|  |
| --- |
| 3GPP TR 33.700-22 V0.1.0 (2024-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of CAPIF Phase3 (FS\_CAPIF\_Ph3-sec)(Release 19) |
|   |
|  | 3GPP-logo_web |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2022, 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 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 8

4 High-level architectures 8

4.1 High-level architecture for RNAA 8

4.2 High-level architecture for CAPIF interconnection 8

5 Key issues 10

5.1 Key issue #1: Nested API invocation 10

5.1.1 Key issue details 10

5.1.2 Security threats 10

5.1.3 Potential security requirements 10

5.2 Key Issue #2: Authorizing API invoker on one UE accessing resources related to another UE 10

5.2.1 Key issue details 10

5.2.2 Security threats 10

5.2.3 Potential security requirements 11

5.3 Key Issue #3: Security of resource owner authorization management and CAPIF-8 reference point 11

5.3.0 Introduction 11

5.3.1 Key Issue #3.1: CAPIF-8 reference point 11

5.3.1.1 Key issue details 11

5.3.1.2 Security threats 11

5.3.1.3 Potential Security Requirement 12

5.3.2 Key Issue #3.2: Resource owner authorization management 12

5.3.2.1 Key issue details 12

5.3.2.2 Security threats 12

5.3.2.3 Potential Security Requirement 12

5.3.3 Key Issue #3.3: Finer granular authorization 12

5.3.3.1 Key issue details 12

5.3.3.2 Security threats 12

5.3.3.3 Potential Security Requirement 13

5.4 Key issue #4: CAPIF interconnection security 13

5.4.1 Key issue details 13

5.4.2 Security threats 14

5.4.3 Potential security requirements 14

5.5 Key Issue KI#5: Authenticating multiple API invokers of the same Resource Owner 15

5.5.1 Key Issue details 15

5.5.2 Security threats 15

5.5.3 Security requirements 15

6 Proposed solutions 15

6.0 Mapping of solutions to key issues 15

6.Y Solution #Y: <Title> 15

6.Y.1 Introduction 15

6.Y.2 Solution details 16

6.Y.3 Evaluation 16

7 Conclusions 16

Annex <X>: Change history 17

# 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 …

# 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 23.222: "Common API Framework for 3GPP Northbound APIs".

[3] 3GPP TR 23.700-22: "Study on CAPIF Phase 3".

[4] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs".

# 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 High-level architectures

## 4.1 High-level architecture for RNAA



Figure 4.1-1: High level functional architecture for CAPIF supporting RNAA

According to TS 23.222[X], the authorization function is an internal entity of the CAPIF core function.

The resource owner function interacts with the authorization function in the CAPIF core function via CAPIF-8. The resource owner function communicates with the authorization function in the CAPIF core function to manage resource owner consent.

## 4.2 High-level architecture for CAPIF interconnection

Accoridng to TS 23.222 [X], figure 4.2-Y shows the architectural model for the CAPIF interconnection which allows API invokers of a CAPIF provider to utilize the service APIs from the 3rd party CAPIF provider.

The API invoker within the trust domain of CAPIF provider A onboads in CCF of CAPIF provider A.

The API invoker within the trust domain of CAPIF provider A interacts with the CAPIF core function of the CAPIF provider A via CAPIF-1 and discovers the service APIs of both CAPIF providers, and invokes the service APIs in the trust domain of CAPIF provider A via CAPIF-2 and invokes the service APIs in the trust domain of CAPIF provider B via CAPIF-2e.



Figure 4.2-1: High level functional architecture for CAPIF interconnection with multiple CAPIF provider domains

Accoridng to TS 23.222 [X], figure 4.2-Z shows the architectural model for the CAPIF interconnection within the same CAPIF provider domain, which allows API invokers of CAPIF core function 1 to utilize the service APIs from CAPIF core function 2, where both CAPIF core function 1 and CAPIF core function 2 are hosted within the trust domain of the CAPIF provider A.

The API invokers of CAPIF core function 1 indicates that API invoker onboards in CAPIF core function 1.



Figure 4.2-2: High level functional architecture for CAPIF interconnection within a CAPIF provider domain

# 5 Key issues

## 5.1 Key Issue #1: Security of resource owner authorization management and CAPIF-8 reference point

### 5.1.0 Introduction

The key issue is addressing KI#1 and KI#3 of TR 23.700-22 [3] and consists of three sub-key issues for security of CAPIF-8 reference point, resource owner authorization management and finer granular authorization.

This key issue identifies the security aspects of resource owner authorization management and enhancements to the CAPIF architecture considering the Resource Owner Function (ROF) functionalities and its interactions with the CAPIF entities (e.g., CAPIF-8 related interactions) studied in TR 23.700-22 [3].

NOTE: Coordination with SA6 is needed.

Editor’s notes: Currently resource owner authorization terminology is used in the present document. Decision on which terminology (resource owner authorization, resource owner permission, or resource owner consent) to use, the definition of the term and alignment between the present document and TR 23.700-22 are FFS.

### 5.1.1 Key Issue #1.1: CAPIF-8 reference point

#### 5.1.1.1 Key issue details

The security requirements, the security models, and the baseline security procedures for the CAPIF have been specified in 3GPP TS 33.122 [4]. Based on CAPIF RNAA architecture specified in TS 23.222 [2], the CAPIF allows the resource owner to provide authorization to the API invocation for resource access. For that purpose, CAPIF-8 reference point was introduced to CAPIF RNAA. However, how to secure the transport of messages over CAPIF-8 was not specified in TS 33.122 [4] Rel-18, and part of the security procedures between the ROF and the authorization function/CCF supporting the Resource owner-aware Northbound API Access (RNAA) are left open in Release 18, as stated in the authorization procedures in the clause 6.5.3 of 3GPP TS 33.122 [4]. It becomes apparent that the security aspects for the architecture enhancements are open issues in the Release 19 study, as also stated in the TR 23.700-22 [3].

#### 5.1.1.2 Security threats

Without integrity protection for CAPIF-8 reference point, messages over the CAPIF-8 reference point can be modified by attackers.

Without confidentiality protection for CAPIF-8 reference point, messages over the CAPIF-8 reference point can be sniffed by attackers.

Without the anti-replay attack mechanism for CAPIF-8 reference point, messages over the CAPIF-8 reference point can be replayed by attackers.

Editor’s note: What privacy threats exist is FFS if CAPIF-8 reference point has been protected by confidentially, integrity and anti-replay mechanisms.

#### 5.1.1.3 Potential Security Requirement

The transport of messages over the CAPIF-8 reference point should be integrity protected.

The transport of messages over the CAPIF-8 reference point should be protected from replay attacks.

The transport of messages over the CAPIF-8 reference point should be confidentiality protected.

### 5.1.2 Key Issue #1.2: Resource owner authorization management

#### 5.1.2.1 Key issue details

KI#1 of TR 23.700-22 [3] is studying resource owner authorization management (e.g., authorizing access to the resource owner's resource or revoking the authorization of access to the resource owner's resource). There is a NOTE in TR 23.700-22 [3]:

NOTE: Aspects pertaining to the definition of resource owner consent/authorization over CAPIF-8 are in the scope of SA3, noting that the R18 security aspects of CAPIF supporting RNAA are specified in 3GPP TS 33.122 [3].

This key issue studies how to authenticate and authorize the resource owner to provide resource owner authorization.

Editor’s note: Further security threats and potential security requirements in this key issue is FFS.

#### 5.1.2.2 Security threats

Without the authentication between resource owner and authorization server, malicious resource owner can impersonate victim resource owner to do resource owner authorization management.

#### 5.1.2.3 Potential Security Requirement

Mutual authentication between the authorization server and the resource owner should be supported.

CAPIF RNAA should support to authorize the resource owner to provide resource owner authorization.

CAPIF RNAA should support authorization of API invoker based on resource owner authorization and should support revocation of the resource owner authorization.

### 5.1.3 Key Issue #1.3: Finer granular authorization

#### 5.1.3.1 Key issue details

One additional aspect regarding the resource owner authorization management is about the granularity of the authorization information. According to TR 23.700-22 [3], one of the open issues is

*How to align and manage* ***access control*** *that is* ***more granular than*** *simply* ***granted/denied*** *for service API (e.g., service operation level, resource level, service API originator/requestor details) with the provided resource owner consent to ensure appropriate usage of resource owner consent at the enabler layer.*

It has been stated in the TR 23.700-22 [3] that the corresponding security aspects are in the scope of SA3. The objective of this sub-key issue is also to study how to secure authorization procedures with finer granularity.

#### 5.1.3.2 Security threats

Without finer granular authorization and revocation, the system can allow resource access more than necessary. This can cause service resources being abused.

#### 5.1.3.3 Potential Security Requirement

CAPIF RNAA should support finer granular authorization and revocation when API invoker access resource(s) of the resource owner provided by the service API.

## 5.2 Key issue #2: CAPIF interconnection security

### 5.2.1 Key issue details

TS 23.222 [Y] defines an architectural model for the CAPIF interconnection which allows API invokers of a CAPIF provider to utilize the service API(s) from the 3rd party CAPIF provider and other CAPIF core function within the same CAPIF provider. TS 23.222[Y] specifies some information, like service API information, shareable information, which is transferred between CAPIF core functions (CCFs) via CAPIF-6/6e. Besides, CCFs coordinate to authenticate and authorize service API access for the AEF service API(s) exposed via CAPIF-6/6e, which is studied in TR 23.700-22 [X]. Figure 5.X.1-1 and 5.X.1-2 shows the architectural models defined in TS 23.222 [Y] clause 6.2.2.



Figure 5.2.1-1: High level functional architecture for CAPIF interconnection with multiple CAPIF provider domains

Figure 5.X.1-1 describes the CAPIF interconnection framework that connects CCFs in two different CAPIF provider domains. For CAPIF interconnection architecture defined in Figure 5.X.1-1, the API provider domain function (AEF) of one domain only communicates with the CCF in CAPIF provider domain A (CCF-A), where it is registered. It does not communicate with the interconnected CCF in CAPIF provider domain (CCF-B), but still must be able to provide AEF service APIs to an API invoker onboarded at CCF-A. Therefore, one target of this key issue is to study how the API invoker onboarded to CCF-A is autheticated and authorized to access API services of the AEF registered to CCF-B.



Figure 5.2.1-2: High level functional architecture for CAPIF interconnection within a CAPIF provider domain

Figure 5.X.1-2 describes the CAPIF interconnection framework that connects CCFs in the same CAPIF provider domains. Another target of this key issue is study how one API invoker onboarded with CAPIF core function 1 (CCF-1) is authenticated and authorized to access AEF registered in CAPIF core function 2 (CCF-2).

### 5.2.2 Security threats

Without integrity protection for CAPIF-6/6e reference points, messages over the CAPIF-6 and CAPIF-6e reference points can be modified by attackers.

Without confidentiality protection for CAPIF-6/6e reference points, messages over the CAPIF-6 and CAPIF-6e reference points can be sniffed by attackers.

Without the anti-replay attacks mechanism for CAPIF-6/6e reference points, messages over the CAPIF-6 and CAPIF-6e reference points can be replayed by the attackers.

Without the API invoker authentication mechanism in CAPIF interconnection scenarios, a malicious API invoker can impersonate another victim API invoker to access service API(s) registered in the other CCFs.

Even if the API invoker is authorized by the CCF which it’s onboarded with, if there is no sufficient API service authorization and verification in CAPIF interconnection scenarios, this API invoker can still invoke AEF's service APIs registered in the other CCFs and get sensitive information (e.g., user's location information) without authorization.

Without the API invoker authorization revocation mechanism in CAPIF interconnection scenarios, the CAPIF system cannot revoke the authorization for API invoker accessing service API(s) registered in the other CCFs.

### 5.2.3 Potential security requirements

Potential security requirements for CAPIF interconnection are as followed:

1. The CAPIF should support mutual authentication between API invoker and AEF when AEF service APIs are published via CAPIF-6/6e reference point in CAPIF interconnection scenarios.

2. The API invoker should support retrieval of the security method needed for accessing service APIs when these AEF service APIs are published via CAPIF-6/6e reference point in CAPIF interconnection scenarios.

3. The CAPIF should support authorization and revocation of the API invoker in CAPIF interconnection scenarios.

4. The transport of messages over the CAPIF-6 and CAPIF-6e reference points should be integrity protected.

5. The transport of messages over the CAPIF-6 and CAPIF-6e reference points should be protected from replay attacks.

6. The transport of messages over the CAPIF-6 and CAPIF-6e reference points should be confidentiality protected.

7. The CAPIF should support mechanisms for mutual authentication between CCFs over the CAPIF-6/6e reference point.

NOTE: Coordination with SA6 is needed.

## 5.3 Key Issue #3: Authorizing API invoker on one UE accessing resources related to another UE

### 5.3.1 Key issue details

This key issue addresses the security aspects of 23.700-22 KI #6 [X].

It studies the security aspects for the case that API invoker(s) are deployed on one UE and requests to access resources (hosted in the network)related to another UE (e.g., application client on UE is fetching location of another UE or setting QoS for PDU sessions of another UE).

As specified in 3GPP TS 23.222 [2], the API invoker may be deployed in any of the following ways:

a. API invoker may be deployed as AF on the UE (i.e. 3rd party application).

b. API invoker may be deployed as AF on the UE supporting several other 3rd party applications deployed on the UE.

c. API invoker may be deployed on the network as AF.

So far, only a UE accessing its own resources is considered if the API invoker is on a UE. Resource owner-aware northbound API access (RNAA) defined in TS 33.122 [4] only supports authorizing API invoker on one UE to request resources related to the same UE.

Therefore, it is proposed to study how to authorize an API invoker on one UE to access resources related to another UE.

### 5.3.2 Security threats

RNAA only supports authorizing API invoker on one UE to request resources related to the same UE. Hence, the CAPIF can only select non-RNAA (i.e., authorization procedure without resource owner involvement) based authorization mechanism for API invoker on one UE request to access resources related to another UE. This may lead to information leakage of the resource owner if the API invoker is authorized without engaging of the resource owner.

Without a proper security mechanism, unauthorized API invokers can access to resources related to a UE, which potentially results in sensitive information leakage and unauthorized modification to the resources accessed by northbound APIs.

### 5.3.3 Potential security requirements

CAPIF should support a mechanism for authorization of the API invoker on one UE to access resources related to another UE.

## 5.4 Key issue #4: Nested API invocation

### 5.4.1 Key issue details

In nested API invocation, the API exposing function (AEF) invokes API service(s) of another AEF which is in the same API provider domain as the first AEF. The procedure specified in clause 8.32 of TS 23.222 [2] in Rel-18 optimized authorization information query. The security aspect of that procedure is left to SA3 with the following note:

NOTE: The security aspects of this procedure are specified in TS 33.122 [4].

To provide security protection for the optimization procedure, the key issue derives a security requirement to mitigate potential security threats.

### 5.4.2 Security threats

If there is a vulnerability in the optimized authorization procedure in nested API invocation, an unauthorized API invoker can consume the API services, resulting in information leakage and unauthorized modification to the resources of the resource owner.

### 5.4.3 Potential security requirements

The AEF (destination AEF handling service API) should be able to authorize the AEF, requesting the API service, in an optimized way.

## 5.5 Key Issue KI#5: Authenticating multiple API invokers of the same Resource Owner

### 5.5.1 Key Issue details

This key issue addresses the security aspects of 29.700-22 KI #2, how multiple API invokers can use one or more AEFs exposing resources related to the same Resource Owner (RO) providing the credentials.

For example, in CAPIF RNAA context, this can enable a Resource Owner to allow one or several API invokers (e.g. gaming apps) running on the same UE to securely authenticate with one or multiple services provided by the AEF (e.g. location and/or QoS). In more detail, a gaming app wants to access the location. RO provides the security information to the gaming app to access the location service. Another API invoker on the same UE, e.g. the weather app, wants to access the location as well. The RO can provide the security information to the weather app to access the location service, without the need for both apps to request separate credentials from the CCF.

This key issue seeks to reducing the process of authenticating several API invokers of the same RO without introducing overhead.

### 5.5.2 Security threats

The same threats as for authentication and authorization in general apply, i.e. an unauthenticated and/or unauthorized API invoker can access to the AEF.

### 5.5.3 Security requirements

AEF should be able to authenticate and authorize multiple API invoker of the same RO.

# 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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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

### 6.Y.1 Introduction

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

# 7 Conclusions

Annex <X>:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-08 | SA3#117 | S3-243637 |  |  |  | Skeleton | 0.0.0 |
| 2024-08 | SA3#117 | S3-243718 |  |  |  | Incorporate pCRs that add S3‑243636, S3‑243638, S3‑243640, S3‑243700, S3‑243716, S3‑243136  | 0.1.0 |