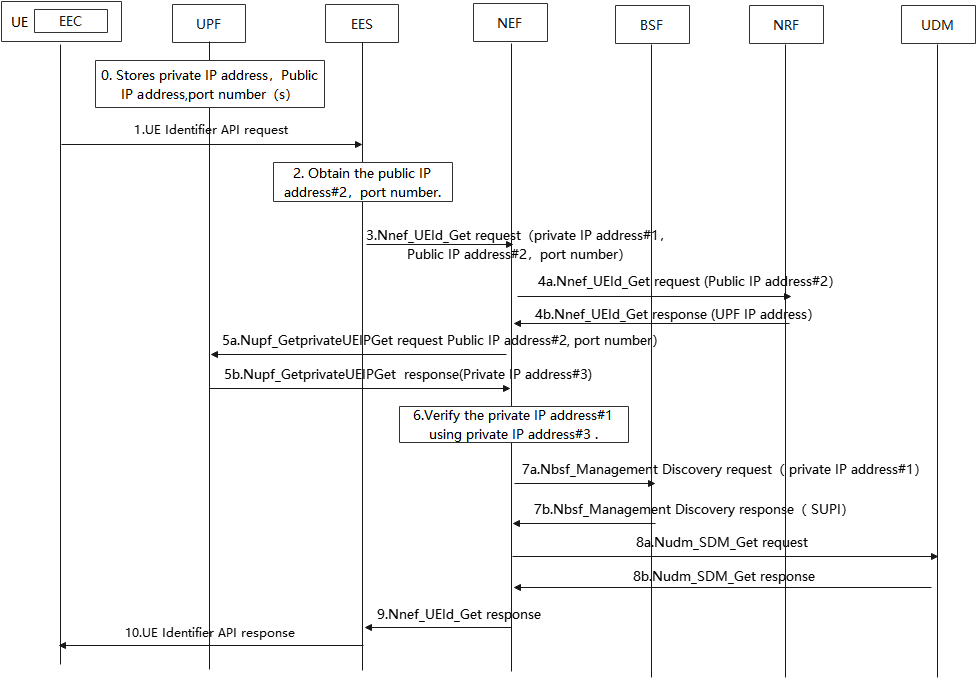


Figure 6.1.2-1 EEC provided IP address verification via existing public IP address and port number

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

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

## 6.Y Solution #Y: <Solution Name>

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

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 |