|  |  |
| --- | --- |
| 3GPP TR 33.892 V18.0.0 (2023-09) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on UE Route Selection Policy (URSP) rules  to securely identify applications  (Release 18) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 6

4 Void 6

5 Key issues 7

5.1 Key issue #1: Determination of application identification 7

5.1.1 Key issue details 7

5.1.2 Threats 7

5.1.3 Potential security requirements 7

6 Proposed solutions 7

6.0 Mapping of solutions to key issues 7

6.1 Solution #1: Provide additional authentication information to enhance URSP policy enforcement 7

6.1.1 Introduction 7

6.1.2 Solution details 8

6.1.3 Evaluation 8

6.2 Solution #2: Solution on enhancing the URSP rule with certificate fingerprint 9

6.2.1 Introduction 9

6.2.2 Solution details 9

6.2.3 Evaluation 10

6.3 Solution on prevention of URSP rule misuse by a non‑genuine application using home network anchor 11

6.3.1 Introduction 11

6.3.2 Solution details 11

6.3.2.1 Overview 11

6.3.2.2 URSPAUTH-MAC-IAUSF generation function 12

6.3.3 Evaluation 12

7 Conclusions 12

Annex A: Change history 13

# 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 analyses mechanisms to ensure the identity of a genuine application in order to apply the URSP rule accordingly, such that malicious applications cannot get access towards the operator regulated resources. The present document identifies key issues and develops solutions for enhancements that enables a URSP rule to securely identify the application for which the URSP rule should be applied.

# 2 References

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

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

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

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

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

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

# 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

Void.

## 3.3 Abbreviations

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

# 4 Void

# 5 Key issues

## 5.1 Key issue #1: Determination of application identification

### 5.1.1 Key issue details

The application identity within the traffic descriptor component of an URSP rule is used in the UE to identify the traffic of an application and to map it to the data connection with specific data connection parameters. Since the application identity can be set during the development of the application, and is non-protected, it is not suitable to uniquely identify the traffic of the application, intended to be managed by the operator. The user may install an application on the UE with the same application identity in order to transmit the traffic based on the URSP rule, which was designed to be applied for the traffic of the genuine application.

The key issue studies mechanisms to help the UE to identify the genuine application for a correct traffic mapping according to the URSP rule.

### 5.1.2 Threats

Applications may use the identity of the genuine operator managed application in order to transmit the traffic based on the URSP rule, which was designed to be applied for the traffic of the genuine application.

### 5.1.3 Potential security requirements

The UE should have sufficient information to identify the genuine application.

# 6 Proposed solutions

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 |
| Provide additional authentication information to enhance URSP policy enforcement | x |  |  |
| Solution #2: Solution on enhancing the URSP rule with certificate fingerprint | X |  |  |
| Solution on prevention of URSP rule misuse by a non-genuine application using home network anchor | X |  |  |

## 6.1 Solution #1: Provide additional authentication information to enhance URSP policy enforcement

### 6.1.1 Introduction

The solution provides a UE platform agnostic method to provide additional authentication information which can be used to enhance URSP policy enforcement in the UE.. The solution provides a method to add additional authentication information to a URSP policy and update the policy in the UE. The solution reuses existing methods to input the additional authentication information and update the policy. The content of the additional authentication information could as an example be token but is out of scope of the present document. The solution provides a mean for the UE to receive additional authentication information accompanying the application ID enabling the UE to enhance the policy enforcement.

NOTE: The additional authentication information is data accompanying the application ID solely used to improve the authentication of rules bound to that application ID. The content of the additional authentication information is out of scope of 3GPP.

### 6.1.2 Solution details

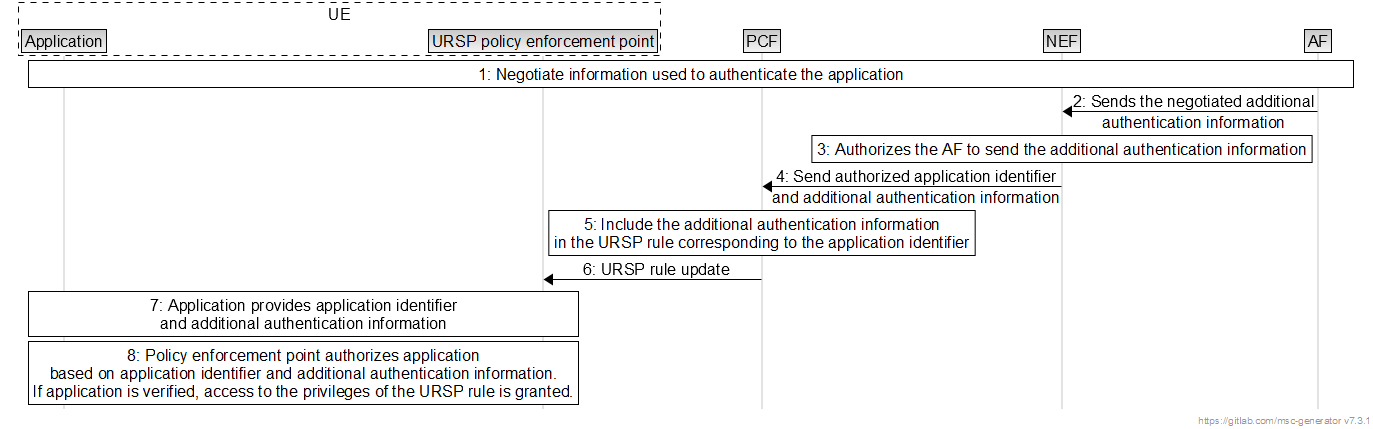


Figure 6.1.2-1

1. UE application and backend application function negotiates authentication data. This can be a token, signature etc. The negotiation protocol is out of scope of the present document. The step can be omitted if data is already pre-provisioned or negotiation is unnecessary for the proprietary application verification method.

2. The AF sends the application authentication information to the NEF to be included in the URSP rule.

3. NEF authorizes the AF to update the URSP rule with the additional authentication information.

4. NEF provides the application ID together with additional authentication information. The interaction between NEF and PCF is described in 3GPP TS 23.503 [2], clause 5.3.10.

5. The PCF includes the application identifier and additional authentication information in the policy as described in 3GPP TS 23.503 [2], clause 6.2.1.2.

6. The PCF triggers a policy update using existing methods.

7. Application provides additional authentication information along application identifier. The interaction between URSP enforcement point and application is out of scope of the present document.

8. The policy enforcement point authenticates the application using the provided additional authentication information.

EXAMPLE: The content of the additional authentication information could be a seed for an OTP generator. When the rule is validated, the genuine application will fetch an OTP from the application function and provide it to the URSP policy enforcement point along with the application identifier. The seed in the URSP policy will enable policy enforcement point to verify the OTP from the application and hereby the application. This is an EXAMPLE of the potential content of the additional authentication information but not part of the solution.

### 6.1.3 Evaluation

The solution proposes a UE platform independent exchange of additional authentication information which enables a scalable method which can be used across platforms. The solution extends the URSP policy with an additional field containing the additional authentication information and reused already existing methods to inject information into the policy and update the policy enforced in the UE. The solution leaves the enforcement of the policy and hereby the usage of the additional authentication information to the application function and UE platform.

System impact:

- Additional field added to the URSP.

- PCF: Injection of additional authentication data into the field.

- UE: Parsing and collecting the additional authentication data from the URSP.

NOTE: Further evaluation is not addressed in the present document.

## 6.2 Solution #2: Solution on enhancing the URSP rule with certificate fingerprint

### 6.2.1 Introduction

This solution is addressing key issue #1 "Determination of application identification".

Every UE application is signed with a unique digital certificate, which typically contains a validity period, the publisher of the application, the public key of the publisher, etc. Before the application is published (e.g. to a mobile marketplace), it is cryptographically signed by using the private key of the publisher, which is a unique key only known by the publisher. An example of an application signing procedure is shown in the figure below. The generated digital signature and the digital certificate that can be used to validate the authenticity of the application, both are included in the application package, which can be published and distributed.



Figure 6.2.1-1: Example of application signing

A non-genuine application with the same application ID as the genuine application would have a different certificate, since the developer of the non-genuine application does not have access to the private key of the genuine application publisher. Therefore the proposal is that the URSP rule is enhanced to include a fingerprint (hash) of the genuine publisher certificate so that the UE can easily compare it with the fingerprint of the certificate of the application which is installed on the UE.

### 6.2.2 Solution details

As a precondition, the UE has installed an application with a specific application ID and it computed the fingerprint of the embedded certificate of the publisher of that application.



Figure 6.2.2-1: URSP rule delivery procedure

1. The PCF is provisioned with the application ID and additionally with the fingerprint of the certificate of the genuine publisher from an AF.

2. If the UE should receive the application specific URSP rule, the PCF will send a URPS rule delivery message with the application ID, certificate fingerprint and routing information, etc., to the UE.

3. If the installed application in the UE wants to send data, the UE determines whether the application ID and the publisher certificate fingerprint of the installed application matches with the ones included in the URSP rule. If the match is successful, the UE applies the URSP rule accordingly.

Since every application is signed with the certificate that is included in the application package, the UE will determine whether a certificate is from a genuine publisher or installed from a different developer, even if the application IDs are the same. A non-genuine application cannot include the genuine certificate since the developer of the non-genuine application does not have the private key of the genuine application to sign it. Thus if the genuine certificate would be included in the non-genuine application package and the signature would be computed with another key, the UE would not install the application because the signature, computed with the public key of the genuine certificate, does not match the one computed by the non-genuine application developer.

### 6.2.3 Evaluation

The PCF needs to be provisioned with the fingerprint of the certificate of the genuine application publisher additionally to the application ID, the URSP rule needs to be enhanced to carry the certificate fingerprint and the UE needs to take the certificate fingerprint into account, additionally to the application ID, when applying a URSP rule. For the same app installed in different UEs, the same fingerprint is used.

This solution does not mitigate the identified threats if an attacker compromises the UE and tampers with any stored app certificates or fingerprints of it.

The mechanism proposed in this solution can also be overcome if the attacker gets access to the execution environment(s) of the UE where the computation or comparison of the fingerprints are performed.

NOTE: Further evaluation is not addressed in the present document.

## 6.3 Solution on prevention of URSP rule misuse by a non‑genuine application using home network anchor

### 6.3.1 Introduction

This solution proposes a method to address key issue #1 "Determination of application identification". The solution can be seen as an extension of Solutions 1 and 2 above. Solution 1 provisions "authentication information" that can be used to check whether an application is genuine. Solution 1 doesn't provide any specific example, while solution 2 is a subset of solution 1, which uses the fingerprint of application certificate signed by the application publisher. In both cases, PCF is provisioned with static materials for each application. The solution proposed below extends the above solution by providing guarantees that, even when a non-genuine application copies the "fingerprint" or "authentication information", UE will not map the data from the non-genuine application according to the URSP rule.

### 6.3.2 Solution details

#### 6.3.2.1 Overview

The PCF may decide to perform URSP Parameters Update anytime after the UE has been successfully authenticated and registered to the 5G system. The security procedure for the URSP rule delivery procedure is described below in figure 6.3.2.1-1.



Figure 6.3.2.1-1: Prevention of URSP rule misuse by non-genuine application

1. The PCF is provisioned with the application ID and the authentication information or token or certificate of the genuine publisher from an AF. The PCF decides to perform the URSP Parameters Update (URSP).

NOTE 1: The scope of what is being provisioned as authentication material should be outside the scope of 3GPP. Static authentication information may include the application's certificate or token shared between the application client and server or any other application-specific information.

2-3 The PCF invokes Nausf\_URSPProtection service operation message by including the 'authentication information or token or certificate to the AUSF to get URSPAUTH-MAC-IAUSF and CounterURSP.

4-5 The PCF uses existing methods for URSP delivery procedure, which contains URSP Parameters Update Data, URSPAUTH-MAC-IAUSF, and CounterURSP.

6. If the installed application in the UE wants to send data, the UE calculates the URSPAUTH-MAC-IAUSF in the same way as the AUSF with the application id and other authentication material or token or certificate. If the match is successful, the UE applies the URSP rule accordingly.

NOTE 2: It is not addressed in the present document whether end-to-end protection is needed.

#### 6.3.2.2 URSPAUTH-MAC-IAUSF generation function

When deriving a URSPAUTH-MAC-IAUSF from KAUSF, the following parameters shall be used to form the input S to the KDF:

- FC = 0xPP.

- P0 = Application ID + Authentication Information.

- L0 = length of Application ID + Authentication Information.

- P1 = CounterURSP.

- L1 = length of CounterURSP.

Key used: KAUSF.

Output: 128 least significant bits of the output of the KDF.

### 6.3.3 Evaluation

The evaluation is not addressed in the present document.

# 7 Conclusions

No agreement could be reached.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| Date | Meeting | TDoc | CR | Rev | Cat | Subject/Comment | New version |
| 2022-07 | SA3#107e-AdHoc | S3-221593 |  |  |  | Skeleton | 0.1.0 |
| 2022-07 | SA3#107e-AdHoc | S3-221594 |  |  |  | KI | 0.1.0 |
| 2022-08 | SA3#108e | S3-221811, S3-221902, S3-222425 |  |  |  | Scope, solution#1, solution#2 | 0.2.0 |
| 2022-10 | SA3#108e-AdHoc | S3-222564, S3-222964,  S3-222968,  S3-223073 |  |  |  | Actor & Attack models, updates of KI#1, solution#1, solution#2 | 0.3.0 |
| 2022-11 | SA3#109 | S3‑224177 |  |  |  | Solution#3 | 0.4.0 |
| 2023-02 | SA3#110 | S3-230944, S3-231542, S3-231543, S3-231544 |  |  |  | Removal of Editor’s Notes and added Evaluations | 0.5.0 |
| 2023-03 | SA#99 | SP-230135 |  |  |  | Presented for information | 1.0.0 |
| 2023-08 | SA3#112 | S3-234316 |  |  |  | Conclusions and clean up | 1.1.0 |
| 2023-09 | SA#101 | SP-230871 |  |  |  | Presented for approval | 2.0.0 |
| 2023-09 | SA#101 |  |  |  |  | EditHelp review and upgrade to change control version | 18.0.0 |