ETSI TS 123 222 V15.7.0 (2024-01)

LTE;
5G;
Common API Framework for 3GPP Northbound APIs
(3GPP TS 23.222 version 15.7.0 Release 15)

Reference
RTS/TSGS-0623222vf70

Keywords
5G,LTE

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 9
Introduction 9
1 Scope 10
2 References 10
3 Definitions and abbreviations 10
3.1 Definitions 10
3.2 Abbreviations 11
4 Architectural requirements 12
4.1 General 12
4.1.1 Introduction 12
4.1.2 Requirements 12
4.1.3 Requirements for supporting 3rd party API providers 12
4.2 Service API publish and discover 12
4.2.1 Introduction 12
4.2.2 Requirements 12
4.3 Security 13
4.3.1 Introduction 13
4.3.2 Requirements 13
4.3.3 Additional requirements for 3rd party API provider 13
4.4 Charging 13
4.4.1 Introduction 13
4.4.2 Requirements 13
4.5 Operations, Administration and Maintenance 14
4.5.1 Introduction 14
4.5.2 Requirements 14
4.6 Service API invocation monitoring 14
4.6.1 Introduction 14
4.6.2 Requirements 14
4.7 Logging 14
4.7.1 Introduction 14
4.7.2 Logging events related to service API invocations 15
4.7.3 Logging events related to API invoker onboarding 15
4.7.4 Logging events related to API invoker interaction with the CAPIF 15
4.8 Auditing service API invocation 15
4.8.1 Introduction 15
4.8.2 Requirements 15
4.9 Onboarding API invoker 15
4.9.1 Introduction 15
4.9.2 Requirements 15
4.10 Policy configuration 16
4.10.1 Introduction 16
4.10.2 Requirements 16
4.11 Protocol design 16
4.11.1 Introduction 16
4.11.2 Requirements 16
5 Involved business relationships 16
6 Functional model 17
6.1 General 17
6.2 Functional model description 17

6.3 Functional entities description 18
6.3.1 General 18
6.3.2 API invoker 18
6.3.3 CAPIF core function 19
6.3.4 API exposing function 19
6.3.5 API publishing function 19
6.3.6 API management function 20
6.4 Reference points 20
6.4.1 General 20
6.4.2 Reference point CAPIF-1 (between the API invoker and the CAPIF core function) 20
6.4.3 Reference point CAPIF-1e (between the API invoker and the CAPIF core function) 20
6.4.4 Reference point CAPIF-2 (between the API invoker and the API exposing function) 20
6.4.5 Reference point CAPIF-2e (between the API invoker and the API exposing function) 21
6.4.6 Reference point CAPIF-3 (between the API exposing function and the CAPIF core function) 21
6.4.7 Reference point CAPIF-4 (between the API publishing function and the CAPIF core function) 21
6.4.8 Reference point CAPIF-5 (between the API management function and the CAPIF core function) 21

7 Application of functional model to deployments 22
7.1 General 22
7.2 Centralized deployment 22
7.3 Distributed deployment 23

8 Procedures and information flows 25
8.1 Onboarding the API invoker to the CAPIF 25
8.1.1 General 25
8.1.2 Information flows 26
8.1.2.1 Onboard API invoker request 26
8.1.2.2 Onboard API invoker response 26
8.1.3 Procedure 26
8.2 Offboarding the API invoker from the CAPIF 27
8.2.1 General 27
8.2.2 Information flows 27
8.2.2.1 Offboard API invoker request 27
8.2.2.2 Offboard API invoker response 28
8.2.3 Procedure 28
8.3 Publish service APIs 29
8.3.1 General 29
8.3.2 Information flows 29
8.3.2.1 Service API publish request 29
8.3.2.2 Service API publish response 29
8.3.3 Procedure 29
8.4 Unpublish service APIs 30
8.4.1 General 30
8.4.2 Information flows 30
8.4.2.1 Service API unpublish request 30
8.4.2.2 Service API unpublish response 30
8.4.3 Procedure 31
8.5 Retrieve service APIs 31
8.5.1 General 31
8.5.2 Information flows 31
8.5.2.1 Service API get request 31
8.5.2.2 Service API get response 32
8.5.3 Procedure 32
8.6 Update service APIs 33
8.6.1 General 33
8.6.2 Information flows 33
8.6.2.1 Service API update request 33
8.6.2.2 Service API update response 33
8.6.3 Procedure 33
8.7 Discover service APIs 34
8.7.1 General 34
8.7.2 Information flows 34

8.7.2.1 Service API discover request 34
8.7.2.2 Service API discover response 34
8.7.3 Procedure 35
8.8 Subscription, unsubscription and notifications for the CAPIF events 36
8.8.1 General 36
8.8.2 Information flows 36
8.8.2.1 Event subscription request 36
8.8.2.2 Event subscription response 36
8.8.2.3 Event notification 37
8.8.2.4 Event notification acknowledgement 37
8.8.2.5 Event unsubscription request 37
8.8.2.6 Event unsubscription response 37
8.8.3 Procedure for CAPIF event subscription 37
8.8.4 Procedure for CAPIF event notifications 38
8.8.5 Procedure for CAPIF event unsubscription 39
8.8.6 List of CAPIF events 39
8.9 Revoking subscription of the CAPIF events 40
8.9.1 General 40
8.9.2 Information flows 40
8.9.2.1 Subscription revoke notification 40
8.9.2.2 Subscription revoke notification acknowledgement 40
8.9.3 Procedure 40
8.10 Authentication between the API invoker and the CAPIF core function 41
8.10.1 General 41
8.10.2 Information flows 41
8.10.3 Procedure 41
8.11 API invoker obtaining authorization to access service API 42
8.11.1 General 42
8.11.2 Information flows 42
8.11.3 Procedure 42
8.12 AEF obtaining service API access control policy 43
8.12.1 General 43
8.12.2 Information flows 43
8.12.2.1 Obtain access control policy request 43
8.12.2.2 Obtain access control policy response 43
8.12.3 Procedure 44
8.13 Topology hiding 44
8.13.1 General 44
8.13.2 Information flows 45
8.13.2.1 Service API invocation request (API invoker – AEF-1) 45
8.13.2.2 Service API invocation request (AEF-1 – AEF-2) 45
8.13.2.3 Service API invocation response (AEF-2 – AEF-1) 45
8.13.2.4 Service API invocation response (AEF-1 – API invoker) 45
8.13.3 Procedure 45
8.14 Authentication between the API invoker and the AEF prior to service API invocation 46
8.14.1 General 46
8.14.2 Information flows 46
8.14.3 Procedure 46
8.15 Authentication between the API invoker and the AEF upon the service API invocation 47
8.15.1 General 47
8.15.2 Information flows 47
8.15.2.1 Service API invocation request with authentication information 47
8.15.2.2 Service API invocation response 48
8.15.3 Procedure 48
8.16 API invoker authorization to access service APIs 49
8.16.1 General 49
8.16.2 Information flows 49
8.16.2.1 Service API invocation request 49
8.16.2.2 Service API invocation response 49
8.16.3 Procedure 50
8.17 CAPIF access control 51
8.17.1 General 51

8.17.2 Information flows 51
8.17.2.1 Service API invocation request 51
8.17.2.2 Service API invocation response 51
8.17.3 Procedure 51
8.18 CAPIF access control with cascaded AEFs 52
8.18.1 General 52
8.18.2 Information flows 52
8.18.2.1 Service API invocation request 52
8.18.2.2 Service API invocation response 52
8.18.3 Procedure 53
8.19 Logging service API invocations 53
8.19.1 General 53
8.19.2 Information flows 54
8.19.2.1 API invocation log request 54
8.19.2.2 API invocation log response 54
8.19.3 Procedure 54
8.20 Charging the invocation of service APIs 55
8.20.1 General 55
8.20.2 Information flows 55
8.20.3 Procedure 55
8.21 Monitoring service API invocation 55
8.21.1 General 55
8.21.2 Information flows 56
8.21.2.1 Monitoring service API event notification 56
8.21.2.2 Monitoring service API event notification acknowledgement 56
8.21.3 Procedure 56
8.22 Auditing service API invocation 56
8.22.1 General 56
8.22.2 Information flows 57
8.22.2.1 Query service API log request 57
8.22.2.2 Query service API log response 57
8.22.3 Procedure 57
8.23 CAPIF revoking API invoker authorization 58
8.23.1 General 58
8.23.2 Information flows 58
8.23.2.1 Revoke API invoker authorization request 58
8.23.2.2 Revoke API invoker authorization response 58
8.23.2.3 Revoke API invoker authorization notify 58
8.23.3 Procedure for CAPIF revoking API invoker authorization initiated by AEF 59
8.23.4 Procedure for CAPIF revoking API invoker authorization initiated by CAPIF core function 60

9 API consistency guidelines 61
9.1 General 61
9.2 Fundamental API Guidelines 61
9.3 Architecture design considerations 61

10 CAPIF core function APIs 62
10.1 General 62
10.2 CAPIF_Discover_Service_API API 63
10.2.1 General 63
10.2.2 Discover_Service_API operation 63
10.2.3 Subscribe_Event operation 64
10.2.4 Notify_Event operation 64
10.2.5 Unsubscribe_Event operation 64
10.3 CAPIF_Publish_Service_API API 64
10.3.1 General 64
10.3.2 Publish_Service_API operation 65
10.3.3 Unpublish_Service_API operation 65
10.3.4 Update_Service_API operation 65
10.3.5 Get_Service_API operation 65
10.3.6 Subscribe_Event operation 65
10.3.7 Notify_Event operation 66

10.3.8 Unsubscribe_Event operation 66
10.4 CAPIF_Events API 66
10.4.1 General 66
10.4.2 Subscribe_Event operation 67
10.4.3 Notify_Event operation 67
10.4.4 Unsubscribe_Event operation 67
10.5 CAPIF_API_invoker_management API 67
10.5.1 General 67
10.5.2 Onboard_API_Invoker operation 67
10.5.3 Offboard_API_Invoker operation 68
10.5.4 Subscribe_Event operation 68
10.5.5 Notify_Event operation 68
10.5.6 Unsubscribe_Event operation 68
10.6 CAPIF_Security API 69
10.6.1 General 69
10.6.2 Obtain_Security_Method operation 69
10.6.3 Obtain_Authorization operation 69
10.6.4 Obtain_API_Invoker_Info operation 69
10.6.5 Revoke_Authorization operation 69
10.7 CAPIF_Monitoring API 70
10.7.1 General 70
10.7.2 Subscribe_Event operation 70
10.7.3 Notify_Monitoring_Service_Event operation 70
10.7.4 Unsubscribe_Event operation 70
10.8 CAPIF_Logging_API_Invocation API 71
10.8.1 General 71
10.8.2 Log_API_Invocation operation 71
10.9 CAPIF_Auditing API 71
10.9.1 General 71
10.9.2 Query_ API_Invocation_Log operation 71
10.10 CAPIF_Access_Control_Policy API 71
10.10.1 General 71
10.10.2 Obtain_Access_Control_Policy operation 71

11 API exposing function APIs 72
11.1 General 72
11.2 AEF_Security API 72
11.2.1 General 72
11.2.2 Revoke_Authorization operation 72
11.2.3 Initiate_Authentication operation 72

Annex A (informative): Overview of CAPIF operations 73

Annex B (informative): CAPIF relationship with network exposure aspects of 3GPP systems 75

B.0 CAPIF utilization by service API provider 75

B.1 CAPIF relationship with 3GPP EPS network exposure 76
B.1.1 General 76
B.1.2 Deployment models 76
B.1.2.1 General 76
B.1.2.2 SCEF implements the CAPIF architecture 76
B.1.2.3 SCEF implements the service specific aspect compliant with the CAPIF architecture 77
B.1.2.4 Distributed deployment of the SCEF compliant with the CAPIF architecture 78

B.2 CAPIF relationship with 3GPP 5GS network exposure 79
B.2.1 General 79
B.2.2 Deployment models 80
B.2.2.1 General 80
B.2.2.2 NEF implements the CAPIF architecture 80
B.2.2.3 NEF implements the service specific aspect compliant with the CAPIF architecture 81
B.2.2.4 Distributed deployment of the NEF compliant with the CAPIF architecture 82

Annex C (informative): CAPIF role in charging 84
C.1 General 84
C.2 CAPIF role in online charging 84
C.3 CAPIF role in offline charging 85
Annex D (informative): CAPIF relationship with external API frameworks 86
Annex E (normative): Configuration data for CAPIF 87
Annex F (informative): Change history 88
History 89

Foreword

This Technical Specification 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.

Introduction

In 3GPP, there are multiple northbound API-related specifications (e.g. APIs for Service Capability Exposure Function (SCEF) functionalities defined in 3GPP TS 23.682 [2], API for the interface between MBMS service provider and BM-SC defined in 3GPP TR 26.981 [5]). To avoid duplication and inconsistency of approach between different API specifications, 3GPP has considered the development of a common API framework (CAPIF) that includes common aspects applicable to any northbound service APIs.

The present document specifies the functional model, procedures and information flows needed to support the CAPIF, and the guidelines for consistent northbound API (service and CAPIF APIs) development in 3GPP.

NOTE: It is possible to use the CAPIF defined common aspects for other APIs as well, apart from northbound APIs.

1 Scope

The present document specifies the architecture, procedures and information flows necessary for the CAPIF. The aspects of this specification include identifying architecture requirements for the CAPIF (e.g. registration, discovery, identity management) that are applicable to any service APIs when used by northbound entities, as well as any interactions between the CAPIF and the service APIs themselves. The common API framework applies to both EPS and 5GS, and is independent of the underlying 3GPP access (e.g. E-UTRA, NR).

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 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[3] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[4] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[5] 3GPP TR 26.981: "MBMS Extensions for Provisioning and Content Ingestion".

[6] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[7] ETSI GS MEC 011 (V1.1.1): "Mobile Edge Computing (MEC); Mobile Edge Platform Application Enablement".

[8] ETSI GS MEC 009 (V1.1.1): "Mobile Edge Computing (MEC); General Principles for Mobile Edge Service APIs".

[9] OMA-ER_Autho4API-V1_0-20141209-A: "Authorization Framework for Network APIs".

[10] OMA-TS-REST_NetAPI_Common-V1_0-20180116-A: "Common definitions for RESTful Network APIs".

[11] OMA-TS-NGSI_Registration_and_Discovery-V1_0-20120529-A: "NGSI Registration and Discovery".

[12] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions 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].

API: The means by which an API invoker can access the service.

API invoker: The entity which invokes the CAPIF or service APIs.

API invoker profile: The set of information associated to an API invoker that allows that API invoker to utilize CAPIF APIs and service APIs.

API exposing function: The entity which provides the service communication entry point for the service APIs.

CAPIF administrator: An authorized user with special permissions for CAPIF operations.

Common API framework: A framework comprising common API aspects that are required to support service APIs.

Northbound API: A service API exposed to higher-layer API invokers.

Onboarding: One time registration process that enables the API invoker to subsequently access the CAPIF and the service APIs.

Resource: The object or component of the API on which the operations are acted upon.

Service API: The interface through which a component of the system exposes its services to API invokers by abstracting the services from the underlying mechanisms.

PLMN trust domain: The entities protected by adequate security and controlled by the PLMN operator or a trusted 3rd party.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 32.240 [6] apply:

Offline charging
Online charging

3.2 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].

5GS	5G System
AEF	API Exposing Function
AF	Application Function
API	Application Program Interface
AS	Application Server
BM-SC	Broadcast Multicast Service Centre
CAPIF	Common API Framework
CDR	Charging Data Record
CRUD	Create, Read, Update, Delete
DDoS	Distributed Denial of Service
E-UTRA	Evolved Universal Terrestrial Radio Access
EPS	Evolved Packet System
ETSI	European Telecommunications Standards Institute
GS	Group Specification
IP	Internet Protocol
MBMS	Multimedia Broadcast and Multicast Service
MEC	Multi-access Edge Computing
NEF	Network Exposure Function
NGSI	Next Generation Service Interfaces
NR	New Radio
OMA	Open Mobile Alliance
OAM	Operations, Administration and Maintenance
OWSER	OMA Web Services
PC	Protocol Converter
PLMN	Public Land Mobile Network
REST	REpresentational State Transfer

RPC	Remote Procedure Call
SCEF	Service Capability Exposure Function
SCS	Service Capability Server
UDDI	Universal Description, Discovery and Integration
URI	Uniform Resource Identifier
WSDL	Web Services Description Language

4 Architectural requirements

4.1 General

4.1.1 Introduction

This subclause specifies the general requirements for CAPIF architecture.

4.1.2 Requirements

[AR-4.1.2-a] The CAPIF shall provide mechanisms (e.g. publish service APIs, authorization, logging, charging) to support service API operations.

[AR-4.1.2-b] The CAPIF shall enable API invoker(s) to discover and communicate with service APIs from the API providers.

[AR-4.1.2-c] Reference points between CAPIF and external applications shall be provided as APIs.

[AR-4.1.2-d] Reference points internal to CAPIF may be provided as APIs.

4.1.3 Requirements for supporting 3rd party API providers

[AR-4.1.3-a] The CAPIF shall provide mechanisms (e.g. publish service APIs, authorization, logging, charging) to support service API operations from trusted 3rd party API providers.

[AR-4.1.3-b] The CAPIF shall enable API invoker(s) to discover and communicate with service APIs from trusted 3rd party API providers.

NOTE: The solutions to the requirements for 3rd party API providers are not addressed in the current release of this specification.

4.2 Service API publish and discover

4.2.1 Introduction

This subclause specifies the service API publish and discover related requirements.

4.2.2 Requirements

[AR-4.2.2-a] The CAPIF shall provide a mechanism to publish the service API information to be used by the API invokers to discover and subsequently invoke the service API.

[AR-4.2.2-b] The CAPIF shall provide a mechanism for the API invokers to discover the published service API information as specified in [AR-4.2.2-a] according to the API invokers' interest.

[AR-4.2.2-c] The CAPIF shall provide a mechanism to restrict the discovery of the published service API information by the API invokers, based on configured policies.

[AR-4.2.2-d] The CAPIF shall provide a mechanism to configure policies to restrict the discovery of the published service API information.

4.3 Security

4.3.1 Introduction

This subclause specifies the security related requirements for API invokers.

4.3.2 Requirements

[AR-4.3.2-a] The CAPIF shall provide mechanisms to hide the topology of the PLMN trust domain from the API invokers accessing the service APIs from outside the PLMN trust domain.

[AR-4.3.2-b] The CAPIF shall provide mechanisms to authenticate API invokers prior to accessing the service APIs.

[AR-4.3.2-c] The CAPIF shall provide mechanisms to authenticate API invokers upon the service API invocation.

[AR-4.3.2-d] The CAPIF shall provide mechanisms to authorize API invokers to access the service APIs.

[AR-4.3.2-e] The CAPIF shall provide mechanisms to validate authorization of the API invokers upon the service API invocation.

[AR-4.3.2-f] The CAPIF shall provide mechanisms for mutual authentication between the CAPIF and the API invoker.

[AR-4.3.2-g] The CAPIF shall provide mechanisms to control the service API access for every API invocation.

[AR-4.3.2-h] The communication between the CAPIF and the API invoker shall be confidentiality protected.

[AR-4.3.2-i] The communication between the CAPIF and the API invoker shall be integrity protected.

[AR-4.3.2-j] The CAPIF shall provide mechanisms to authenticate the service API publishers to publish and manage the service API information.

[AR-4.3.2-k] The CAPIF shall provide mechanisms to authorize the service API publishers to publish and manage service API information.

[AR-4.3.2-l] The CAPIF shall provide mechanisms to validate authorization of the service API publishers to publish and manage service API information.

4.3.3 Additional requirements for 3rd party API provider

[AR-4.3.3-a] The CAPIF shall provide mechanisms to hide the topology of the 3rd party API provider trust domain from the API invokers accessing the service APIs from outside the 3rd party API provider trust domain.

[AR-4.3.3-b] The CAPIF shall provide authorization mechanism for service APIs from the 3rd party API providers.

[AR-4.3.3-c] The CAPIF shall provide data confidentiality (across API providers) for data (e.g. logging, charging) related to service APIs from multiple API providers.

4.4 Charging

4.4.1 Introduction

This subclause specifies the charging related requirements for the usage of service APIs.

4.4.2 Requirements

[AR-4.4.2-a] The CAPIF shall support online and offline charging for service APIs usage.