ETSI TS 129 222 V18.6.0 (2024-07)

LTE;
5G;
Common API Framework for 3GPP Northbound APIs
(3GPP TS 29.222 version 18.6.0 Release 18)

Reference
RTS/TSGC-0329222vi60

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 14
1 Scope 15
2 References 15
3 Definitions and abbreviations 16
3.1 Definitions 16
3.2 Abbreviations 16
4 Overview 17
4.1 Introduction 17
4.2 Service Architecture 17
4.3 Functional Entities 17
4.3.1 API invoker 17
4.3.2 CAPIF core function 17
4.3.3 API exposing function 17
4.3.4 API publishing function 17
4.3.5 API management function 17
5 Services offered by the CAPIF Core Function 17
5.1 Introduction of Services 17
5.2 CAPIF_Discover_Service_API 19
5.2.1 Service Description 19
5.2.1.1 Overview 19
5.2.2 Service Operations 19
5.2.2.1 Introduction 19
5.2.2.2 Discover_Service_API 20
5.2.2.2.1 General 20
5.2.2.2.2 Consumer discovering service API using Discover_Service_API service operation 20
5.3 CAPIF_Publish_Service_API 20
5.3.1 Service Description 20
5.3.1.1 Overview 20
5.3.2 Service Operations 21
5.3.2.1 Introduction 21
5.3.2.2 Publish_Service_API 21
5.3.2.2.1 General 21
5.3.2.2.2 API publishing function publishing service APIs on CAPIF core function using Publish_Service_API service operation 21
5.3.2.2.3 CAPIF core function publishing service APIs on other CAPIF core function using Publish_Service_API service operation 22
5.3.2.3 Unpublish_Service_API 23
5.3.2.3.1 General 23
5.3.2.3.2 Consumer un-publishing service APIs from CAPIF core function using Unpublish_Service_API service operation 23
5.3.2.4 Get_Service_API 23
5.3.2.4.1 General 23
5.3.2.4.2 Consumer retrieving service APIs from CAPIF core function using Get_Service_API service operation 23
5.3.2.5 Update_Service_API 24
5.3.2.5.1 General 24
5.3.2.5.2 Consumer updating published service APIs on CAPIF core function using Update_Service_API service operation 24
5.4 CAPIF_Events_API 25
5.4.1 Service Description 25

5.4.1.1 Overview 25
5.4.2 Service Operations 25
5.4.2.1 Introduction 25
5.4.2.2 Subscribe_Event 25
5.4.2.2.1 General 25
5.4.2.2.2 Subscribing to CAPIF events using Subscribe_Event service operation 25
5.4.2.3 Unsubscribe_Event 26
5.4.2.3.1 General 26
5.4.2.3.2 Unsubscribing from CAPIF events using Unsubscribe_Event service operation 26
5.4.2.4 Notify_Event 27
5.4.2.4.1 General 27
5.4.2.4.2 Notifying CAPIF events using Notify_Event service operation 27
5.4.2.5 Update_Event_Subscription 27
5.4.2.5.1 General 27
5.4.2.5.2 Update Subscription to CAPIF events using Update_Event_Subscription service operation 27
5.5 CAPIF_API_Invoker_Management_API 28
5.5.1 Service Description 28
5.5.1.1 Overview 28
5.5.2 Service Operations 28
5.5.2.1 Introduction 28
5.5.2.2 Onboard_API_Invoker 28
5.5.2.2.1 General 28
5.5.2.2.2 API invoker on-boarding itself as a recognized user of CAPIF using Onboard_API_Invoker service operation 28
5.5.2.3 Offboard_API_Invoker 29
5.5.2.3.1 General 29
5.5.2.3.2 API invoker off-boarding itself as a recognized user of CAPIF using Offboard_API_Invoker service operation 29
5.5.2.4 Notify_Onboarding_Completion 30
5.5.2.4.1 General 30
5.5.2.4.2 Notifying Onboarding completion using Notify_Onboarding_Completion service operation 30
5.5.2.5 Update_API_Invoker_Details 30
5.5.2.5.1 General 30
5.5.2.5.2 API invoker updating its details on CAPIF using Update_API_Invoker_Details service operation 30
5.5.2.6 Notify_Update_Completion 31
5.5.2.6.1 General 31
5.5.2.6.2 Notifying API invoker update completion using Notify_Update_Completion service operation 31
5.6 CAPIF_Security_API 32
5.6.1 Service Description 32
5.6.1.1 Overview 32
5.6.2 Service Operations 32
5.6.2.1 Introduction 32
5.6.2.2 Obtain_Security_Method 32
5.6.2.2.1 General 32
5.6.2.2.2 Request service API security method from CAPIF using Obtain_Security_Method service operation 33
5.6.2.3 Obtain_Authorization 33
5.6.2.3.1 General 33
5.6.2.3.2 Obtain authorization using Obtain_Authorization service operation 33
5.6.2.3.3 Void 34
5.6.2.4 Obtain_API_Invoker_Info 34
5.6.2.4.1 General 34
5.6.2.4.2 Obtain API invoker's security information using Obtain_API_Invoker_Info service operation 34
5.6.2.5 Revoke_Authentication 34
5.6.2.5.1 General 34
5.6.2.5.2 Invalidate authorization using Revoke_Authorization service operation 35
5.7 CAPIF_Monitoring_API 35
5.8 CAPIF_Logging_API_Invocation_API 35
5.8.1 Service Description 35
5.8.1.1 Overview 35

5.8.2 Service Operations 35
5.8.2.1 Introduction 35
5.8.2.2 Log_API_Invocation_API 36
5.8.2.2.1 General 36
5.8.2.2.2 Logging service API invocations using Log_API_Invocation service operation 36
5.9 CAPIF_Auditing_API 36
5.9.1 Service Description 36
5.9.1.1 Overview 36
5.9.2 Service Operations 36
5.9.2.1 Introduction 36
5.9.2.2 Query_Invocation_Logs_API 37
5.9.2.2.1 General 37
5.9.2.2.2 Query API invocation information logs using Query_Invocation_Logs service operation 37
5.10 CAPIF_Access_Control_Policy_API 37
5.10.1 Service Description 37
5.10.1.1 Overview 37
5.10.2 Service Operations 37
5.10.2.1 Introduction 37
5.10.2.2 Obtain_Access_Control_Policy 38
5.10.2.2.1 General 38
5.10.2.2.2 API exposing function obtaining access control policy from the CAPIF core function using Obtain_Access_Control_Policy service operation 38
5.10.3 Related Events 38
5.11 CAPIF_API_Provider_Management_API 38
5.11.1 Service Description 38
5.11.1.1 Overview 38
5.11.2 Service Operations 38
5.11.2.1 Introduction 38
5.11.2.2 Register_API_Provider 39
5.11.2.2.1 General 39
5.11.2.2.2 API provider domain functions registering as a recognized API provider domain function of CAPIF using Register_API_Provider service operation 39
5.11.2.3 Update_API_Provider 39
5.11.2.3.1 General 39
5.11.2.3.2 API management function updating API provider domain function details on CAPIF using Update_API_Provider service operation 39
5.11.2.4 Deregister_API_Provider 40
5.11.2.4.1 General 40
5.11.2.4.2 API provider domain functions deregistering as a recognized API provider domain function of CAPIF using Deregister_API_Provider service operation 40
5.12 CAPIF_Routing_Info_API 41
5.12.1 Service Description 41
5.12.1.1 Overview 41
5.12.2 Service Operations 41
5.12.2.1 Introduction 41
5.12.2.2 Obtain_Routing_Info 41
5.12.2.2.1 General 41
5.12.2.2.2 API exposing function obtaining API routing information from the CAPIF core function using Obtain_Routing_Info service operation 41

6 Services offered by the API exposing function 41
6.1 Introduction of Services 41
6.2 AEF_Security_API 42
6.2.1 Service Description 42
6.2.1.1 Overview 42
6.2.2 Service Operations 42
6.2.2.1 Introduction 42
6.2.2.2 Initiate_Authentication 42
6.2.2.2.1 General 42
6.2.2.2.2 API invoker initiating authentication using Initiate_Authentication service operation 43
6.2.2.3 Revoke_Authorization 43
6.2.2.3.1 General 43

6.2.2.3.2 CAPIF core function initiating revocation using Revoke_Authorization service operation.....43
7 CAPIF Design Aspects Common for All APIs.....43
7.1 General.....43
7.2 Data Types.....44
7.2.1 General.....44
7.2.2 Referenced structured data types.....44
7.2.3 Referenced Simple data types and enumerations.....44
7.3 Usage of HTTP.....45
7.4 Content type.....45
7.5 URI structure.....45
7.6 Notifications.....45
7.7 Error handling.....45
7.8 Feature negotiation.....46
7.9 HTTP custom headers.....46
7.10 Conventions for Open API specification files.....46
7.11 CAPIF vendor-specifc extensions.....46
8 CAPIF Core Function API Definition.....46
8.1 CAPIF_Discover_Service_API.....46
8.1.1 API URI.....46
8.1.2 Resources.....46
8.1.2.1 Overview.....46
8.1.2.2 Resource: All published service APIs.....47
8.1.2.2.1 Description.....47
8.1.2.2.2 Resource Definition.....47
8.1.2.2.3 Resource Standard Methods.....47
8.1.2.2.3.1 GET.....47
8.1.2.2.4 Resource Custom Operations.....49
8.1.2A Custom Operations without associated resources.....49
8.1.3 Notifications.....49
8.1.4 Data Model.....49
8.1.4.1 General.....49
8.1.4.2 Structured data types.....50
8.1.4.2.1 Introduction.....50
8.1.4.2.2 Type: DiscoveredAPIs.....50
8.1.4.2.3 Void.....51
8.1.4.2.4 Type: IpAddrInfo.....51
8.1.4.3 Simple data types and enumerations.....51
8.1.4.3.1 Introduction.....51
8.1.4.3.2 Simple data types.....51
8.1.4.4 Data types describing alternative data types or combinations of data types.....51
8.1.5 Error Handling.....51
8.1.5.1 General.....51
8.1.5.2 Protocol Errors.....51
8.2.5.3 Application Errors.....51
8.1.6 Feature negotiation.....52
8.2 CAPIF_Publish_Service_API.....52
8.2.1 API URI.....52
8.2.2 Resources.....52
8.2.2.1 Overview.....52
8.2.2.2 Resource: APF published APIs.....53
8.2.2.2.1 Description.....53
8.2.2.2.2 Resource Definition.....53
8.2.2.2.3 Resource Standard Methods.....54
8.2.2.2.3.1 POST.....54
8.2.2.2.3.2 GET.....54
8.2.2.2.4 Resource Custom Operations.....55
8.2.2.3 Resource: Individual APF published API.....56
8.2.2.3.1 Description.....56
8.2.2.3.2 Resource Definition.....56
8.2.2.3.3 Resource Standard Methods.....56

8.2.2.3.3.1 GET 56
8.2.2.3.3.2 PUT 57
8.2.2.3.3.3 DELETE 58
8.2.2.3.3.4 PATCH 59
8.2.2.3.4 Resource Custom Operations 60
8.2.2A Custom Operations without associated resources 60
8.2.3 Notifications 60
8.2.4 Data Model 61
8.2.4.1 General 61
8.2.4.2 Structured data types 62
8.2.4.2.1 Introduction 62
8.2.4.2.2 Type: ServiceAPIDescription 63
8.2.4.2.3 Type: InterfaceDescription 64
8.2.4.2.4 Type: AefProfile 65
8.2.4.2.5 Type: Version 65
8.2.4.2.6 Type: Resource 66
8.2.4.2.7 Type: CustomOperation 66
8.2.4.2.8 Type: ShareableInformation 66
8.2.4.2.9 Type: PublishedApiPath 67
8.2.4.2.10 Type: AefLocation 67
8.2.4.2.11 Type: ServiceAPIDescriptionPatch 68
8.2.4.2.12 Type: ApiStatus 68
8.2.4.2.13 Type: ServiceKpis 69
8.2.4.2.14 Type: IpAddrRange 71
8.2.4.3 Simple data types and enumerations 71
8.2.4.3.1 Introduction 71
8.2.4.3.2 Simple data types 71
8.2.4.3.3 Enumeration: Protocol 71
8.2.4.3.4 Enumeration: DataFormat 72
8.2.4.3.5 Enumeration: CommunicationType 72
8.2.4.3.6 Enumeration: SecurityMethod 72
8.2.4.3.7 Enumeration: Operation 72
8.2.5 Error Handling 72
8.2.5.1 General 72
8.2.5.2 Protocol Errors 73
8.2.5.3 Application Errors 73
8.2.6 Feature negotiation 73
8.3 CAPIF_Events_API 74
8.3.1 API URI 74
8.3.2 Resources 74
8.3.2.1 Overview 74
8.3.2.2 Resource: CAPIF Events Subscriptions 75
8.3.2.2.1 Description 75
8.3.2.2.2 Resource Definition 75
8.3.2.2.3 Resource Standard Methods 75
8.3.2.2.3.1 POST 75
8.3.2.2.4 Resource Custom Operations 76
8.3.2.3 Resource: Individual CAPIF Events Subscription 76
8.3.2.3.1 Description 76
8.3.2.3.2 Resource Definition 76
8.3.2.3.3 Resource Standard Methods 76
8.3.2.3.3.1 DELETE 76
8.3.2.3.3.2 PUT 77
8.3.2.3.3.3 PATCH 78
8.3.2.3.4 Resource Custom Operations 79
8.3.2A Custom Operations without associated resources 79
8.3.3 Notifications 79
8.3.3.1 General 79
8.3.3.2 Event Notification 80
8.3.3.2.1 Description 80
8.3.3.2.2 Notification definition 80
8.3.4 Data Model 81

8.3.4.1 General 81
8.3.4.2 Structured data types 81
8.3.4.2.1 Introduction 81
8.3.4.2.2 Type: EventSubscription 82
8.3.4.2.3 Type: EventNotification 82
8.3.4.2.4 Type: CAPIFEventFilter 83
8.3.4.2.5 Type: CAPIFEventDetail 83
8.3.4.2.6 Type: AccessControlPolicyListExt 83
8.3.4.2.7 Type: TopologyHiding 83
8.3.4.2.8 Type: EventSubscriptionPatch 84
8.3.4.3 Simple data types and enumerations 84
8.3.4.3.1 Introduction 84
8.3.4.3.2 Simple data types 84
8.3.4.3.3 Enumeration: CAPIFEvent 85
8.3.5 Error Handling 85
8.3.5.1 General 85
8.3.5.2 Protocol Errors 85
8.3.5.3 Application Errors 85
8.3.6 Feature negotiation 86
8.4 CAPIF_API_Invoker_Management_API 86
8.4.1 API URI 86
8.4.2 Resources 86
8.4.2.1 Overview 86
8.4.2.2 Resource: On-boarded API invokers 87
8.4.2.2.1 Description 87
8.4.2.2.2 Resource Definition 87
8.4.2.2.3 Resource Standard Methods 88
8.4.2.2.3.1 POST 88
8.4.2.2.4 Resource Custom Operations 88
8.4.2.3 Resource: Individual On-boarded API Invoker 89
8.4.2.3.1 Description 89
8.4.2.3.2 Resource Definition 89
8.4.2.3.3 Resource Standard Methods 89
8.4.2.3.3.1 DELETE 89
8.4.2.3.3.2 PUT 90
8.4.2.3.3.3 PATCH 91
8.4.2.3.4 Resource Custom Operations 92
8.4.2A Custom Operations without associated resources 92
8.4.3 Notifications 92
8.4.3.1 General 92
8.4.3.2 Notify_Onboarding_Completion 93
8.4.3.2.1 Description 93
8.4.3.2.2 Notification definition 93
8.4.3.3 Notify_Update_Completion 94
8.4.3.3.1 Description 94
8.4.3.3.2 Notification definition 94
8.4.4 Data Model 95
8.4.4.1 General 95
8.4.4.2 Structured data types 97
8.4.4.2.1 Introduction 97
8.4.4.2.2 Type: APIInvokerEnrolmentDetails 97
8.4.4.2.3 Type: Void 98
8.4.4.2.4 Type: APIList 98
8.4.4.2.5 Type: OnboardingInformation 98
8.4.4.2.6 Type: Void 98
8.4.4.2.7 Type: OnboardingNotification 98
8.4.4.2.8 Type: APIInvokerEnrolmentDetailsPatch 99
8.4.4.3 Simple data types and enumerations 99
8.4.5 Error Handling 99
8.4.5.1 General 99
8.4.5.2 Protocol Errors 99
8.4.5.3 Application Errors 99

8.4.6 Feature negotiation 99
8.5 CAPIF_Security_API 100
8.5.1 API URI 100
8.5.2 Resources 100
8.5.2.1 Overview 100
8.5.2.2 Resource: Trusted API invokers 101
8.5.2.2.1 Description 101
8.5.2.2.2 Resource Definition 102
8.5.2.2.3 Resource Standard Methods 102
8.5.2.2.3.1 Void 102
8.5.2.2.4 Resource Custom Operations 102
8.5.2.3 Resource: Individual trusted API invokers 102
8.5.2.3.1 Description 102
8.5.2.3.2 Resource Definition 102
8.5.2.3.3 Resource Standard Methods 102
8.5.2.3.3.1 GET 102
8.5.2.3.3.2 DELETE 103
8.5.2.3.3.3 PUT 104
8.5.2.3.4 Resource Custom Operations 105
8.5.2.3.4.1 Overview 105
8.5.2.3.4.2 Operation: update 105
8.5.2.3.4.2.1 Description 105
8.5.2.3.4.2.2 Operation Definition 106
8.5.2.3.4.3 Operation: delete 107
8.5.2.3.4.3.1 Description 107
8.5.2.3.4.3.2 Operation Definition 107
8.5.2.3.4.4 Operation: token 108
8.5.2.3.4.4.1 Description 108
8.5.2.3.4.4.2 Operation Definition 108
8.5.2.3.4.5 Void 109
8.5.2A Custom Operations without associated resources 109
8.5.3 Notifications 109
8.5.3.1 General 109
8.5.3.2 Authorization revoked notification 109
8.5.3.2.1 Description 109
8.5.3.2.2 Notification definition 109
8.5.4 Data Model 110
8.5.4.1 General 110
8.5.4.2 Structured data types 112
8.5.4.2.1 Introduction 112
8.5.4.2.2 Type: ServiceSecurity 112
8.5.4.2.3 Type: SecurityInformation 113
8.5.4.2.4 Void 113
8.5.4.2.5 Type: SecurityNotification 113
8.5.4.2.6 Type: AccessTokenReq 114
8.5.4.2.7 Type: AccessTokenRsp 116
8.5.4.2.8 Type: AccessTokenClaims 117
8.5.4.2.9 Type: AccessTokenErr 118
8.5.4.2.10 Void 118
8.5.4.2.11 Type: ResOwnerId 118
8.5.4.3 Simple data types and enumerations 118
8.5.4.3.1 Introduction 118
8.5.4.3.2 Simple data types 118
8.5.4.3.3 Enumeration: Cause 119
8.5.4.3.4 Enumeration: OAuthGrantType 119
8.5.5 Error Handling 119
8.5.5.1 General 119
8.5.5.2 Protocol Errors 119
8.5.5.3 Application Errors 119
8.5.6 Feature negotiation 120
8.6 CAPIF_Access_Control_Policy_API 120
8.6.1 API URI 120

8.6.2 Resources 121
8.6.2.1 Overview 121
8.6.2.2 Resource: Access Control Policy List 121
8.6.2.2.1 Description 121
8.6.2.2.2 Resource Definition 121
8.6.2.2.3 Resource Standard Methods 122
8.6.2.2.3.1 GET 122
8.6.2.2.4 Resource Custom Operations 123
8.6.2A Custom Operations without associated resources 123
8.6.3 Notifications 123
8.6.4 Data Model 123
8.6.4.1 General 123
8.6.4.2 Structured data types 123
8.6.4.2.1 Introduction 123
8.6.4.2.2 Type: AccessControlPolicyList 124
8.6.4.2.3 Type: ApiInvokerPolicy 124
8.6.4.2.4 Type: TimeRangeList 124
8.6.4.3 Simple data types and enumerations 124
8.6.5 Error Handling 124
8.6.5.1 General 124
8.6.5.2 Protocol Errors 124
8.6.5.3 Application Errors 124
8.6.6 Feature negotiation 125
8.7 CAPIF_Logging_API_Invocation_API 125
8.7.1 API URI 125
8.7.2 Resources 125
8.7.2.1 Overview 125
8.7.2.2 Resource: Logs 126
8.7.2.2.1 Description 126
8.7.2.2.2 Resource Definition 126
8.7.2.2.3 Resource Standard Methods 126
8.7.2.2.3.1 POST 126
8.7.2.2.4 Resource Custom Operations 127
8.7.2A Custom Operations without associated resources 127
8.7.3 Notifications 127
8.7.4 Data Model 127
8.7.4.1 General 127
8.7.4.2 Structured data types 128
8.7.4.2.1 Introduction 128
8.7.4.2.2 Type: InvocationLog 128
8.7.4.2.3 Type: Log 129
8.7.4.3 Simple data types and enumerations 129
8.7.4.3.1 Introduction 129
8.7.4.3.2 Simple data types 129
8.7.5 Error Handling 130
8.7.5.1 General 130
8.7.5.2 Protocol Errors 130
8.7.5.3 Application Errors 130
8.7.6 Feature negotiation 130
8.8 CAPIF_Auditing_API 130
8.8.1 API URI 130
8.8.2 Resources 131
8.8.2.1 Overview 131
8.8.2.2 Resource: All service API invocation logs 131
8.8.2.2.1 Description 131
8.8.2.2.2 Resource Definition 131
8.8.2.2.3 Resource Standard Methods 132
8.8.2.2.3.1 GET 132
8.8.2.2.4 Resource Custom Operations 133
8.8.2A Custom Operations without associated resources 133
8.8.3 Notifications 133
8.8.4 Data Model 133

8.8.4.1 General 133
8.8.4.2 Structured data types 134
8.8.4.2.1 Introduction 134
8.8.4.2.2 Type: InvocationLogs 134
8.8.4.3 Simple data types and enumerations 134
8.8.4.4 Data types describing alternative data types or combinations of data types 134
8.8.4.4.1 Type: InvocationLogsRetrieveRes 134
8.8.5 Error Handling 134
8.8.5.1 General 134
8.8.5.2 Protocol Errors 135
8.8.5.3 Application Errors 135
8.8.6 Feature negotiation 135
8.9 CAPIF_API_Provider_Management_API 135
8.9.1 API URI 135
8.9.2 Resources 135
8.9.2.1 Overview 135
8.9.2.2 Resource: All API Provider Domains Registrations 136
8.9.2.2.1 Description 136
8.9.2.2.2 Resource Definition 136
8.9.2.2.3 Resource Standard Methods 137
8.9.2.2.3.1 POST 137
8.9.2.2.4 Resource Custom Operations 137
8.9.2.3 Resource: Individual API Provider Domain Registration 137
8.9.2.3.1 Description 137
8.9.2.3.2 Resource Definition 137
8.9.2.3.3 Resource Standard Methods 138
8.9.2.3.3.1 PUT 138
8.9.2.3.3.2 DELETE 139
8.9.2.3.3.3 PATCH 140
8.9.2.3.4 Resource Custom Operations 141
8.9.2A Custom Operations without associated resources 141
8.9.3 Notifications 141
8.9.4 Data Model 142
8.9.4.1 General 142
8.9.4.2 Structured data types 143
8.9.4.2.1 Introduction 143
8.9.4.2.2 Type: APIProviderEnrolmentDetails 143
8.9.4.2.3 Type: APIProviderFunctionDetails 144
8.9.4.2.4 Type: RegistrationInformation 144
8.9.4.2.5 Type: APIProviderEnrolmentDetailsPatch 145
8.9.4.3 Simple data types and enumerations 145
8.9.4.3.1 Introduction 145
8.9.4.3.2 Simple data types 145
8.9.4.3.3 Enumeration: ApiProviderFuncRole 145
8.9.5 Error Handling 145
8.9.5.1 General 145
8.9.5.2 Protocol Errors 145
8.9.5.3 Application Errors 146
8.9.6 Feature negotiation 146
8.10 CAPIF_Routing_Info_API 146
8.10.1 API URI 146
8.10.2 Resources 146
8.10.2.1 Overview 146
8.10.2.2 Resource: Individual Service API routing info 147
8.10.2.2.1 Description 147
8.10.2.2.2 Resource Definition 147
8.10.2.2.3 Resource Standard Methods 147
8.10.2.2.3.1 GET 147
8.10.2.2.4 Resource Custom Operations 148
8.10.2A Custom Operations without associated resources 148
8.10.3 Notifications 149
8.10.4 Data Model 149

8.10.4.1 General 149
8.10.4.2 Structured data types 149
8.10.4.2.1 Introduction 149
8.10.4.2.2 Type: RoutingInfo 149
8.10.4.2.3 Type: RoutingRule 150
8.10.4.2.4 Type: Ipv6AddressRange 150
8.10.4.3 Simple data types and enumerations 150
8.10.5 Error Handling 150
8.10.5.1 General 150
8.10.5.2 Protocol Errors 150
8.10.5.3 Application Errors 150
8.10.6 Feature negotiation 150

9 AEF API Definition 151
9.1 AEF_Security_API 151
9.1.1 API URI 151
9.1.2 Resources 151
9.1.2A Custom Operations without associated resources 151
9.1.2A.1 Overview 151
9.1.2A.2 Operation: check-authentication 151
9.1.2A.2.1 Description 151
9.1.2A.2.2 Operation Definition 152
9.1.2A.3 Operation: revoke-authorization 152
9.1.2A.3.1 Description 152
9.1.2A.3.2 Operation Definition 153
9.1.3 Notifications 153
9.1.4 Data Model 154
9.1.4.1 General 154
9.1.4.2 Structured data types 154
9.1.4.2.1 Introduction 154
9.1.4.2.2 Type: CheckAuthenticationReq 154
9.1.4.2.3 Type: CheckAuthenticationRsp 154
9.1.4.2.4 Type: RevokeAuthorizationReq 155
9.1.4.2.5 Type: RevokeAuthorizationRsp 155
9.1.4.3 Simple data types and enumerations 155
9.1.5 Error Handling 155
9.1.5.1 General 155
9.1.5.2 Protocol Errors 155
9.1.5.3 Application Errors 155
9.1.6 Feature negotiation 155

10 Security 156
10.1 General 156
10.2 CAPIF-1/1e security 156
10.3 CAPIF-2/2e security and securely invoking service APIs 156

Annex A (normative): OpenAPI specification 157

A.1 General 157
A.2 CAPIF_Discover_Service_API 157
A.3 CAPIF_Publish_Service_API 159
A.4 CAPIF_Events_API 169
A.5 CAPIF_API_Invoker_Management_API 175
A.6 CAPIF_Security_API 181
A.7 CAPIF_Access_Control_Policy_API 188
A.8 CAPIF_Logging_API_Invocation_API 190
A.9 CAPIF_Auditing_API 192

A.10 AEF_Security_API.....194
A.11 CAPIF_API_Provider_Management_API.....196
A.12 CAPIF_Routing_Info_API.....201
Annex B (informative): Change history.....203
History.....209

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.

1 Scope

The present specification describes the protocol for the Common API Framework (CAPIF) for 3GPP Northbound APIs. The CAPIF and the related stage 2 architecture and functional requirements are defined in 3GPP TS 23.222 [2].

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: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

[3] Open API: "OpenAPI Specification Version 3.0.0", https://spec.openapis.org/oas/v3.0.0.

[4] IETF RFC 9112: "HTTP/1.1".

[5] IETF RFC 9110: "HTTP Semantics".

[6] Void.

[7] Void.

[8] IETF RFC 9111: "HTTP Caching".

[9] Void.

[10] IETF RFC 9113: "HTTP/2".

[11] Void.

[12] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".

[13] IETF RFC 6455: "The Websocket Protocol".

[14] 3GPP TS 29.122: "T8 reference point for northbound Application Programming Interfaces (APIs)".

[15] 3GPP TS 29.522: "5G System; Network Exposure Function Northbound APIs; Stage 3".

[16] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[17] Void.

[18] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[19] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces Stage 3".

[20] IETF RFC 7239: "Forwarded HTTP Extension".

[21] Void.

[22] W3C HTML 4.01 Specification, https://www.w3.org/TR/2018/SPSD-html401-20180327/.

[23] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[24] IETF RFC 7519: "JSON Web Token (JWT)".

[25] IETF RFC 7515: "JSON Web Signature (JWS)".

[26] 3GPP TS 29.523: "5G System; Policy Control Event Exposure Service; Stage 3".

[27] 3GPP TR 21.900: "Technical Specification Group working methods".

[28] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3"

[29] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[30] 3GPP TS 29.572: "5G System; Location Management Services; Stage 3".

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].

For the purposes of the present document, the terms and definitions given in clause 3 of 3GPP TS 23.222 [2] shall also apply:

API registry: API registry is a registry maintained by the CAPIF core function to store information about the service APIs based on the data models defined in this specification. The structure of the API registry is out of scope of this specification.

Subscriber: A functional entity that subscribes to another functional entity for notifications.

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].

AEF	API Exposing Function
AMF	API Management Function
APF	API Publishing Function
AS	Application Server
CAPIF	Common API Framework
CCF	CAPIF Core Function
JSON	JavaScript Object Notation
REST	Representational State Transfer
RNAA	Resource owner-aware Northbound API Access
SCEF	Service Capability Exposure Function
SCS	Service Capability Server
SNPN	Stand-alone Non-Public Network

4 Overview

4.1 Introduction

In 3GPP, there are multiple northbound API-related specifications. To avoid duplication and inconsistency of approaches between different API specifications and to specify common services (e.g. authorization), 3GPP has considered in 3GPP TS 23.222 [2] the development of a common API framework (CAPIF) that includes common aspects applicable to any northbound service APIs.

The present document specifies the APIs needed to support CAPIF.

4.2 Service Architecture

3GPP TS 23.222 [2] clause 6 specifies the functional entities and domains of the functional model.

4.3 Functional Entities

4.3.1 API invoker

The API invoker is typically provided by a 3rd party application provider who has service agreement with PLMN operator or SNPN. The API invoker may reside within the same trust domain as the PLMN operator network or SNPN.

The API invoker supports several capabilities as defined in 3GPP TS 23.222 [2].

4.3.2 CAPIF core function

The CAPIF core function (CCF) supports the capabilities as defined in 3GPP TS 23.222 [2].

4.3.3 API exposing function

The API exposing function (AEF) is the provider of the Service APIs and is also the service communication entry point of the service API to the API invokers as defined in 3GPP TS 23.222 [2].

4.3.4 API publishing function

The API publishing function (APF) enables the API provider to publish the Service APIs information as defined in 3GPP TS 23.222 [2].

4.3.5 API management function

The API management function (AMF) enables the API provider to perform administration of the Service APIs. The API capabilities are defined in 3GPP TS 23.222 [2].

5 Services offered by the CAPIF Core Function

5.1 Introduction of Services

The table 5.1-1 lists the CAPIF Core Function APIs below the service name. A service description clause for each API gives a general description of the related API.

Table 5.1-1: List of CAPIF Services

Service Name	Service Operations	Operation Semantics	Consumer(s)
CAPIF_Discover_Service_API	Discover_Service_API	Request/ Response	API Invoker, CAPIF core function
	Event operations (NOTE)	(NOTE)	API Invoker
CAPIF_Publish_Service_API	Publish_Service_API	Request/ Response	API Publishing Function, CAPIF core function
	Unpublish_Service_API	Request/ Response	API Publishing Function, CAPIF core function
	Update_Service_API	Request/ Response	API Publishing Function, CAPIF core function
	Get_Service_API	Request/ Response	API Publishing Function, CAPIF core function
CAPIF_Events_API	Subscribe_Event	Subscribe/Notify	API Invoker, API Publishing Function, API Management Function, API Exposing Function
	Update_Event_Subscription	Subscribe/Notify	API Invoker, API Publishing Function, API Management Function, API Exposing Function
	Notify_Event	Subscribe/Notify	API Invoker, API Publishing Function, API Management Function, API Exposing Function
	Unsubscribe_Event	Subscribe/Notify	API Invoker, API Publishing Function, API Management Function, API Exposing Function
CAPIF_API_Invoker_Management_API	Onboard_API_Invoker	Request/ Response	API Invoker
	Offboard_API_Invoker	Request/ Response	API Invoker
	Notify_Onboarding_Completion	Subscribe/Notify	API Invoker
	Update_API_Invoker_Details	Request/Response	API Invoker
	Notify_Update_Completion	Subscribe/Notify	API Invoker
CAPIF_Security_API	Obtain_Security_Method	Request/ Response	API Invoker
	Obtain_Authorization	Request/ Response	API Invoker
	Obtain_API_Invoker_Info	Request/ Response	API exposing function
	Revoke_Authorization	Request/ Response	API exposing function
CAPIF_Monitoring_API	Event operations (NOTE)	(NOTE)	API Management Function
CAPIF_Logging_API_Invocation_API	Log_API_Invocation	Request/ Response	API exposing function
CAPIF_Auditing_API	Query_API_Invocation_Log	Request/ Response	API management function
CAPIF_Access_Control_Policy_API	Obtain_Access_Control_Policy	Request/Response	API Exposing Function
CAPIF_API_Provider_Management_API	Register_API_Provider	Request/Response	API Management Function
	Update_API_Provider	Request/Response	API Management Function
	Deregister_API_Provider	Request/Response	API Management Function
CAPIF_Routing_Info_API	Obtain_ Routing_Info	Request/Response	API exposing function
NOTE: The service operations of CAPIF Events API are reused by the CAPIF_Discover_Service_API, CAPIF_Publish_Service_API and CAPIF_Monitoring_API for events related services.			

Table 5.1-2 summarizes the corresponding APIs defined in this specification.

Table 5.1-2: API Descriptions

Service Name	Clause	Description	OpenAPI Specification File	apiName	Annex
CAPIF_Discover_Service_API	8.1	CAPIF API discovery service	TS29222_CAPIF_Discover_Service_API.yaml	service-apis	A.2
CAPIF_Publish_Service_API	8.2	CAPIF API Publish Service	TS29222_CAPIF_Publish_Service_API.yaml	published-apis	A.3
CAPIF_Events_API	8.3	CAPIF event service	TS29222_CAPIF_Events_API.yaml	capif-events	A.4
CAPIF_API_Invoker_Management_API	8.4	CAPIF API Invoker Management Service	TS29222_CAPIF_API_Invoker_Management_API.yaml	api-invoker-management	A.5
CAPIF_Security_API	8.5	CAPIF Security Service	TS29222_CAPIF_Security_API.yaml	capif-security	A.6
CAPIF_Access_Control_Policy_API	8.6	CAPIF Access Control Policy API Service	TS29222_CAPIF_Access_Control_Policy_API.yaml	access-control-policy	A.7
CAPIF_Logging_API_Invocation_API	8.7	CAPIF Logging API Invocation Service	TS29222_CAPIF_Logging_API_Invocation_API.yaml	api-invocation-logs	A.8
CAPIF_Auditing_API	8.8	CAPIF Auditing API Service	TS29222_CAPIF_Auditing_API.yaml	logs	A.9
CAPIF_API_Provider_Management_API	8.9	CAPIF API Provider Management API Service	TS29222_CAPIF_API_Provider_Management_API.yaml	api-provider-management	A.11
CAPIF_Routing_Info_API	8.10	CAPIF Routing Information API Service	TS29222_CAPIF_Routing_Info_API.yaml	capif-routing-info	A.12

5.2 CAPIF_Discover_Service_API

5.2.1 Service Description

5.2.1.1 Overview

The CAPIF discover service APIs, as defined in 3GPP TS 23.222 [2], allow API invokers via CAPIF-1/1e reference points to discover service API available at the CAPIF core function, and allow CAPIF core function via CAPIF-6 and CAPIF-6e reference points to discover service API available at other CAPIF core function.

5.2.2 Service Operations

5.2.2.1 Introduction

The service operation defined for CAPIF_Discover_Service_API is shown in table 5.2.2.1-1.

Table 5.2.2.1-1: Operations of the CAPIF_Discover_Service_API

Service operation name	Description	Initiated by
Discover_Service_API	This service operation is used by an API invoker to discover service API available at the CAPIF core function. This service operation is also used by CAPIF core function to discover service APIs available at other CAPIF core function.	API invoker, CAPIF core function

5.2.2.2 Discover_Service_API

5.2.2.2.1 General

This service operation is used by:

- an API invoker to discover service API available at the CAPIF core function; or
- a CAPIF core function to discover service API available at other CAPIF core function in interconnection scenario.

5.2.2.2.2 Consumer discovering service API using Discover_Service_API service operation

To discover service APIs available at the CAPIF core function, the consumer (e.g. API invoker) shall send an HTTP GET message with the API invoker Identifier or CAPIF core function Identifier and query parameters to the CAPIF core function as specified in clause 8.1.2.2.3.1.

Upon receiving the above described HTTP GET message, the CAPIF core function shall:

1. verify the identity of the consumer (e.g. API invoker) and check if the consumer is authorized to discover the service APIs;
2. if the consumer is authorized to discover the service APIs, the CAPIF core function shall:
   a. search the CAPIF core function (API registry) for APIs matching the query criteria;
   b. apply the discovery policy, if any, on the search results and filter the search results to obtain the list of service API information or the information of the CAPIF core function which is required to be contacted further for discovering the service APIs; and
   c. return the filtered search results or the information of the CAPIF core function in the response message. The shareableInformation for each of serviceAPIDescription is not provided in the filtered search results;

NOTE: The {apiRoot} part of the URI structure (defined in clause 5.2.4 of 3GPP TS 29.122 [14]) for the discovered APIs can be constructed by the API invoker based on either the "domainName" attribute (which contains all the required information, e.g. FQDN or IP address, port, a deployment specific string in the form of a sequence of path segments) or the "interfaceDescriptions" attribute of the AefProfile data type.

and

3. if errors occur when processing the request, the CAPIF core function shall respond to the consumer with an appropriate error status code as defined in clause 8.1.5.

5.3 CAPIF_Publish_Service_API

5.3.1 Service Description

5.3.1.1 Overview

The CAPIF publish service APIs, as defined in 3GPP TS 23.222 [2], allow API publishing function via CAPIF-4 and CAPIF-4e reference points to publish and manage published service APIs at the CAPIF core function, and allow CAPIF core function via CAPIF-6 and CAPIF-6e reference points to publish and manage published service APIs at other CAPIF core function.

NOTE: Functions from 3rd party API provider domain can also access this API with sufficient permissions.

5.3.2 Service Operations

5.3.2.1 Introduction

The service operations defined for the CAPIF_Publish_Service API are shown in table 5.3.2.1-1.

Table 5.3.2.1-1: Operations of the CAPIF_Publish_Service_API

Service operation name	Description	Initiated by
Publish_Service_API	This service operation is used by an API publishing function to publish service APIs on the CAPIF core function. This service operation is also used by CAPIF core function to publish service APIs on other CAPIF core function.	API publishing function, CAPIF core function
Unpublish_Service_API	This service operation is used by an API publishing function to un-publish service APIs from the CAPIF core function. This service operation is also used by CAPIF core function to un-publish service APIs on other CAPIF core function.	API publishing function, CAPIF core function
Get_Service_API	This service operation is used by an API publishing function to retrieve service APIs from the CAPIF core function. This service operation is also used by CAPIF core function to retrieve service APIs on other CAPIF core function.	API publishing function, CAPIF core function
Update_Service_API	This service operation is used by an API publishing function to update published service APIs on the CAPIF core function. This service operation is also used by CAPIF core function to update published service APIs on other CAPIF core function.	API publishing function, CAPIF core function

5.3.2.2 Publish_Service_API

5.3.2.2.1 General

This service operation is used by:

- an API publishing function to publish service APIs on the CAPIF core function: or
- a CAPIF core function to publish service APIs on other CAPIF core function in interconnection scenario.

5.3.2.2.2 API publishing function publishing service APIs on CAPIF core function using Publish_Service_API service operation

To publish service APIs at the CAPIF core function, the API publishing function shall send an HTTP POST message to the CAPIF core function. The body of the HTTP POST message shall include API Information as specified in clause 8.2.2.2.3.1.

Upon receiving the above described HTTP POST message, the CAPIF core function shall:

1. verify the identity of the API publishing function and check if the API publishing function is authorized to publish service APIs;
2. if the API publishing function is authorized to publish service APIs, the CAPIF core function shall:
   a. verify the API Information present in the HTTP POST message and add the service APIs in the CAPIF core function (API registry);
   b. If topology hiding is enabled as per policy, the CAPIF core function shall:
      i. determine the service APIs which require topology hiding as per policy;
      ii. determine the API exposing function(s) responsible for the topology hiding for each service API which requires topology hiding;

iii. create a API topology hiding information for each service API which requires topology hiding by extracting the API identification information and the API exposing function(s) information from the service API information added to the CAPIF core function (API registry);

iv. replace the API exposing function(s) information in the service API information added to the CAPIF core function (API registry) with the corresponding API exposing function(s) information responsible for the topology hiding for service API;

v. send a notification message with the API topology hiding information to the API exposing function(s) which is responsible for the topology hiding for a service API and that has subscribed to the API_TOPOLOGY_HIDING_CREATED event; and

vi. store the API topology hiding information in the CAPIF core function;

c. create a new resource using the service API information in the CAPIF core function (API registry) as specified in clause 8.2.2.1;

d. send a notification message with the updated service API, to all API Invokers that subscribed to the Service API Update event; and

e. return the CAPIF Resource URI in the response message;

and

3. if errors occur when processing the request, the CAPIF core function shall respond to the API publishing function with an appropriate error status code as defined in clause 8.2.5.

5.3.2.2.3 CAPIF core function publishing service APIs on other CAPIF core function using Publish_Service_API service operation

To publish service APIs at other CAPIF core function, the requesting CAPIF core function shall send an HTTP POST message to the peer CAPIF core function. The body of the HTTP POST message shall include API Information as specified in clause 8.2.2.2.3.1. For service API publishing on CAPIF-6 reference point, the requesting CAPIF core function shall also include the published API path "pubApiPath" as specified in clause 8.2.4.2.2. The "pubApiPath" includes a list of CAPIF core function Identifiers within the same CAPIF provider domain, such list includes own CAPIF core function identifier of the requesting CAPIF core function and received CAPIF core function identifier(s) from other CAPIF core function.

If the requesting CAPIF core function knows the peer CAPIF core function identifier, it shall not send the HTTP POST message to the peer CAPIF core function if the peer CAPIF core function identifier is included in the published API path.

Upon receiving the above described HTTP POST message, the peer CAPIF core function shall:

1. verify the identity of the requesting CAPIF core function in the URI and check if the requesting CAPIF core function is authorized to publish service APIs;

2. if the requesting CAPIF core function is authorized to publish service APIs, the peer CAPIF core function shall check if own CAPIF core function identifier is within the published API path (if received). If it is not within the path, the peer CAPIF core function shall add its own identifier in the path; otherwise reject the HTTP POST request and skip step 3;

3. then the peer CAPIF core function shall:

   a. verify the rest API Information present in the HTTP POST message and add the service APIs in the peer CAPIF core function (API registry);

   b. create a new resource as specified in clause 8.2.2.1;

   c. send a notification message with the updated service API, to all API Invokers that subscribed to the Service API Update event; and

   d. return the CAPIF Resource URI in the response message;

and

4. if errors occur when processing the request, the peer CAPIF core function shall respond to the peer CAPIF core function with an appropriate error status code as defined in clause 8.2.5.

5.3.2.3 Unpublish_Service_API

5.3.2.3.1 General

This service operation is used by:

- an API publishing function to un-publish service APIs from the CAPIF core function; or
- a CAPIF core function to un-publish service APIs on other CAPIF core function in interconnection scenario.

5.3.2.3.2 Consumer un-publishing service APIs from CAPIF core function using Unpublish_Service_API service operation

To un-publish service APIs from the CAPIF core function, the consumer (e.g. API publishing function) shall send an HTTP DELETE message using the CAPIF Resource URI received during the publish operation to the CAPIF core function as specified in clause 8.2.2.3.3.3.

Upon receiving the above described HTTP DELETE message, the CAPIF core function shall

1. verify the identity of the consumer (e.g. API publishing function) and check if the consumer is authorized to un-publish service APIs;
2. if the consumer is authorized to un-publish service APIs, the CAPIF core function shall:
   a. delete the resource pointed by the CAPIF Resource URI;
   b. delete the relevant service APIs from the CAPIF core function (API registry);
   c. If topology hiding is enabled as per policy, the CAPIF core function shall:
      i. determine the API topology hiding information associated with the service API and delete the corresponding API topology hiding information in the CAPIF core function; and
      ii. send a notification message with the deleted API topology hiding information to the corresponding API exposing function(s) which were responsible for the topology hiding of the service API and that subscribed to the API_TOPOLOGY_HIDING_REVOKED event; and
   d. send a notification message with the deleted service API, to all API Invokers that subscribed to the Service API Update event;

   and
3. if errors occur when processing the request, the CAPIF core function shall respond to the consumer with an appropriate error status code as defined in clause 8.2.5.

5.3.2.4 Get_Service_API

5.3.2.4.1 General

This service operation is used by:

- an API publishing function to retrieve service APIs from the CAPIF core function; or
- a CAPIF core function to retrieve service APIs from other CAPIF core function in interconnection scenario.

5.3.2.4.2 Consumer retrieving service APIs from CAPIF core function using Get_Service_API service operation

To retrieve information about the published service APIs from the CAPIF core function, the consumer (e.g. API publishing function) shall send an HTTP GET message to the CAPIF core function. For retrieving the entire list of

service APIs, the HTTP GET message shall be sent to the collection of service APIs resource representation URI as specified in clause 8.2.2.2.3.2. For retrieving a specific service API, the HTTP GET message shall be sent to that service API's resource representation URI as described in clause 8.2.2.3.3.1.

Upon receiving the above described HTTP GET message, the CAPIF core function shall:

1. verify the identity of the consumer (e.g. API publishing function) and check if the consumer is authorized to retrieve information about the published service APIs;
2. if the consumer is authorized to retrieve information about the published service APIs, the CAPIF core function shall:
   a. respond with the requested API Information;

and

3. if errors occur when processing the request, the CAPIF core function shall respond to the consumer with an appropriate error status code as defined in clause 8.2.5.

5.3.2.5 Update_Service_API

5.3.2.5.1 General

This service operation is used by:

- an API publishing function to update published service APIs on the CAPIF core function; or
- a CAPIF core function to update published service APIs on other CAPIF core function in interconnection scenario.

5.3.2.5.2 Consumer updating published service APIs on CAPIF core function using Update_Service_API service operation

To update information of published service APIs, the consumer (e.g. API publishing function) shall send an HTTP PUT message to that service API's resource representation URI in the CAPIF core function. The body of the HTTP PUT message shall include updated API Information as specified in clause 8.2.2.3.3.2; otherwise, if the "PatchUpdate" feature defined in clause 8.2.6 is supported, the consumer (e.g. API publishing function) may send an HTTP PATCH request message to the concerned service API resource URI in the CAPIF core function. The body of the HTTP PATCH request message shall include the requested modifications as specified in clause 8.2.2.3.3.4.

Upon receiving the above described HTTP PUT or PATCH request message, the CAPIF core function shall:

1. verify the identity of the consumer (e.g. API publishing function) and check if the consumer is authorized to update information of published service APIs;
2. if the consumer is authorized to update information of published service APIs, the CAPIF core function shall:
   a. verify the API Information present in the HTTP PUT or PATCH request message and replace/modify the service APIs in the CAPIF core function (API registry);
   b. if topology hiding is enabled as per policy, the CAPIF core function shall:
      i. if the service API being updated has a corresponding API topology hiding information in the CAPIF core function, then update the API topology hiding information with any updated API exposing function(s) information from the service API information replaced at the CAPIF core function (API registry);
      ii. replace/modify the API exposing function(s) information in the service API information added to the CAPIF core function (API registry) with the corresponding API exposing function(s) information responsible for the topology hiding for service API;
      iii. send a notification message with the API topology hiding information to the API exposing function(s) which is responsible for the topology hiding for a service API and that has subscribed to the API_TOPOLOGY_HIDING_CREATED event; and

iv. update the API topology hiding information in the CAPIF core function;

c. replace/modify the existing resource accordingly using the updated service API information in the CAPIF core function (API registry); and

d. send a notification message with the updated service API, to all API Invokers that subscribed to the Service API Update event;

and

3. if errors occur when processing the request, the CAPIF core function shall respond to the consumer with an appropriate error status code as defined in clause 8.2.5.

5.4 CAPIF_Events_API

5.4.1 Service Description

5.4.1.1 Overview

The CAPIF events APIs, as defined in 3GPP TS 23.222 [2], allow an API invoker via CAPIF-1/1e reference points, API exposure function via CAPIF-3/3e reference points, API publishing function via CAPIF-4/4e reference points and API management function via CAPIF-5/5e reference points to subscribe to and unsubscribe from CAPIF events and to receive notifications from CAPIF core function.

NOTE: The functional elements listed above are referred to as Subscriber in the service operations described in the clauses below.

5.4.2 Service Operations

5.4.2.1 Introduction

The service operations defined for the CAPIF_Events_API are shown in table 5.4.2.1-1.

Table 5.4.2.1-1: Operations of the CAPIF_Events_API

Service operation name	Description	Initiated by
Subscribe_Event	This service operation is used by a Subscriber to subscribe to CAPIF events.	Subscriber
Unsubscribe_Event	This service operation is used by a Subscriber to unsubscribe from CAPIF events	Subscriber
Notify_Event	This service operation is used by CAPIF core function to send a notification to a Subscriber	CAPIF core function
Update_Event_Subscription	This service operation is used by a Subscriber to update the subscription to CAPIF events	Subscriber

5.4.2.2 Subscribe_Event

5.4.2.2.1 General

This service operation is used by a Subscriber to subscribe to CAPIF events.

5.4.2.2.2 Subscribing to CAPIF events using Subscribe_Event service operation

To subscribe to CAPIF events, the Subscriber shall send an HTTP POST message to the CAPIF core function. The body of the HTTP POST message shall include Subscriber's Identifier, Event Type and a Notification Destination URI as specified in clause 8.3.2.2.3.1.

For all events included in the HTTP POST message, if the Enhanced_event_report feature is supported, the Subscriber may include an event report requirement in the "eventReq" attribute including:

- event notification method (periodic, one time, on event detection) in the "notifMethod" attribute;
- maximum Number of Reports in the "maxReportNbr" attribute;
- monitoring duration in the "monDur" attribute;
- repetition period for periodic reporting in the "repPeriod" attribute; and/or
- immediate reporting indication in the "immRep" attribute.

If the Enhanced_event_report feature is supported, the Subscriber may also include an event filter in the "eventFilters" attribute. The "eventFilters" attribute shall include:

- if the event is SERVICE_API_AVAILABLE, SERVICE_API_UNAVAILABLE or SERVICE_API_UPDATE, the API IDs in the "apiIds" attribute;
- if the event is API_INVOKER_ONBOARDED or API_INVOKER_OFFBOARDED or API_INVOKER_UPDATED, the API invoker IDs in the "apiInvokerIds" attribute;
- if the event is ACCESS_CONTROL_POLICY_UPDATE, the API invoker IDs in the "apiInvokerIds" attribute and/or API identifications in the "apiIds" attribute; and/or
- if the event is SERVICE_API_INVOCATION_SUCCESS or SERVICE_API_INVOCATION_FAILURE, the API invoker IDs in the "apiInvokerIds" attribute, AEF identifiers in the "aefIds" attribute and/or API IDs in the "apiIds" attribute.

Upon receiving the above described HTTP POST message, the CAPIF core function shall:

1. verify the identity of the Subscriber and check if the Subscriber is authorized to subscribe to the CAPIF events mentioned in the HTTP POST message;
2. if the Subscriber is authorized to subscribe to the CAPIF events, the CAPIF core function shall:
   a. create a new resource as specified in clause 8.3.2.1; and
   b. return the CAPIF Resource URI in the response message;

   and
3. if errors occur when processing the request, the CAPIF core function shall respond to the Subscriber with an appropriate error status code as defined in clause 8.3.5.

5.4.2.3 Unsubscribe_Event

5.4.2.3.1 General

This service operation is used by a Subscriber to un-subscribe from CAPIF events.

5.4.2.3.2 Unsubscribing from CAPIF events using Unsubscribe_Event service operation

To unsubscribe from CAPIF events, the Subscriber shall send an HTTP DELETE message to the resource representing the event in the CAPIF core function as specified in clause 8.3.2.3.3.1.

Upon receiving the HTTP DELETE message, the CAPIF core function shall:

1. verify the identity of the Unsubscribing functional entity and check if the Unsubscribing functional entity is authorized to Unsubscribe from the CAPIF event associated with the CAPIF Resource URI;
2. if the Unsubscribing functional entity is authorized to unsubscribe from the CAPIF events, the CAPIF core function shall delete the resource pointed by the CAPIF Resource URI; and
3. if errors occur when processing the request, the CAPIF core function shall respond to the Subscriber with an appropriate error status code as defined in clause 8.3.5.

5.4.2.4 Notify_Event

5.4.2.4.1 General

This service operation is used by CAPIF core function to send a notification to a Subscriber.

5.4.2.4.2 Notifying CAPIF events using Notify_Event service operation

To notify CAPIF events, the CAPIF core function shall send an HTTP POST message using the Notification Destination URI received in the subscription request. The body of the HTTP POST message shall include an Event Notification and CAPIF Resource URI.

If the Enhanced_event_report feature is supported, the CAPIF core function may include an event detail in the "eventDetail" attribute. The "eventDetail" attribute shall include:

- if the event is SERVICE_API_AVAILABLE or SERVICE_API_UNAVAILABLE, the API IDs in the "apiIds" attribute and, if the "ApiStatusMonitoring" feature is supported, additionally, the service API information in the "serviceAPIDescriptions" attribute;
- if the event is SERVICE_API_UPDATE, the API information in the "serviceAPIDescriptions" attribute;
- if the event is API_INVOKER_ONBOARDED or API_INVOKER_OFFBOARDED or API_INVOKER_UPDATED, the API invoker IDs in the "apiInvokerIds" attribute;
- if the event is ACCESS_CONTROL_POLICY_UPDATE, the access control policy information in the "accCtrlPolList" attribute;
- if the event is SERVICE_API_INVOCATION_SUCCESS or SERVICE_API_INVOCATION_FAILURE, the API invocation logs in the "invocationLogs" attribute; or
- if the event is API_TOPOLOGY_HIDING_CREATED or API_TOPOLOGY_HIDING_REVOKED, the API topology hiding information in the "apiTopoHide" attribute.

Upon receiving the HTTP POST message, the Subscriber shall process the Event Notification.

5.4.2.5 Update_Event_Subscription

5.4.2.5.1 General

This service operation is used by a Subscriber to update the subscription to CAPIF events.

5.4.2.5.2 Update Subscription to CAPIF events using Update_Event_Subscription service operation

To update the subscription details to CAPIF events, the Subscriber shall send an HTTP PUT/PATCH request message to the CAPIF core function. The body of the HTTP PUT request message shall include the EventSubscription data structure specified in clause 8.3.4.2.2. The body of the HTTP PATCH request message shall include the EventSubscriptionPatch data structure specified in clause 8.3.4.2.8.

Upon receiving the HTTP PUT or PATCH message described above, the CAPIF core function shall:

1. verify the identity of the Subscriber and check if the Subscriber is authorized to update/modify the subscription;
2. update the resource and respond to the CAPIF core function with either a "200 OK" status code with the response body containing an updated representation of the resource within the EventSubscription data structure, or a "204 No Content" status code.

5.5 CAPIF_API_Invoker_Management_API

5.5.1 Service Description

5.5.1.1 Overview

The CAPIF API invoker management APIs, as defined in 3GPP TS 23.222 [2], allow API invokers via CAPIF-1/1e reference points to on-board and off-board itself as a recognized user of the CAPIF or update the API invoker's details on the CAPIF core function.

5.5.2 Service Operations

5.5.2.1 Introduction

The service operations defined for the CAPIF API Invoker Management API are shown in table 5.5.2.1-1.

Table 5.5.2.1-1: Operations of the CAPIF_API_Invoker_Management_API

Service operation name	Description	Initiated by
Onboard_API_Invoker	This service operation is used by an API invoker to on-board itself as a recognized user of CAPIF	API invoker
Offboard_API_Invoker	This service operation is used by an API invoker to off-board itself as a recognized user of CAPIF	API invoker
Notify_Onboarding_Completion	This service operation is used by CAPIF core function to send an on-boarding notification to the API invoker.	CAPIF core function
Update_API_Invoker_Details	This service operation is used by an API invoker to update API invoker's details in the CAPIF core function.	API Invoker
Notify_Update_Completion	This service operation is used by CAPIF core function to send an update notification to the API invoker	CAPIF core function

5.5.2.2 Onboard_API_Invoker

5.5.2.2.1 General

This service operation is used by an API invoker to on-board itself as a recognized user of CAPIF

5.5.2.2.2 API invoker on-boarding itself as a recognized user of CAPIF using Onboard_API_Invoker service operation

To on-board itself as a recognized user of the CAPIF, the API invoker shall send an HTTP POST message to the CAPIF core function. The body of the HTTP POST message shall include API invoker Enrolment Details, API List and a Notification Destination URI for on-boarding notification as specified in clause 8.4.2.2.3.1.

Upon receiving the above described HTTP POST message, the CAPIF core function shall check if it can determine authorization of the request and on-board the API invoker automatically. If the CAPIF core function:

1. can determine authorization of the request and on-board the API invoker automatically, the CAPIF core function:

   a. shall process the API invoker Enrolment Details and the API List received in the HTTP POST message and determine if the request sent by the API invoker is authorized or not; and

   b. if the API invoker's request is authorized, the CAPIF core function shall:

      i. create the API invoker Profile consisting of an API invoker Identifier, Authentication Information, Authorization Information and CAPIF Identity Information;

ii. verify the API List present in the HTTP POST message and create a API List of APIs the API invoker is allowed to access;

iii. create a new resource as defined in clause 8.4.2.1;

iv. return the API invoker Profile, API List of APIs the API invoker is allowed to access and the CAPIF Resource URI in the response message.

2. cannot determine authorization of the request to on-board the API invoker automatically, the CAPIF core function:

a. shall acknowledge the receipt of the on-boarding request to the API invoker.

b. shall request the CAPIF administrator to validate the on-boarding request or the API management to validate the on-boarding request by sharing the API invoker Enrolment Details and the API List received in the HTTP POST message;

c. on receiving confirmation of successful validation of the on-boarding request from the CAPIF administrator or the API management, the CAPIF core function shall:

i. create the API invoker Profile consisting of an API invoker Identifier, Authentication Information, Authorization Information and CAPIF Identity Information;

ii. create a new resource as defined in clause 8.4.3; and

iii. deliver the API invoker Profile, API List of APIs the API invoker is allowed to access and the CAPIF Resource URI to the API invoker in a notification;

and

3. if errors occur when processing the request, the CAPIF core function shall respond to the API invoker with an appropriate error status code as defined in clause 8.4.5.

NOTE 1: How the CAPIF core function determines that the CAPIF core function can process the request and on-board the API invoker automatically is out-of-scope of this specification.

NOTE 2: How the CAPIF core function determines that the API invoker's request to on-board is authorized is specified in 3GPP TS 33.122 [16].

NOTE 3: Interactions between the CAPIF core function and the CAPIF administrator or the API management is out-of-scope of this specification.

NOTE 4: The onboarding credential received by the API invoker from the service provider as specified in 3GPP TS 33.122 [16] is included in the Authorization header field of the HTTP request message as described in IETF RFC 9110 [5].

NOTE 5: After the onboarding operation is completed the API Invoker no longer needs to maintain the Notification Destination URI and may delete it.

5.5.2.3 Offboard_API_Invoker

5.5.2.3.1 General

This service operation is used by an API invoker to stop being as a recognized user of CAPIF

5.5.2.3.2 API invoker off-boarding itself as a recognized user of CAPIF using Offboard_API_Invoker service operation

To off-board itself as a recognized user of the CAPIF, the API invoker shall send an HTTP DELETE message to its resource representation in the CAPIF core function as specified in clause 8.4.2.3.3.1.

Upon receiving the HTTP DELETE message, the CAPIF core function shall:

1. determine if the request sent by the API invoker is authorized or not;

2. if the API invoker's request is authorized, the CAPIF core function shall:

   a. delete the resource representation pointed by the CAPIF Resource Identifier; and

   b. delete the related API invoker profile;

and

3. if errors occur when processing the request, the CAPIF core function shall respond to the API invoker with an appropriate error status code as defined in clause 8.4.5.

5.5.2.4 Notify_Onboarding_Completion

5.5.2.4.1 General

This service operation is used by the CAPIF core function to send a notification about the completion of the Onboarding operation to the API Invoker.

5.5.2.4.2 Notifying Onboarding completion using Notify_Onboarding_Completion service operation

When the CAPIF core function cannot immediately authorize the API invoker that issued an Onboarding request (see clause 5.5.2.2.2) it will send a response acknowledging the request and begin processing it. After completion, the CAPIF core function shall send an HTTP POST message using the Notification Destination URI received in the Onboarding request. The body of the HTTP POST message shall include the API Invoker Profile, API List of the APIs the API invoker is allowed to access and the CAPIF Resource URI.

Upon receiving the HTTP POST message, the API invoker shall process the message in the same manner it would have processed an immediate response to the Onboarding request, and respond to the HTTP POST message with an acknowledgement and no body.

5.5.2.5 Update_API_Invoker_Details

5.5.2.5.1 General

This service operation is used by an API invoker to update the API invoker's profile details on the CAPIF core function.

5.5.2.5.2 API invoker updating its details on CAPIF using Update_API_Invoker_Details service operation

To update the API invoker's profile details on the CAPIF core function, the API invoker shall send a HTTP PUT message to the CAPIF core function to its resource representation, requesting to replace all properties in the existing resource, addressed by the URI received in the response to the request that has created the API invoker profile resource. The properties "apiInvokerId" and "onboardingInformation" shall remain unchanged from the previously provided values. The body of the HTTP PUT message shall include the APIInvokerEnrolmentDetails data structure with API invoker identity information, API invoker details that need to be updated and a Notification Destination URI for update notification as specified in clause 8.4.2.3.3.2. API invoker details may include API invoker information and API List. Otherwise, if the "PatchUpdate" feature defined in clause 8.4.6 is supported, the consumer (e.g. API invoker function) may send an HTTP PATCH request message to the concerned service API resource URI in the CAPIF core function to modify the API invoker's profile. The body of the HTTP PATCH request message shall include the APIInvokerEnrolmentDetailsPatch data structure.

Upon receiving the above described HTTP PUT or PATCH request message:

1. if the CAPIF core function decides to update the API list of the API invoker without validation by CAPIF administrator, then the CAPIF core function:

   a. shall determine if the request in the HTTP PUT or PATCH request message by the API invoker is authorized or not;

   b. verify that the "apiInvokerId" and "onboardingInformation" properties are same as in API invoker resource on CAPIF core function;

c. if the API invoker's request is authorized and the properties "apiInvokerId" and "onboardingInformation" match, the CAPIF core function shall:

i. if the request contains an API list:

- create a list of APIs the API invoker is allowed to access; and

- update the resource identified by the CAPIF Resource URI of the API invoker's HTTP PUT or PATCH request with the updated information in the request and the API list created in step A;

ii. if the request does not contain an API list, update the resource identified by the CAPIF Resource URI of the API invoker's HTTP PUT or PATCH request with the updated information in the request; and

iii. return the updated API invoker details;

2. otherwise, the CAPIF core function:

a. shall acknowledge the receipt of the update API invoker details request to the API invoker;

b. verify that the "apiInvokerId" and "onboardingInformation" properties are same as in API invoker resource on CAPIF core function;

c. if the properties "apiInvokerId" and "onboardingInformation" match, then shall request the CAPIF administrator to validate the request or the API management to validate the request by sharing the API invoker identity information and the updated information received in the HTTP PUT message or PATCH request;

d. on receiving confirmation of successful validation of the request from the CAPIF administrator or the API management, the CAPIF core function shall:

i. update the resource identified by the CAPIF Resource URI of the API invoker's HTTP PUT or PATCH request, with validated information; and

ii. return the updated API invoker details;

and

3. if errors occur when processing the request, the CAPIF core function shall respond to the API invoker with an appropriate error status code as defined in clause 8.4.5.

NOTE 1: How the CAPIF core function determines that the CAPIF core function can process the request and update the API list of the API invoker automatically is out-of-scope of this specification.

NOTE 2: Interactions between the CAPIF core function and the CAPIF administrator or the API management is out-of-scope of this specification.

NOTE 3: After the operation is completed the API Invoker no longer needs to maintain the Notification Destination URI and may delete it.

5.5.2.6 Notify_Update_Completion

5.5.2.6.1 General

This service operation is used by the CAPIF core function to send a notification about the completion of the update of API invoker's details.

5.5.2.6.2 Notifying API invoker update completion using Notify_Update_Completion service operation

When the CAPIF core function cannot immediately grant the update request (see clause 5.5.2.5.2) it will send a response acknowledging the request and begin processing it. After completion, the CAPIF core function shall send an HTTP POST message using the Notification Destination URI received in the update details request. The body of the HTTP POST message shall include the updated API Invoker details.

Upon receiving the HTTP POST message, the API invoker shall process the message in the same manner it would have processed an immediate response to the update the details of the API invoker request, and respond to the HTTP POST message with HTTP response 204 No content.

5.6 CAPIF_Security_API

5.6.1 Service Description

5.6.1.1 Overview

The CAPIF security APIs, as defined in 3GPP TS 23.222 [2], allow:

- API invokers via CAPIF-1/1e reference points to (re-)negotiate the service security method and obtain authorization for invoking service APIs; and
- API exposing function via CAPIF-3/3e reference points to obtain authentication information of the API invoker for authentication of the API invoker and revoke the authorization for service APIs.

5.6.2 Service Operations

5.6.2.1 Introduction

The service operations defined for CAPIF_Security_API are shown in table 5.6.2.1-1.

Table 5.6.2.1-1: Operations of the CAPIF_Security_API

Service operation name	Description	Initiated by
Obtain_Security_Method	This service operation is used by an API invoker to negotiate and obtain service API security methods from the CAPIF core function. This information is used by the API invoker for service API invocations at the API Exposing Function.	API invoker
Obtain_Authorization	This service operation is used by an API invoker to obtain authorization to access service APIs.	API invoker
Obtain_API_Invoker_Info	This service operation is used by an API exposing function to obtain the authentication or authorization information related to an API invoker.	API exposing function
Revoke_Authorization	This service operation is used by an API exposing function to invalidate the authorization of an API invoker.	API exposing function

Security information is generated when requested by an API invoker, and is stored in the CAPIF Core function. The information can be accessed via a resource representation URI using the API invoker ID as described in clause 8.5.2.3. The URI is provided to the API invoker in the HTTP response to the creation request (via the Obtain_Security_Method service operation name).

Refer to clause 9.1.2a.2 for details about verifying that the API Exposing function has the ability to authorize API invokers prior to invoking service APIs.

5.6.2.2 Obtain_Security_Method

5.6.2.2.1 General

This service operation is used by an API invoker to negotiate and obtain service API security method from the CAPIF core function. The information received by API invoker shall be used for authentication with the API exposing function.

5.6.2.2.2 Request service API security method from CAPIF using Obtain_Security_Method service operation

To negotiate and obtain service API security method information from the CAPIF core function, the API invoker shall send an HTTP PUT message to the CAPIF core function. The body of the HTTP PUT message shall include Security Method Request and a Notification Destination URI for security related notifications. The Security Method Request from the API invoker contains the unique interface details of the service APIs and may contain a preferred method for each unique service API interface as specified in clause 8.5.2.3.3.3.

Upon receiving the above described HTTP PUT message, the CAPIF core function shall:

1. determine the security method for each service API interface as specified in 3GPP TS 33.122 [16];
2. store the Notification Destination URI for security related notification;
3. create a new resource as defined in clause 8.5.2.1;
4. return the security method information and the CAPIF Resource URI in the response message; and
5. if errors occur when processing the request, the CAPIF core function shall respond to the API invoker with an appropriate error status code as defined in clause 8.5.5.

5.6.2.3 Obtain_Authorization

5.6.2.3.1 General

This service operation is used by an API invoker to negotiate and obtain authorization information from the CAPIF core function. The information received by API invoker shall be used for authorization to invoke service APIs exposed by the API exposing function.

5.6.2.3.2 Obtain authorization using Obtain_Authorization service operation

To obtain authorization information from the CAPIF core function to invoke service APIs, the API invoker shall perform the functions of the resource owner, client and redirection endpoints as described in clause 6.5.2.3 of 3GPP TS 33.122 [16].

The API invoker shall send a POST request to the "Token Endpoint", as described in IETF RFC 6749 [23], clause 3.2. The "Token Endpoint" URI shall be:

{apiRoot}/capif-security/v1/securities/{securityId}/token

where {securityId} is the API invoker identifier and represents the "Individual trusted API invoker" resource created during obtain security method, as described in clause 5.6.2.2.

The body of the HTTP POST request shall indicate that the required OAuth2 grant shall be of type "client_credentials", or when the "RNAA" feature is supported, either "client_credentials" or "authorization_code" (applicable for both the "authorization code" and "authorization code with PKCE" grant types). The "scope" parameter (if present) shall include a list of AEF identifiers and its associated API names the API invoker is trying to access (i.e., the API invoker expected scope).

For RNAA:

- if the "authorization code" grant type is used, the request shall include the resource owner ID and the authorization code and may include the redirection URI (see also IETF RFC 6749 [23] and clause 6.5.3 of TS 33.122 [16]); and

NOTE: When the "authorization code" grant type is used for RNAA, the authorization code is obtained by the API invoker prior to the invocation of this service operation using the procedures defined in clause 4.1 of IETF RFC 6749 [23].

- if the "client credentials" grant type is used, the request shall include the resource owner ID, as defined in clause 6.5.3.1 of TS 33.122 [16].

NOTE: When the "client credentials" grant type is used for RNAA, the CCF has to verify whether the API Invoker is authorized to invoke this service operation for acquiring a token to be subsequently used while accessing a protected resource of the resource owner identified by the resource owner ID.

The API invoker may use HTTP Basic authentication towards this endpoint, using the API invoker identifier as "username" and the onboarding secret as "password". Such username and password may be included in the header or body of the HTTP POST request.

On success, "200 OK" shall be returned. The content of the POST response shall contain the requested access token, the token type and the expiration time for the token. The access token shall be a JSON Web Token (JWT) as specified in IETF RFC 7519 [24]. The access token returned by the CAPIF core function shall include the claims encoded as a JSON object as specified in clause 8.5.4.2.8 and then digitally signed using JWS as specified in IETF RFC 7515 [25] and in Annex C.1 of 3GPP TS 33.122 [16].

The digitally signed access token shall be converted to the JWS Compact Serialization encoding as a string as specified in clause 7.1 of IETF RFC 7515 [25].

If the access token request fails at the CAPIF core function, the CAPIF core function shall return "400 Bad Request" status code, including a JSON object in the response content, that includes details about the specific error that occurred.

5.6.2.3.3 Void

5.6.2.4 Obtain_API_Invoker_Info

5.6.2.4.1 General

This service operation is used by an API exposing function to obtain the security information of API Invokers to be able to authenticate them and authorize each service API invocation by them.

5.6.2.4.2 Obtain API invoker's security information using Obtain_API_Invoker_Info service operation

To obtain authentication or authorization information from the CAPIF core function to authenticate or authorize an API invoker, the API exposing function shall send an HTTP GET message to that API invoker's resource representation URI in the CAPIF core function with an indication to request authentication and/or authorization information, as specified in clause 8.5.2.3.3.1.

Upon receiving the above described HTTP GET message, the CAPIF core function shall:

1. determine the security information of API invoker for all the service API interfaces of the API exposing function;
2. return the security information in the response message; and

NOTE: Functions from 3rd party API provider domain can also access this service operation with sufficient permissions.

3. if errors occur when processing the request, the CAPIF core function shall respond to the API invoker with an appropriate error status code as defined in clause 8.5.5.

5.6.2.5 Revoke_Authentication

5.6.2.5.1 General

This service operation is used by an API exposing function to invalidate the authorization of a specified API Invoker to invoke service APIs exposed by the calling API exposing function.

5.6.2.5.2 Invalidate authorization using Revoke_Authorization service operation

To invalidate authorization of an API invoker for all service APIs, the API exposing function shall send an HTTP DELETE message to that API invoker's resource representation URI in the CAPIF core function using the API invoker ID as specified in clause 8.5.2.3.3.2.

Upon receiving the HTTP DELETE message, the CAPIF core function shall delete the resource representation and shall notify the API invoker of the authorization invalidation using the Notification Destination URI received in the Obtain_Security_Method message.

The CAPIF core function shall also invalidate the previously assigned access token when the authorization of all service APIs are revoked for the API invoker.

To invalidate authorization of an API invoker for some service APIs, the API exposing function shall send an HTTP POST message to that API invoker's "delete" custom resource representation URI in the CAPIF core function with a list of the service APIs that should be revoked.

Upon receiving the HTTP POST message, the CAPIF core function shall revoke the authorization of the API invoker for the indicated service APIs (e.g. it may update the list of unauthorized APIs locally); and shall notify the API invoker of the authorization invalidation using the Notification Destination URI received in the Obtain_Security_Method message.

In both alternatives, the CAPIF core function shall acknowledge the HTTP request from the API exposing function.

NOTE: Functions from 3rd party API provider domain can also access this service operation with sufficient permissions.

5.7 CAPIF_Monitoring_API

The CAPIF monitoring API as defined in 3GPP TS 23.222 [2], allow the API management function via CAPIF-5/5e reference points to monitor service API invocations and receive such monitoring events from the CAPIF core function.

The CAPIF_Monitoring_API shall use the CAPIF_Events_API as described in clause 8.3 by setting the CAPIFEvent to one of the events as described in clause 8.3.4.3.3.

5.8 CAPIF_Logging_API_Invocation_API

5.8.1 Service Description

5.8.1.1 Overview

The Logging API invocations APIs, as defined in 3GPP TS 23.222 [2], allow API exposing functions via CAPIF-3/3e reference points to log the information related to service API invocations on the CAPIF core function.

NOTE: Functions from 3rd party API provider domain can also access this API with sufficient permissions.

5.8.2 Service Operations

5.8.2.1 Introduction

Table 5.8.2.1-1: Operations of the CAPIF_Logging_API_Invocation_API

Service operation name	Description	Initiated by
Log_API_Invocation	This service operation is used by an API exposing function to log API invocation information on CAPIF core function.	API exposing function

5.8.2.2 Log_API_Invocation_API

5.8.2.2.1 General

This service operation is used by an API exposing function to log API invocation information on CAPIF core function.

5.8.2.2.2 Logging service API invocations using Log_API_Invocation service operation

To log service API invocations at the CAPIF core function, the API exposing function shall send an HTTP POST message to the CAPIF core function. The body of the HTTP POST message shall include API exposing function identity information and API invocation log information as specified in clause 8.7.2.2.3.1.

Upon receiving the above described HTTP POST message, the CAPIF core function shall:

1. verify the identity of the API exposing function and check if the API exposing function is authorized to create service API invocation logs;
2. if the API exposing function is authorized to create service API invocation logs, the CAPIF core function shall:
   a. process the API invocation log information received in the HTTP POST message and store the API invocation log information in the API repository;
   b. create a new resource as defined in clause 8.7.2.1; and
   c. return the CAPIF Resource Identifier in the response message;

and

3. if errors occur when processing the request, the CAPIF core function shall respond to the API exposing function with an appropriate error status code as defined in clause 8.7.5.

5.9 CAPIF_Auditing_API

5.9.1 Service Description

5.9.1.1 Overview

The Auditing API, as defined in 3GPP TS 23.222 [2], allows API management functions via CAPIF-5/5e reference points to query the log information stored on the CAPIF core function.

NOTE: Functions from 3rd party API provider domain can also access this API with sufficient permissions.

5.9.2 Service Operations

5.9.2.1 Introduction

Table 5.9.2.1-1: Operations of the CAPIF_Auditing_API

Service operation name	Description	Initiated by
Query_Invocation_Logs	This service operation is used by an API management function to query API invocation information logs stored on CAPIF core function.	API management function

5.9.2.2 Query_Invocation_Logs_API

5.9.2.2.1 General

This service operation is used by an API management function to query API invocation information logs stored on CAPIF core function.

5.9.2.2.2 Query API invocation information logs using Query_Invocation_Logs service operation

To query service API invocation logs at the CAPIF core function, the API management function shall send an HTTP GET message with the API management function identity information and optionally a set of log query parameters to the CAPIF core function as specified in clause 8.8.2.2.3.1.

Upon receiving the above described HTTP GET message, the CAPIF core function shall:

1. verify the identity of the API management function and check if the API management function is authorized to query the service API invocation logs;
2. if the API management function is authorized to query the service API invocation logs, the CAPIF core function shall:
   a. search the API invocation logs for logs matching the log query parameters, if any; and
   b. return the search results in the response message;

and

3. if errors occur when processing the request, the CAPIF core function shall respond to the API management function with an appropriate error status code as defined in clause 8.8.5.

5.10 CAPIF_Access_Control_Policy_API

5.10.1 Service Description

5.10.1.1 Overview

The CAPIF access control policy APIs allow API exposing function via CAPIF-3/3e reference points to obtain the service API access policy from the CAPIF core function.

NOTE: Functions from 3rd party API provider domain can also access this API with sufficient permissions.

5.10.2 Service Operations

5.10.2.1 Introduction

Table 5.3.2.1-1: Operations of the CAPIF_Access_Control_Policy_API

Service operation name	Description	Initiated by
Obtain_Access_Control_Policy	This service operation is used by an API exposing function to obtain the access control policy from the CAPIF core function.	API exposing function

5.10.2.2 Obtain_Access_Control_Policy

5.10.2.2.1 General

This service operation is used by an API exposing function to obtain the access control policy from the CAPIF core function.

5.10.2.2.2 API exposing function obtaining access control policy from the CAPIF core function using Obtain_Access_Control_Policy service operation

To obtain the access control policy from the CAPIF core function, the API exposing function shall send an HTTP GET message to the CAPIF core function with the API exposing function Identifier and API identification. The GET message may include API invoker ID for retrieving access control policy of the requested API invoker as specified in clause 8.6.2.2.3.1.

Upon receiving the above described HTTP GET message, the CAPIF core function shall:

1. verify the identity of the API exposing function and check if the API exposing function is authorized to obtain the access control policy corresponding to the API identification;
2. if the API exposing function is authorized to obtain the access control policy, the CAPIF core function shall respond with the access control policy information corresponding to the API identification and API invoker ID (if present) in the HTTP GET message; and
3. if errors occur when processing the request, the CAPIF core function shall respond to the API exposing function with an appropriate error status code as defined in clause 8.6.5.

5.10.3 Related Events

The CAPIF_Access_Control_Policy_API supports the subscription and notification of the status of access control information via the CAPIF_Events_API. The related events are specified in clause 8.3.4.3.3.

5.11 CAPIF_API_Provider_Management_API

5.11.1 Service Description

5.11.1.1 Overview

The CAPIF API provider management APIs, as defined in 3GPP TS 23.222 [2], allow API management functions via CAPIF-5 and CAPIF-5e reference points to register, deregister and update registration information of API provider domain functions (API Exposing Function, API Publishing Function, API management Function) as a recognized API provider domain of the CAPIF domain.

5.11.2 Service Operations

5.11.2.1 Introduction

The service operations defined for the CAPIF API Provider Management API are shown in table 5.11.2.1-1.

Table 5.11.2.1-1: Operations of the CAPIF_API_Provider_Management_API

Service operation name	Description	Initiated by
Register_API_Provider	This service operation is used by an API management function to register API provider domain functions as a recognized API provider domain of the CAPIF domain.	API Management Function
Update_API_Provider	This service operation is used by an API management function to update the API provider domain functions details in the CAPIF domain.	API Management Function
Deregister_API_Provider	This service operation is used by an API management function to deregister API provider domain functions as a recognized API provider domain of the CAPIF domain.	API Management Function

5.11.2.2 Register_API_Provider

5.11.2.2.1 General

This service operation is used by an API management function to register API provider domain functions as a recognized API provider of CAPIF domain.

5.11.2.2.2 API provider domain functions registering as a recognized API provider domain function of CAPIF using Register_API_Provider service operation

To register API provider domain as a recognized API provider of the CAPIF, the API management function shall send a HTTP POST message to the CAPIF core function. The body of the HTTP POST message shall include API provider Enrolment Details, consisting of details of all API provider domain functions and security information for CAPIF core function to validate the registration request.

Upon receiving the above described HTTP POST message, the CAPIF core function validates the security information and determine if the request sent by API management function is authorized or not. If the API management function is authorized, CAPIF core function shall:

a. create the API provider domain profile consisting of API provider domain ID, API provider domain functions profiles as per the request. CAPIF core function shall assign the identities for the API provider domain functions;

b. create a new resource as defined in clause 8.9.2.2.3.1;

c. return the API provider domain profile, the CAPIF Resource URI in the response message and registration failure information specific to individual API provider domain functions; and

d. if errors occur when processing the request, the CAPIF core function shall respond to the API management function with an appropriate error status code as defined in clause 8.9.5.

5.11.2.3 Update_API_Provider

5.11.2.3.1 General

This service operation is used by an API management function to update API provider domain function details on the CAPIF domain.

5.11.2.3.2 API management function updating API provider domain function details on CAPIF using Update_API_Provider service operation

To update the API provider domain profile and its individual functions details on CAPIF domain, the API management function shall send a HTTP PUT message to its resource representation in the CAPIF core function as specified in clause 8.9.2.3.3.1, requesting to replace all properties in the existing resource, addressed by the URI received in the response to the request that has created the API provider domain profile resource. The property "apiProviderDomainId", shall remain unchanged from the previously provided values. The body of the HTTP PUT message shall include the APIProviderEnrolmentDetails data structure that need to be updated. If the "PatchUpdate" feature defined in

clause 8.9.6 is supported for modification of the API provider domain profile, the consumer (e.g. API publishing function) may send an HTTP PATCH request message to the concerned service API resource URI in the CAPIF core function. The body of the HTTP PATCH request message shall include the APIProviderEnrolmentDetailsPatch data structure.

Upon receiving the described HTTP PUT or PATCH request message:

1. the CAPIF core function shall process the updates received in the HTTP PUT or PATCH request message and determine if the request sent by API management function is authorized or not;

2. verify that the "apiProviderDomainId" property is same as in the API provider domain resource on CAPIF Core Function;

3. if the API management function is authorized and the property "apiProviderDomainId" matches, then the CAPIF core function shall:

   a. replace/modify the representation of the resource identified by the CAPIF Resource URI of the API management function's HTTP PUT or PATCH request with updated information in the request;

   b. update the individual API provider domain function profiles as per the request. CAPIF core function shall create new API provider domain function profiles along with assignment of identities, if the API provider domain functions profiles in the request do not exist in CAPIF; and

   c. return a "200 OK" status code with the updated API provider domain information, or a "204 No Content" status code;

and

4. if errors occur when processing the request, the CAPIF core function shall respond to the API management function with an appropriate error status code as defined in clause 8.9.5.

5.11.2.4 Deregister_API_Provider

5.11.2.4.1 General

This service operation is used by an API management function to deregister the API provider domain function as a recognized API provider of the CAPIF domain.

5.11.2.4.2 API provider domain functions deregistering as a recognized API provider domain function of CAPIF using Deregister_API_Provider service operation

To deregister API provider domain as a recognized API provider of the CAPIF domain, the API management function shall send an HTTP DELETE message to its resource representation in the CAPIF core function as specified in clause 8.9.2.3.3.2.

Upon receiving the HTTP DELETE message, the CAPIF core function shall:

1. determine if the request sent by the API management functions is authorized or not;

2. if the API management function's request is authorized, the CAPIF core function shall:

   a. delete the resource representation pointed by the CAPIF Resource Identifier; and

   b. delete the related API provider domain profile;

and

3. if errors occur when processing the request, the CAPIF core function shall respond to the API management function with an appropriate error status code as defined in clause 8.9.5.

5.12 CAPIF_Routing_Info_API

5.12.1 Service Description

5.12.1.1 Overview

The CAPIF routing info API allows an API exposing function via CAPIF-3/3e reference point to obtain the API routing information from the CAPIF core function.

NOTE: Functions from 3rd party API provider domain can also access this API routing information with sufficient permissions.

5.12.2 Service Operations

5.12.2.1 Introduction

Table 5.12.2.1-1: Operations of the CAPIF_Routing_Info_API

Service operation name	Description	Initiated by
Obtain_Routing_Info	This service operation is used by an API exposing function to obtain the API routing information from the CAPIF core function.	API exposing function

5.12.2.2 Obtain_Routing_Info

5.12.2.2.1 General

This service operation is used by an API exposing function to obtain the API routing information from the CAPIF core function.

5.12.2.2.2 API exposing function obtaining API routing information from the CAPIF core function using Obtain_Routing_Info service operation

To obtain the API routing information from the CAPIF core function, the API exposing function shall send an HTTP GET request message to the CAPIF core function with the API exposing function Identifier and API identification as specified in clause 8.10.2.2.3.1.

Upon receiving the above described HTTP GET message, the CAPIF core function shall

1. verify the identity of the API exposing function and check if the API exposing function is authorized to obtain the API routing information corresponding to the API identification;
2. if the API exposing function is authorized to obtain the API routing information, the CAPIF core function shall respond with the API routing information corresponding to the API identification in the HTTP GET response message; and
3. if errors occur when processing the request, the CAPIF core function shall respond to the API exposing function with an appropriate error status code as defined in clause 8.10.5.

6 Services offered by the API exposing function

6.1 Introduction of Services

The table 6.1-1 lists the API exposing function APIs below the service name. A service description clause for each API gives a general description of the related API.

Table 6.1-1: List of AEF Services

Service Name	Service Operations	Operation Semantics	Consumer(s)
AEF_Security_API	Initiate_Authentication	Request/ Response	API Invoker
	Revoke_Authorization	Request/ Response	CAPIF core function

Table 6.1-2 summarizes the corresponding APIs defined in this specification.

Table 6.1-2: API Descriptions

Service Name	Clause	Description	OpenAPI Specification File	apiName	Annex
AEF_Security_API	9.1	AEF Security API Service	TS29222_AEF_Security_API.yaml	aef-security	A.10

6.2 AEF_Security_API

6.2.1 Service Description

6.2.1.1 Overview

The AEF securityAPI, allows an API invokers via CAPIF-2/2e reference points to request API exposing function to ensure that authentication parameters necessary for authentication of the API invoker are available with the API exposing function. If the necessary authentication parameters are not available, the API exposing function fetches necessary authentication parameters from CAPIF core function to authenticate the API invoker.

The AEF security API, also allows the CAPIF core function via CAPIF-3/3e reference points to request API exposing function to revoke the authorization of service APIs for an API invoker.

6.2.2 Service Operations

6.2.2.1 Introduction

The service operation defined for AEF_Security_API is shown in table 6.2.2.1-1.

Table 6.2.2.1-1: Operations of the AEF_Security_API

Service operation name	Description	Initiated by
Initiate_Authentication	This service operation is used by an API invoker to request API exposing function to confirm necessary authentication data is available to authenticate the API invoker	API invoker
Revoke_Authorization	This service operation is used by the CAPIF core function to request the API exposing function to revoke the authorization of service APIs for an API invoker.	CAPIF core function

6.2.2.2 Initiate_Authentication

6.2.2.2.1 General

This service operation is used by an API invoker to initiate authentication with the API exposing function. On receiving the Initiate_Authentication the API exposing function fetches the authentication information of the API invoker from the CAPIF core function, if required.

6.2.2.2.2 API invoker initiating authentication using Initiate_Authentication service operation

To initiate authentication with the API exposing function, the API invoker shall send an HTTP POST message to the API exposing function with the API invoker ID to the URI "{apiRoot}/aef-security/v1/check-authentication".

Upon receiving the above described HTTP POST message, the API exposing function shall check if the credentials of the API invoker for authentication are available with the API exposing function. If the credentials of the API invoker for authentication are not available, the API exposing function shall use the service defined in clause 5.6.2.4.2 to fetch the credentials from the CAPIF core function.

The API exposing function shall store the received credentials and respond to the API invoker with 200 OK status code.

6.2.2.3 Revoke_Authorization

6.2.2.3.1 General

This service operation is used by CAPIF core function to revoke authorization of service APIs (e.g. due to policy change in the CAPIF core function). On receiving the Revoke_Authorization the API exposing function revokes authorization of the API invoker for the service APIs indicated in the request.

6.2.2.3.2 CAPIF core function initiating revocation using Revoke_Authorization service operation

To revoke authorization, the CAPIF core function shall send an HTTP POST message to the API exposing function with the API invoker ID and a list of service API IDs on the URI "{apiRoot}/aef-security/v1/revoke-authorization".

Upon receiving the HTTP POST message, the API exposing function shall revoke the authorization of the API invoker for the indicated service APIs (e.g. it may update the list of unauthorized APIs locally), and then respond to the CAPIF core function with 200 OK status code.

The CAPIF core function shall also notify the API invoker of the authorization invalidation using the Notification Destination URI received in the Obtain_Security_Method message.

7 CAPIF Design Aspects Common for All APIs

7.1 General

CAPIF APIs are RESTful APIs that allow secure access to the capabilities provided by CAPIF.

This document specifies the procedures triggered at different functional entities as a result of API invocation requests and event notifications. The stage-2 level requirements and signalling flows are defined in 3GPP TS 23.222 [2].

Several design aspects, as mentioned in the following clauses, are specified in 3GPP TS 29.122 [14] and referenced by this specification.

The common API design aspects defined in the clauses under clause 5.2 of 3GPP TS 29.122 [14] that are not defined in the following clauses (e.g., clauses 5.2.10, 5.2.11, 5.2.12 of 3GPP TS 29.122 [14]) shall also apply to the CAPIF APIs defined in this specification, with the following differences:

- the CCF/AEF plays the role of the SCEF;
- the service consumer (e.g., API Invoker, AEF, APF, AMF, CCF) plays the role of the SCS/AS; and
- the provisions related to the T8 APIs shall apply for the CAPIF APIs.

7.2 Data Types

7.2.1 General

This clause defines structured data types, simple data types and enumerations that are applicable to several APIs defined in the present specification and can be referenced from data structures defined in the subsequent clauses.

In addition, data types that are defined in OpenAPI Specification [3] can also be referenced from data structures defined in the subsequent clauses.

NOTE: As a convention, data types in the present specification follow the UpperCamel case convention. Attributes of structured data types follow the lowerCamel case convention. Enumerations follow the UPPER_WITH_UNDERSCORE case convention. As an exception, data types that are also defined in OpenAPI Specification [3] can use a lower-case case letter in the beginning for consistency.

Table 7.2.1-1 specifies data types re-used by the CAPIF APIs from other specifications, including a reference to their respective specifications and when needed, a short description of their use within the CAPIF.

Table 7.2.1-1: Re-used Data Types

Data type	Reference	Comments
Uri	3GPP TS 29.122 [14]	Represents a URI.
TestNotification	3GPP TS 29.122 [14]	Following clarifications apply: - The SCEF is the CAPIF core function; and - The SCS/AS is the Subscriber.
WebsockNotifConfig	3GPP TS 29.122 [14]	Following clarifications apply: - The SCEF is the CAPIF core function; and - The SCS/AS is the Subscriber.

7.2.2 Referenced structured data types

Table 7.2.2-1 lists structured data types defined in this specification referenced by multiple services:

Table 7.2.2-1: Referenced Structured Data Types

Data type	Reference	Description
AefLocation	Clause 8.2.4.2.10	Represents the AEF location.
AefProfile	Clause 8.2.4.2.4	Represents the AEF profile.
CommunicationType	Clause 8.2.4.3.5	Represents the communication type used by the API.
InterfaceDescription	Clause 8.2.4.2.3	Represents the description of the API interface.
InvocationLog	Clause 8.7.4.2.2	Represents logs of service API invocations stored on the CAPIF core function.
Log	Clause 8.7.4.2.3	Represents individual log entries.
SecurityNotification	Clause 8.5.4.2.5	Represents information about the revoked APIs.
ServiceAPIDescription	Clause 8.2.4.2.2	Represents the description of the service API

7.2.3 Referenced Simple data types and enumerations

Following simple data types defined in Table 7.2.3.1-1 are applicable to several APIs in this document:

Table 7.2.3.1-1: Simple data types applicable to several APIs

Type name	Reference	Description
DataFormat	Clause 8.2.4.3.4	Data format used by the API
Operation	Clause 8.2.4.3.7	Used to indicate the HTTP operation
Protocol	Clause 8.2.4.3.3	Protocol used by the API

7.3 Usage of HTTP

For CAPIF APIs, the support of HTTP/1.1 (IETF RFC 9112 [4], IETF RFC 9110 [5], and IETF RFC 9111 [8]) over TLS is mandatory and the support of HTTP/2 (IETF RFC 9113 [10]) over TLS is recommended. TLS shall be used as specified in 3GPP TS 33.122 [16].

A functional entity desiring to use HTTP/2 shall use the HTTP upgrade mechanism to negotiate applicable HTTP version as described in IETF RFC 9113 [10].

7.4 Content type

The provisions of clause 5.2.3 of 3GPP TS 29.122 [14] shall apply to the CAPIF APIs defined in this specification.

7.5 URI structure

7.5.1 Resource URI structure

The provisions of clause 5.2.4.1 of 3GPP TS 29.122 [14] shall apply to the CAPIF APIs defined in this specification.

7.5.2 Custom operations URI structure

The provisions of clause 5.2.4.2 of 3GPP TS 29.122 [14] shall apply to the CAPIF APIs defined in this specification.

7.6 Notifications

The functional entities

- shall support the delivery of notifications using a separate HTTP connection towards an address;
- may support testing delivery of notifications; and
- may support the delivery of notification using WebSocket protocol (see IETF RFC 6455 [13]),

as described in clause 5.2.5 of 3GPP TS 29.122 [14], with the following clarifications:

- the CCF/AEF plays the role of the SCEF; and
- the service consumer (e.g., API Invoker, AEF, APF, AMF, CCF) plays the role of the SCS/AS.

7.7 Error handling

HTTP error handling described in clause 5.2.6 of 3GPP TS 29.122 [14] is applicable to the CAPIF APIs defined in the present specification unless specified otherwise, with the following clarifications:

- the CCF/AEF plays the role of the SCEF; and
- the service consumer (e.g., API Invoker, AEF, APF, AMF, CCF) plays the role of the SCS/AS.

7.8 Feature negotiation

The service consumer or functional entity invoking an API (e.g., API invoker, AEF, the APF, AMF, CCF) and the CCF shall support the feature negotiation procedures defined in clause 5.2.7 of 3GPP TS 29.122 [14] to negotiate the supported features, with the following clarifications:

- the CCF/AEF plays the role of the SCEF; and
- the service consumer (e.g., API Invoker, AEF, APF, AMF, CCF) plays the role of the SCS/AS.

7.9 HTTP custom headers

The HTTP custom headers defined in clause 5.2.8 of 3GPP TS 29.122 [14] shall apply to the CAPIF APIs defined in this specification.

7.10 Conventions for Open API specification files

The conventions for Open API specification files as specified in clause 5.2.9 of 3GPP TS 29.122 [14] shall be applicable for the CAPIF APIs defined in this specifications.

7.11 CAPIF vendor-specifc extensions

The data model of any the CAPIF API shall be extensible with vendor-specific data as specified in clause 5.2.13.2 of 3GPP TS 29.122 [14].

The query parameters used in GET requests in the CAPIF APIs shall be extensible with vendor-specific query parameters as specified in clause 5.2.13.3 of 3GPP TS 29.122 [14].

8 CAPIF Core Function API Definition

8.1 CAPIF_Discover_Service_API

8.1.1 API URI

The CAPIF_Discover_Service_API service shall use the CAPIF_Discover_Service_API.

The request URIs used in HTTP requests from the API invoker towards the CCF shall have the Resource URI structure defined in clause 7.5 with the following clarifications:

- The <apiName> shall be "service-apis".
- The <apiVersion> shall be "v1".
- The <apiSpecificSuffixes> shall be set as described in clause 8.1.2.

All the resource URIs and the custom operation URIs specified in the clauses below are defined relative to the above API URI.

8.1.2 Resources

8.1.2.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 8.1.2.1-1 depicts the resource URIs structure for the CAPIF_Discover_Service_API.

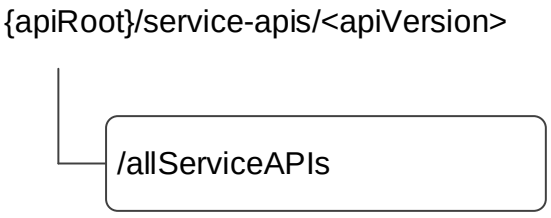

Figure 8.1.2.1-1: Resource URI structure of the CAPIF_Discover_Service_API

Table 8.1.2.1-1 provides an overview of the resources and applicable HTTP methods.

Table 8.1.2.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
All published service APIs	/allServiceAPIs (NOTE)	GET	Discover service APIs according to certain filter criteria.
NOTE: The path segment "allServiceAPIs" does not follow the related naming convention defined in clause 7.5.1. The path segment is however kept as currently defined in this specification for backward compatibility considerations.			

8.1.2.2 Resource: All published service APIs

8.1.2.2.1 Description

This resource represents the collection of published service APIs at the CCF.

This resource is modelled using the Store resource archetype (see Annex C.3 of 3GPP TS 29.501 [18]).

8.1.2.2.2 Resource Definition

Resource URI: **{apiRoot}/service-apis/<apiVersion>/allServiceAPIs**

This resource shall support the resource URI variables defined in table 8.1.2.2.2-1.

Table 8.1.2.2.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5.

8.1.2.2.3 Resource Standard Methods

8.1.2.2.3.1 GET

The HTTP GET method enables to retrieve a list of APIs currently registered at the CCF and satisfying a number of filter criteria.

Table 8.1.2.2.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	P	Cardinality	Description	Applicability
api-invoker-id	string	M	1	It represents the identifier (assigned by the CCF) ofthe API invoker that is sending the request. It may also represent the identifier of the CCF that is sending the request if the request is sent over the CAPIF-6/6e reference point. (NOTE 1)	
api-name	string	O	0..1	Contains the API name as {apiName} part of the URI structure as defined in clause 5.2.4 of 3GPP TS 29.122 [14].	
api-version	string	O	0..1	Contains the API major version conveyed in the URI (e.g. v1).	
comm-type	CommunicationType	O	0..1	Communication type used by the API (e.g. REQUEST_RESPONSE).	
protocol	Protocol	O	0..1	Protocol used by the API.	
aef-id	string	O	0..1	AEF identifier.	
data-format	DataFormat	O	0..1	Data format used by the API (e.g. serialization protocol JSON).	
api-cat	string	O	0..1	The service API category to which the service API belongs.	
preferred-aef-loc	AefLocation	O	0..1	The preferred AEF location. If this parameter is present, the CCF shall try to discover a matched AEF location the service API supports. This parameter is ignored by the CCF if there is no matching record found.	
req-api-prov-name	string	O	0..1	Represents the required API provider name.	RNAA
supported-features	SupportedFeatures	O	0..1	To filter irrelevant responses related to unsupported features.	
api-supported-features	SupportedFeatures	C	0..1	Features supported by the discovered service API indicated by api-name parameter. This may only be present if the api-name query parameter is present.	ApiSupportedFeatureQuery
ue-ip-addr	IpAddrInfo	O	0..1	Represents the UE IP address information.	RNAA
service-kpis	ServiceKpis	O	0..1	Contains information about service characteristics provided by the targeted service API(s).	EdgeApp_2
NOTE 1: This parameter is not part of the API filter criteria so that it is not used in matching APIs published in the CCF. NOTE 2: In addition to the above standardized query parameters, the service consumer may also provide vendor-specific query parameter(s) as specified in clause 5.2.13.3 of 3GPP TS 29.122 [14]. The CCF shall use any received vendor-specific query parameters in the filtering process of the results to be returned in the response in a similar way and in addition to the standardized query parameters defined in this table. This capability may be signalled using the "VendSpecQueryParams" feature.					

This method shall support the request data structures specified in table 8.1.2.2.3.1-2 and the response data structures and response codes specified in table 8.1.2.2.3.1-3.

Table 8.1.2.2.3.1-2: Data structures supported by the GET Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 8.1.2.2.3.1-3: Data structures supported by the GET Response Body on this resource

Data type	P	Cardinality	Response codes	Description
DiscoveredAPIs	M	1	200 OK	The response body contains the result of the search over the list of registered APIs.
n/a			307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative target URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative target URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
ProblemDetails	O	0..1	414 URI Too Long	Indicates that the server refuses to process the request because the request-target is too long.
NOTE: The mandatory HTTP error status codes for the HTTP GET method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] shall also apply.				

Table 8.1.2.2.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative target URI of the resource located in an alternative CCF.

Table 8.1.2.2.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative target URI of the resource located in an alternative CCF.

8.1.2.2.4 Resource Custom Operations

There are no resource custom operations defined for this resource in this release of the specification.

8.1.2A Custom Operations without associated resources

There are no custom operations without associated resources defined for this API in this release of the specification.

8.1.3 Notifications

There are no notifications defined for this API in this release of the specification.

8.1.4 Data Model

8.1.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 7.2 also apply to this API.

Table 8.1.4.1-1 specifies the data types defined specifically for the CAPIF_Discover_Service_API.

Table 8.1.4.1-1: CAPIF_Discover_Service_API specific Data Types

Data type	Section defined	Description	Applicability
DiscoveredAPIs	Clause 8.1.4.2.2	Represents a list of APIs currently registered at the CCF and satisfying a number of filter criteria provided by the service consumer.	
IpAddrInfo	Clause 8.1.4.2.4	Represents the UE IP address information.	RNAA

Table 8.1.4.1-2 specifies data types re-used by the CAPIF_Discover_Service_API from other specifications, including a reference to their respective specifications, and when needed, a short description of their use within the CAPIF_Discover_Service_API.

Table 8.1.4.1-2: Re-used Data Types

Data type	Reference	Comments	Applicability
AefLocation	Clause 8.2.4.2.10	Used to indicate the AEF location.	
CommunicationType	Clause 8.2.4.3.5	Used to indicate the communication type used by the API.	
Ipv4Addr	3GPP TS 29.122 [14]	Used to indicate an IPv4 address.	RNAA
Ipv6Addr	3GPP TS 29.122 [14]	Used to indicate an IPv6 address.	RNAA
ProblemDetails	3GPP TS 29.122 [14]	Used to represent additional information and details on an error response.	
ServiceKpis	Clause 8.2.4.2.13	Represents information about the service characteristics provided by a service API.	EdgeApp_2
SupportedFeatures	3GPP TS 29.571 [19]	Used to negotiate the applicability of optional features defined in table 8.1.6-1.	

8.1.4.2 Structured data types

8.1.4.2.1 Introduction

This clause defines the structured data types to be used in resource representations of the CAPIF_Discover_Service_API.

8.1.4.2.2 Type: DiscoveredAPIs

Table 8.1.4.2.2-1: Definition of type DiscoveredAPIs

Attribute name	Data type	P	Cardinality	Description	Applicability
serviceAPIDescriptions	array(ServiceAPIDescription)	O	1..N	Description of the service API as published by the service.	
NOTE: For the CAPIF_Discover_Service_API, the supportedFeatures attribute of the ServiceAPIDescription data type shall be provided in the HTTP GET response of a successful query. In addition, the supportedFeatures attribute may include one or more supported feature(s) as defined in clause 8.1.6.					

8.1.4.2.3 Void

8.1.4.2.4 Type: IpAddrInfo

Table 8.1.4.2.4-1: Definition of type IpAddrInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
ipv4Addr	Ipv4Addr	C	0..1	Contains the IPv4 address of the UE. (NOTE)	
ipv6Addr	Ipv6Addr	C	0..1	Contains the IPv6 address of the UE. (NOTE)	
NOTE: These attributes are mutually exclusive. Either one of them shall be present.					

8.1.4.3 Simple data types and enumerations

8.1.4.3.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

8.1.4.3.2 Simple data types

The simple data types defined in table 8.1.4.3.2-1 shall be supported.

Table 8.1.4.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability

8.1.4.4 Data types describing alternative data types or combinations of data types

There are no data types describing alternative data types or combinations of data types defined for this API in this release of the specification.

8.1.5 Error Handling

8.1.5.1 General

HTTP error handling shall be supported as specified in clause 7.7.

In addition, the requirements in the following clauses shall apply.

8.1.5.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the CAPIF_Discover_Service_API.

8.2.5.3 Application Errors

The application errors defined for the CAPIF_Publish_Service_API are listed in table 8.2.5.3-1.

Table 8.2.5.3-1: Application errors

Application Error	HTTP status code	Description	Applicability

8.1.6 Feature negotiation

The optional features in table 8.1.6-1 are defined for the the CAPIF_Discover_Service_API. General feature negotiation procedures are defined in clause 7.8.

Table 8.1.6-1: Supported Features

Feature number	Feature Name	Description
1	ApiSupportedFeatureQuery	Indicates the support of the query filter indicating the supported feature(s) of a service API.
2	VendSpecQueryParams	Indicates the support of vendor specific API discovery query filter parameters.
3	RNAA	Indicates the support of the RNAA functionality. This feature enables the following functionalities: - provisioning the API provider name and the related filtering criteria enhancement. - provisioning the UE IP address information and the related filtering criteria enhancement.

8.2 CAPIF_Publish_Service_API

8.2.1 API URI

The CAPIF_Publish_Service_API service shall use the CAPIF_Publish_Service_API.

The request URIs used in HTTP requests from the API publishing function towards the CCF shall have the Resource URI structure as defined in clause 7.5 with the following clarifications:

- The <apiName> shall be "published-apis".
- The <apiVersion> shall be "v1".
- The <apiSpecificSuffixes> shall be set as described in clause 8.2.2.

All the resource URIs and the custom operation URIs specified in the clauses below are defined relative to the above API URI.

8.2.2 Resources

8.2.2.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 8.2.2.1-1 depicts the resource URIs structure for the CAPIF_Publish_Service_API.

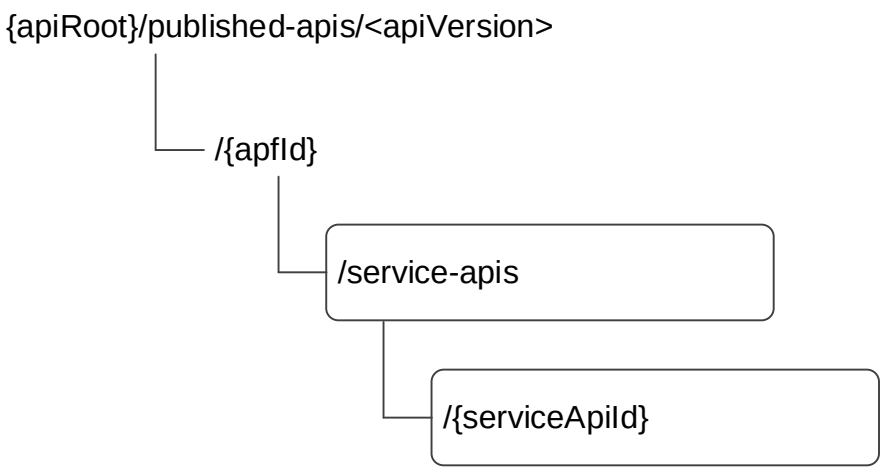

Figure 8.2.2.1-1: Resource URI structure of the CAPIF_Publish_Service_API

Table 8.2.2.1-1 provides an overview of the resources and applicable HTTP methods.

Table 8.2.2.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
APF published APIs	/{apfId}/service-apis	POST	Publish a new API
		GET	Retrieve all the published service APIs.
Individual APF published API	/{apfId}/service-apis/{serviceApiId}	GET	Retrieve an existing published service API.
		PUT	Update an existing published service API.
		PATCH	Modify an existing published service API.
		DELETE	Delete an existing published service API.

8.2.2.2 Resource: APF published APIs

8.2.2.2.1 Description

This resource represents all the published service APIs at the CCF for a given APF.

The resource is modelled using the Collection resource archetype (see Annex C.2 of 3GPP TS 29.501 [18]).

8.2.2.2.2 Resource Definition

Resource URI: **{apiRoot}/published-apis/<apiVersion>/{apfId}/service-apis**

This resource shall support the resource URI variables defined in table 8.2.2.2.2-1.

Table 8.2.2.2.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5.
apfId	string	Identifies the API publishing function that is publishing the service API. For the CAPIF interconnection case, this string identifies the CCF that is publishing the service API.

8.2.2.2.3 Resource Standard Methods

8.2.2.2.3.1 POST

The HTTP POST method enables a service consumer to request to publish a new API at the CCF.

This method shall support the URI query parameters specified in table 8.2.2.2.3.1-1.

Table 8.2.2.2.3.1-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.2.2.2.3.1-2 and the response data structures and response codes specified in table 8.2.2.2.3.1-3.

Table 8.2.2.2.3.1-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
ServiceAPIDescription	M	1	Contains the parameters defining the service API to be published.

Table 8.2.2.2.3.1-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
ServiceAPIDescription	M	1	201 Created	Successful case. The service API is successfully published. The URI of the created "Individual APF published API" resource shall be returned in an HTTP "Location" header.
NOTE: The mandatory HTTP error status codes for the HTTP POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] shall also apply.				

Table 8.2.2.2.3.1-4: Headers supported by the 201 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/published-apis/<apiVersion>/{apfId}/service-apis/{serviceApiId}

8.2.2.2.3.2 GET

The HTTP GET method enables a service consumer to retrieve all the published service APIs at the CCF.

This method shall support the URI query parameters specified in table 8.2.2.2.3.2-1.

Table 8.2.2.2.3.2-1: URI query parameters supported by the GET method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.2.2.2.3.2-2 and the response data structures and response codes specified in table 8.2.2.2.3.2-3.

Table 8.2.2.2.3.2-2: Data structures supported by the GET Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 8.2.2.2.3.2-3: Data structures supported by the GET Response Body on this resource

Data type	P	Cardinality	Response codes	Description
array(ServiceAPIDescription)	O	0..N	200 OK	Successful case. The representation(s) of the "Individual APF published API" resource(s) of the requested service API(s) shall be returned in the response body. If there are no active "Individual APF published API" resources at the CCF, an empty array is returned.
n/a			307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative target URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative target URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the HTTP GET method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] shall also apply.				

Table 8.2.2.2.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative target URI of the resource located in an alternative CCF.

Table 8.2.2.2.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative target URI of the resource located in an alternative CCF.

8.2.2.2.4 Resource Custom Operations

There are no resource custom operations defined for this resource in this release of the specification.

8.2.2.3 Resource: Individual APF published API

8.2.2.3.1 Description

The Individual APF published API resource represents an individual published service API.

The resource is modelled using the Document resource archetype (see Annex C.1 of 3GPP TS 29.501 [18]).

8.2.2.3.2 Resource Definition

Resource URI: **{apiRoot}/published-apis/<apiVersion>/{apfId}/service-apis/{serviceApiId}**

This resource shall support the resource URI variables defined in table 8.2.2.3.2-1.

Table 8.2.2.3.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5
apfId	string	Identifies the API publishing function that is publishing the service API. For the CAPIF interconnection case, this string identifies the CCF that is publishing the service API.
serviceApiId	string	Identifies an "Individual APF published API" resource.

8.2.2.3.3 Resource Standard Methods

8.2.2.3.3.1 GET

The HTTP GET method allows a service consumer to retrieve an existing "Individual APF published API" resource at the CCF.

This method shall support the URI query parameters specified in table 8.2.2.3.3.1-1.

Table 8.2.2.3.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.2.2.3.3.1-2 and the response data structures and response codes specified in table 8.2.2.3.3.1-3.

Table 8.2.2.3.3.1-2: Data structures supported by the GET Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 8.2.2.3.3.1-3: Data structures supported by the GET Response Body on this resource

Data type	P	Cardinality	Response codes	Description
ServiceAPIDescription	M	1	200 OK	Successful case. The service API is successfully published and a representation of the created "Individual APF published API" resource shall be returned.
n/a			307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative target URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative target URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the HTTP GET method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] shall also apply.				

Table 8.2.2.3.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative target URI of the resource located in an alternative CCF.

Table 8.2.2.3.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative target URI of the resource located in an alternative CCF.

8.2.2.3.3.2 PUT

The HTTP PUT method allows a service consumer to update an existing "Individual APF published API" resource at the CCF.

This method shall support the URI query parameters specified in table 8.2.2.3.3.2-1.

Table 8.2.2.3.3.2-1: URI query parameters supported by the PUT method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.2.2.3.3.2-2 and the response data structures and response codes specified in table 8.2.2.3.3.2-3.

Table 8.2.2.3.3.2-2: Data structures supported by the PUT Request Body on this resource

Data type	P	Cardinality	Description
ServiceAPIDescription	M	1	Contains the updated representation of the "Individual APF published API" resource.

Table 8.2.2.3.3.2-3: Data structures supported by the PUT Response Body on this resource

Data type	P	Cardinality	Response codes	Description
ServiceAPIDescription	M	1	200 OK	Successful case. The "Individual APF published API" resource is successfully updated and a representation of the updated resource shall be returned in the response body.
n/a			204 No Content	Successful case. The "Individual APF published API" resource is successfully updated and no content is returned in the response body.
n/a			307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative target URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative target URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the HTTP PUT method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] shall also apply.				

Table 8.2.2.3.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative target URI of the resource located in an alternative CCF.

Table 8.2.2.3.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative target URI of the resource located in an alternative CCF.

8.2.2.3.3.3 DELETE

The HTTP DELETE method allows a service consumer to delete an existing "Individual APF published API" resource at the CCF.

This method shall support the URI query parameters specified in table 8.2.2.3.3.3-1.

Table 8.2.2.3.3.3-1: URI query parameters supported by the GET method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.2.2.3.3.3-2 and the response data structures and response codes specified in table 8.2.2.3.3.3-3.

Table 8.2.2.3.3.3-2: Data structures supported by the DELETE Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 8.2.2.3.3.3-3: Data structures supported by the DELETE Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	Successful case. The "Individual APF published API" resource is successfully deleted.
n/a			307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative target URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative target URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the HTTP DELETE method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] shall also apply.				

Table 8.2.2.3.3.3-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative target URI of the resource located in an alternative CCF.

Table 8.2.2.3.3.3-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative target URI of the resource located in an alternative CCF.

8.2.2.3.3.4 PATCH

The HTTP PATCH method allows a service consumer to modify an existing "Individual APF published API" resource at the CCF.

This method shall support the URI query parameters specified in table 8.2.2.3.3.4-1.

Table 8.2.2.3.3.4-1: URI query parameters supported by the PATCH method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.2.2.3.3.4-2 and the response data structures and response codes specified in table 8.2.2.3.3.4-3.

Table 8.2.2.3.3.4-2: Data structures supported by the PATCH Request Body on this resource

Data type	P	Cardinality	Description
ServiceAPIDescriptionPatch	M	1	Contains the modifications to be applied to the "Individual APF published API" resource.

Table 8.2.2.3.3.4-3: Data structures supported by the PATCH Response Body on this resource

Data type	P	Cardinality	Response codes	Description
ServiceAPIDescription	M	1	200 OK	Successful case. The "Individual APF published API" resource is successfully modified and a representation of the updated resource shall be returned in the response body.
n/a			204 No Content	Successful case. The "Individual APF published API" resource is successfully updated and no content is returned in the response body.
n/a			307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative target URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative target URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the HTTP PATCH method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] shall also apply.				

Table 8.2.2.3.3.4-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative target URI of the resource located in an alternative CCF.

Table 8.2.2.3.3.4-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative target URI of the resource located in an alternative CCF.

8.2.2.3.4 Resource Custom Operations

There are no resource custom operations defined for this resource in this release of the specification.

8.2.2A Custom Operations without associated resources

There are no custom operations without associated resources defined for this API in this release of the specification.

8.2.3 Notifications

There are no notifications defined for this API in this release of the specification.

8.2.4 Data Model

8.2.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 7.2 also apply to this API.

Table 8.2.4.1-1 specifies the data types defined specifically for the CAPIF_Publish_Service_API service.

Table 8.2.4.1-1: CAPIF_Publish_Service_API specific Data Types

Data type	Section defined	Description	Applicability
ApiStatus	Clause 8.2.4.2.12	Represents the API status.	ApiStatusMonitoring
AefLocation	Clause 8.2.4.2.10	Represents the location information (e.g. civic address, GPS coordinates, data center ID) where the AEF providing the service API is located.	
AefProfile	Clause 8.2.4.2.4	Represents the AEF profile data.	
CommunicationType	Clause 8.2.4.3.5	Indicates a communication type of the resource or a custom operation.	
CustomOperation	Clause 8.2.4.2.7	Represents the description of a custom operation.	
DataFormat	Clause 8.2.4.3.4	Indicates a data format, e.g., JSON.	
InterfaceDescription	Clause 8.2.4.2.3	Represents the description of the API interface.	
IpAddrRange	Clause 8.2.4.2.14	Represents the list of IP address ranges information.	
Operation	Clause 8.2.4.3.7	Indicates an HTTP method (e.g. PUT).	
Protocol	Clause 8.2.4.3.3	Indicates a protocol and protocol version used by the API.	
PublishedApiPath	Clause 8.2.4.2.9	Represents the published API path within the same CAPIF provider domain.	
Resource	Clause 8.2.4.2.6	Represents the API resource data.	
SecurityMethod	Clause 8.2.4.3.6	Indicates the security method (e.g. PKI).	
ServiceAPIDescription	Clause 8.2.4.2.2	Represents the description of a service API as published by the APF.	
ServiceAPIDescriptionPatch	Clause 8.2.4.2.11	Represents the parameters to request the modification of an APF published API resource.	PatchUpdate
ServiceKpis	Clause 8.2.4.2.13	Represents information about the service characteristics provided by a service API.	EdgeApp_2
ShareableInformation	Clause 8.2.4.2.8	Indicates whether the service API and/or the service API category can be shared to the list of CAPIF provider domains.	
Version	Clause 8.2.4.2.5	Represents the API version information	

Table 8.2.4.1-2 specifies data types re-used by the CAPIF_Publish_Service_API service:

Table 8.2.4.1-2: Re-used Data Types

Data type	Reference	Comments	Applicability
CivicAddress	3GPP TS 29.572 [30]	Used to indicate a civic address.	
DateTime	3GPP TS 29.122 [14]	Used to indicate an expiration timer.	
DurationSec	3GPP TS 29.122 [14]	Indicates the duration in seconds.	
Fqdn	3GPP TS 29.571 [19]	Used to indicate a FQDN.	
GeographicArea	3GPP TS 29.572 [30]	Used to indicate a geographic area.	
Ipv4Addr	3GPP TS 29.122 [14]	Used to indicate an IPv4 address.	
Ipv6Addr	3GPP TS 29.122 [14]	Used to indicate an IPv6 address.	
Ipv4AddressRange	3GPP TS 29.571 [19]	Used to indicate the IPv4 address range.	RNAA
Ipv6AddressRange	3GPP TS 29.571 [19]	Used to indicate the IPv6 address range.	RNAA
Port	3GPP TS 29.122 [14]	Used to indicate a port.	
SupportedFeatures	3GPP TS 29.571 [19]	Used to negotiate the applicability of optional features defined in table 8.2.6-1.	ApiSupportedFeaturePublishing
Uinteger	3GPP TS 29.571 [19]	Unsigned Integer, i.e. only value 0 and integers above 0 are permissible. Minimum = 0.	

8.2.4.2 Structured data types

8.2.4.2.1 Introduction

This clause defines the structured data types to be used in resource representations of the CAPIF_Publish_Service_API.

8.2.4.2.2 Type: ServiceAPIDescription

Table 8.2.4.2.2-1: Definition of type ServiceAPIDescription

Attribute name	Data type	P	Cardinality	Description	Applicability
apiName	string	M	1	API name, it is set as {apiName} part of the URI structure as defined in clause 5.2.4 of 3GPP TS 29.122 [14].	
apiId	string	O	0..1	API identifier assigned by the CCF to the published service API. Shall not be present in the HTTP POST request from the API publishing function to the CCF. Shall be present in the HTTP POST response from the CCF to the API publishing function and in the HTTP GET response from the CCF to the API invoker (discovery API).	
apiStatus	ApiStatus	O	0..1	Indicates the API status. If this attribute is omitted, the Service API is active at all AEF(s) present in the "aefProfiles" attribute.	ApiStatusMonitoring
aefProfiles	array(AefProfile)	C	1..N	AEF profile information, which includes the exposed API details (e.g. protocol). For CAPIF-4/4e interface, API publishing function shall provide this attribute to the CCF in service API publishing. For CAPIF-1/1e interface, the CCF shall provide this attribute to the API Invoker during service API discovery. (NOTE 2)	
description	string	O	0..1	Text description of the API.	
supportedFeatures	SupportedFeatures	O	0..1	The supported optional features of the CAPIF API. (NOTE 1)	
shareableInfo	ShareableInformation	O	0..1	Represents whether the service API and/or the service API category can be published to other CCFs.	
serviceAPICategory	string	C	0..1	The service API category to which the service API belongs to. This attribute is only applicable for CAPIF-6/6e interface. (NOTE 2)	
ccfId	string	C	0..1	CCF identifier which can be contacted further for discovering the details of service API information. This attribute is only applicable for CAPIF-6/6e interface and shall be provided with serviceAPICategory. (NOTE 2)	
apiSuppFeats	SupportedFeatures	O	0..1	Provided by the consumer to indicate the features supported by the service API.	ApiSupportedFeaturePublishing
pubApiPath	PublishedApiPath	C	0..1	It contains the published API path within the same CAPIF provider domain. it shall be provided by the CCF when publishing the service API to other CCF via the CAPIF-6 reference point.	
apiProvName	string	O	0..1	Represents the API provider name.	RNAA

NOTE 1: For the CAPIF_Publish_Service_API, the "supportedFeatures" attribute shall be provided in the HTTP POST request and in the response of successful resource creation. In addition, the "supportedFeatures" attribute may include one or more of the supported features as defined in clause 8.2.6.

NOTE 2: When this data type is used over the CAPIF-6/6e interface, at least one of the "aefProfiles" attribute or the "serviceAPICategory" attribute (together with the corresponding "ccfId" attribute) shall be present.

8.2.4.2.3 Type: InterfaceDescription

Table 8.2.4.2.3-1: Definition of type InterfaceDescription

Attribute name	Data type	P	Cardinality	Description	Applicability
ipv4Addr	Ipv4Addr	C	0..1	String identifying an IPv4 address (NOTE 1, NOTE 2)	
ipv6Addr	Ipv6Addr	C	0..1	String identifying an IPv6 address (NOTE 1, NOTE 2)	
fqdn	Fqdn	C	0..1	String containing a Fully Qualified Domain Name. (NOTE 1, NOTE 2)	ExtendedIntfDesc
port	Port	O	0..1	Port (NOTE 2)	
apiPrefix	string	O	0..1	A string representing an optional deployment-specific string (API prefix) in the form of a sequence of path segments that starts with a "/" character. (NOTE 2)	ExtendedIntfDesc
securityMethods	array(SecurityMethod)	O	1..N	Security methods supported by the interface. It takes precedence over the security methods provided in AefProfile, for this specific interface	
NOTE 1: Exactly one of the attributes "ipv4Addr", "ipv6Addr" and "fqdn" shall be included. NOTE 2: When the contents of this data type are used to construct the apiRoot of an API, they are used as described in clause 4.4.1 of 3GPP TS 29.501 [18]. NOTE 3: If the VendorExt feature is supported, vendor-specific extensions to the InterfaceDescription data structure, using the mechanism defined in clause 7.11, may be used to convey vendor-specific information.					

8.2.4.2.4 Type: AefProfile

Table 8.2.4.2.4-1: Definition of type AefProfile

Attribute name	Data type	P	Cardinality	Description	Applicability
aefId	string	M	1	AEF identifier	
versions	array(Version)	M	1..N	API version	
protocol	Protocol	O	0..1	Protocol used by the API. (NOTE 3)	
dataFormat	DataFormat	O	0..1	Data format used by the API (NOTE 3)	
securityMethods	array(SecurityMethod)	O	1..N	Security methods supported by the AEF for all interfaces. Certain interfaces may have different security methods supported in the attribute interfaceDescriptions. (NOTE 4)	
domainName	string	O	0..1	Contains the domain name information used to construct the “apiRoot” variable of the API URI. (NOTE 1)	
interfaceDescriptions	array(InterfaceDescription)	O	1..N	Interface details (NOTE 1)	
aefLocation	AefLocation	O	0..1	The location information (e.g. civic address, GPS coordinates, data center ID) where the AEF providing the service API is located.	
serviceKpis	ServiceKpis	O	0..1	Contains information about the service characteristics provided by the service API.	EdgeApp_2
ueIpRange	IpAddrRange	O	0..1	The list of public IP ranges of UEs.	RNAA

NOTE 1: Only one of the attributes "domainName" or "interfaceDescriptions" shall be included.
NOTE 2: Notification or callback type of resource is not included.
NOTE 3: If the VendorExt feature is supported, vendor-specific extensions to the AefProfile data structure, using the mechanism defined in clause 7.11, may be used to convey vendor-specific information.
NOTE 4: For AEFs defined by 3GPP interacting with API invokers via CAPIF-2e, at least one of the "securityMethods" attribute within this data type or the "securityMethods" attribute within the "interfaceDescriptions" attribute shall be present. For AEFs defined by 3GPP interacting with API invokers via CAPIF-2, the "securityMethods" attribute is optional. For AEFs not defined by 3GPP, the "securityMethods" attribute is optional.

8.2.4.2.5 Type: Version

Table 8.2.4.2.5-1: Definition of type Version

Attribute name	Data type	P	Cardinality	Description	Applicability
apiVersion	string	M	1	API major version in URI (e.g. v1)	
expiry	DateTime	O	0..1	Expiry date and time of the AEF service. This represents the planned retirement date as specified in clause 4.3.1.5 of 3GPP TS 29.501 [18].	
resources	array(Resource)	O	1..N	Resources supported by the API. It may include the custom operations with resource association.	
custOperations	array(CustomOperation)	O	1..N	Custom operations without resource association.	

8.2.4.2.6 Type: Resource

Table 8.2.4.2.6-1: Definition of type Resource

Attribute name	Data type	P	Cardinality	Description	Applicability
resourceName	string	M	1	Resource name.	
commType	CommunicationType	M	1	Communication type used by the API resource. (NOTE 1)	
uri	string	M	1	Relative URI of the API resource, it is set as {apiSpecificSuffixes} part of the URI structure as defined in clause 5.2.4 of 3GPP TS 29.122 [14].	
custOpName	string	O	0..1	it is set as {custOpName} part of the URI structure for the case where there is only a single custom operation associated with this resource as defined in clause 5.2.4 of 3GPP TS 29.122 [14]. (NOTE 2)	
custOperations	array(CustomOperation)	O	1..N	List of custom operations associated to this resource. (NOTE 2)	MultipleCustomOperations
operations	array(Operation)	C	1..N	Supported HTTP methods for the API resource. Only applicable when the protocol in AefProfile indicates HTTP.	
description	string	O	0..1	Text description of the API resource.	
NOTE 1: The communication type refers to the semantics of the resource or custom operation and is independent of the HTTP methods that are supported (e.g. if a resource is used for subscriptions then its CommunicationType shall be SUBSCRIBE_NOTIFY even if it supports also the GET method for retrieving the subscriptions). NOTE 2: The attributes "custOpName" and "custOperations" are mutually exclusive.					

8.2.4.2.7 Type: CustomOperation

Table 8.2.4.2.7-1: Definition of type CustomOperation

Attribute name	Data type	P	Cardinality	Description	Applicability
commType	CommunicationType	M	1	Communication type used by the custom operation.	
custOpName	string	M	1	it is set as {custOpName} part of the URI structure for a custom operation without resource association as defined in clause 5.2.4 of 3GPP TS 29.122 [14].	
operations	array(Operation)	C	1..N	Supported HTTP methods for the custom operation. Only applicable when the protocol in AefProfile indicates HTTP.	
description	string	O	0..1	Text description of the custom operation.	

8.2.4.2.8 Type: ShareableInformation

Table 8.2.4.2.8-1: Definition of type ShareableInformation

Attribute name	Data type	P	Cardinality	Description	Applicability
isShareable	boolean	M	1	Set to "true" indicates that the service API and/or the service API category can be shared to the list of CAPIF provider domain information. Otherwise set to "false". Default value is "false" if omitted.	
capifProvDoms	array(string)	O	1..N	List of CAPIF provider domains to which the service API information to be shared. (NOTE)	
NOTE: Only one CAPIF provider domain information shall be provided via the CAPIF-6e interface.					

8.2.4.2.9 Type: PublishedApiPath

Table 8.2.4.2.9-1: Definition of type PublishedApiPath

Attribute name	Data type	P	Cardinality	Description	Applicability
ccfIds	array(string)	O	1..N	A list of CCF identifiers where the service API is already published.	

8.2.4.2.10 Type: AefLocation

Table 8.2.4.2.10-1: Definition of type AefLocation

Attribute name	Data type	P	Cardinality	Description	Applicability
civicAddr	CivicAddress	O	0..1	Identifies the civic address where the AEF providing the service API is located. (NOTE)	
geoArea	GeographicArea	O	0..1	Identifies the geographic area where the AEF providing the service API is located. (NOTE)	
dcId	string	O	0..1	Identifies the data center where the AEF providing the service API is located. (NOTE)	
NOTE: At least one of the attributes shall be included.					

8.2.4.2.11 Type: ServiceAPIDescriptionPatch

Table 8.2.4.2.11-1: Definition of type ServiceAPIDescriptionPatch

Attribute name	Data type	P	Cardinality	Description	Applicability
apiStatus	ApiStatus	O	0..1	Indicates the API status.	ApiStatusMonotiring
aefProfiles	array(AefProfile)	O	1..N	Contains AEF profile information, which includes the exposed API details (e.g., protocol). (NOTE)	
description	string	O	0..1	Contains a textual description of the service API.	
shareableInfo	ShareableInformation	O	0..1	Indicates whether the service API and/or the service API category can be published to other CCFs.	
serviceAPICategory	string	O	0..1	Contains the service API category to which the service API belongs. (NOTE)	
ccfId	string	O	0..1	Contains the CCF identifier which can be contacted further for discovering the details of service API information. This attribute is only applicable for the CAPIF-6/6e interface and shall be present only when the "serviceAPICategory" attribute is also present. (NOTE)	
apiSuppFeats	SupportedFeatures	O	0..1	Contains the list of features supported by the service API.	ApiSupportedFeaturePublishing
pubApiPath	PublishedApiPath	O	0..1	Contains the published API path within the same CAPIF provider domain. This attribute is applicable only over the CAPIF-6 interface.	
NOTE: When this data type is used over the CAPIF-6/6e interface, either the "aefProfiles" attribute or the "serviceAPICategory" attribute (together with the corresponding "ccfId" attribute) may be present.					

8.2.4.2.12 Type: ApiStatus

Table 8.2.4.2.12-1: Definition of type ApiStatus

Attribute name	Data type	P	Cardinality	Description	Applicability
aefIds	array(string)	M	0..N	Indicates the list of AEF ID(s) where the API is active. If an empty array is provided, it indicates that the API is inactive in all AEF(s).	

8.2.4.2.13 Type: ServiceKpis

Table 8.2.4.2.13-1: Definition of type ServiceKpis

Attribute name	Data type	P	Cardinality	Description	Applicability
maxReqRate	Uinteger	C	0..1	Contains the maximum request rate (i.e., number of requests per second) from the API Invoker that is supported by any service producer of the service API.	
maxRestime	DurationSec	C	0..1	Contains the maximum response time (expressed in seconds) supported for the API Invoker's service requests.	
availability	Uinteger	C	0..1	Contains the advertised percentage of time any service producer of the service API is available for the API Invoker's use. Minimum: 0 Maximum: 100	
avalComp	string	C	0..1	Contains the maximum compute resource available for the API Invoker. It is encoded as a string representing a compute resource in FLOPS that shall be formatted as follows: Pattern: '^\d+(\.\d+)?(kFLOPS|MFLOPS|GFLOPS|TFLOPS|PFLOPS|EFLOPS|ZFLOPS)$' Examples: "125 PFLOPS", "0.125 EFLOPS", "125000 TFLOPS"	
avalGraComp	string	C	0..1	Contains the maximum graphical compute resource available for the API Invoker. It is encoded as a string representing a graphical compute resource in FLOPS that shall be formatted as follows: Pattern: '^\d+(\.\d+)?(kFLOPS|MFLOPS|GFLOPS|TFLOPS|PFLOPS|EFLOPS|ZFLOPS)$' Examples: "1250 TFLOPS", "1.25 PFLOPS", "1250000 GFLOPS"	
avalMem	string	C	0..1	Contains the maximum memory resource available for the API Invoker. It is encoded as a string representing a memory resource that shall be formatted as follows: Pattern: '^\d+(\.\d+)?(KB|MB|GB|TB|PB|EB|ZB|YB)$' Examples: "128 GB", "0.128 TB", "128000 MB"	
avalStor	string	C	0..1	Contains the maximum storage resource available for the API Invoker. It is encoded as a string representing a storage resource that shall be formatted as follows: Pattern: '^\d+(\.\d+)?(KB|MB|GB|TB|PB|EB|ZB|YB)$' Examples: "128 TB", "0.128 PB", "128000 GB"	
conBand	Uinteger	C	0..1	Contains the connection bandwidth (expressed in kbps) advertised for the API Invoker's use.	
NOTE: At least one of the attributes of this data structure shall be present.					

8.2.4.2.14 Type: IpAddrRange

Table 8.2.4.2.14-1: Definition of type IpAddrRange

Attribute name	Data type	P	Cardinality	Description	Applicability
ueIpv4AddrRanges	array(Ipv4AddressRange)	C	1..N	Represents the IPv4 Address ranges of the UE(s). (NOTE)	
ueIpv6AddrRanges	array(Ipv6AddressRange)	C	1..N	Represents the IPv6 Address ranges of the UE(s). (NOTE)	
NOTE: At least one of these attributes shall be provided.					

8.2.4.3 Simple data types and enumerations

8.2.4.3.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

8.2.4.3.2 Simple data types

The simple data types defined in table 8.2.4.3.2-1 shall be supported.

Table 8.2.4.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
n/a			

8.2.4.3.3 Enumeration: Protocol

Table 8.2.4.3.3-1: Enumeration Protocol

Enumeration value	Description	Applicability
HTTP_1_1	Indicates that the protocol is HTTP version 1.1.	
HTTP_2	Indicates that the protocol is HTTP version 2.	
MQTT	Indicates that the protocol is Message Queuing Telemetry Transport. (NOTE)	ProtocDataFormats_Ext1
WEBSOCKET	Indicates that the protocol is Websocket. (NOTE)	ProtocDataFormats_Ext1
NOTE: In this release of the specification, this enumeration value shall not be provided for AEFs defined by 3GPP (e.g. SCEF, NEF). It may only be provided for AEFs defined outside 3GPP (e.g. by other SDOs).		

8.2.4.3.4 Enumeration: DataFormat

Table 8.2.4.3.4-1: Enumeration DataFormat

Enumeration value	Description	Applicability
JSON	Indicates that the data format is JSON (JavaScript Object Notation).	
XML	Indicates that the data format is Extensible Markup Language. (NOTE)	ProtocDataFormats_Ext1
PROTOBUF3	Indicates that the data format is Protocol buffers version 3. (NOTE)	ProtocDataFormats_Ext1
NOTE: In this release of the specification, this enumeration value shall not be provided for AEFs defined by 3GPP (e.g. SCEF, NEF). It may only be provided for AEFs defined outside 3GPP (e.g. by other SDOs).		

8.2.4.3.5 Enumeration: CommunicationType

Table 8.2.4.3.5-1: Enumeration CommunicationType

Enumeration value	Description	Applicability
REQUEST_RESPONSE	The communication is of the type request-response.	
SUBSCRIBE_NOTIFY	The communication is of the type subscribe-notify	

8.2.4.3.6 Enumeration: SecurityMethod

Table 8.2.4.3.6-1: Enumeration SecurityMethod

Enumeration value	Description	Applicability
PSK	Security method 1 (Using TLS-PSK) as described in 3GPP TS 33.122 [16].	
PKI	Security method 2 (Using PKI) as described in 3GPP TS 33.122 [16].	
OAUTH	Security method 3 (TLS with OAuth token) as described in 3GPP TS 33.122 [16].	

8.2.4.3.7 Enumeration: Operation

Table 8.2.4.3.7-1: Enumeration Operation

Enumeration value	Description	Applicability
GET	HTTP GET method	
POST	HTTP POST method	
PUT	HTTP PUT method	
PATCH	HTTP PATCH method	
DELETE	HTTP DELETE method	

8.2.5 Error Handling

8.2.5.1 General

HTTP error handling shall be supported as specified in clause 7.7.

In addition, the requirements in the following clauses shall apply.

8.2.5.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the CAPIF_Publish_Service_API.

8.2.5.3 Application Errors

The application errors defined for the CAPIF_Publish_Service_API are listed in table 8.2.5.3-1.

Table 8.2.5.3-1: Application errors

Application Error	HTTP status code	Description	Applicability

8.2.6 Feature negotiation

The optional features in table 8.1.6-1 are defined for the the CAPIF_Publish_Service_API. General feature negotiation procedures are defined in clause 7.8.

Table 8.2.6-1: Supported Features

Feature number	Feature Name	Description
1	ApiSupportedFeaturePublishing	Indicates the support of publishing with supported feature for a service API.
2	PatchUpdate	Indicates the support of the PATCH method for updating an APF published API resource.
3	ExtendedIntfDesc	Indicates the support of extended interface descriptions.
4	MultipleCustomOperations	Indicates the support of modelling multiple custom operations associated with a resource.
5	ProtocDataFormats_Ext1	Indicates the support of additional protocols and data formats with standardized values. (NOTE)
6	ApiStatusMonitoring	Indicates the support of the API status monitoring in CAPIF layer as a part of enhancement of SEAL framework. This feature enables the following functionality: - support API status information management.
7	EdgeApp_2	This feature indicates the support of the enhancements to the Edge Applications. Within this feature, the following enhancements are covered: - support of Service KPI.
8	RNAA	Indicates the support of the RNAA functionality. This feature enables the following functionality: - provisioning of the API provider name and the related filtering criteria. - provisioning of the list of public IP ranges of UEs for service API publish and update enhancements.
9	VendorExt	Indicates the support for CAPIF vendor specific extensions. (NOTE)
NOTE: In this release of the specification, this feature is only applicable for AEFs defined outside 3GPP (e.g. by other SDOs). It does not apply to AEFs defined by 3GPP (e.g. SCEF, NEF).		

8.3 CAPIF_Events_API

8.3.1 API URI

The CAPIF_Events_API service shall use the CAPIF_Events_API.

The request URIs used in HTTP requests from the Subscriber towards the CAPIF core function shall have the Resource URI structure as defined in clause 7.5 with the following clarifications:

- The <apiName> shall be "capif-events".
- The <apiVersion> shall be "v1".
- The <apiSpecificSuffixes> shall be set as described in clause 8.3.2.

All the resource URIs and the custom operation URIs specified in the clauses below are defined relative to the above API URI.

8.3.2 Resources

8.3.2.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 8.3.2.1-1 depicts the resource URIs structure for the CAPIF_Events_API.

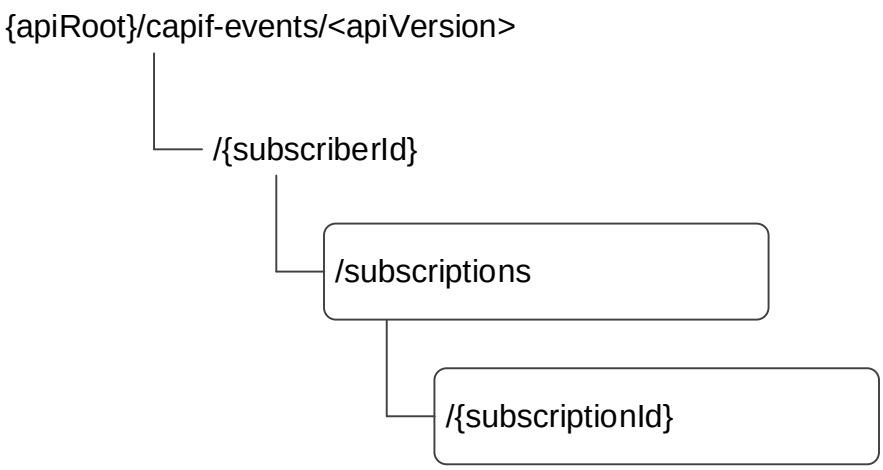

Figure 8.3.2.1-1: Resource URI structure of the CAPIF_Events_API

Table 8.3.2.1-1 provides an overview of the resources and applicable HTTP methods.

Table 8.3.2.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
CAPIF Events Subscriptions	/{subscriberId}/subscriptions	POST	Creates a new individual CAPIF Event Subscription
Individual CAPIF Events Subscription	/{subscriberId}/subscriptions/{subscriptionId}	DELETE	Deletes an individual CAPIF Event Subscription identified by the subscriptionId

8.3.2.2 Resource: CAPIF Events Subscriptions

8.3.2.2.1 Description

The CAPIF Events Subscriptions resource represents all subscriptions of aSubscriber.

8.3.2.2.2 Resource Definition

Resource URI: **{apiRoot}/capif-events/<apiVersion>/{subscriberId}/subscriptions**

This resource shall support the resource URI variables defined in table 8.3.2.2.2-1.

Table 8.3.2.2.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5
subscriberId	string	ID of the Subscriber

8.3.2.2.3 Resource Standard Methods

8.3.2.2.3.1 POST

This method shall support the URI query parameters specified in table 8.3.2.2.3.1-1.

Table 8.3.2.2.3.1-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.3.2.2.3.1-2 and the response data structures and response codes specified in table 8.3.2.2.3.1-3.

Table 8.3.2.2.3.1-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
EventSubscription	M	1	Create a new individual CAPIF Events Subscription resource.

Table 8.3.2.2.3.1-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
EventSubscription	M	1	201 Created	CAPIF Events Subscription resource created successfully. The URI of the created resource shall be returned in the "Location" HTTP header
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.3.2.2.3.1-4: Headers supported by the 201 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/capif-events/<apiVersion>/{subscriberId}/subscriptions/{subscriptionId}

8.3.2.2.4 Resource Custom Operations

None.

8.3.2.3 Resource: Individual CAPIF Events Subscription

8.3.2.3.1 Description

The Individual CAPIF Events Subscription resource represents an individual event subscription of aSubscriber.

8.3.2.3.2 Resource Definition

Resource URI: **{apiRoot}/capif-events/<apiVersion>/{subscriberId}/subscriptions/{subscriptionId}**

This resource shall support the resource URI variables defined in table 8.3.2.3.2-1.

Table 8.3.2.3.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5
subscriberId	string	ID of the Subscriber
subscriptionId	string	Identifies an individual Events Subscription

8.3.2.3.3 Resource Standard Methods

8.3.2.3.3.1 DELETE

This method shall support the URI query parameters specified in table 8.3.2.3.3.1-1.

Table 8.3.2.3.3.1-1: URI query parameters supported by the DELETE method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.3.2.3.3.1-2 and the response data structures and response codes specified in table 8.3.2.3.3.1-3.

Table 8.3.2.3.3.1-2: Data structures supported by the DELETE Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 8.3.2.3.3.1-3: Data structures supported by the DELETE Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The individual CAPIF Events Subscription matching the subscriptionId is deleted.
n/a			307 Temporary Redirect	Temporary redirection, during resource termination. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during resource termination. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the DELETE method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.3.2.3.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.3.2.3.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.3.2.3.3.2 PUT

The PUT method is used to update an existing subscription resource.

The susbcribing entity shall initiate the HTTP PUT request message and the CAPIF core function shall respond to the message.

This method shall support the request data structures specified in table 8.3.2.3.3.2-1 and the response data structures and response codes specified in table 8.3.2.3.3.2-2.

Table 8.3.2.3.3.2-1: Data structures supported by the PUT Request Body on this resource

Data type	P	Cardinality	Description
EventSubscription	M	1	Contains the updated representation of the existing individual CAPIF Events Subscription resource.

Table 8.3.2.3.3.2-2: Data structures supported by the PUT Response Body on this resource

Data type	P	Cardinality	Response codes	Description
EventSubscription	M	1	200 OK	The event subscription was successfully updated, and a representation of the updated resource is returned.
N/A			204 No Content	The event subscription was successfully updated and no content is returned in the reponse body.
N/A			307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
N/A			308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the HTTP PUT method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] shall also apply.				

Table 8.3.2.3.3.2-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI of the resource located in an alternative CAPIF core function.

Table 8.3.2.3.3.2-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI of the resource located in an alternative CAPIF core function.

8.3.2.3.3.3 PATCH

The PATCH method allows to modify an existing subscription.

The subscribing entity shall initiate the HTTP PATCH request message and the CAPIF core function shall respond to the message.

This method shall support the request data structures specified in table 8.3.2.3.3.3-1 and the response data structures and response codes specified in table 8.3.2.3.3.3-2.

Table 8.3.2.3.3.3-1: Data structures supported by the PATCH Request Body on this resource

Data type	P	Cardinality	Description
EventSubscriptionPatch	M	1	Contains the parameters to request the modification of the existing individual CAPIF Events Subscription resource.

Table 8.3.2.3.3.3-2: Data structures supported by the PATCH Response Body on this resource

Data type	P	Cardinality	Response codes	Description
EventSubscription	M	1	200 OK	The subscription was successfully modified and a representation of the updated resource is returned in the response body.
N/A			204 No Content	The subscription was successfully modified and no content was returned in the response body.
N/A			307 Temporary Redirect	Temporary redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
N/A			308 Permanent Redirect	Permanent redirection. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the HTTP PATCH method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] shall also apply.				

Table 8.3.2.3.3.3-3: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI of the resource located in an alternative CAPIF core function.

Table 8.3.2.3.3.3-4: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI of the resource located in an alternative CAPIF core function.

8.3.2.3.4 Resource Custom Operations

None.

8.3.2A Custom Operations without associated resources

There are no custom operations without associated resources defined for this API in this release of the specification.

8.3.3 Notifications

8.3.3.1 General

The delivery of notifications shall conform to clause 7.6.

Table 8.3.3.1-1: Notifications overview

Notification	Callback URI	HTTP method or custom operation	Description (service operation)
Event notification	{notificationDestination}	POST	Notifies Subscriber of a CAPIF Event

8.3.3.2 Event Notification

8.3.3.2.1 Description

Event Notification is used by the CAPIF core function to notify a Subscriber of an Event. The Subscriber shall be subscribed to such Event Notification via the Individual CAPIF Events Subscription Resource.

8.3.3.2.2 Notification definition

The POST method shall be used for Event notification and the URI shall be the one provided by the Subscriber during the subscription to the event.

Callback URI: **{notificationDestination}**

This method shall support the URI query parameters specified in table 8.3.3.2.2.1-1.

Table 8.3.3.2.2-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.3.3.2.2-2 and the response data structures and response codes specified in table 8.3.3.2.2-3.

Table 8.3.3.2.2-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
EventNotification	M	1	Notification information of a CAPIF Event

Table 8.3.3.2.2-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The receipt of the Notification is acknowledged.
n/a			307 Temporary Redirect	Temporary redirection, during notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative notification destination where the notification should be sent. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative notification destination where the notification should be sent. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.3.3.2.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative notification destination towards which the notification should be redirected.

Table 8.3.3.2.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative notification destination towards which the notification should be redirected.

8.3.4 Data Model

8.3.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 7.2 also apply to this API.

Table 8.3.4.1-1 specifies the data types defined specifically for the CAPIF_Events_API service.

Table 8.3.4.1-1: CAPIF_Events_API specific Data Types

Data type	Section defined	Description	Applicability
AccessControlPolicyListExt	Clause 8.3.4.2.6	Represents the extension for access control policies.	
CAPIFEvent	Clause 8.3.4.3.2	Describes the CAPIF event.	
CAPIFEventDetail	Clause 8.3.4.2.5	Represents the CAPIF event detail.	Enhanced_event_report
CAPIFEventFilter	Clause 8.3.4.2.4	Represents the CAPIF event filter.	Enhanced_event_report
EventNotification	Clause 8.3.4.2.3	Represents an individual CAPIF Event Subscription Notification.	
EventSubscription	Clause 8.3.4.2.2	Represents an individual CAPIF Event Subscription resource.	
TopologyHiding	Clause 8.3.4.2.7	Represents the routing rules information of a service API.	

Table 8.3.4.1-2 specifies data types re-used by the CAPIF_Events_API service:

Table 8.3.4.1-2: Re-used Data Types

Data type	Reference	Comments	Applicability
ReportingInformation	3GPP TS 29.523 [26]	Used to indicate the reporting requirement, only the following information are applicable for CAPIF: - immRep - notifMethod - maxReportNbr - monDur - repPeriod	Enhanced_event_report
SupportedFeatures	3GPP TS 29.571 [19]	Used to negotiate the applicability of optional features defined in table 8.3.6-1.	

8.3.4.2 Structured data types

8.3.4.2.1 Introduction

This clause defines the structures to be used in resource representations.

8.3.4.2.2 Type: EventSubscription

Table 8.3.4.2.2-1: Definition of type EventSubscription

Attribute name	Data type	P	Cardinality	Description	Applicability
events	array(CAPIFEvent)	M	1..N	Subscribed events	
eventFilters	array(CAPIFEventFilter)	O	1..N	Subscribed event filters. The n^{th} entry in the "eventFilters" attribute shall correspond to the n^{th} entry in the "events" attribute. For event not having event filter, an empty event filter entry without any sub-attribute shall be provided.	Enhanced_event_report
eventReq	ReportingInformation	O	0..1	Represents the reporting requirements of the event subscription.	Enhanced_event_report
notificationDestination	Uri	M	1	URI where the notification should be delivered to.	
requestTestNotification	boolean	O	0..1	Set to "true" by Subscriber to request the CAPIF core function to send a test notification as defined in clause 7.6. Set to "false" not request the CAPIF core function to send a test notification. Default value is "false" if omitted.	Notification_test_event
websockNotifConfig	WebsockNotifConfig	O	0..1	Configuration parameters to set up notification delivery over Websocket protocol as defined in clause 7.6.	Notification_websocket
supportedFeatures	SupportedFeatures	C	0..1	Used to negotiate the supported optional features of the API as described in clause 7.8. This attribute shall be provided in the HTTP POST request and in the response of successful resource creation.	

8.3.4.2.3 Type: EventNotification

Table 8.3.4.2.3-1: Definition of type EventNotification

Attribute name	Data type	P	Cardinality	Description	Applicability
subscriptionId	string	M	1	Identifier of the subscription resource to which the notification is related – CAPIF resource identifier	
events	CAPIFEvent	M	1	Notifications of individual events	
eventDetail	CAPIFEventDetail	C	0..1	Detailed information for the event. (NOTE)	Enhanced_event_report
NOTE: Within the CAPIFEventDetail data type, the "serviceAPIDescriptions" attribute shall be provided if the event is SERVICE_API_UPDATE, the "apiIds" attribute shall be provided if the event is SERVICE_API_AVAILABLE, SERVICE_API_UNAVAILABLE, the "apiInvokerIds" attribute shall be provided only if the event is attribute shall be provided if the event is API_INVOKER_ONBOARDED or API_INVOKER_OFFBOARDED, or API_INVOKER_UPDATED, the "accCtrlPolList" attribute shall be provided if the event is ACCESS_CONTROL_POLICY_UPDATE, the "invocationLogs" attribute shall be provided if the event is SERVICE_API_INVOCATION_SUCCESS or SERVICE_API_INVOCATION_FAILURE, the "apiTopoHide" attribute shall be provided if the event is API_TOPOLOGY_HIDING_CREATED or API_TOPOLOGY_HIDING_REVOKED.					

8.3.4.2.4 Type: CAPIFEventFilter

Table 8.3.4.2.4-1: Definition of type CAPIFEventFilter

Attribute name	Data type	P	Cardinality	Description	Applicability
apiIds	array(string)	O	1..N	API identifiers that the event subscriber wants to know in the interested event.	
apiInvokerIds	array(string)	O	1..N	API invokers that the event subscriber wants to know in the interested event.	
aefIds	array(string)	O	1..N	String identifying the AEF.	

8.3.4.2.5 Type: CAPIFEventDetail

Table 8.3.4.2.5-1: Definition of type CAPIFEventDetail

Attribute name	Data type	P	Cardinality	Description	Applicability
serviceAPIDescriptions	array(ServiceAPIDescription)	O	1..N	Description of the service API as published by the APF.	
apiIds	array(string)	O	1..N	API identifiers.	
apiInvokerIds	array(string)	O	1..N	API invokers that are onboarded/offboarded.	
accCtrlPolList	AccessControlPolicyListExt	O	0..1	Access control policy updated list.	
invocationLogs	array(InvocationLog)	O	1..N	Invocation logs	
apiTopoHide	Topology Hiding	O	0..1	Topology hiding information for a service API	

8.3.4.2.6 Type: AccessControlPolicyListExt

Table 8.3.4.2.6-1: Definition of type AccessControlPolicyListExt

Attribute name	Data type	P	Cardinality	Description	Applicability
apiId	string	M	1	Identifier of the service API	
NOTE: This data type also contains all the properties defined for AccessControlPolicyList data type.					

8.3.4.2.7 Type: TopologyHiding

Table 8.3.4.2.7-1: Definition of type TopologyHiding

Attribute name	Data type	P	Cardinality	Description	Applicability
apiId	string	M	1	Identifier of the service API	
routingRules	array(RoutingRule)	M	1..N	Routing rules	

8.3.4.2.8 Type: EventSubscriptionPatch

Table 8.3.4.2.8-1: Definition of type EventSubscriptionPatch

Attribute name	Data type	P	Cardinality	Description	Applicability
events	array(CAPIFEvent)	O	1..N	Subscribed events (NOTE).	
eventFilters	array(CAPIFEventFilter)	O	1..N	Subscribed event filters. The n^{th} entry in the "eventFilters" attribute shall correspond to the n^{th} entry in the "events" attribute. For event not having event filter, an empty event filter entry without any sub-attribute shall be provided (NOTE).	
eventReq	ReportingInformation	O	0..1	Represents the reporting requirements of the event subscription (NOTE).	
notificationDestination	Uri	O	0..1	URI where the notification should be delivered to (NOTE).	
NOTE: At least one attribute shall be present.					

8.3.4.3 Simple data types and enumerations

8.3.4.3.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

8.3.4.3.2 Simple data types

None.

The simple data types defined in table 8.3.4.3.2-1 shall be supported.

Table 8.3.4.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
n/a			

8.3.4.3.3 Enumeration: CAPIFEvent

Table 8.3.4.3.3-1: Enumeration CAPIFEvent

Enumeration value	Description	Applicability
SERVICE_API_AVAILABLE	Events related to the availability of service APIs after the service APIs are published.	
SERVICE_API_UNAVAILABLE	Events related to the unavailability of service APIs after the service APIs are unpublished.	
SERVICE_API_UPDATE	Events related to change in service API information	
API_INVOKER_ONBOARDED	Events related to API invoker onboarded to CAPIF	
API_INVOKER_OFFBOARDED	Events related to API invoker offboarded from CAPIF	
SERVICE_API_INVOCATION_SUCCESS	Events related to the successful invocation of service APIs	
SERVICE_API_INVOCATION_FAILURE	Events related to the failed invocation of service APIs	
ACCESS_CONTROL_POLICY_UPDATE	Events related to the update for the access control policy related to the service APIs	
ACCESS_CONTROL_POLICY_UNAVAILABLE	Events related to the unavailability of the access control policy related to the service APIs (NOTE)	
API_INVOKER_AUTHORIZATION_REVOKED	Events related to the revocation of the authorization of API invokers to access the service APIs. (NOTE)	
API_INVOKER_UPDATED	Events related to API invoker profile updated to CAPIF.	
API_TOPOLOGY_HIDING_CREATED	Events related to the creation or update of the API topology hiding information of the service API after the service APIs are published	
API_TOPOLOGY_HIDING_REVOKED	Events related to the revocation of the API topology information of the service API after the service APIs are unpublished	
NOTE: The present release does not specify further details (e.g. event filters) for this event.		

8.3.5 Error Handling

8.3.5.1 General

HTTP error handling shall be supported as specified in clause 7.7.

In addition, the requirements in the following clauses shall apply.

8.3.5.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the CAPIF_Events_API.

8.3.5.3 Application Errors

The application errors defined for the CAPIF_Events_API are listed in table 8.3.5.3-1.

Table 8.3.5.3-1: Application errors

Application Error	HTTP status code	Description	Applicability

8.3.6 Feature negotiation

General feature negotiation procedures are defined in clause 7.8. Table 8.3.6-1 lists the supported features for CAPIF_Events_API.

Table 8.3.6-1: Supported Features

Feature number	Feature Name	Description
1	Notification_test_event	Testing of notification connection is supported according to clause 7.6.
2	Notification_websocket	The delivery of notifications over Websocket is supported according to clause 7.6. This feature requires that the Notification_test_event feature is also supported.
3	Enhanced_event_report	This feature supports the enhanced event report including event reporting requirement and event reporting details as defined in clause 5.4.2.2.2.
4	ApiStatusMonitoring	Indicates the support of the API status monitoring in CAPIF layer as a part of enhancement of SEAL framework. This feature enables the following functionality: - enhancement of the CAPIF event notification.

8.4 CAPIF_API_Invoker_Management_API

8.4.1 API URI

The CAPIF_API_Invoker_Management_API service shall use the CAPIF_API_Invoker_Management_API.

The request URIs used in HTTP requests from the API invoker towards the CAPIF core function shall have the Resource URI structure as defined in clause 7.5 with the following clarifications:

- The <apiName> shall be "api-invoker-management".
- The <apiVersion> shall be "v1".
- The <apiSpecificSuffixes> shall be set as described in clause 8.4.2.

All the resource URIs and the custom operation URIs specified in the clauses below are defined relative to the above API URI.

8.4.2 Resources

8.4.2.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 8.4.2.1-1 depicts the resource URIs structure for the CAPIF_API_Invoker_Management_API.

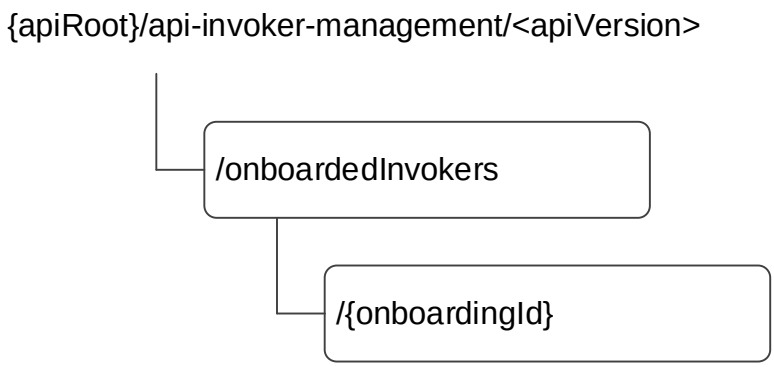

Figure 8.4.2.1-1: Resource URI structure of the CAPIF_API_Invoker_Management_API

Table 8.4.2.1-1 provides an overview of the resources and applicable HTTP methods.

Table 8.4.2.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
On-boarded API Invokers	/onboardedInvokers (NOTE)	POST	On-boards a new API invoker by creating an API invoker profile
Individual On-boarded API Invoker	/onboardedInvokers/{onboardingId} (NOTE)	DELETE	Off-boards an individual API invoker by deleting the associated API invoker profile identified by {onboardingId}
		PATCH	Modifies the API invoker details of an individual API invoker identified by the {onboardingId}
		PUT	Updates the API invoker details of an individual API invoker identified by the {onboardingId}
NOTE: The path segment "onboardedInvokers" does not follow the related naming convention defined in clause 7.5.1. The path segment is however kept as currently defined in this specification for backward compatibility considerations.			

8.4.2.2 Resource: On-boarded API invokers

8.4.2.2.1 Description

The On-boarded API Invokers resource represents all the API invokers that are on-boarded at a given CAPIF core function.

8.4.2.2.2 Resource Definition

Resource URI: **{apiRoot}/api-invoker-management/<apiVersion>/onboardedInvokers**

This resource shall support the resource URI variables defined in table 8.4.2.2.2-1.

Table 8.4.2.2.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5

8.4.2.2.3 Resource Standard Methods

8.4.2.2.3.1 POST

This method shall support the URI query parameters specified in table 8.4.2.2.3.1-1.

Table 8.4.2.2.3.1-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.4.2.2.3.1-2 and the response data structures and response codes specified in table 8.4.2.2.3.1-3.

Table 8.4.2.2.3.1-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
APIInvokerEnrolmentDetails	M	1	Enrolment details of the API invoker including notification destination URI for any on-boarding related notifications and an optional list of APIs the API invoker intends to invoke while on-board.

Table 8.4.2.2.3.1-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
APIInvokerEnrolmentDetails	M	1	201 Created	API invoker on-boarded successfully The URI of the created resource shall be returned in the "Location" HTTP header. A list of APIs the API invoker is allowed to invoke while on-board may also be included as part of the APIInvokerEnrolmentDetails which is provided in the response body, if requested in the POST request.
n/a			202 Accepted	The CAPIF core has accepted the Onboarding request and is processing it. When processing is completed, the CAPIF core function will send a Notify_Onboarding_Completion notification to the requesting API invoker. See clause 8.4.3.2.
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.4.2.2.3.1-4: Headers supported by the 201 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/api-invoker-management/<apiVersion>/onboardedInvokers/{onboardingId}

8.4.2.2.4 Resource Custom Operations

None.

8.4.2.3 Resource: Individual On-boarded API Invoker

8.4.2.3.1 Description

The Individual On-boarded API Invokers resource represents an individual API invoker that is on-boarded at a given CAPIF core function.

8.4.2.3.2 Resource Definition

Resource URI: **{apiRoot}/api-invoker-management/<apiVersion>/onboardedInvokers/{onboardingId}**

This resource shall support the resource URI variables defined in table 8.4.2.3.2-1.

Table 8.4.2.3.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5
onboardingId	string	String identifying an individual on-boarded API invoker resource

8.4.2.3.3 Resource Standard Methods

8.4.2.3.3.1 DELETE

This method shall support the URI query parameters specified in table 8.4.2.3.3.1-1.

Table 8.4.2.3.3.1-1: URI query parameters supported by the DELETE method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the response codes specified in table 8.4.2.3.3.1-2 and the response data structures and response codes specified in table 8.4.2.3.3.1-3.

Table 8.4.2.3.3.1-2: Data structures supported by the DELETE Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 8.4.2.3.3.1-3: Data structures supported by the DELETE Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The individual on-boarded API invoker matching the onboardingId is deleted
n/a			307 Temporary Redirect	Temporary redirection, during resource termination. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during resource termination. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the DELETE method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.4.2.3.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.4.2.3.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.4.2.3.3.2 PUT

The PUT method allows updating the API invoker details of the onboarded API invoker. This method shall support the URI query parameters specified in table 8.4.2.3.3.2-1.

Table 8.4.2.3.3.2-1: URI query parameters supported by the PUT method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in the table 8.4.2.3.3.2-2 and the response data structures and response codes specified in the table 8.4.2.3.3.2-3.

Table 8.4.2.3.3.2-2: Data structures supported by the PUT Request Body on this resource

Data type	P	Cardinality	Description
APIInvokerEnrolmentDetails	M	1	Updated details of the API invoker and a notification destination URI for any update request related notifications.

Table 8.4.2.3.3.2-3: Data structures supported by the PUT Response Body on this resource

Data type	P	Cardinality	Response codes	Description
APIInvokerEnrolmentDetails	M	1	200 OK	API invoker's information updated successfully. Updated details of the API invoker as part of the APIInvokerEnrolmentDetails, which is provided in the response body.
n/a			202 Accepted	The CAPIF core has accepted the Update details request and is processing it. When processing is completed, the CAPIF core function will send a Notify_Update_Completion notification to the requesting API invoker. See clause 8.4.3.3.
n/a			204 No Content	API invoker's information updated successfully, with no content to be sent in the response body.
n/a			307 Temporary Redirect	Temporary redirection, during resource modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during resource modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the PUT method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.4.2.3.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.4.2.3.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.4.2.3.3.3 PATCH

This method shall support the URI query parameters specified in table 8.4.2.3.3.3-1.

Table 8.4.2.3.3.3-1: URI query parameters supported by the PATCH method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.4.2.3.3.3-2 and the response data structures and response codes specified in table 8.4.2.3.3.3-3.

Table 8.4.2.3.3.3-2: Data structures supported by the PATCH Request Body on this resource

Data type	P	Cardinality	Description
APIInvokerEnrolmentDetailsPatch	M	1	Modified details of the API invoker and a notification destination URI for any modify request related notifications.

Table 8.4.2.3.3.3-3: Data structures supported by the PATCH Response Body on this resource

Data type	P	Cardinality	Response codes	Description
APIInvokerEnrolmentDetails	M	1	200 OK	API invoker's information modified successfully. Modified details of the API invoker as part of the APIInvokerEnrolmentDetails, which is provided in the response body.
n/a			202 Accepted	The CAPIF core has accepted the modify details request and is processing it. When processing is completed, the CAPIF core function will send a Notify_Update_Completion notification to the requesting API invoker. See sub clause 8.4.3.3.
n/a			204 No Content	API invoker's information modified successfully, with no content to be sent in the response body.
n/a			307 Temporary Redirect	Temporary redirection, during resource modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during resource modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the HTTP PATCH method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.4.2.3.3.3-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	String	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.4.2.3.3.3-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	String	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.4.2.3.4 Resource Custom Operations

None.

8.4.2A Custom Operations without associated resources

There are no custom operations without associated resources defined for this API in this release of the specification.

8.4.3 Notifications

8.4.3.1 General

The delivery of notifications shall conform to clause 7.6.

Table 8.4.3.1-1: Notifications overview

Notification	Callback URI	HTTP method or custom operation	Description (service operation)
Notify_Onboarding_Completion	{notificationDestination}	POST	Notify API invoker of on-boarding result
Notify_Update_Completion	{notificationDestination}	POST	Notify API invoker of update result details.

8.4.3.2 Notify_Onboarding_Completion

8.4.3.2.1 Description

Notify_Onboarding_Completion is used by the CAPIF core function to notify an API invoker of the on-boarding result.

8.4.3.2.2 Notification definition

The POST method shall be used for Notify_Onboarding_Completion and the URI shall be the one provided by the API invoker during the on-boarding request.

Callback URI: **{notificationDestination}**

This method shall support the URI query parameters specified in table 8.4.3.2.2-1.

Table 8.4.3.2.2-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.4.3.2.2-2 and the response data structures and response codes specified in table 8.4.3.2.2-3.

Table 8.4.3.2.2-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
OnboardingNotification	M	1	Notification with on-boarding result

Table 8.4.3.2.2-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The receipt of the Notification is acknowledged.
n/a			307 Temporary Redirect	Temporary redirection, during notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative notification destination where the notification should be sent. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative notification destination where the notification should be sent. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.4.3.2.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative notification destination towards which the notification should be redirected.

Table 8.4.3.2.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative notification destination towards which the notification should be redirected.

8.4.3.3 Notify_Update_Completion

8.4.3.3.1 Description

Notify_Update_Completion is used by the CAPIF core function to notify of the update of API Invoker's details result.

8.4.3.3.2 Notification definition

The POST method shall be used for Notify_Update_Completion and the URI shall be the one provided by the API invoker during the API invoker details update request.

Callback URI: **{notificationDestination}**

This method shall support the URI query parameters specified in table 8.4.3.3.2-1.

Table 8.4.3.3.2-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.4.3.3.2-2 and the response data structures and response codes specified in table 8.4.3.3.2-3.

Table 8.4.3.3.2-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
OnboardingNotification	M	1	Notification with API Invoker's details update result.

Table 8.4.3.3.2-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The receipt of the Notification is acknowledged.
n/a			307 Temporary Redirect	Temporary redirection, during notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative notification destination where the notification should be sent. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative notification destination where the notification should be sent. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.4.3.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative notification destination towards which the notification should be redirected.

Table 8.4.3.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative notification destination towards which the notification should be redirected.

8.4.4 Data Model

8.4.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 7.2 also apply to this API.

Table 8.4.4.1-1 specifies the data types defined specifically for the CAPIF_API_Invoker_Management_API service.

Table 8.4.4.1-1: CAPIF_API_Invoker_Management_API specific Data Types

Data type	Section defined	Description	Applicability
APIInvokerEnrolmentDetails	Clause 8.4.4.2.2	Represents information about the API Invoker that requested to onboard.	
APIInvokerEnrolmentDetailsPatch	Clause 8.4.4.2.8	Represents an API Invoker's enrolment details to be updated.	PatchUpdate
APIList	Clause 8.4.4.2.4	The list of service APIs that the API Invoker is allowed to invoke.	
OnboardingInformation	Clause 8.4.4.2.5	Represents on-boarding information of the API invoker.	
OnboardingNotification	Clause 8.4.4.2.7	Represents the notification with on-boarding or update result.	

Table 8.4.4.1-2 specifies data types re-used by the CAPIF_API_Invoker_Management_API service.

Table 8.4.4.1-2: Re-used Data Types

Data type	Reference	Comments	Applicability
DateTime	3GPP TS 29.122 [14]	Used to indicate a date and a time.	
DateTimeRm	3GPP TS 29.122 [14]	Used to indicate the same as the DateTime data structure but with the OpenAPI "nullable: true" property.	
SupportedFeatures	3GPP TS 29.571 [19]	Used to negotiate the applicability of optional features defined in table 8.4.6-1.	

8.4.4.2 Structured data types

8.4.4.2.1 Introduction

8.4.4.2.2 Type: APIInvokerEnrolmentDetails

Table 8.4.4.2.2-1: Definition of type APIInvokerEnrolmentDetails

Attribute name	Data type	P	Cardinality	Description	Applicability
apiInvokerId	string	O	0..1	API invoker ID assigned by the CAPIF core function to the API invoker while on-boarding the API invoker. Shall not be present in the HTTP POST request from the API invoker to the CAPIF core function, to on-board itself. Shall be present in all other HTTP requests and responses.	
onboardingInformation	OnboardingInformation	M	1	On-boarding information about the API invoker necessary for the CAPIF core function to on-board the API invoker.	
notificationDestination	Uri	M	1	URI where the notification should be delivered to.	
requestTestNotification	boolean	O	0..1	CAPIF core function to send a test notification as defined in in clause 7.6. Set to "false" to request the CAPIF core function not to send a test notification.Default value is "false" if omitted.	Notification_test_event
websockNotifConfig	WebsockNotifConfig	O	0..1	Configuration parameters to set up notification delivery over Websocket protocol as defined in clause 7.6.	Notification_websocket
apiList	APIList	O	0..1	A list of APIs. When included by the API invoker in the HTTP request message, it lists the APIs that the API invoker intends to invoke while onboard or API invoker update. When included by the CAPIF core function in the HTTP response message, it lists the APIs that the API invoker is allowed to invoke while onboard or API invoker update.	
apiInvokerInformation	string	O	0..1	Generic information related to the API invoker such as details of the device or the application.	
expTime	DateTime	O	0..1	Represents the expiration time of the onboarding. If this attribute is absent, this means that the onboarding timer shall not expire until explicitly included, updated or deleted by the service consumer.	ExpirationTime
supportedFeatures	SupportedFeatures	C	0..1	Used to negotiate the supported optional features of the API as described in clause 7.8. This attribute shall be provided in the HTTP POST request and in the response of successful resource creation.	

8.4.4.2.3 Type: Void

8.4.4.2.4 Type: APIList

Table 8.4.4.2.4-1: Definition of type APIList

Attribute name	Data type	P	Cardinality	Description	Applicability
serviceAPIDescriptions	array(ServiceAPIDescription)	O	1..N	Definition of the service API.	

8.4.4.2.5 Type: OnboardingInformation

Table 8.4.4.2.5-1: Definition of type OnboardingInformation

Attribute name	Data type	P	Cardinality	Description	Applicability
apiInvokerPublicKey	string	M	1	Public Key of API Invoker	
apiInvokerCertificate	string	O	0..1	API invoker's generic client certificate. The subject field in the certificate shall be encoded with API invoker ID as Common Name as specified in IETF RFC 5280 [29].	
onboardingSecret	string	O	0..1	API invoker's onboarding secret, provided by the CAPIF core function.	

8.4.4.2.6 Type: Void

8.4.4.2.7 Type: OnboardingNotification

Table 8.4.4.2.7-1: Definition of type OnboardingNotification

Attribute name	Data type	P	Cardinality	Description	Applicability
result	boolean	M	1	Set to "true" indicate successful on-boarding. Set to "false" indicate unsuccessful onboarding. Default value is "false" if omitted.	
resourceLocation	Uri	C	0..1	URI pointing to the new CAPIF resource created as a result of successful on-boarding. This attribute shall be present if 'result' attribute is set to "true". Otherwise it shall not be present.	
apiInvokerEnrolmentDetails	APIInvokerEnrolmentDetails	C	0..1	Enrolment details of the API invoker which are verified by the CAPIF administrator or API management. This attribute shall be present if 'result' attribute is set to "true". Otherwise it shall not be present.	
apiList	APIList	O	0..1	List of APIs API invoker is allowed to access. This attribute may be present if 'result' attribute is set to "true". Otherwise it shall not be present.	

8.4.4.2.8 Type: APIInvokerEnrolmentDetailsPatch

Table 8.4.4.2.8-1: Definition of type APIInvokerEnrolmentDetailsPatch

Attribute name	Data type	P	Cardinality	Description	Applicability
onboardingInformation	OnboardingInformation	O	0..1	On-boarding information about the API invoker necessary for the CAPIF core function to on-board the API invoker.	
notificationDestination	Uri	O	0..1	URI where the notification should be delivered to.	
apiList	APIList	O	0..1	A list of APIs. When included by the API invoker in the HTTP request message, it lists the APIs that the API invoker intends to invoke while onboard or API invoker update.	
apiInvokerInformation	string	O	0..1	Generic information related to the API invoker such as details of the device or the application.	
expTime	DateTime Rm	O	0..1	Represents the updated expiration time of the onboarding.	ExpirationTime

8.4.4.3 Simple data types and enumerations

None.

8.4.5 Error Handling

8.4.5.1 General

HTTP error handling shall be supported as specified in clause 7.7.

In addition, the requirements in the following clauses shall apply.

8.4.5.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the CAPIF_API_Invoker_Management_API.

8.4.5.3 Application Errors

The application errors defined for the CAPIF_API_Invoker_Management_API are listed in table 8.4.5.3-1.

Table 8.4.5.3-1: Application errors

Application Error	HTTP status code	Description	Applicability

8.4.6 Feature negotiation

General feature negotiation procedures are defined in clause 7.8. Table 8.4.6-1 lists the supported features for CAPIF_API_Invoker_Management_API.

Table 8.4.6-1: Supported Features

Feature number	Feature Name	Description
1	Notification_test_event	Testing of notification connection is supported according to clause 7.6.
2	Notification_websocket	The delivery of notifications over Websocket is supported according to clause 7.6. This feature requires that the Notification_test_event feature is also supported.
3	PatchUpdate	Indicates the support of the PATCH method for updating an On-boarded API Invoker resource.
4	ExpirationTime	Indicates the support of expiration time for the API invoker onboarding functionality as part of the support of network slice capability exposure application layer framework. This feature enables the following functionalities: - provisioning/updating/deleting the expiration time of an onboarding.

8.5 CAPIF_Security_API

8.5.1 API URI

The CAPIF_Security_API service shall use the CAPIF_Security_API.

The request URIs used in HTTP requests from the API invoker or the API exposing function towards the CAPIF core function shall have the Resource URI structure as defined in clause 7.5 with the following clarifications:

- The <apiName> shall be "capif-security".
- The <apiVersion> shall be "v1".
- The <apiSpecificSuffixes> shall be set as described in clause 8.5.2.

All the resource URIs and the custom operation URIs specified in the clauses below are defined relative to the above API URI.

8.5.2 Resources

8.5.2.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 8.5.2.1-1 depicts the resource URIs structure for the CAPIF_Security_API.

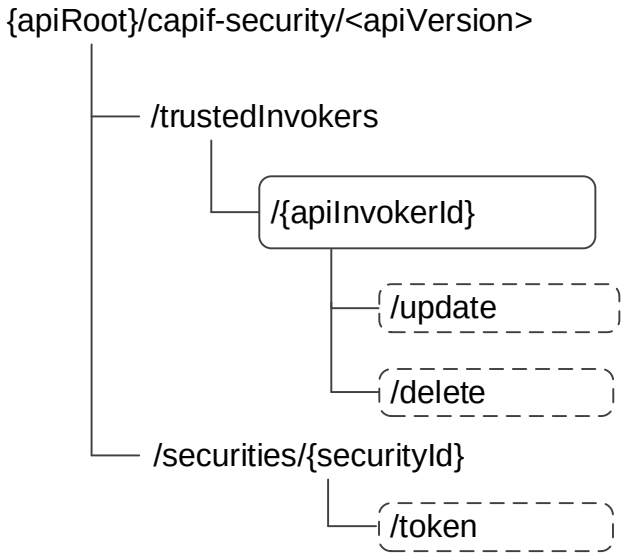

Figure 8.5.2.1-1: Resource URI structure of the CAPIF_Security_API

Table 8.5.2.1-1 provides an overview of the resources and applicable HTTP methods.

Table 8.5.2.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
Trusted API invokers	/trustedInvokers (NOTE)	n/a	
Individual trusted API invoker	/trustedInvokers/{apiInvokerId} (NOTE)	GET	Retrieve authentication information of an API invoker
		PUT	Create a security context for individual API invoker
		DELETE	Revoke the authorization of the API invoker
	/trustedInvokers/{apiInvokerId}/update (NOTE)	update (POST)	Update the security context (e.g. re-negotiate the security methods).
	/trustedInvokers/{apiInvokerId}/delete (NOTE)	delete (POST)	Revoke the authorization of the API invoker for some APIs
	/securities/{securityId}/token (NOTE)	token (POST)	Obtain the OAuth 2.0 authorization information
NOTE: The path segment "trustedInvokers" does not follow the related naming convention defined in clause 7.5.1. The path segment is however kept as currently defined in this specification for backward compatibility considerations.			

8.5.2.2 Resource: Trusted API invokers

8.5.2.2.1 Description

The Trusted API Invokers resource represents all the API invokers that are trusted by the CAPIF core function and have received authentication information from the CAPIF core function.

8.5.2.2.2 Resource Definition

Resource URI: **{apiRoot}/capif-security/<apiVersion>/trustedInvokers**

This resource shall support the resource URI variables defined in table 8.5.2.2.2-1.

Table 8.5.2.2.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5

8.5.2.2.3 Resource Standard Methods

8.5.2.2.3.1 Void

8.5.2.2.4 Resource Custom Operations

None.

8.5.2.3 Resource: Individual trusted API invokers

8.5.2.3.1 Description

The Individual trusted API Invokers resource represents an individual API invokers that is trusted by the CAPIF core function and have received security related information from the CAPIF core function.

8.5.2.3.2 Resource Definition

Resource URI: **{apiRoot}/capif-security/<apiVersion>/trustedInvokers/{apiInvokerId}**

This resource shall support the resource URI variables defined in table 8.5.2.3.2-1.

Table 8.5.2.3.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5
apiInvokerId	string	Identifies an individual API invoker

8.5.2.3.3 Resource Standard Methods

8.5.2.3.3.1 GET

This method shall support the URI query parameters specified in table 8.5.2.3.3.1-1.

Table 8.5.2.3.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	P	Cardinality	Description
authenticationInfo	boolean	O	0..1	When set to "true", it indicates the CCF to send the authentication information of the API invoker. Set to "false" or omitted. (NOTE)
authorizationInfo	boolean	O	0..1	When set to "true", it indicates the CCF to send the authorization information of the API invoker. Set to "false" indicates the CCF not to send the authorization information of the API invoker. Default value is "false" if omitted. (NOTE)
NOTE: The query parameters "authenticationInfo" and "authorizationInfo" do not follow the related naming convention defined in clause 7.5.1. These query parameters are however kept as currently defined in this specification for backward compatibility considerations.				

This method shall support the request data structures specified in table 8.5.2.3.3.1-2 and the response data structures and response codes specified in table 8.5.2.3.3.1-3.

Table 8.5.2.3.3.1-2: Data structures supported by the GET Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 8.5.2.3.3.1-3: Data structures supported by the GET Response Body on this resource

Data type	P	Cardinality	Response codes	Description
ServiceSecurity	M	1	200 OK	The security related information of the API Invoker based on the request from the API exposing function.
n/a			307 Temporary Redirect	Temporary redirection, during resource retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during resource retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CCF. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the GET method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.5.2.3.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CCF.

Table 8.5.2.3.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CCF.

8.5.2.3.3.2 DELETE

This method shall support the URI query parameters specified in table 8.5.2.3.3.2-1.

Table 8.5.2.3.3.2-1: URI query parameters supported by the DELETE method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.5.2.3.3.2-2 and the response data structures and response codes specified in table 8.5.2.3.3.2-3.

Table 8.5.2.3.3.2-2: Data structures supported by the DELETE Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 8.5.2.3.3.2-3: Data structures supported by the DELETE Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	Authorization of the API invoker revoked, and a notification is sent to the API invoker as specified in clause 8.5.3.2
n/a			307 Temporary Redirect	Temporary redirection, during resource termination. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during resource termination. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the DELETE method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.5.2.3.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.5.2.3.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.5.2.3.3.3 PUT

This method shall support the URI query parameters specified in table 8.5.2.3.3.3-1.

Table 8.5.2.3.3.3-1: URI query parameters supported by the PUT method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.5.2.3.3.3-2 and the response data structures and response codes specified in table 8.5.2.3.3.3-3.

Table 8.5.2.3.3.3-2: Data structures supported by the PUT Request Body on this resource

Data type	P	Cardinality	Description
ServiceSecurity	M	1	Security method request from the API invoker to the CAPIF core function. The request indicates a list of service APIs and a preferred method of security for the service APIs. The request also includes a notification destination URI for security related notifications.

Table 8.5.2.3.3.3-3: Data structures supported by the PUT Response Body on this resource

Data type	P	Cardinality	Response codes	Description
ServiceSecurity	M	1	201 Created	Security method from the CAPIF core function to the API invoker is based on the received request. The response indicates the security method to be used for the service APIs The URI of the created resource shall be returned in the "Location" HTTP header.
NOTE: The mandatory HTTP error status codes for the PUT method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.5.2.3.3.3-4: Headers supported by the 201 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/capif-security/v1/trustedInvokers/{apiInvokerId}

8.5.2.3.4 Resource Custom Operations

8.5.2.3.4.1 Overview

Table 8.5.2.3.4.1-1: Custom operations

Operation name	Custom operation URI	Mapped HTTP method	Description
update	/trustedInvokers/{apiInvokerId}/update	POST	Update the security instance (e.g. re-negotiate the security methods).
delete	/trustedInvokers/{apiInvokerId}/delete	POST	Revoke the authorization of the API invoker for some APIs
token	/securities/{securityId}/token	POST	Obtain the OAuth 2.0 authorization information

8.5.2.3.4.2 Operation: update

8.5.2.3.4.2.1 Description

This custom operation updates an existing Individual security instance resource in the CAPIF core function.

8.5.2.3.4.2.2 Operation Definition

This method shall support the URI query parameters specified in table 8.5.2.3.4.2.2-1.

Table 8.5.2.3.4.2.2-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This operation shall support the request data structures specified in table 8.5.2.3.4.2.2-2 and the response data structure and response codes specified in table 8.5.2.3.4.2.2-3.

Table 8.5.2.3.4.2.2-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
ServiceSecurity	M	1	Security method request from the API invoker to the CAPIF core function. The request indicates a list of service APIs and a preferred method of security for the service APIs. The request also includes a notification destination URI for security related notifications.

Table 8.5.2.3.4.2.2-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
ServiceSecurity	M	1	200 OK	Security method from the CAPIF core function to the API invoker is based on the received request. The response indicates the security method to be used for the service APIs
n/a			307 Temporary Redirect	Temporary redirection, during security instance modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during security instance modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.5.2.3.4.2.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.5.2.3.4.2.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.5.2.3.4.3 Operation: delete

8.5.2.3.4.3.1 Description

This custom operation revokes authorization for some service APIs of an existing Individual security instance resource in the CAPIF core function.

8.5.2.3.4.3.2 Operation Definition

This method shall support the URI query parameters specified in table 8.5.2.3.4.3.2-1.

Table 8.5.2.3.4.3.2-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This operation shall support the request data structures specified in table 8.5.2.3.4.3.2-2 and the response data structure and response codes specified in table 8.5.2.3.4.3.2-3.

Table 8.5.2.3.4.3.2-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
SecurityNotification	M	1	It includes a list of API identifiers for which authorization needs to be revoked for an API invoker.

Table 8.5.2.3.4.3.2-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	Successful case. The CAPIF core function revoked the authorization of the API invoker for the requested APIs.
n/a			307 Temporary Redirect	Temporary redirection, during authorization revocation. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during authorization revocation. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.5.2.3.4.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.5.2.3.4.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.5.2.3.4.4 Operation: token

8.5.2.3.4.4.1 Description

This custom operation obtains OAuth 2.0 authorization information from an existing Individual security instance resource in the CAPIF core function.

8.5.2.3.4.4.2 Operation Definition

This method shall support the URI query parameters specified in table 8.5.2.3.4.4.2-1.

Table 8.5.2.3.4.4.2-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This operation shall support the request data structures specified in table 8.5.2.3.4.4.2-2 and the response data structure and response codes specified in table 8.5.2.3.4.4.2-3.

Table 8.5.2.3.4.4.2-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
AccessTokenReq	M	1	This IE shall contain the request information for the access token request.

Table 8.5.2.3.4.4.2-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
AccessTokenRsp	M	1	200 OK	This IE shall contain the access token response information.
n/a			307 Temporary Redirect	Temporary redirection, during obtaining authorization information. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during obtaining authorization information. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
AccessTokenErr	M	1	400 Bad Request	See IETF RFC 6749 [23] clause 5.2. The specific error shall be indicated in the "error" attribute of the AccessTokenErr data type, containing any of the values: - invalid_request - invalid_client - invalid_grant - unauthorized_client - unsupported_grant_type - invalid_scope
AccessTokenErr	M	1	401 Unauthorized	See IETF RFC 6749 [23] clause 5.2. The specific error shall be indicated in the "error" attribute of the AccessTokenErr data type, containing value: - invalid_client
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.5.2.3.4.4.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.5.2.3.4.4.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.5.2.3.4.5 Void

8.5.2A Custom Operations without associated resources

There are no custom operations without associated resources defined for this API in this release of the specification.

8.5.3 Notifications

8.5.3.1 General

The delivery of notifications shall conform to clause 7.6.

Table 8.5.3.1-1: Notifications overview

Notification	Callback URI	HTTP method or custom operation	Description (service operation)
Authorization revoked notification	{notificationDestination}	POST	Notify API invoker that the authorization rights are revoked by the API exposing function.

8.5.3.2 Authorization revoked notification

8.5.3.2.1 Description

Authorization revoked notification is used by the CAPIF core function to notify an API invoker that the authorization rights are revoked by the API exposing function.

8.5.3.2.2 Notification definition

The POST method shall be used for Authorization revoked notification and the URI shall be the one provided by the API invoker during the Obtain_Security_Method service operation.

Callback URI: **{notificationDestination}**

This method shall support the URI query parameters specified in table 8.5.3.2.2-1.

Table 8.5.3.2.2-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.5.3.2.2-2 and the response data structures and response codes specified in table 8.5.3.2.2-3.

Table 8.5.3.2.2-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
SecurityNotification	M	1	Notification with information related to revoked authorization.

Table 8.5.3.2.2-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The receipt of the Notification is acknowledged.
n/a			307 Temporary Redirect	Temporary redirection, during notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative notification destination where the notification should be sent. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative notification destination where the notification should be sent. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.5.3.2.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative notification destination towards which the notification should be redirected.

Table 8.5.3.2.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative notification destination towards which the notification should be redirected.

8.5.4 Data Model

8.5.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 7.2 also apply to this API.

Table 8.5.4.1-1 specifies the data types defined specifically for the CAPIF_Security_API service.

Table 8.5.4.1-1: CAPIF_Security_API specific Data Types

Data type	Section defined	Description	Applicability
AccessTokenClaims	Clause 8.5.4.2.8	Represents the claims data structure for the access token.	
AccessTokenErr	Clause 8.5.4.2.9	Represents an error in the access token request.	
AccessTokenReq	Clause 8.5.4.2.6	Represents the access token request information.	
AccessTokenRsp	Clause 8.5.4.2.7	Represents the access token response information.	
Cause	Clause 8.5.4.3.3	Indicates the cause for revoking the API invoker's authorization to the service API.	
ResOwnerId	Clause 8.5.4.2.11	Represents the identifier of the resource owner.	RNAA
SecurityInformation	Clause 8.5.4.2.3	Represents the interface details and the security method.	
SecurityNotification	Clause 8.5.4.2.5	Represents the revoked authorization notification details.	
ServiceSecurity	Clause 8.5.4.2.2	Represents the details of the security method for each service API interface. When included by the API invoker, it shall indicate the preferred method of security. When included by the CAPIF core function, it shall indicate the security method to be used for the service API interface.	
OAuthGrantType	Clause 8.5.4.3.4	Represents the OAuth grant type.	RNAA

Table 8.5.4.1-2 specifies data types re-used by the CAPIF_Security_API service-based interface:

Table 8.5.4.1-2: Re-used Data Types

Data type	Reference	Comments	Applicability
DurationSec	3GPP TS 29.122 [14]	Indicates the duration in seconds.	
SecurityMethod	Clause 8.2.4.3.6	Indicates the security method (e.g. PKI).	
SupportedFeatures	3GPP TS 29.571 [19]	Used to negotiate the applicability of optional features defined in table 8.5.6-1.	
Uri	3GPP TS 29.122 [14]	Represents a URI.	RNAA

8.5.4.2 Structured data types

8.5.4.2.1 Introduction

8.5.4.2.2 Type: ServiceSecurity

Table 8.5.4.2.2-1: Definition of type ServiceSecurity

Attribute name	Data type	P	Cardinality	Description	Applicability
securityInfo	array(SecurityInformation)	M	1..N	Security information for each API interface.	
notificationDestination	Uri	M	1	URI where the notification should be delivered to.	
requestTestNotification	boolean	O	0..1	Set to "true" by API invoker to request the CAPIF core function to send a test notification as defined in in clause 7.6. Set to "false" not to request the CAPIF core function to send a test notification. Default value is "false" if omitted.	Notification_test_event
websockNotifConfig	WebsockNotifConfig	O	0..1	Configuration parameters to set up notification delivery over Websocket protocol as defined in clause 7.6.	Notification_websocket
supportedFeatures	SupportedFeatures	C	0..1	Used to negotiate the supported optional features of the API as described in clause 7.8. This attribute shall be provided in the HTTP POST request and in the response of successful resource creation.	

8.5.4.2.3 Type: SecurityInformation

Table 8.5.4.2.3-1: Definition of type SecurityInformation

Attribute name	Data type	P	Cardinality	Description	Applicability
interfaceDetails	InterfaceDescription	O	0..1	Details of the interface (NOTE)	
aefId	string	O	0..1	AEF identifier (NOTE)	
apiId	string	C	0..1	API identifier. If API invoker supplies this IE in the PUT request, CCF shall respond back with this IE and its associated security information.	SecurityInfoPerAPI
prefSecurityMethods	array(SecurityMethod)	M	1..N	Security methods preferred by the API invoker for the API interface	
selSecurityMethod	SecurityMethod	O	0..1	Supplied by the CAPIF core function, it indicates the selected security method for the API interface. If it is not provided, it means no common supported security method by the API invoker and the AEF, or the selected security method is not allowed by the local policy in the CAPIF core function.	
authenticationInfo	string	O	0..1	Authentication related information	
authorizationInfo	string	O	0..1	Authorization related information	
grantTypes	array(OAuthGrantType)	O	1..N	Contains the supported OAuth grant type(s). This attribute shall be present only for RNAA, as defined in clause 6.5.3 of TS 33.122 [16]. Otherwise, it is not applicable and shall not be present.	RNAA
NOTE: Only one of the attributes "aefId" or "interfaceDetails" shall be included.					

8.5.4.2.4 Void

8.5.4.2.5 Type: SecurityNotification

Table 8.5.4.2.5-1: Definition of type SecurityNotification

Attribute name	Data type	P	Cardinality	Description	Applicability
apiInvokerId	string	M	1	String identifying the API invoker assigned by the CAPIF core function	
aefId	string	O	0..1	String identifying the AEF.	
apiIds	array(string)	M	1..N	Identifier of the service API	
cause	Cause	M	1	The cause for revoking the API invoker authorization to the service API	

8.5.4.2.6 Type: AccessTokenReq

Table 8.5.4.2.6-1: Definition of type AccessTokenReq

Attribute name	Data type	P	Cardinality	Description	Applicability
grant_type	string	M	1	This attribute shall contain the grant type as "client_credentials", or when the "RNAA" feature is supported, either "client_credentials" or "authorization_code". (NOTE 3, NOTE 4)	
client_id	string	M	1	This attribute shall contain the API invoker Identifier. (NOTE 3)	
resOwnerId	ResOwnerId	O	0..1	Contains the identifier of the resource owner. This attribute shall be present only when the access token request is used for RNAA.	RNAA
client_secret	string	O	0..1	This attribute when present shall contain the onboarding secret which is got during API invoker onboarding. (NOTE 3)	
scope	string	O	0..1	This attribute when present shall contain a list of AEF identifiers and its associated API names for which the access_token is authorized for use. It takes the format of 3gpp#aefId1:apiName1,apiName2,…apiNameX;aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZ Using delimiter "#" after the discriminator "3gpp", ":" after AEF identifier, "," between API names and ";" between the last API name of the previous AEF identifier and the next AEF identifier. (NOTE 2) Example: '3gpp#aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management'	
authCode	string	C	0..1	Contains the authorization code. This attribute shall be included only when the access token request is used for RNAA and the OAuth "authorization code" grant type is used.	RNAA
redirect_uri	string	O	0..1	Contains the redirection URI that was used to obtain the authorization code provided within the "authCode" attribute. This attribute may be included only when the access token request is used for RNAA and the OAuth "authorization code" grant type is used. (NOTE 3)	RNAA
NOTE 1: This data structure shall not be treated as a JSON object. It shall be treated as a key, value pair data structure to be encoded using x-www-urlencoded format as specified in clause 17.13.4.1 of W3C HTML 4.01 Specification [22]. NOTE 2: The scope may contain more space-delimited strings which further add additional access ranges to the scope, the definition of those additional strings is out of the scope of the present document. NOTE 3: The "grant_type", "client_id", "client_secret" and "redirect_uri" attributes do not follow the related naming convention defined in clause 7.2.1. These attributes are however kept as currently defined in this specification in order to keep them aligned with corresponding claims defined in IETF RFC 6749 [23] and for backward compatibility considerations. NOTE 4: The enumeration value "client_credentials" or "authorization_code" of the "grant_type" attribute does not follow the related naming convention defined in clause 7.2.1. This enumeration is however kept as currently defined in this specification for backward compatibility considerations.					

8.5.4.2.7 Type: AccessTokenRsp

Table 8.5.4.2.7-1: Definition of type AccessTokenRsp

Attribute name	Data type	P	Cardinality	Description
access_token	string	M	1	This IE shall contain JWS Compact Serialized representation of the JWS signed JSON object containing AccessTokenClaims (see clause 8.5.4.2.8). (NOTE 2)
token_type	string	M	1	This IE shall contain the token type (i.e. "Bearer"). (NOTE 2, NOTE 3)
expires_in	DurationSec	M	1	This IE when present shall contain the number of seconds after which the access_token is considered to be expired. (NOTE 2)
scope	string	O	0..1	This IE when present shall contain a list of AEF identifiers and its associated API names for which the access_token is authorized for use. It takes the format of 3gpp#aefId1:apiName1,apiName2,…apiNameX;aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZ Using delimeter "#" after the discriminator "3gpp", ":" after AEF identifier, "," between API names and ";" between the last API name of the previous AEF identifier and the next AEF identifier. (NOTE 1) Example: '3gpp#aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management'

NOTE 1: The scope may contain more space-delimited strings which further add additional access ranges to the scope, the definition of those additional strings is out of the scope of the present document.
NOTE 2: The "access_token", "token_type" and "expires_in" attributes do not follow the related naming convention defined in clause 7.2.1. These attributes are however kept as currently defined in this specification for backward compatibility considerations.
NOTE 3: The enumeration value "Bearer" of the "token_type" attribute does not follow the related naming convention defined in clause 7.2.1. This enumeration is however kept as currently defined in this specification for backward compatibility considerations.

8.5.4.2.8 Type: AccessTokenClaims

Table 8.5.4.2.8-1: Definition of type AccessTokenClaims

Attribute name	Data type	P	Cardinality	Description	Applicability
iss	string	M	1	This attribute shall contain the API invoker Identifier.	
scope	string	M	1	This attribute shall contain a list of AEF identifiers and its associated API names for which the access_token is authorized for use. It takes the format of 3gpp#aefId1:apiName1,apiName2,…apiNameX;aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZ Using delimeter "#" after the discriminator "3gpp", ":" after AEF identifier, "," between API names and ";" between the last API name of the previous AEF identifier and the next AEF identifier. (NOTE) Example: '3gpp#aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management'	
exp	DurationSec	M	1	This attribute shall contain the number of seconds after which the access_token is considered to be expired.	
resOwnerId	ResOwnerId	O	0..1	Contains the identifier of the resource owner. This attribute shall be present only when the access token is used for RNAA.	RNAA
NOTE: The scope may contain more space-delimited strings which further add additional access ranges to the scope, the definition of those additional strings is out of the scope of the present document.					

8.5.4.2.9 Type: AccessTokenErr

Table 8.5.4.2.9-1: Definition of type AccessTokenErr

Attribute name	Data type	P	Cardinality	Description
error	string	M	1	This IE shall contain the error described in IETF RFC 6749 [23], clause 5.2. Enum: "invalid_request" "invalid_client" "invalid_grant" "unauthorized_client" "unsupported_grant_type" "invalid_scope" (NOTE 1)
error_description	string	O	0..1	When present, this IE shall contain the human-readable additional information to indicate the error that occurred, as described in IETF RFC 6749 [23], clause 5.2. (NOTE 2)
error_uri	string	O	0..1	When present, this IE shall contain the URI identifying a human-readable additional information about the error, as described in IETF RFC 6749 [23], clause 5.2. (NOTE 2)
NOTE 1: The enumeration values "invalid_request", "invalid_client", "invalid_grant", "unauthorized_client", "unsupported_grant_type" and "invalid_scope" of the "error" attribute do not follow the related naming convention defined in clause 7.2.1. These enumeration values are however kept as currently defined in this specification for alignment with definitions in IETF RFC 6749 [23] and backward compatibility considerations. NOTE 2: The "error_description" and "error_uri" attributes do not follow the related naming convention defined in clause 7.2.1. These attributes are however kept as currently defined in this specification for alignment with definitions in IETF RFC 6749 [23] and backward compatibility considerations.				

8.5.4.2.10 Void

8.5.4.2.11 Type: ResOwnerId

Table 8.5.4.2.11-1: Definition of type ResOwnerId

Attribute name	Data type	P	Cardinality	Description
gpsi	Gpsi	C	0..1	This attribute shall contain identifier of the resource owner in the form of a GPSI. (NOTE)
NOTE: At least one of these attributes shall be present.				

8.5.4.3 Simple data types and enumerations

8.5.4.3.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

8.5.4.3.2 Simple data types

The simple data types defined in table 8.5.4.3.2-1 shall be supported.

Table 8.5.4.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
n/a			

8.5.4.3.3 Enumeration: Cause

Table 8.5.4.3.3-1: Enumeration Cause

Enumeration value	Description	Applicability
OVERLIMIT_USAGE	The revocation of the authorization of the API invoker is due to the overlimit usage of the service API	
UNEXPECTED_REASON	The revocation of the authorization of the API invoker is due to unexpected reason.	
AUTHORIZATION_ISSUE	The revocation of the authorization of the API invoker is due to API Invoker not being authorized anymore by the API Provider.	RNAA
OTHER_REASON	The revocation of the authorization of the API invoker is due to other reason.	RNAA

8.5.4.3.4 Enumeration: OAuthGrantType

Table 8.5.4.3.4-1: Enumeration OAuthGrantType

Enumeration value	Description	Applicability
CLIENT_CREDENTIALS	Indicates that the OAuth grant type is "client credentials" defined in clause 6.5.2 of TS 33.122 [16].	
AUTHORIZATION_CODE	Indicates that the OAuth grant type is "authorization code" defined in clause 6.5.3 of TS 33.122 [16].	
AUTHORIZATION_CODE_WITH_PKCE	Indicates that the OAuth grant type is "authorization code with PKCE" defined in clause 6.5.3 of TS 33.122 [16].	

8.5.5 Error Handling

8.5.5.1 General

General error responses are defined in clause 7.7.

In addition, the requirements in the following clauses shall apply.

8.5.5.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the CAPIF_Security_API.

8.5.5.3 Application Errors

The application errors defined for the Obtain_Authorization service operation are listed in Table 8.5.5.3-1, and correspond to the values of the "error" attribute (see clause 8.5.4.2.9).

Table 8.5.5.3-1: Application errors

Application Error	HTTP status code	Description
invalid_request	400 Bad Request	See IETF RFC 6749 [23]
invalid_client	400 Bad Request, 401 Unauthorized	See IETF RFC 6749 [23]
invalid_grant	400 Bad Request	See IETF RFC 6749 [23]
unauthorized_client	400 Bad Request	See IETF RFC 6749 [23]
unsupported_grant_type	400 Bad Request	See IETF RFC 6749 [23]
invalid_scope	400 Bad Request	See IETF RFC 6749 [23]
NOTE: These enumeration values defined in this table do not follow the related naming convention defined in clause 7.2.1. These enumeration values are however kept as currently defined in this specification for alignment with definitions in IETF RFC 6749 [23].		

8.5.6 Feature negotiation

General feature negotiation procedures are defined in clause 7.8. Table 8.5.6-1 lists the supported features for CAPIF_Security_API.

Table 8.5.6-1: Supported Features

Feature number	Feature Name	Description
1	Notification_test_event	Testing of notification connection is supported according to clause 7.6.
2	Notification_websocket	The delivery of notifications over Websocket is supported according to clause 7.6. This feature requires that the Notification_test_event feature is also supported.
3	SecurityInfoPerAPI	Indicates the support of negotiating and obtaining service API security method information per API.
4	RNAA	Indicates the support of the RNAA functionality. This feature enables the following functionalities: - Support the OAuth grant types for RNAA. - Support to convey the authorization code in access token requests to support the "authorization code" grant type for RNAA. - Support to communicate the resource owner ID for RNAA access token requests/responses. - Support to communicate the new cause codes for AEF authorization revocation.

8.6 CAPIF_Access_Control_Policy_API

8.6.1 API URI

The CAPIF_Access_Control_Policy_API service shall use the CAPIF_Access_Control_Policy_API.

The request URIs used in HTTP requests from the API exposing function towards the CAPIF core function shall have the Resource URI structure as defined in clause 7.5 with the following clarifications:

- The <apiName> shall be "access-control-policy".
- The <apiVersion> shall be "v1".
- The <apiSpecificSuffixes> shall be set as described in clause 8.6.2.

All the resource URIs and the custom operation URIs specified in the clauses below are defined relative to the above API URI.

8.6.2 Resources

8.6.2.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 8.6.2.1-1 depicts the resource URIs structure for the CAPIF_Access_Control_Policy_API.

This resource is created by the CAPIF administrator on the CAPIF core function.

NOTE: The details of the mechanisms used to create the Access Control Policy List resource on the CAPIF core function is out of the scope of the present document.

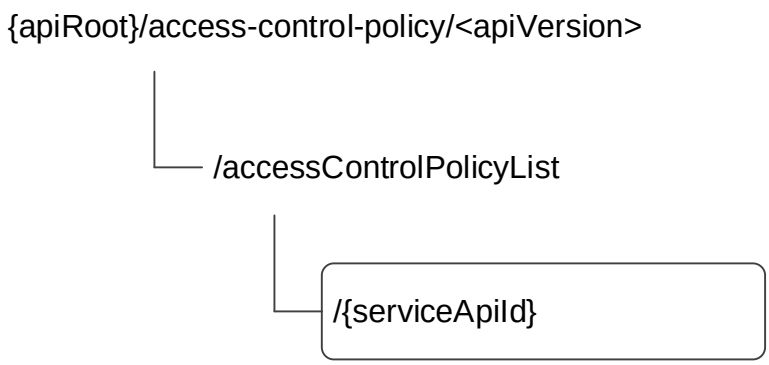

Figure 8.6.2.1-1: Resource URI structure of the CAPIF_Access_Control_Policy_API

Table 8.6.2.1-1 provides an overview of the resources and applicable HTTP methods.

Table 8.6.2.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
Access Control Policy List	/accessControlPolicyList/{serviceApiId} (NOTE)	GET	Retrieves the access control policy list for a published service API.
NOTE: The path segment "accessControlPolicyList" does not follow the related naming convention defined in clause 7.5.1. The path segment is however kept as currently defined in this specification for backward compatibility considerations.			

8.6.2.2 Resource: Access Control Policy List

8.6.2.2.1 Description

The Access Control Policy List resource represents the access control information for all the service APIs per API invoker.

8.6.2.2.2 Resource Definition

Resource URI: **{apiRoot}/access-control-policy/<apiVersion>/accessControlPolicyList/{serviceApiId}**

This resource shall support the resource URI variables defined in table 8.6.2.2.2-1.

Table 8.6.2.2.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5
serviceApiId	string	Identifies an individual published service API

8.6.2.2.3 Resource Standard Methods

8.6.2.2.3.1 GET

This method shall support the URI query parameters specified in table 8.6.2.2.3.1-1.

Table 8.6.2.2.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	P	Cardinality	Description
aef-id	string	M	1	AEF identifier
api-invoker-id	string	O	1	String identifying the API invoker
supported-features	SupportedFeatures	O	0..1	To filter irrelevant responses related to unsupported features.

This method shall support the request data structures specified in table 8.6.2.2.3.1-2 and the response data structures and response codes specified in table 8.6.2.2.3.1-3.

Table 8.6.2.2.3.1-2: Data structures supported by the GET Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 8.6.2.2.3.1-3: Data structures supported by the GET Response Body on this resource

Data type	P	Cardinality	Response codes	Description
AccessControlPolicyList	M	1	200 OK	List of the access control policy applicable for the service API requested.
n/a			307 Temporary Redirect	Temporary redirection, during resource retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during resource retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the GET method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.6.2.2.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.6.2.2.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.6.2.2.4 Resource Custom Operations

There are no notifications defined for this API in this release of the specification.

8.6.2A Custom Operations without associated resources

There are no custom operations without associated resources defined for this API in this release of the specification.

8.6.3 Notifications

None.

8.6.4 Data Model

8.6.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 7.2 also apply to this API.

Table 8.6.4.1-1 specifies the data types defined specifically for the CAPIF_Access_Control_Policy_API service.

Table 8.6.4.1-1: CAPIF_Access_Control_Policy_API specific Data Types

Data type	Section defined	Description	Applicability
AccessControlPolicyList	Clause 8.6.4.2.2	Represents the access control policy list for a published service API.	
ApiInvokerPolicy	Clause 8.6.4.2.3	Represents the policy of an API Invoker.	
TimeRangeList	Clause 8.6.4.2.4	Represents the time range during which the invocation of a service API is allowed by the API invoker.	

Table 8.6.4.1-2 specifies data types re-used by the CAPIF_Access_Control_Policy_API service.

Table 8.6.4.1-2: Re-used Data Types

Data type	Reference	Comments	Applicability
DateTime	3GPP TS 29.122 [14]	Used to indicate start and end times.	
SupportedFeatures	3GPP TS 29.571 [19]	Used to negotiate the applicability of optional features defined in table 8.6.6-1.	

8.6.4.2 Structured data types

8.6.4.2.1 Introduction

This clause defines data structures to be used in resource representations.

8.6.4.2.2 Type: AccessControlPolicyList

Table 8.6.4.2.2-1: Definition of type AccessControlPolicyList

Attribute name	Data type	P	Cardinality	Description	Applicability
apiInvokerPolicies	array(ApiInvokerPolicy)	O	0..N	Policy of each API invoker.	

8.6.4.2.3 Type: ApiInvokerPolicy

Table 8.6.4.2.3-1: Definition of type ApiInvokerPolicy

Attribute name	Data type	P	Cardinality	Description	Applicability
apiInvokerId	string	M	1	API invoker ID assigned by the CAPIF core function	
allowedTotalInvocations	integer	O	0..1	Total number of invocations allowed on the service API by the API invoker.	
allowedInvocationsPerSecond	integer	O	0..1	Invocations per second allowed on the service API by the API invoker.	
allowedInvocationTimeRangeList	array(TimeRangeList)	O	0..N	The time ranges during which the invocations are allowed on the service API by the API invoker.	

8.6.4.2.4 Type: TimeRangeList

Table 8.6.4.2.4-1: Definition of type TimeRangeList

Attribute name	Data type	P	Cardinality	Description	Applicability
startTime	DateTime	M	1	The start time for the invocations to be allowed on the service API by the API invoker.	
stopTime	DateTime	M	1	The end time for the invocations to be allowed on the service API by the API invoker.	

8.6.4.3 Simple data types and enumerations

None.

8.6.5 Error Handling

8.6.5.1 General

HTTP error handling shall be supported as specified in clause 7.7.

In addition, the requirements in the following clauses shall apply.

8.6.5.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the CAPIF_Access_Control_Policy_API.

8.6.5.3 Application Errors

The application errors defined for the CAPIF_Access_Control_Policy_API are listed in table 8.6.5.3-1.

Table 8.6.5.3-1: Application errors

Application Error	HTTP status code	Description	Applicability

8.6.6 Feature negotiation

General feature negotiation procedures are defined in clause 7.8.

Table 8.6.6-1: Supported Features

Feature number	Feature Name	Description
n/a		

8.7 CAPIF_Logging_API_Invocation_API

8.7.1 API URI

The CAPIF_Logging_API_Invocation_API service shall use the CAPIF_Logging_API_Invocation_API.

The request URIs used in HTTP requests from the API exposing function towards the CAPIF core function shall have the Resource URI structure as defined in clause 7.5 with the following clarifications:

- The <apiName> shall be "api-invocation-logs".
- The <apiVersion> shall be "v1".
- The <apiSpecificSuffixes> shall be set as described in clause 8.7.2

All the resource URIs and the custom operation URIs specified in the clauses below are defined relative to the above API URI.

8.7.2 Resources

8.7.2.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 8.7.2.1-1 depicts the resource URIs structure for the CAPIF_Logging_API_Invocation_API.

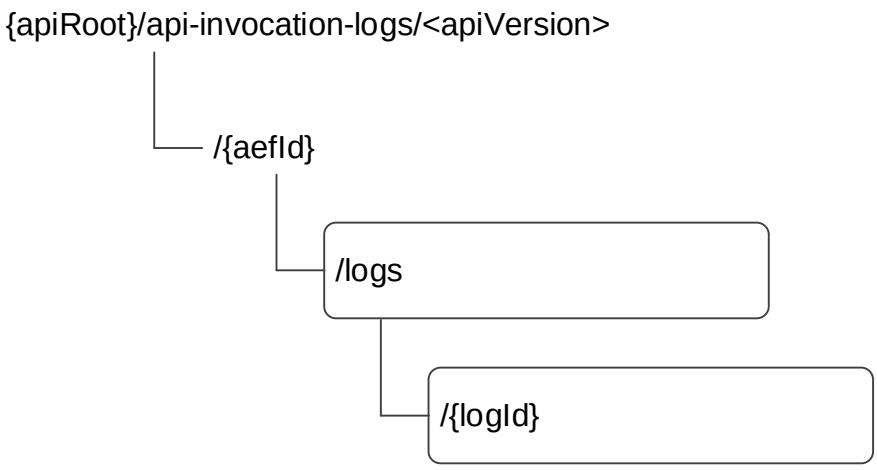

Figure 8.7.2.1-1: Resource URI structure of the CAPIF_Logging_API_Invocation_API

Table 8.7.2.1-1 provides an overview of the resources and applicable HTTP methods.

Table 8.7.2.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
Logs	/{aefId}/logs	POST	Creates a new log entry for service API invocations
Individual log	/{aefId}/logs/{logId}	n/a	Individual log entry

8.7.2.2 Resource: Logs

8.7.2.2.1 Description

The Logs resource represents all the log entries created by a API exposing function at CAPIF core function.

8.7.2.2.2 Resource Definition

Resource URI: **{apiRoot}/api-invocation-logs/<apiVersion>/{aefId}/logs**

This resource shall support the resource URI variables defined in table 8.7.2.2.2-1.

Table 8.7.2.2.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5
aefId	string	Identifies of the API exposing function

8.7.2.2.3 Resource Standard Methods

8.7.2.2.3.1 POST

This method shall support the URI query parameters specified in table 8.7.2.2.3.1-1.

Table 8.7.2.2.3.1-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.7.2.2.3.1-2 and the response data structures and response codes specified in table 8.7.2.2.3.1-3.

Table 8.7.2.2.3.1-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
InvocationLog	M	1	Log of service API invocations provided by API exposing function to store on the CAPIF core function.

Table 8.7.2.2.3.1-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
InvocationLog	M	1	201 Created	Log of service API invocations provided by API exposing function successfully stored on the CAPIF core function. The URI of the created resource shall be returned in the "Location" HTTP header.
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.7.2.2.3.1-4: Headers supported by the 201 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/api-invocation-logs/<apiVersion>/{aefId}/logs/{logId}

8.7.2.2.4 Resource Custom Operations

None.

8.7.2A Custom Operations without associated resources

There are no custom operations without associated resources defined for this API in this release of the specification.

8.7.3 Notifications

There are no notifications defined for this API in this release of the specification.

8.7.4 Data Model

8.7.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 7.2 also apply to this API.

Table 8.7.4.1-1 specifies the data types defined specifically for the CAPIF_Logging_API_Invocation_API service.

Table 8.7.4.1-1: CAPIF_Logging_API_Invocation_API specific Data Types

Data type	Section defined	Description	Applicability
DurationMs	Clause 8.7.4.3.2	Represents the period of time in units of milliseconds.	
InvocationLog	Clause 8.7.4.2.2	Represents the set of Service API invocation logs to be stored on CAPIF core function.	
Log	Clause 8.7.4.2.3	Represents the individual service API invocation log entry.	

Table 8.7.4.1-2 specifies data types re-used by the CAPIF_Logging_API_Invocation_API service.

Table 8.7.4.1-2: Re-used Data Types

Data type	Reference	Comments	Applicability
DateTime	3GPP TS 29.122 [14]	Used to indicate the invocation time.	
Operation	Clause 8.2.4.3.7	Used to indicate the HTTP operation	
SupportedFeatures	3GPP TS 29.571 [19]	Used to negotiate the applicability of optional features defined in table 8.7.6-1.	

8.7.4.2 Structured data types

8.7.4.2.1 Introduction

This clause defines the structured data types to be used in resource representations of the CAPIF_Logging_API_Invocation_API.

8.7.4.2.2 Type: InvocationLog

Table 8.7.4.2.2-1: Definition of type InvocationLog

Attribute name	Data type	P	Cardinality	Description	Applicability
aefId	string	M	1	Identity information of the API exposing function requesting logging of service API invocations	
apiInvokerId	string	M	1	Identity of the API invoker which invoked the service API	
logs	array(Log)	M	1..N	Service API invocation log	
supportedFeatures	Supported Features	O	0..1	Used to negotiate the supported optional features of the API as described in clause 7.8. This attribute shall be provided in the HTTP POST request and in the response of successful resource creation.	

8.7.4.2.3 Type: Log

Table 8.7.4.2.3-1: Definition of type Log

Attribute name	Data type	P	Cardinality	Description	Applicability
apiId	string	M	1	String identifying the API invoked.	
apiName	string	M	1	Name of the API which was invoked, it is set as {apiName} part of the URI structure as defined in clause 5.2.4 of 3GPP TS 29.122 [14].	
apiVersion	string	M	1	Version of the API which was invoked	
resourceName	String	M	1	Name of the specific resource invoked	
uri	Uri	O	0..1	Full URI of the API resource as defined in clause 5.2.4 of 3GPP TS 29.122 [14].	
protocol	Protocol	M	1	Protocol invoked.	
operation	Operation	C	0..1	Operation that was invoked on the API, only applicable for HTTP protocol.	
result	string	M	1	For HTTP protocol, it contains HTTP status code of the invocation	
invocationTime	DateTime	O	0..1	Date on which it was invoked	
invocationLatency	DurationMs	O	0..1	Latency for the API invocation.	
inputParameters	ANY TYPE (NOTE)	O	0..1	List of input parameters	
OutputParameters	ANY TYPE (NOTE)	O	0..1	List of output parameters	
srcInterface	InterfaceDescription	O	0..1	Interface description of the API invoker.	
destInterface	InterfaceDescription	O	0..1	Interface description of the API invoked.	
fwdInterface	string	O	0..1	It includes the node identifier (as defined in IETF RFC 7239 [20] of all forwarding entities between the API invoker and the AEF, concatenated with comma and space, e.g. 192.0.2.43:80, unknown:_OBFport, 203.0.113.60	
NOTE: Any basic data type defined in OpenAPI Specification [3] may be used.					

8.7.4.3 Simple data types and enumerations

8.7.4.3.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

8.7.4.3.2 Simple data types

The simple data types defined in table 8.7.4.3.2-1 shall be supported.

Table 8.7.4.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
DurationMs	integer	Unsigned integer identifying a period of time in units of milliseconds.	

8.7.5 Error Handling

8.7.5.1 General

HTTP error handling shall be supported as specified in clause 7.7.

In addition, the requirements in the following clauses shall apply.

8.7.5.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the CAPIF_Logging_API_Invocation_API.

8.7.5.3 Application Errors

The application errors defined for the CAPIF_Logging_API_Invocation_API are listed in table 8.7.5.3-1.

Table 8.7.5.3-1: Application errors

Application Error	HTTP status code	Description	Applicability

8.7.6 Feature negotiation

Table 8.7.8-1: Supported Features

Feature number	Feature Name	Description
n/a		

8.8 CAPIF_Auditing_API

8.8.1 API URI

The CAPIF_Auditing_API service shall use the CAPIF_Auditing_API.

The request URIs used in HTTP requests from the API management function towards the CAPIF core function shall have the Resource URI structure as defined in clause 7.5 with the following clarifications:

- The <apiName> shall be "logs".
- The <apiVersion> shall be "v1".
- The <apiSpecificSuffixes> shall be set as described in clause 8.8.2.

All the resource URIs and the custom operation URIs specified in the clauses below are defined relative to the above API URI.

8.8.2 Resources

8.8.2.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 8.8.2.1-1 depicts the resource URIs structure for the CAPIF_Auditing_API.

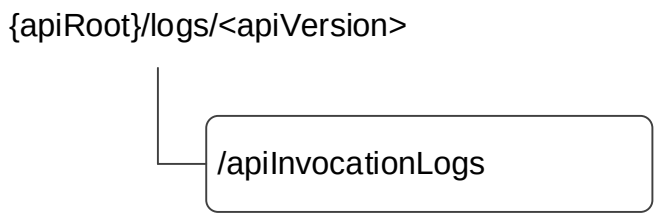

Figure 8.8.2.1-1: Resource URI structure of the CAPIF_Auditing_API

Table 8.8.2.1-1 provides an overview of the resources and applicable HTTP methods.

Table 8.8.2.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
All service API invocation logs (Store)	/apiInvocationLogs (NOTE)	GET	Query and retrieve service API invocation logs stored on the CAPIF core function
NOTE: The path segment "apiInvocationLogs" does not follow the related naming convention defined in clause 7.5.1. The path segment is however kept as currently defined in this specification for backward compatibility considerations.			

8.8.2.2 Resource: All service API invocation logs

8.8.2.2.1 Description

The All service API invocation logs resource represents a collection of service API invocation logs stored on the CAPIF core function. The resource is modelled as a Store resource archetype (see annex C.3 of 3GPP TS 29.501 [18])

8.8.2.2.2 Resource Definition

Resource URI: **{apiRoot}/logs/<apiVersion>/apiInvocationLogs**

This resource shall support the resource URI variables defined in table 8.8.2.2.2-1.

Table 8.8.2.2.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5

8.8.2.2.3 Resource Standard Methods

8.8.2.2.3.1 GET

This method shall support the URI query parameters specified in table 8.8.2.2.3.1-1.

Table 8.8.2.2.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	P	Cardinality	Description
aef-id	string	O	0..1	String identifying the API exposing function
api-invoker-id	string	O	0..1	String identifying the API invoker which invoked the service API
time-range-start	DateTime	O	0..1	Start time of the invocation time range
time-range-end	DateTime	O	0..1	End time of the invocation time range
api-id	string	O	0..1	String identifying the API invoked.
api-name	string	O	0..1	API name, it is set as {apiName} part of the URI structure as defined in clause 5.2.4 of 3GPP TS 29.122 [14].
api-version	string	O	0..1	Version of the API which was invoked
protocol	Protocol	O	0..1	Protocol invoked
operation	Operation	O	0..1	Operation that was invoked on the API
result	string	O	0..1	HTTP status code of the invocation
resource-name	string	O	0..1	Name of the specific resource invoked
src-interface	InterfaceDescription	O	0..1	Interface description of the API invoker.
dest-interface	InterfaceDescription	O	0..1	Interface description of the API invoked.
supported-features	SupportedFeatures	O	0..1	To filter irrelevant responses related to unsupported features.

This method shall support the request data structures specified in table 8.8.2.2.3.1-2 and the response data structures and response codes specified in table 8.8.2.2.3.1-3.

Table 8.8.2.2.3.1-2: Data structures supported by the GET Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 8.8.2.2.3.1-3: Data structures supported by the GET Response Body on this resource

Data type	P	Cardinality	Response codes	Description
InvocationLogsRetrieveRes	O	0..1	200 OK	Result of the query operation along with fetched service API invocation log data.
n/a			307 Temporary Redirect	Temporary redirection, during resource retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during resource retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
ProblemDetails	O	0..1	414 URI Too Long	Indicates that the server is refusing to service the request because the request-target is too long.
NOTE: The mandatory HTTP error status codes for the GET method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.8.2.2.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.8.2.2.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.8.2.2.4 Resource Custom Operations

None.

8.8.2A Custom Operations without associated resources

There are no custom operations without associated resources defined for this API in this release of the specification.

8.8.3 Notifications

There are no notifications defined for this API in this release of the specification.

8.8.4 Data Model

8.8.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 7.2 also apply to this API.

Table 8.8.4.1-1 specifies the data types defined specifically for the CAPIF_Auditing_API service.

Table 8.8.4.1-1: CAPIF_Auditing_API specific Data Types

Data type	Section defined	Description	Applicability
InvocationLogs	8.8.4.2.2	Contains multiple invocation logs.	EnQueryInvokeLog
InvocationLogsRetrieveRes	8.8.4.2.3	Contains the result of an invocation logs retrieval request.	

Table 8.8.4.1-2 specifies data types re-used by the CAPIF_Auditing_API service:

Table 8.8.4.1-2: Re-used Data Types

Data type	Reference	Comments	Applicability
DateTime	3GPP TS 29.122 [14]	Used to indicate the start and end times.	
InvocationLog	Clause 8.7.4.2.2	Used to represent logs of service API invocations stored on the CAPIF core function.	
Operation	Clause 8.2.4.3.7	Used to indicate the HTTP operation.	
ProblemDetails	3GPP TS 29.122 [14]	Used to represent the problem details in an error message.	
SupportedFeatures	3GPP TS 29.571 [19]	Used to negotiate the applicability of optional features defined in table 8.8.6-1.	

8.8.4.2 Structured data types

8.8.4.2.1 Introduction

This clause defines the structured data types to be used in resource representations of the CAPIF_Auditing_API.

8.8.4.2.2 Type: InvocationLogs

Table 8.8.4.2.2-1: Definition of type InvocationLogs

Attribute name	Data type	P	Cardinality	Description	Applicability
multipleInvocationLogs	array(InvocationLog)	M	1..N	Contains a multiple API invocation logs. The "supportedFeatures" attribute within the InvocationLog data type shall not be provided.	
supportedFeatures	SupportedFeatures	C	0..1	Used to negotiate the supported optional features of the API as described in clause 8.8.6. This parameter shall be included in HTTP GET response, if the consumer includes "supported-features" in the GET request.	

8.8.4.3 Simple data types and enumerations

None.

8.8.4.4 Data types describing alternative data types or combinations of data types

8.8.4.4.1 Type: InvocationLogsRetrieveRes

Table 8.8.4.4.1-1: Definition of type InvocationLogsRetrieveRes as a list of mutually exclusive alternatives

Data type	P	Cardinality	Description	Applicability
InvocationLog	C	0..1	Contains a single API invocation log. (NOTE)	
InvocationLogs	C	0..1	Contains multiple (more than one) API invocation logs. (NOTE)	EnQueryInvokeLog
NOTE: The InvocationLogs attribute shall be provided if the EnQueryInvokeLog feature is supported and requested by the API invoker, otherwise only the InvocationLog data type shall be provided.				

8.8.5 Error Handling

8.8.5.1 General

HTTP error handling shall be supported as specified in clause 7.7.

In addition, the requirements in the following clauses shall apply.

8.8.5.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the CAPIF_Auditing_API.

8.8.5.3 Application Errors

The application errors defined for the CAPIF_Auditing_API are listed in table 8.8.5.3-1.

Table 8.8.5.3-1: Application errors

Application Error	HTTP status code	Description	Applicability

8.8.6 Feature negotiation

General feature negotiation procedures are defined in clause 7.8.

Table 8.8.6-1: Supported Features

Feature number	Feature Name	Description
1	EnQueryInvokeLog	This feature indicates support for the enhancements of query invocation log.

8.9 CAPIF_API_Provider_Management_API

8.9.1 API URI

The CAPIF_API_Provider_Management_API service shall use the CAPIF_API_Provider_Management_API.

The request URIs used in HTTP requests from the API management function towards the CAPIF core function shall have the Resource URI structure as defined in clause 7.5 with the following clarifications:

- The <apiName> shall be "api-provider-management".
- The <apiVersion> shall be "v1".
- The <apiSpecificSuffixes> shall be set as described in clause 8.9.2.

All the resource URIs and the custom operation URIs specified in the clauses below are defined relative to the above API URI.

8.9.2 Resources

8.9.2.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 8.9.2.1-1 depicts the resource URIs structure for the CAPIF_API_Provider_Management_API.

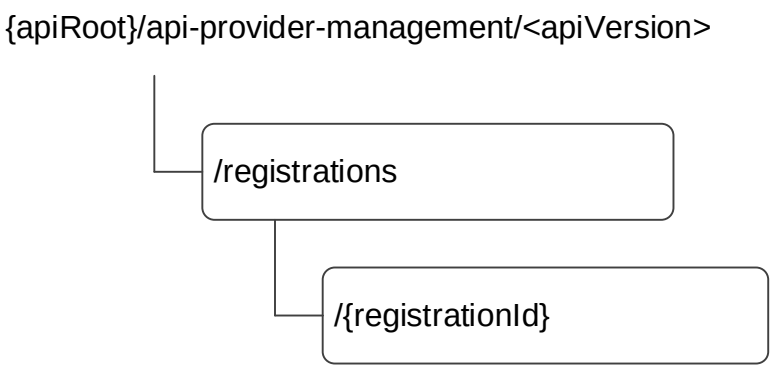

Figure 8.9.2.1-1: Resource URI structure of the CAPIF_API_Provider_Management_API

Table 8.9.2.1-1 provides an overview of the resources and applicable HTTP methods.

Table 8.9.2.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
All API Provider Domains Registrations	/registrations	POST	Registers a new API provider domain by creating an API provider domain with API provider domain functions profiles.
Individual API Provider Domain Registration	/registrations/{registrationId}	PUT	Updates an individual API provider domain identified by {registrationId}
		PATCH	Modifies an individual API provider domain identified by {registrationId}
		DELETE	Deregisters an API provider domain by deleting the API provider domain and functions, identified by {registrationId}.

8.9.2.2 Resource: All API Provider Domains Registrations

8.9.2.2.1 Description

The All API provider domains registrations resource represents all the API provider domains that are registered at a given CAPIF core function.

8.9.2.2.2 Resource Definition

Resource URI: **{apiRoot}/api-provider-management/<apiVersion>/registrations**

This resource shall support the resource URI variables defined in table 8.9.2.2.2-1.

Table 8.9.2.2.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5

8.9.2.2.3 Resource Standard Methods

8.9.2.2.3.1 POST

This method shall support the URI query parameters specified in table 8.9.2.2.3.1-1.

Table 8.9.2.2.3.1-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.9.2.2.3.1-2 and the response data structures and response codes specified in table 8.9.2.2.3.1-3.

Table 8.9.2.2.3.1-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
APIProviderEnrolmentDetails	M	1	Enrolment details of the API provider domain including individual API provider domain function details.

Table 8.9.2.2.3.1-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
APIProviderEnrolmentDetails	M	1	201 Created	API provider domain registered successfully The URI of the created resource shall be returned in the "Location" HTTP header. The list of successfully registered individual API provider domain functions, registration specific failure information of failed API provider domain function registrations, are included in APIProviderEnrolmentDetails which is provided in the response body.
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.9.2.2.3.1-4: Headers supported by the 201 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/api-provider-management/<apiVersion>/registrations/{registrationId}

8.9.2.2.4 Resource Custom Operations

None.

8.9.2.3 Resource: Individual API Provider Domain Registration

8.9.2.3.1 Description

The Individual API Provide Domain Registration resource represents an individual API provider domain that is registered at a given CAPIF core function.

8.9.2.3.2 Resource Definition

Resource URI: **{apiRoot}/api-provider-management/<apiVersion>/registrations/{registrationId}**

This resource shall support the resource URI variables defined in table 8.9.2.3.2-1.

Table 8.9.2.3.2-1: Resource URI variables for this resource

Name	Data Type	Definition
apiRoot	string	See clause 7.5
registrationId	string	Identifies an individual registered API Provider domain resource

8.9.2.3.3 Resource Standard Methods

8.9.2.3.3.1 PUT

The PUT method allows updating the registered API provider domain's detail. The properties "apiProviderDomainId", and "supportedFeatures" shall remain unchanged from previously provided values. This method shall support the URI query parameters specified in table 8.9.2.3.3.1-1.

Table 8.9.2.3.3.1-1: URI query parameters supported by the PUT method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in the table 8.9.2.3.3.1-2 and the response data structures and response codes specified in the table 8.9.2.3.3.1-3.

Table 8.9.2.3.3.1-2: Data structures supported by the PUT Request Body on this resource

Data type	P	Cardinality	Description
APIProviderEnrolmentDetails	M	1	Updated details of the API provider domain.

Table 8.9.2.3.3.1-3: Data structures supported by the PUT Response Body on this resource

Data type	P	Cardinality	Response codes	Description
APIProviderEnrolmentDetails	M	1	200 OK	API provider domain's information updated successfully. Updated details of the API provider domain is part of the APIProviderEnrolmentDetails, which is provided in the response body. The list of successfully updated individual API provider domain functions, registration update specific failure information of failed API provider domain function registration updates, are included in APIProviderEnrolmentDetails which is provided in the response body.
n/a			204 No Content	API provider domain's information updated successfully.
n/a			307 Temporary Redirect	Temporary redirection, during resource modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during resource modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the PUT method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.9.2.3.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.9.2.3.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.9.2.3.3.2 DELETE

This method shall support the URI query parameters specified in table 8.9.2.3.3.2-1.

Table 8.9.2.3.3.2-1: URI query parameters supported by the DELETE method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the response codes specified in table 8.9.2.3.3.2-2 and the response data structures and response codes specified in table 8.9.2.3.3.2-3.

Table 8.9.2.3.3.2-2: Data structures supported by the DELETE Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 8.9.2.3.3.2-3: Data structures supported by the DELETE Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The individual registered API provider domain matching the registrationId is deleted. All the individual API provider domain functions of the API provider domain are deleted.
n/a			307 Temporary Redirect	Temporary redirection, during resource termination. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during resource termination. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the DELETE method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.9.2.3.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.9.2.3.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.9.2.3.3.3 PATCH

This method shall support the URI query parameters specified in table 8.9.2.3.3.3-1.

Table 8.9.2.3.3.3-1: URI query parameters supported by the PATCH method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 8.9.2.3.3.3-2 and the response data structures and response codes specified in table 8.9.2.3.3.3-3.

Table 8.9.2.3.3.3-2: Data structures supported by the PATCH Request Body on this resource

Data type	P	Cardinality	Description
APIProviderEnrolmentDetailsPatch	M	1	Modified details of the API provider domain.

Table 8.9.2.3.3.3-3: Data structures supported by the PATCH Response Body on this resource

Data type	P	Cardinality	Response codes	Description
APIProviderEnrolmentDetails	M	1	200 OK	API provider domain's information updated successfully. Updated details of the API provider domain is part of the APIProviderEnrolmentDetails, which is provided in the response body. The list of successfully updated individual API provider domain functions, registration update specific failure information of failed API provider domain function registration updates, are included in APIProviderEnrolmentDetails which is provided in the response body.
n/a			204 No Content	API provider domain's information modified successfully.
n/a			307 Temporary Redirect	Temporary redirection, during resource modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during resource modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the HTTP PATCH method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.9.2.3.3.3-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.9.2.3.3.3-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.9.2.3.4 Resource Custom Operations

None.

8.9.2A Custom Operations without associated resources

There are no custom operations without associated resources defined for this API in this release of the specification.

8.9.3 Notifications

There are no notifications defined for this API in this release of the specification.

8.9.4 Data Model

8.9.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 7.2 also apply to this API.

Table 8.9.4.1-1 specifies the data types defined specifically for the CAPIF_API_Provider_Management_API service.

Table 8.9.4.1-1: CAPIF_API_Provider_Management_API specific Data Types

Data type	Section defined	Description	Applicability
APIProviderEnrolmentDetails	Clause 8.9.4.2.2	Represents the API provider domain's enrolment details.	
APIProviderEnrolmentDetailsPatch	Clause 8.9.4.2.5	Represents the list of modifications for the API provider domain's enrolment details.	PatchUpdate
ApiProviderFuncRole	Clause 8.9.4.3.3	Indicates the role (e.g. AEF, APF, etc.) of an API provider domain function.	
APIProviderFunctionDetails	Clause 8.9.4.2.3	Represents the API provider domain function's details.	
RegistrationInformation	Clause 8.9.4.2.4	Represents registration information of an individual API provider domain function.	

Table 8.9.4.1-2 specifies data types re-used by the CAPIF_API_Provider_Management_API service.

Table 8.9.4.1-2: Re-used Data Types

Data type	Reference	Comments	Applicability
SupportedFeatures	3GPP TS 29.571 [19]	Used to negotiate the applicability of optional features defined in table 8.9.6-1.	

8.9.4.2 Structured data types

8.9.4.2.1 Introduction

8.9.4.2.2 Type: APIProviderEnrolmentDetails

Table 8.9.4.2.2-1: Definition of type APIProviderEnrolmentDetails

Attribute name	Data type	P	Cardinality	Description	Applicability
apiProvDomId	string	O	0..1	API provider domain ID assigned by the CAPIF core function to the API management function while registering the API provider domain. Shall not be present in the HTTP POST request from the API management function to the CAPIF core function, to on-board itself. Shall be present in all other HTTP requests and responses.	
regSec	string	M	1	Security information necessary for the CAPIF core function to validate the registration of the API provider domain. Shall be present in HTTP request from API management function to CAPIF core function for API provider domain registration.	
apiProvFuncs	array(APIProviderFunctionDetails)	O	1..N	A list of individual API provider domain functions details. When included by the API management function in the HTTP request message, it lists the API provider domain functions that the API management function intends to register/update in registration or update registration procedure. When included by the CAPIF core function in the HTTP response message, it lists the API domain functions details that are registered or updated successfully.	
apiProvDomInfo	string	O	0..1	Generic information related to the API provider domain such as details of the API provider applications.	
suppFeat	SupportedFeatures	C	0..1	Used to negotiate the supported optional features of the API as described in clause 7.8. This attribute shall be provided in the HTTP POST request and in the response of successful resource creation.	
failReason	string	C	0..1	Registration or update specific failure information of failed API provider domain function registrations. Shall be present in the HTTP response body if atleast one of the API provider domain function registration or update registration fails.	
apiProvName	string	O	0..1	Represents the API provider name.	RNAA

8.9.4.2.3 Type: APIProviderFunctionDetails

Table 8.9.4.2.3-1: Definition of type APIProviderFunctionDetails

Attribute name	Data type	P	Cardinality	Description	Applicability
apiProvFuncId	string	C	0..1	API provider domain functionID assigned by the CAPIF core function to the API provider domain function while registering/updating the API provider domain. Shall not be present in the HTTP POST request from the API management function to the CAPIF core function, to register itself. Shall be present in all other HTTP requests and responses.	
regInfo	RegistrationInformation	M	1	Information necessary for the CAPIF core function to register the API provider domain function. This information shall be present in HTTP POST/PUT request from API management function to CAPIF core function for API provider domain registration. In the HTTP response message from CAPIF core function, shall include the updated registration information for API provider domain function.	
apiProvFuncRole	ApiProviderFuncRole	M	1	Role of API provider domain function. The role shall be present in the HTTP POST/PUT request that the API management function intends to register/update the API provider domain function as. CAPIF core function shall register the role of API provider domain function as per the request.	
apiProvFuncInfo	string	O	0..1	Generic information related to the API provider domain function such as details of the API provider applications.	

8.9.4.2.4 Type: RegistrationInformation

Table 8.9.4.2.4-1: Definition of type RegistrationInformation

Attribute name	Data type	P	Cardinality	Description	Applicability
apiProvPubKey	string	M	1	Public Key of API Provider domain function.	
apiProvCert	string	O	0..1	API provider domain function's generic client certificate	

8.9.4.2.5 Type: APIProviderEnrolmentDetailsPatch

Table 8.9.4.2.5-1: Definition of type APIProviderEnrolmentDetailsPatch

Attribute name	Data type	P	Cardinality	Description	Applicability
apiProvFuncs	array(APIProviderFunctionDetails)	O	1..N	A list of individual API provider domain functions details. When included by the API management function in the HTTP request message, it lists the API provider domain functions that the API management function intends to register/update in registration or update registration procedure.	
apiProvDomInfo	string	O	0..1	Generic information related to the API provider domain such as details of the API provider applications.	

8.9.4.3 Simple data types and enumerations

8.9.4.3.1 Introduction

This clause defines simple data types and enumerations that will be referenced from data structures defined in the previous clauses.

8.9.4.3.2 Simple data types

The simple data types defined in table 8.9.4.3.2-1 shall be supported.

Table 8.9.4.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
n/a			

8.9.4.3.3 Enumeration: ApiProviderFuncRole

Table 8.9.4.3.3-1: Enumeration ApiProviderFuncRole

Enumeration value	Description	Applicability
AEF	API provider function is API Exposing Function.	
APF	API provider function is API Publishing Function.	
AMF	API provider function is API Management Function.	

8.9.5 Error Handling

8.9.5.1 General

HTTP error handling shall be supported as specified in clause 7.7.

In addition, the requirements in the following clauses shall apply.

8.9.5.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the CAPIF_API_Provider_Management_API.

8.9.5.3 Application Errors

The application errors defined for the CAPIF_API_Provider_Management_API are listed in table 8.9.5.3-1.

Table 8.9.5.3-1: Application errors

Application Error	HTTP status code	Description	Applicability

8.9.6 Feature negotiation

General feature negotiation procedures are defined in clause 7.8. Table 8.9.6-1 lists the supported features for CAPIF_API_Invoker_Management_API.

Table 8.9.6-1: Supported Features

Feature number	Feature Name	Description
1	PatchUpdate	Indicates the support of the PATCH method for updating an API Provider Domain Registration resource.
2	RNAA	Indicates the support of RNAA functionality. This feature enables the following functionality: - provisioning of the API provider name and the related filtering criteria.

8.10 CAPIF_Routing_Info_API

8.10.1 API URI

The CAPIF_Routing_Info_API service shall use the CAPIF_Routing_Info_API.

The request URIs used in HTTP requests from the API exposing function towards the CAPIF core function shall have the Resource URI structure as defined in clause 7.5 with the following clarifications:

- The <apiName> shall be "capif-routing-info".
- The <apiVersion> shall be "v1".
- The <apiSpecificSuffixes> shall be set as described in clause 8.10.2.

All the resource URIs and the custom operation URIs specified in the clauses below are defined relative to the above API URI.

8.10.2 Resources

8.10.2.1 Overview

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 8.10.2.1-1 depicts the resource URIs structure for the CAPIF_Routing_Info_API.

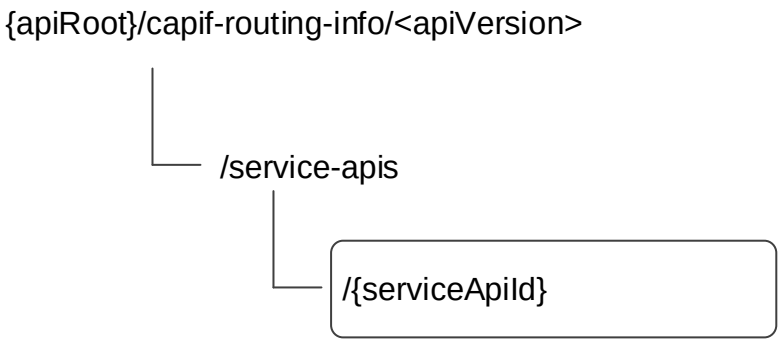

Figure 8.10.2.1-1: Resource URI structure of the CAPIF_Routing_Info_API

Table 8.10.2.1-1 provides an overview of the resources and applicable HTTP methods.

Table 8.10.2.1-1: Resources and methods overview

Resource name	Resource URI	HTTP method or custom operation	Description
Individual Service API routing info	/service-apis/{serviceApiId}	GET	Retrieves the API routing information for a published service API and API exposing function which applies the topology hiding.

8.10.2.2 Resource: Individual Service API routing info

8.10.2.2.1 Description

The API Routing Information resource represents the API routing information for the service API per API Exposing Function.

8.10.2.2.2 Resource Definition

Resource URI: **{apiRoot}/capif-routing-info/<apiVersion>/service-apis/{serviceApiId}**

This resource shall support the resource URI variables defined in table 8.10.2.2.2-1.

Table 8.10.2.2.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 7.5
serviceApiId	string	Identifies an individual published service API

8.10.2.2.3 Resource Standard Methods

8.10.2.2.3.1 GET

This method shall support the URI query parameters specified in table 8.10.2.2.3.1-1.

Table 8.10.2.2.3.1-1: URI query parameters supported by the GET method on this resource

Name	Data type	P	Cardinality	Description
aef-id	string	M	1	AEF identifier
supp-feat	SupportedFeatures	O	0..1	To filter irrelevant responses related to unsupported features.

This method shall support the request data structures specified in table 8.10.2.2.3.1-2 and the response data structures and response codes specified in table 8.10.2.2.3.1-3.

Table 8.10.2.2.3.1-2: Data structures supported by the GET Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 8.10.2.2.3.1-3: Data structures supported by the GET Response Body on this resource

Data type	P	Cardinality	Response Codes	Description
RoutingInfo	M	1	200 OK	The Routing information applicable for the service API requested.
n/a			307 Temporary Redirect	Temporary redirection, during resource retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during resource retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative CAPIF core function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the GET method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 8.10.2.2.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

Table 8.10.2.2.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative CAPIF core function.

8.10.2.2.4 Resource Custom Operations

None.

8.10.2A Custom Operations without associated resources

There are no custom operations without associated resources defined for this API in this release of the specification.

8.10.3 Notifications

There are no notifications defined for this API in this release of the specification.

8.10.4 Data Model

8.10.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 7.2 also apply to this API.

Table 8.10.4.1-1 specifies the data types defined specifically for the CAPIF_Routing_Info_API service.

Table 8.10.4.1-1: CAPIF_Routing_Info_API specific Data Types

Data type	Section defined	Description	Applicability
Ipv6AddressRange	Clause 8.10.4.2.4	Represents IPv6 address range.	
RoutingInfo	Clause 8.10.4.2.2	Represents API routing information.	
RoutingRule	Clause 8.10.4.2.3	Represents API routing rule.	

Table 8.10.4.1-2 specifies data types re-used by the CAPIF_Routing_Info_API service.

Table 8.10.4.1-2: Re-used Data Types

Data type	Reference	Comments	Applicability
AefProfile	Clause 8.2.4.2.4	Used to indicate the AEF profile.	
Ipv4AddressRange	3GPP TS 29.510 [28]	Used to indicate the IPv4 address range.	
Ipv6Addr	3GPP TS 29.122 [14]	Used to indicate the IPv6 address.	
SupportedFeatures	3GPP TS 29.571 [19]	Used to negotiate the applicability of optional features defined in table 8.10.6-1.	

8.10.4.2 Structured data types

8.10.4.2.1 Introduction

This clause defines data structures to be used in resource representations.

8.10.4.2.2 Type: RoutingInfo

Table 8.10.4.2.2-1: Definition of type RoutingInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
routingRules	array(RoutingRule)	M	1..N	Routing rules	

8.10.4.2.3 Type: RoutingRule

Table 8.10.4.2.3-1: Definition of type RoutingRule

Attribute name	Data type	P	Cardinality	Description	Applicability
ipv4AddrRanges	array(Ipv4AddressRange)	O	1..N	The IPv4 address range for the API invocation source IP address. (NOTE)	
ipv6AddrRanges	array(Ipv6AddressRange)	O	1..N	The IPv6 address range for the API invocation source IP address. (NOTE)	
aefProfile	AefProfile	M	1	The target AEF profile	
NOTE: If no IP address range is provided, it means the service API invocation from any source IP address can be routed to the target AEF.					

8.10.4.2.4 Type: Ipv6AddressRange

Table 8.10.4.2.4-1: Definition of type Ipv6AddressRange

Attribute name	Data type	P	Cardinality	Description	Applicability
start	Ipv6Addr	M	1	First value identifying the start of an IPv6 address range	
end	Ipv6Addr	M	1	Last value identifying the end of an IPv6 address range	

8.10.4.3 Simple data types and enumerations

None.

8.10.5 Error Handling

8.10.5.1 General

HTTP error handling shall be supported as specified in clause 7.7.

In addition, the requirements in the following clauses shall apply.

8.10.5.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the CAPIF_Routing_Info_API.

8.10.5.3 Application Errors

The application errors defined for the CAPIF_Routing_Info_API are listed in table 8.10.5.3-1.

Table 8.10.5.3-1: Application errors

Application Error	HTTP status code	Description	Applicability

8.10.6 Feature negotiation

General feature negotiation procedures are defined in clause 7.8.

Table 8.10.6-1: Supported Features

Feature number	Feature Name	Description
n/a		

9 AEF API Definition

9.1 AEF_Security_API

9.1.1 API URI

The AEF_Security_API service shall use the AEF_Security_API.

The request URIs used in HTTP requests from the API invoker towards the API exposing function shall have the Resource URI structure defined in clause 7.5 with the following clarifications:

- The <apiName> shall be "aef-security".
- The <apiVersion> shall be "v1".
- The <custOpName> shall be set as described in clause 9.1.2a.

All the resource URIs and the custom operation URIs specified in the clauses below are defined relative to the above API URI.

9.1.2 Resources

There is no resource defined for this API.

9.1.2A Custom Operations without associated resources

9.1.2A.1 Overview

Custom operations used for this API are summarized in table 9.1.2A.1-1. "{apiRoot}" and "<apiVersion>" are set as described in clause 7.5 and clause 9.1.1 respectively.

Table 9.1.2A.1-1: Custom operations without associated resources

Operation name	Custom operation URI	Mapped HTTP method	Description
check-authentication	/check-authentication	POST	Check authentication request.
revoke-authentication	/revoke-authorization	POST	Revoke authorization for service APIs.

9.1.2A.2 Operation: check-authentication

9.1.2A.2.1 Description

This custom operation allows the API invoker to confirm from the API exposing function, that necessary authentication data is available to authenticate the API invoker on API invocation.

9.1.2A.2.2 Operation Definition

This method shall support the URI query parameters specified in table 9.1.2A.2.2-1.

Table 9.1.2A.2.2-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This operation shall support the request and response data structures, and response codes specified in tables 9.1.2A.2.2-2 and 9.1.2A.2.2-3.

Table 9.1.2A.2.2-2: Data structures supported by the POST Request Body on this operation

Data type	P	Cardinality	Description
CheckAuthenticationReq	M	1	Authentication check request data

Table 9.1.2A.2.2-3: Data structures supported by the POST Response Body on this operation

Data type	P	Cardinality	Response codes	Description
CheckAuthenticationRsp	M	1	200 OK	The request was successful.
n/a			307 Temporary Redirect	Temporary redirection, during authentication confirmation. The response shall include a Location header field containing an alternative URI of the resource located in an alternative API exposing function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during authentication confirmation. The response shall include a Location header field containing an alternative URI of the resource located in an alternative API exposing function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 9.1.2A.2.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative API exposing function.

Table 9.1.2A.2.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative API exposing function.

9.1.2A.3 Operation: revoke-authorization

9.1.2A.3.1 Description

This custom operation allows the CAPIF core function to request the API exposing function to revoke the authorization of the API invoker for the indicated service APIs.

9.1.2A.3.2 Operation Definition

This method shall support the URI query parameters specified in table 9.1.2A.3.2-1.

Table 9.1.2A.3.2-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This operation shall support the request and response data structures, and response codes specified in tables 9.1.2A.3.2-2 and 9.1.2A.3.2-3.

Table 9.1.2A.3.2-2: Data structures supported by the POST Request Body on this operation

Data type	P	Cardinality	Description
RevokeAuthorizationReq	M	1	Authorization revocation request data

Table 9.1.2A.3.2-3: Data structures supported by the POST Response Body on this operation

Data type	P	Cardinality	Response codes	Description
RevokeAuthorizationRsp	M	1	200 OK	The request was successful.
n/a			307 Temporary Redirect	Temporary redirection, during authorization revocation. The response shall include a Location header field containing an alternative URI of the resource located in an alternative API exposing function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
n/a			308 Permanent Redirect	Permanent redirection, during authorization revocation. The response shall include a Location header field containing an alternative URI of the resource located in an alternative API exposing function. Redirection handling is described in clause 5.2.10 of 3GPP TS 29.122 [14].
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.6-1 of 3GPP TS 29.122 [14] also apply.				

Table 9.1.2A.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative API exposing function.

Table 9.1.2A.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI of the resource located in an alternative API exposing function.

9.1.3 Notifications

There are no notifications defined for this API in this release of the specification.

9.1.4 Data Model

9.1.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 7.2 apply to this API.

Table 9.1.4.1-1 specifies the data types defined specifically for the AEF_Security_API service.

Table 9.1.4.1-1: AEF_Security_API specific Data Types

Data type	Section defined	Description	Applicability
CheckAuthenticationReq	Clause 9.1.4.2.2	Represents authentication check request data.	
CheckAuthenticationRsp	Clause 9.1.4.2.3	Represents authentication check response data.	
RevokeAuthorizationReq	Clause 9.1.4.2.4	Represents authorization revocation request data.	
RevokeAuthorizationRsp	Clause 9.1.4.2.5	Represents authorization revocation response data.	

Table 9.1.4.1-2 specifies data types re-used by the AEF_Security_API service.

Table 9.1.4.1-2: Re-used Data Types

Data type	Reference	Comments	Applicability
SecurityNotification	Clause 8.5.4.2.5	Used to indicate information about the revoked APIs.	
SupportedFeatures	3GPP TS 29.571 [19]	Used to negotiate the applicability of optional features defined in table 9.1.6-1.	

9.1.4.2 Structured data types

9.1.4.2.1 Introduction

This clause defines the structures to be used in resource representations for the AEF_Security_API.

9.1.4.2.2 Type: CheckAuthenticationReq

Table 9.1.4.2.2-1: Definition of type CheckAuthenticationReq

Attribute name	Data type	P	Cardinality	Description	Applicability
apiInvokerId	string	M	1	API invoker ID assigned by the CAPIF core function to the API invoker while on-boarding the API invoker.	
supportedFeatures	Supported Features	M	1	Used to negotiate the supported optional features of the API as described in clause 7.8.	

9.1.4.2.3 Type: CheckAuthenticationRsp

Table 9.1.4.2.3-1: Definition of type CheckAuthenticationRsp

Attribute name	Data type	P	Cardinality	Description	Applicability
supportedFeatures	Supported Features	M	1	Used to negotiate the supported optional features of the API as described in clause 7.8.	

9.1.4.2.4 Type: RevokeAuthorizationReq

Table 9.1.4.2.4-1: Definition of type RevokeAuthorizationReq

Attribute name	Data type	P	Cardinality	Description	Applicability
revokeInfo	SecurityNotification	M	1	It contains detailed revocation information.	
supportedFeatures	SupportedFeatures	M	1	Used to negotiate the supported optional features of the API as described in clause 7.8.	

9.1.4.2.5 Type: RevokeAuthorizationRsp

Table 9.1.4.2.5-1: Definition of type RevokeAuthorizationRsp

Attribute name	Data type	P	Cardinality	Description	Applicability
supportedFeatures	SupportedFeatures	M	1	Used to negotiate the supported optional features of the API as described in clause 7.8.	

9.1.4.3 Simple data types and enumerations

None.

9.1.5 Error Handling

9.1.5.1 General

HTTP error handling shall be supported as specified in clause 7.7.

In addition, the requirements in the following clauses shall apply.

9.1.5.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the AEF_Security_API.

9.1.5.3 Application Errors

The application errors defined for the AEF_Security_API are listed in table 9.1.5.3-1.

Table 9.1.5.3-1: Application errors

Application Error	HTTP status code	Description	Applicability

9.1.6 Feature negotiation

General feature negotiation procedures are defined in clause 7.8.

Table 9.1.6-1: Supported Features

Feature number	Feature Name	Description
n/a		

10 Security

10.1 General

Security methods for CAPIF are specified in 3GPP TS 33.122 [16].

10.2 CAPIF-1/1e security

Secure communication between API invoker and CAPIF core function over CAPIF-1/1e reference points, using a TLS protocol based connection is defined in 3GPP TS 33.122 [16].

For Onboard_API_Invoker service operation of the CAPIF_API_Invoker_Management_API, the TLS protocol based connection shall be established using server certificate as defined in 3GPP TS 33.122 [16].

For rest of the CAPIF APIs, the TLS protocol based connection shall be established with certificate based mutual authentication as defined in 3GPP TS 33.122 [16].

10.3 CAPIF-2/2e security and securely invoking service APIs

For secure communication between API invoker and API exposing function and ensuring secure invocations of service APIs, the API invoker:

- shall negotiate the security method with the CAPIF core function using the Obtain_Security_Method service operation of the CAPIF_Security_API;
- shall initiate the authentication with the API exposing function using the Initiate_Authentication service operation of the AEF_Security_API; and
- shall establish a secure connection with the API exposing function as defined in 3GPP TS 33.122 [16], using the method negotiated with the CAPIF core function.

Annex A (normative): OpenAPI specification

A.1 General

This Annex is based on the OpenAPI Specification [3] and provides corresponding representations of all APIs defined in the present specification, in YAML format.

This Annex shall take precedence when being discrepant to other parts of the specification with respect to the encoding of information elements and methods within the API.

NOTE: The semantics and procedures, as well as conditions, e.g. for the applicability and allowed combinations of attributes or values, not expressed in the OpenAPI definitions but defined in other parts of the specification also apply.

Informative copies of the OpenAPI specification file contained in this 3GPP Technical Specification are available on a Git-based repository that uses the GitLab software version control system (see clause 5B of 3GPP TR 21.900 [27] and clause 5.3.1 of 3GPP TS 29.501 [18] for further information).

A.2 CAPIF_Discover_Service_API

```
openapi: 3.0.0

info:
  title: CAPIF_Discover_Service_API
  description: |
    API for discovering service APIs.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
  version: "1.3.0"

externalDocs:
  description: 3GPP TS 29.222 V18.6.0 Common API Framework for 3GPP Northbound APIs
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.222/

servers:
  - url: '{apiRoot}/service-apis/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 7.5 of 3GPP TS 29.222.

paths:
  /allServiceAPIs:
    get:
      description: >
        Discover published service APIs and retrieve a collection of APIs according
        to certain filter criteria.
      parameters:
        - name: api-invoker-id
          in: query
          description: >
             String identifying the API invoker assigned by the CAPIF core function.
             It also represents the CCF identifier in the CAPIF-6/6e interface.
          required: true
          schema:
            type: string
        - name: api-name
          in: query
          description: >
            API name, it is set as {apiName} part of the URI structure as defined
            in clause 5.2.4 of 3GPP TS 29.122.
          schema:
            type: string
        - name: api-version
          in: query
          description: API major version the URI (e.g. v1).
```

```
      schema:
        type: string
    - name: comm-type
      in: query
      description: Communication type used by the API (e.g. REQUEST_RESPONSE).
      schema:
        $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/CommunicationType'
    - name: protocol
      in: query
      description: Protocol used by the API.
      schema:
        $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/Protocol'
    - name: aef-id
      in: query
      description: AEF identifer.
      schema:
        type: string
    - name: data-format
      in: query
      description: Data formats used by the API (e.g. serialization protocol JSON used).
      schema:
        $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/DataFormat'
    - name: api-cat
      in: query
      description: The service API category to which the service API belongs to.
      schema:
        type: string
    - name: preferred-aef-loc
      in: query
      description: The preferred AEF location.
      content:
        application/json:
          schema:
            $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/AefLocation'
    - name: req-api-prov-name
      in: query
      description: Represents the required API provider name.
      schema:
        type: string
    - name: supported-features
      in: query
      description: Features supported by the NF consumer for the CAPIF Discover Service API.
      schema:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
    - name: api-supported-features
      in: query
      description: >
        Features supported by the discovered service API indicated by api-name parameter.
        This may only be present if api-name query parameter is present.
      schema:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
    - name: ue-ip-addr
      in: query
      description: Represents the UE IP address information.
      schema:
        $ref: '#/components/schemas/IpAddrInfo'
    - name: service-kpis
      in: query
      description: >
        Contains iInformation about service characteristics provided by the targeted
        service API(s).
      schema:
        $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/ServiceKpis'
  responses:
    '200':
      description: >
        The response body contains the result of the search over the list of registered APIs.
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/DiscoveredAPIs'
    '307':
      $ref: 'TS29122_CommonData.yaml#/components/responses/307'
    '308':
      $ref: 'TS29122_CommonData.yaml#/components/responses/308'
    '400':
      $ref: 'TS29122_CommonData.yaml#/components/responses/400'
    '401':
```

```
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29122_CommonData.yaml#/components/responses/406'
        '414':
          $ref: 'TS29122_CommonData.yaml#/components/responses/414'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'

components:
  schemas:
    DiscoveredAPIs:
      type: object
      description: >
        Represents a list of APIs currently registered in the CAPIF core function
        and satisfying a number of filter criteria provided by the API consumer.
      properties:
        serviceAPIDescriptions:
          type: array
          items:
            $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/ServiceAPIDescription'
          minItems: 1
          description: >
            Description of the service API as published by the service. Each service
            API information shall include AEF profiles matching the filter criteria.

    IpAddrInfo:
      type: object
      description: Represents the UE IP address information.
      properties:
        ipv4Addr:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Ipv4Addr'
        ipv6Addr:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Ipv6Addr'
      oneOf:
        - required: [ipv4Addr]
        - required: [ipv6Addr]
```

A.3 CAPIF_Publish_Service_API

```
openapi: 3.0.0

info:
  title: CAPIF_Publish_Service_API
  description: |
    API for publishing service APIs.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
  version: "1.3.0"

externalDocs:
  description: 3GPP TS 29.222 V18.6.0 Common API Framework for 3GPP Northbound APIs
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.222/

servers:
  - url: '{apiRoot}/published-apis/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 7.5 of 3GPP TS 29.222.

paths:
# APF published API
  /{apfId}/service-apis:
    post:
      description: Publish a new API.
      parameters:
```

```
      - name: apfId
        in: path
        required: true
        schema:
          type: string
    requestBody:
      required: true
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/ServiceAPIDescription'
    responses:
      '201':
        description: >
          Service API published successfully The URI of the created resource
          shall be returned in the "Location" HTTP header.
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ServiceAPIDescription'
        headers:
          Location:
            description: >
              Contains the URI of the newly created resource, according to the structure
              {apiRoot}/published-apis/v1/{apfId}/service-apis/{serviceApiId}
            required: true
            schema:
              type: string
      '400':
        $ref: 'TS29122_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29122_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29122_CommonData.yaml#/components/responses/404'
      '411':
        $ref: 'TS29122_CommonData.yaml#/components/responses/411'
      '413':
        $ref: 'TS29122_CommonData.yaml#/components/responses/413'
      '415':
        $ref: 'TS29122_CommonData.yaml#/components/responses/415'
      '429':
        $ref: 'TS29122_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29122_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29122_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29122_CommonData.yaml#/components/responses/default'
  get:
    description: Retrieve all published APIs.
    parameters:
      - name: apfId
        in: path
        required: true
        schema:
          type: string
    responses:
      '200':
        description: Definition of all service API(s) published by the API publishing function.
        content:
          application/json:
            schema:
              type: array
              items:
                $ref: '#/components/schemas/ServiceAPIDescription'
              minItems: 0
      '307':
        $ref: 'TS29122_CommonData.yaml#/components/responses/307'
      '308':
        $ref: 'TS29122_CommonData.yaml#/components/responses/308'
      '400':
        $ref: 'TS29122_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29122_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
```

```
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29122_CommonData.yaml#/components/responses/406'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'

# Individual APF published API
  /{apfId}/service-apis/{serviceApiId}:
    get:
      description: Retrieve a published service API.
      parameters:
        - name: serviceApiId
          in: path
          required: true
          schema:
            type: string
        - name: apfId
          in: path
          required: true
          schema:
            type: string
      responses:
        '200':
          description: >
            Definition of individual service API published by the API publishing function.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/ServiceAPIDescription'
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29122_CommonData.yaml#/components/responses/406'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'
    put:
      description: Update a published service API.
      parameters:
        - name: serviceApiId
          in: path
          required: true
          schema:
            type: string
        - name: apfId
          in: path
          required: true
          schema:
            type: string
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ServiceAPIDescription'
      responses:
```

```
      '200':
        description: Definition of service API updated successfully.
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ServiceAPIDescription'
      '204':
        description: No Content
      '307':
        $ref: 'TS29122_CommonData.yaml#/components/responses/307'
      '308':
        $ref: 'TS29122_CommonData.yaml#/components/responses/308'
      '400':
        $ref: 'TS29122_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29122_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29122_CommonData.yaml#/components/responses/404'
      '411':
        $ref: 'TS29122_CommonData.yaml#/components/responses/411'
      '413':
        $ref: 'TS29122_CommonData.yaml#/components/responses/413'
      '415':
        $ref: 'TS29122_CommonData.yaml#/components/responses/415'
      '429':
        $ref: 'TS29122_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29122_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29122_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29122_CommonData.yaml#/components/responses/default'
  patch:
    description: Modify an existing published service API.
    operationId: ModifyIndAPFPubAPI
    tags:
      - Individual APF published API
    parameters:
      - name: serviceApiId
        in: path
        required: true
        schema:
          type: string
      - name: apfId
        in: path
        required: true
        schema:
          type: string
    requestBody:
      required: true
      content:
        application/merge-patch+json:
          schema:
            $ref: '#/components/schemas/ServiceAPIDescriptionPatch'
    responses:
      '200':
        description: >
          The definition of the service API is modified successfully and a
          representation of the updated service API is returned in the request body.
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ServiceAPIDescription'
      '204':
        description: No Content. The definition of the service API is modified successfully.
      '307':
        $ref: 'TS29122_CommonData.yaml#/components/responses/307'
      '308':
        $ref: 'TS29122_CommonData.yaml#/components/responses/308'
      '400':
        $ref: 'TS29122_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29122_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
      '404':
```

```
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29122_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29122_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29122_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'
    delete:
      description: Unpublish a published service API.
      parameters:
        - name: serviceApiId
          in: path
          required: true
          schema:
            type: string
        - name: apfId
          in: path
          required: true
          schema:
            type: string
      responses:
        '204':
          description: The individual published service API matching the serviceAPiId is deleted.
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'

# Components

components:
  schemas:
# Data Type for representations
    ServiceAPIDescription:
      type: object
      description: Represents the description of a service API as published by the APF.
      properties:
        apiName:
          type: string
          description: >
             API name, it is set as {apiName} part of the URI structure as defined in
             clause 5.2.4 of 3GPP TS 29.122.
        apiId:
          type: string
          description: >
            API identifier assigned by the CAPIF core function to the published service API.
            Shall not be present in the HTTP POST request from the API publishing function
            to the CAPIF core function. Shall be present in the HTTP POST response from the
            CAPIF core function to the API publishing function and in the HTTP GET response
            from the CAPIF core function to the API invoker (discovery API).
        apiStatus:
          $ref: '#/components/schemas/ApiStatus'
        aefProfiles:
          type: array
```

```
        items:
          $ref: '#/components/schemas/AefProfile'
        minItems: 1
        description: >
          AEF profile information, which includes the exposed API details (e.g. protocol).
      description:
        type: string
        description: Text description of the API
      supportedFeatures:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      shareableInfo:
        $ref: '#/components/schemas/ShareableInformation'
      serviceAPICategory:
        type: string
        description: The service API category to which the service API belongs to.
      apiSuppFeats:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      pubApiPath:
        $ref: '#/components/schemas/PublishedApiPath'
      ccfId:
        type: string
        description: CAPIF core function identifier.
      apiProvName:
        type: string
        description: Represents the API provider name.
    required:
      - apiName

  InterfaceDescription:
    type: object
    description: Represents the description of an API's interface.
    properties:
      ipv4Addr:
        $ref: 'TS29122_CommonData.yaml#/components/schemas/Ipv4Addr'
      ipv6Addr:
        $ref: 'TS29122_CommonData.yaml#/components/schemas/Ipv6Addr'
      fqdn:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Fqdn'
      port:
        $ref: 'TS29122_CommonData.yaml#/components/schemas/Port'
      apiPrefix:
        type: string
        description: >
          A string representing a sequence of path segments that starts with the slash character.
      securityMethods:
        type: array
        items:
          $ref: '#/components/schemas/SecurityMethod'
        minItems: 1
        description: >
          Security methods supported by the interface, it take precedence over
          the security methods provided in AefProfile, for this specific interface.
    oneOf:
      - required: [ipv4Addr]
      - required: [ipv6Addr]
      - required: [fqdn]

  AefProfile:
    type: object
    description: Represents the AEF profile data.
    properties:
      aefId:
        type: string
        description: Identifier of the API exposing function
      versions:
        type: array
        items:
          $ref: '#/components/schemas/Version'
        minItems: 1
        description: API version
      protocol:
        $ref: '#/components/schemas/Protocol'
      dataFormat:
        $ref: '#/components/schemas/DataFormat'
      securityMethods:
        type: array
        items:
          $ref: '#/components/schemas/SecurityMethod'
```

```
        minItems: 1
        description: Security methods supported by the AEF
      domainName:
        type: string
        description: Domain to which API belongs to
      interfaceDescriptions:
        type: array
        items:
          $ref: '#/components/schemas/InterfaceDescription'
        minItems: 1
        description: Interface details
      aefLocation:
        $ref: '#/components/schemas/AefLocation'
      serviceKpis:
        $ref: '#/components/schemas/ServiceKpis'
      ueIpRange:
        $ref: '#/components/schemas/IpAddrRange'
    required:
      - aefId
      - versions
    oneOf:
      - required: [domainName]
      - required: [interfaceDescriptions]

  Resource:
    type: object
    description: Represents the API resource data.
    properties:
      resourceName:
        type: string
        description: Resource name
      commType:
        $ref: '#/components/schemas/CommunicationType'
      uri:
        type: string
        description: >
          Relative URI of the API resource, it is set as {apiSpecificSuffixes} part
          of the URI structure as defined in clause 5.2.4 of 3GPP TS 29.122.
      custOpName:
        type: string
        description: >
          it is set as {custOpName} part of the URI structure for a custom operation
          associated with a resource as defined in clause 5.2.4 of 3GPP TS 29.122.
      custOperations:
        type: array
        items:
          $ref: '#/components/schemas/CustomOperation'
        minItems: 1
        description: >
          Custom operations associated with this resource.
      operations:
        type: array
        items:
          $ref: '#/components/schemas/Operation'
        minItems: 1
        description: >
          Supported HTTP methods for the API resource. Only applicable when the
          protocol in AefProfile indicates HTTP.
      description:
        type: string
        description: Text description of the API resource
    required:
      - resourceName
      - commType
      - uri

  CustomOperation:
    type: object
    description: Represents the description of a custom operation.
    properties:
      commType:
        $ref: '#/components/schemas/CommunicationType'
      custOpName:
        type: string
        description: >
          it is set as {custOpName} part of the URI structure for a custom operation
          without resource association as defined in clause 5.2.4 of 3GPP TS 29.122.
      operations:
```

```
        type: array
        items:
          $ref: '#/components/schemas/Operation'
        minItems: 1
        description: >
          Supported HTTP methods for the API resource. Only applicable when the
          protocol in AefProfile indicates HTTP.
      description:
        type: string
        description: Text description of the custom operation
    required:
      - commType
      - custOpName

  Version:
    type: object
    description: Represents the API version information.
    properties:
      apiVersion:
        type: string
        description: API major version in URI (e.g. v1)
      expiry:
        $ref: 'TS29122_CommonData.yaml#/components/schemas/DateTime'
      resources:
        type: array
        items:
          $ref: '#/components/schemas/Resource'
        minItems: 1
        description: Resources supported by the API.
      custOperations:
        type: array
        items:
          $ref: '#/components/schemas/CustomOperation'
        minItems: 1
        description: Custom operations without resource association.
    required:
      - apiVersion

  ShareableInformation:
    type: object
    description: >
      Indicates whether the service API and/or the service API category can be shared
      to the list of CAPIF provider domains.
    properties:
      isShareable:
        type: boolean
        description: >
          Set to "true" indicates that the service API and/or the service API
          category can be shared to the list of CAPIF provider domain information.
          Otherwise set to "false".
      capifProvDoms:
        type: array
        items:
          type: string
        minItems: 1
        description: >
          List of CAPIF provider domains to which the service API information to be shared.
    required:
      - isShareable

  PublishedApiPath:
    type: object
    description: Represents the published API path within the same CAPIF provider domain.
    properties:
      ccfIds:
        type: array
        items:
          type: string
        minItems: 1
        description: A list of CCF identifiers where the service API is already published.

  AefLocation:
    description: >
      Represents the location information (e.g. civic address, GPS coordinates, data center ID)
      where the AEF providing the service API is located.
    type: object
    properties:
      civicAddr:
```

```
        $ref: 'TS29572_Nlmf_Location.yaml#/components/schemas/CivicAddress'
      geoArea:
        $ref: 'TS29572_Nlmf_Location.yaml#/components/schemas/GeographicArea'
      dcId:
        type: string
        description: >
          Identifies the data center where the AEF providing the service API is located.

  ServiceAPIDescriptionPatch:
    type: object
    description: >
      Represents the parameters to request the modification of an APF published API resource.
    properties:
      apiStatus:
        $ref: '#/components/schemas/ApiStatus'
      aefProfiles:
        type: array
        items:
          $ref: '#/components/schemas/AefProfile'
        description: AEF profile information, which includes the exposed API details.
        minItems: 1
      description:
        type: string
        description: Text description of the API
      shareableInfo:
        $ref: '#/components/schemas/ShareableInformation'
      serviceAPICategory:
        type: string
        description: The service API category to which the service API belongs to.
      apiSuppFeats:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      pubApiPath:
        $ref: '#/components/schemas/PublishedApiPath'
      ccfId:
        type: string
        description: CAPIF core function identifier.

  ApiStatus:
    type: object
    description: >
      Represents the API status.
    properties:
      aefIds:
        type: array
        items:
          type: string
        description: >
          Indicates the list of AEF ID(s) where the API is active.
          If this attribute is omitted, the API is inactive at all AEF(s)
          defined in the "aefProfiles" attribute within
          the ServiceAPIDescription data structure.
    required:
      - aefIds

  ServiceKpis:
    type: object
    description: >
      Represents information about the service characteristics provided by a service API.
    properties:
      maxReqRate:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
      maxRestime:
        $ref: 'TS29122_CommonData.yaml#/components/schemas/DurationSec'
      availability:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
      avalComp:
        type: string
        pattern: '^\d+(\.\d+)? (kFLOPS|MFLOPS|GFLOPS|TFLOPS|PFLOPS|EFLOPS|ZFLOPS)$'
        description: >
          The maximum compute resource available in FLOPS for the API Invoker.
      avalGraComp:
        type: string
        pattern: '^\d+(\.\d+)? (kFLOPS|MFLOPS|GFLOPS|TFLOPS|PFLOPS|EFLOPS|ZFLOPS)$'
        description: >
          The maximum graphical compute resource in FLOPS available for the API Invoker.
      avalMem:
        type: string
        pattern: '^\d+(\.\d+)? (KB|MB|GB|TB|PB|EB|ZB|YB)$'
```

```
      description: >
        The maximum memory resource available for the API Invoker.
    avalStor:
      type: string
      pattern: '^\d+(\.\d+)? (KB|MB|GB|TB|PB|EB|ZB|YB)$'
      description: >
        The maximum storage resource available for the API Invoker.
    conBand:
      $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'

IpAddrRange:
  description: Represents the list of public IP ranges
  type: object
  properties:
    ueIpv4AddrRanges:
      type: array
      items:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4AddressRange'
      description: Represents the IPv4 Address ranges of the UE(s).
      minItems: 1
    ueIpv6AddrRanges:
      type: array
      items:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6AddressRange'
      description: Represents the Ipv6 Address ranges of the UE(s).
      minItems: 1
  anyOf:
    - required: [ueIpv4AddrRanges]
    - required: [ueIpv6AddrRanges]

Protocol:
  anyOf:
  - type: string
    enum:
      - HTTP_1_1
      - HTTP_2
      - MQTT
      - WEBSOCKET
  - type: string
    description: >
      This string provides forward-compatibility with future
      extensions to the enumeration but is not used to encode
      content defined in the present version of this API.
  description: |
    Indicates a protocol and protocol version used by the API.
    Possible values are:
    - HTTP_1_1: Indicates that the protocol is HTTP version 1.1.
    - HTTP_2: Indicates that the protocol is HTTP version 2.
    - MQTT: Indicates that the protocol is Message Queuing Telemetry Transport.
    - WEBSOCKET: Indicates that the protocol is Websocket.

CommunicationType:
  anyOf:
  - type: string
    enum:
      - REQUEST_RESPONSE
      - SUBSCRIBE_NOTIFY
  - type: string
    description: >
      This string provides forward-compatibility with future
      extensions to the enumeration but is not used to encode
      content defined in the present version of this API.
  description: |
    Indicates a communication type of the resource or the custom operation.
    Possible values are:
    - REQUEST_RESPONSE: The communication is of the type request-response.
    - SUBSCRIBE_NOTIFY: The communication is of the type subscribe-notify.

DataFormat:
  anyOf:
  - type: string
    enum:
      - JSON
      - XML
      - PROTOBUF3
  - type: string
    description: >
      This string provides forward-compatibility with future
```

```
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Indicates a data format.
        Possible values are:
        - JSON: Indicates that the data format is JSON.
        - XML: Indicates that the data format is Extensible Markup Language.
        - PROTOBUF3: Indicates that the data format is Protocol buffers version 3.

    SecurityMethod:
      anyOf:
      - type: string
        enum:
          - PSK
          - PKI
          - OAUTH
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Indicates the security method.
        Possible values are:
        - PSK: Security method 1 (Using TLS-PSK) as described in 3GPP TS 33.122.
        - PKI: Security method 2 (Using PKI) as described in 3GPP TS 33.122.
        - OAUTH: Security method 3 (TLS with OAuth token) as described in 3GPP TS 33.122.

    Operation:
      anyOf:
      - type: string
        enum:
          - GET
          - POST
          - PUT
          - PATCH
          - DELETE
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Indicates an HTTP method.
        Possible values are:
        - GET: HTTP GET method.
        - POST: HTTP POST method.
        - PUT: HTTP PUT method.
        - PATCH: HTTP PATCH method.
        - DELETE: HTTP DELETE method.
```

A.4 CAPIF_Events_API

```
openapi: 3.0.0

info:
  title: CAPIF_Events_API
  description: |
    API for event subscription management.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
  version: "1.3.0"

externalDocs:
  description: 3GPP TS 29.222 V18.6.0 Common API Framework for 3GPP Northbound APIs
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.222/

servers:
  - url: '{apiRoot}/capif-events/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 7.5 of 3GPP TS 29.222

paths:
```

```
  /{subscriberId}/subscriptions:
    post:
      description: Creates a new individual CAPIF Event Subscription.
      parameters:
        - name: subscriberId
          in: path
          description: Identifier of the Subscriber
          required: true
          schema:
            type: string
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/EventSubscription'
      callbacks:
        notificationDestination:
          '{$request.body#/notificationDestination}':
            post:
              requestBody:  # contents of the callback message
                required: true
                content:
                  application/json:
                    schema:
                      $ref: '#/components/schemas/EventNotification'
              responses:
                '204':
                  description: No Content (successful notification)
                '307':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/307'
                '308':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/308'
                '400':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/400'
                '401':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/401'
                '403':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/403'
                '404':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/404'
                '411':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/411'
                '413':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/413'
                '415':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/415'
                '429':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/429'
                '500':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/500'
                '503':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/503'
                default:
                  $ref: 'TS29122_CommonData.yaml#/components/responses/default'
      responses:
        '201':
          description: Created (Successful creation of subscription)
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/EventSubscription'
          headers:
            Location:
              description: >
                Contains the URI of the newly created resource, according to the structure
                {apiRoot}/capif-events/v1/{subscriberId}/subscriptions/{subscriptionId}
              required: true
              schema:
                type: string
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
```

```
        '411':
          $ref: 'TS29122_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29122_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29122_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'

  /{subscriberId}/subscriptions/{subscriptionId}:
    delete:
      description: Deletes an individual CAPIF Event Subscription.
      parameters:
        - name: subscriberId
          in: path
          description: Identifier of the Subscriber
          required: true
          schema:
            type: string
        - name: subscriptionId
          in: path
          description: Identifier of an individual Events Subscription
          required: true
          schema:
            type: string
      responses:
        '204':
          description: >
            The individual CAPIF Events Subscription matching the subscriptionId is deleted.
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'

    put:
      description: Update of an existing individual CAPIF Event Subscription.
      parameters:
        - name: subscriberId
          in: path
          description: Identifier of the Subscriber
          required: true
          schema:
            type: string
        - name: subscriptionId
          in: path
          description: Identifier of the individual Subscriber
          required: true
          schema:
            type: string
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/EventSubscription'
      responses:
```

```
      '200':
        description: OK (Successful update of the subscription).
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/EventSubscription'
      '204':
        description: No Content
      '400':
        $ref: 'TS29122_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29122_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29122_CommonData.yaml#/components/responses/404'
      '411':
        $ref: 'TS29122_CommonData.yaml#/components/responses/411'
      '413':
        $ref: 'TS29122_CommonData.yaml#/components/responses/413'
      '415':
        $ref: 'TS29122_CommonData.yaml#/components/responses/415'
      '429':
        $ref: 'TS29122_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29122_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29122_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29122_CommonData.yaml#/components/responses/default'

  patch:
    description: Modification of an existing individual CAPIF Event Subscription.
    parameters:
      - name: subscriberId
        in: path
        description: Identifier of the Subscriber
        required: true
        schema:
          type: string
      - name: subscriptionId
        in: path
        description: Identifier of the individual Subscriber
        required: true
        schema:
          type: string
    requestBody:
      required: true
      content:
        application/merge-patch+json:
          schema:
            $ref: '#/components/schemas/EventSubscriptionPatch'
    responses:
      '200':
        description: OK (Successful update of the subscription)
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/EventSubscription'
      '204':
        description: No Content
      '400':
        $ref: 'TS29122_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29122_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29122_CommonData.yaml#/components/responses/404'
      '411':
        $ref: 'TS29122_CommonData.yaml#/components/responses/411'
      '413':
        $ref: 'TS29122_CommonData.yaml#/components/responses/413'
      '415':
        $ref: 'TS29122_CommonData.yaml#/components/responses/415'
      '429':
        $ref: 'TS29122_CommonData.yaml#/components/responses/429'
      '500':
```

```
        $ref: 'TS29122_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29122_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29122_CommonData.yaml#/components/responses/default'

components:
  schemas:
    EventSubscription:
      type: object
      description: Represents an individual CAPIF Event Subscription resource.
      properties:
        events:
          type: array
          items:
            $ref: '#/components/schemas/CAPIFEvent'
          minItems: 1
          description: Subscribed events
        eventFilters:
          type: array
          items:
            $ref: '#/components/schemas/CAPIFEventFilter'
          minItems: 1
          description: Subscribed event filters
        eventReq:
          $ref: 'TS29523_Npcf_EventExposure.yaml#/components/schemas/ReportingInformation'
        notificationDestination:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Uri'
        requestTestNotification:
          type: boolean
          description: >
            Set to true by Subscriber to request the CAPIF core function to send a
            test notification as defined in in clause 7.6. Set to false or omitted otherwise.
        websockNotifConfig:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/WebsockNotifConfig'
        supportedFeatures:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - events
        - notificationDestination

    EventNotification:
      type: object
      description: Represents an individual CAPIF Event notification.
      properties:
        subscriptionId:
          type: string
          description: >
            Identifier of the subscription resource to which the notification
            is related – CAPIF resource identifier
        events:
          $ref: '#/components/schemas/CAPIFEvent'
        eventDetail:
          $ref: '#/components/schemas/CAPIFEventDetail'
      required:
        - subscriptionId
        - events

    CAPIFEventFilter:
      type: object
      description: Represents a CAPIF event filter.
      properties:
        apiIds:
          type: array
          items:
            type: string
          minItems: 1
          description: Identifier of the service API
        apiInvokerIds:
          type: array
          items:
            type: string
          minItems: 1
          description: Identity of the API invoker
        aefIds:
          type: array
          items:
            type: string
```

```
          minItems: 1
          description: Identifier of the API exposing function

    CAPIFEventDetail:
      type: object
      description: Represents a CAPIF event details.
      properties:
        serviceAPIDescriptions:
          type: array
          items:
            $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/ServiceAPIDescription'
          minItems: 1
          description: Description of the service API as published by the APF.
        apiIds:
          type: array
          items:
            type: string
          minItems: 1
          description: Identifier of the service API
        apiInvokerIds:
          type: array
          items:
            type: string
          minItems: 1
          description: Identity of the API invoker
        accCtrlPolList:
          $ref: '#/components/schemas/AccessControlPolicyListExt'
        invocationLogs:
          type: array
          items:
            $ref: 'TS29222_CAPIF_Logging_API_Invocation_API.yaml#/components/schemas/InvocationLog'
          minItems: 1
          description: Invocation logs.
        apiTopoHide:
          $ref: '#/components/schemas/TopologyHiding'

    AccessControlPolicyListExt:
      description: Represents the extension for access control policies.
      allOf:
        - $ref:
'TS29222_CAPIF_Access_Control_Policy_API.yaml#/components/schemas/AccessControlPolicyList'
        - type: object
          properties:
            apiId:
              type: string
      required:
        - apiId

    TopologyHiding:
      type: object
      description: Represents the routing rules information of a service API.
      properties:
        apiId:
          type: string
        routingRules:
          type: array
          items:
            $ref: 'TS29222_CAPIF_Routing_Info_API.yaml#/components/schemas/RoutingRule'
          minItems: 1
      required:
        - apiId
        - routingRules

    EventSubscriptionPatch:
      type: object
      description: >
        Represents the parameters to request the updated of an individual CAPIF Event
        Subscription resource.
      properties:
        events:
          type: array
          items:
            $ref: '#/components/schemas/CAPIFEvent'
          minItems: 1
          description: Subscribed events
        eventFilters:
          type: array
          items:
```

```
            $ref: '#/components/schemas/CAPIFEventFilter'
          minItems: 1
          description: Subscribed event filters
        eventReq:
          $ref: 'TS29523_Npcf_EventExposure.yaml#/components/schemas/ReportingInformation'
        notificationDestination:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Uri'

    CAPIFEvent:
      anyOf:
      - type: string
        enum:
          - SERVICE_API_AVAILABLE
          - SERVICE_API_UNAVAILABLE
          - SERVICE_API_UPDATE
          - API_INVOKER_ONBOARDED
          - API_INVOKER_OFFBOARDED
          - SERVICE_API_INVOCATION_SUCCESS
          - SERVICE_API_INVOCATION_FAILURE
          - ACCESS_CONTROL_POLICY_UPDATE
          - ACCESS_CONTROL_POLICY_UNAVAILABLE
          - API_INVOKER_AUTHORIZATION_REVOKED
          - API_INVOKER_UPDATED
          - API_TOPOLOGY_HIDING_CREATED
          - API_TOPOLOGY_HIDING_REVOKED
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Describes the CAPIF event.
        Possible values are:
        - SERVICE_API_AVAILABLE:
          Events related to the availability of service APIs after the service APIs are
          published.
        - SERVICE_API_UNAVAILABLE:
          Events related to the unavailability of service APIs after the service APIs are
          unpublished.
        - SERVICE_API_UPDATE: Events related to change in service API information.
        - API_INVOKER_ONBOARDED: Events related to API invoker onboarded to CAPIF.
        - API_INVOKER_OFFBOARDED: Events related to API invoker offboarded from CAPIF.
        - SERVICE_API_INVOCATION_SUCCESS:
          Events related to the successful invocation of service APIs.
        - SERVICE_API_INVOCATION_FAILURE: Events related to the failed invocation of service APIs.
        - ACCESS_CONTROL_POLICY_UPDATE:
          Events related to the update for the access control policy related to the service APIs.
        - ACCESS_CONTROL_POLICY_UNAVAILABLE:
          Events related to the unavailability of the access control policy related to
          the service APIs.
        - API_INVOKER_AUTHORIZATION_REVOKED: Events related to the revocation of the authorization
          of API invokers to access the service APIs.
        - API_INVOKER_UPDATED: Events related to API invoker profile updated to CAPIF.
        - API_TOPOLOGY_HIDING_CREATED:
          Events related to the creation or update of the API topology hiding
          information of the service APIs after the service APIs are published.
        - API_TOPOLOGY_HIDING_REVOKED:
          Events related to the revocation of the API topology hiding information of
          the service APIs after the service APIs are unpublished.
```

A.5 CAPIF_API_Invoker_Management_API

```
openapi: 3.0.0

info:
  title: CAPIF_API_Invoker_Management_API
  description: |
    API for API invoker management.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
  version: "1.3.0"

externalDocs:
  description: 3GPP TS 29.222 V18.6.0 Common API Framework for 3GPP Northbound APIs
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.222/
```

```
servers:
  - url: '{apiRoot}/api-invoker-management/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 7.5 of 3GPP TS 29.222

paths:
  /onboardedInvokers:
    post:
      description: Creates a new individual API Invoker profile.
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/APIInvokerEnrolmentDetails'
      callbacks:
        notificationDestination:
          '{$request.body#/notificationDestination}':
            post:
              description: Notify the API Invoker about the onboarding completion
              requestBody:  # contents of the callback message
                required: true
                content:
                  application/json:
                    schema:
                      $ref: '#/components/schemas/OnboardingNotification'
              responses:
                '204':
                  description: No Content (successful onboarding notification)
                '307':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/307'
                '308':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/308'
                '400':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/400'
                '401':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/401'
                '403':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/403'
                '404':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/404'
                '411':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/411'
                '413':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/413'
                '415':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/415'
                '429':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/429'
                '500':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/500'
                '503':
                  $ref: 'TS29122_CommonData.yaml#/components/responses/503'
                default:
                  $ref: 'TS29122_CommonData.yaml#/components/responses/default'
      responses:
        '201':
          description: API invoker on-boarded successfully.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/APIInvokerEnrolmentDetails'
          headers:
            Location:
              description: >
                Contains the URI of the newly created resource, according to the structure
                {apiRoot}/api-invoker-management/v1/onboardedInvokers/{onboardingId}
              required: true
              schema:
                type: string
        '202':
          description: The CAPIF core has accepted the Onboarding request and is processing it.
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
```

```
        $ref: 'TS29122_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29122_CommonData.yaml#/components/responses/404'
      '411':
        $ref: 'TS29122_CommonData.yaml#/components/responses/411'
      '413':
        $ref: 'TS29122_CommonData.yaml#/components/responses/413'
      '415':
        $ref: 'TS29122_CommonData.yaml#/components/responses/415'
      '429':
        $ref: 'TS29122_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29122_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29122_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29122_CommonData.yaml#/components/responses/default'

/onboardedInvokers/{onboardingId}:
  delete:
    description: Deletes an individual API Invoker.
    parameters:
      - name: onboardingId
        in: path
        description: String identifying an individual on-boarded API invoker resource
        required: true
        schema:
          type: string
    responses:
      '204':
        description: The individual API Invoker matching onboardingId was offboarded.
      '307':
        $ref: 'TS29122_CommonData.yaml#/components/responses/307'
      '308':
        $ref: 'TS29122_CommonData.yaml#/components/responses/308'
      '400':
        $ref: 'TS29122_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29122_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29122_CommonData.yaml#/components/responses/404'
      '429':
        $ref: 'TS29122_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29122_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29122_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29122_CommonData.yaml#/components/responses/default'
  put:
    description: Updates an individual API invoker details.
    parameters:
      - name: onboardingId
        in: path
        description: String identifying an individual on-boarded API invoker resource
        required: true
        schema:
          type: string
    requestBody:
      description: representation of the API invoker details to be updated in CAPIF core function
      required: true
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/APIInvokerEnrolmentDetails'
    callbacks:
      notificationDestination:
        '{$request.body#/notificationDestination}':
          post:
            description: Notify the API Invoker about the API invoker update completion
            requestBody:  # contents of the callback message
              required: true
              content:
                application/json:
```

```
                schema:
                  $ref: '#/components/schemas/OnboardingNotification'
          responses:
            '204':
              description: No Content (successful API invoker update notification)
            '307':
              $ref: 'TS29122_CommonData.yaml#/components/responses/307'
            '308':
              $ref: 'TS29122_CommonData.yaml#/components/responses/308'
            '400':
              $ref: 'TS29122_CommonData.yaml#/components/responses/400'
            '401':
              $ref: 'TS29122_CommonData.yaml#/components/responses/401'
            '403':
              $ref: 'TS29122_CommonData.yaml#/components/responses/403'
            '404':
              $ref: 'TS29122_CommonData.yaml#/components/responses/404'
            '411':
              $ref: 'TS29122_CommonData.yaml#/components/responses/411'
            '413':
              $ref: 'TS29122_CommonData.yaml#/components/responses/413'
            '415':
              $ref: 'TS29122_CommonData.yaml#/components/responses/415'
            '429':
              $ref: 'TS29122_CommonData.yaml#/components/responses/429'
            '500':
              $ref: 'TS29122_CommonData.yaml#/components/responses/500'
            '503':
              $ref: 'TS29122_CommonData.yaml#/components/responses/503'
            default:
              $ref: 'TS29122_CommonData.yaml#/components/responses/default'
    responses:
      '200':
        description: API invoker details updated successfully.
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/APIInvokerEnrolmentDetails'
      '202':
        description: >
          The CAPIF core has accepted the API invoker update details request and is processing it.
      '204':
        description: >
          API invoker's information updated successfully, with no content to be
          sent in the response body.
      '307':
        $ref: 'TS29122_CommonData.yaml#/components/responses/307'
      '308':
        $ref: 'TS29122_CommonData.yaml#/components/responses/308'
      '400':
        $ref: 'TS29122_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29122_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29122_CommonData.yaml#/components/responses/404'
      '411':
        $ref: 'TS29122_CommonData.yaml#/components/responses/411'
      '413':
        $ref: 'TS29122_CommonData.yaml#/components/responses/413'
      '415':
        $ref: 'TS29122_CommonData.yaml#/components/responses/415'
      '429':
        $ref: 'TS29122_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29122_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29122_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29122_CommonData.yaml#/components/responses/default'
  patch:
    description: Modify an individual API invoker details.
    operationId: ModifyIndApiInvokeEnrolment
    tags:
      - Individual API Invoker enrolment details
    parameters:
      - name: onboardingId
```

```
          in: path
          required: true
          schema:
            type: string
      requestBody:
        required: true
        content:
          application/merge-patch+json:
            schema:
              $ref: '#/components/schemas/APIInvokerEnrolmentDetailsPatch'
      responses:
        '200':
          description: >
            The definition of the service API is modified successfully and a
            representation of the updated service API is returned in the request body.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/APIInvokerEnrolmentDetails'
        '202':
          description: The request is accepted and under processing.
        '204':
          description: No Content. The definition of the service API is modified successfully.
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29122_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29122_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29122_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'
components:
  schemas:
    OnboardingInformation:
      type: object
      description: Represents on-boarding information of the API invoker.
      properties:
        apiInvokerPublicKey:
          type: string
          description: The API Invoker's public key
        apiInvokerCertificate:
          type: string
          description: >
            The API Invoker's generic client certificate, provided by the CAPIF core function.
        onboardingSecret:
          type: string
          description: >
            The API Invoker's onboarding secret, provided by the CAPIF core function.
      required:
        - apiInvokerPublicKey

    APIList:
      type: object
      description: Represents a list of APIs.
      properties:
        serviceAPIDescriptions:
          type: array
          items:
            $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/ServiceAPIDescription'
          minItems: 1
```

```
          description: Represents the list of service APIs that the API Invoker is allowed to
invoke.

    APIInvokerEnrolmentDetails:
      type: object
      properties:
        apiInvokerId:
          type: string
          description: >
            API invoker ID assigned by the CAPIF core function to the API invoker while
            on-boarding the API invoker. Shall not be present in the HTTP POST request
            from the API invoker to the CAPIF core function, to on-board itself. Shall be
            present in all other HTTP requests and responses.
          readOnly: true
        onboardingInformation:
          $ref: '#/components/schemas/OnboardingInformation'
        notificationDestination:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Uri'
        requestTestNotification:
          type: boolean
          description: >
            Set to true by Subscriber to request the CAPIF core function to send a
            test notification as defined in in clause 7.6. Set to false or omitted otherwise.
        websockNotifConfig:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/WebsockNotifConfig'
        apiList:
          $ref: '#/components/schemas/APIList'
        apiInvokerInformation:
          type: string
          description: >
             Generic information related to the API invoker such as details of
             the device or the application.
        expTime:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/DateTime'
        supportedFeatures:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - onboardingInformation
        - notificationDestination
      description: Represents information about the API Invoker that requested to onboard.

    OnboardingNotification:
      type: object
      description: Represents a notification of on-boarding or update result.
      properties:
        result:
          type: boolean
          description: Set to "true" indicate successful on-boarding. Otherwise set to "false"
        resourceLocation:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Uri'
        apiInvokerEnrolmentDetails:
          $ref: '#/components/schemas/APIInvokerEnrolmentDetails'
        apiList:
          $ref: '#/components/schemas/APIList'
      required:
        - result

    APIInvokerEnrolmentDetailsPatch:
      type: object
      description: Represents an API Invoker's enrolment details to be updated.
      properties:
        onboardingInformation:
          $ref: '#/components/schemas/OnboardingInformation'
        notificationDestination:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Uri'
        apiList:
          $ref: '#/components/schemas/APIList'
        apiInvokerInformation:
          type: string
          description: >
            Generic information related to the API invoker such as details of
            the device or the application.
        expTime:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/DateTimeRm'
```

A.6 CAPIF_Security_API

```
openapi: 3.0.0

info:
  title: CAPIF_Security_API
  description: |
    API for CAPIF security management.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
  version: "1.3.0"

externalDocs:
  description: 3GPP TS 29.222 V18.6.0 Common API Framework for 3GPP Northbound APIs
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.222/

servers:
  - url: '{apiRoot}/capif-security/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 7.5 of 3GPP TS 29.222.

paths:
  /trustedInvokers/{apiInvokerId}:
    get:
      parameters:
        - name: apiInvokerId
          in: path
          description: Identifier of an individual API invoker
          required: true
          schema:
            type: string
        - name: authenticationInfo
          in: query
          description: >
            When set to 'true', it indicates the CAPIF core function to send the
            authentication information of the API invoker. Set to false or omitted otherwise.
          schema:
            type: boolean
        - name: authorizationInfo
          in: query
          description: >
            When set to 'true', it indicates the CAPIF core function to send the
            authorization information of the API invoker. Set to false or omitted otherwise.
          schema:
            type: boolean
      responses:
        '200':
          description: >
            The security related information of the API Invoker based on the request
            from the API exposing function.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/ServiceSecurity'
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29122_CommonData.yaml#/components/responses/406'
        '414':
          $ref: 'TS29122_CommonData.yaml#/components/responses/414'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
```

```
        $ref: 'TS29122_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29122_CommonData.yaml#/components/responses/default'
  put:
    parameters:
      - name: apiInvokerId
        in: path
        description: Identifier of an individual API invoker
        required: true
        schema:
          type: string
    requestBody:
      description: create a security context for an API invoker
      required: true
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/ServiceSecurity'
    callbacks:
      notificationDestination:
        '{$request.body#/notificationDestination}':
          post:
            requestBody:
              required: true
              content:
                application/json:
                  schema:
                    $ref: '#/components/schemas/SecurityNotification'
            responses:
              '204':
                description: No Content (successful notification)
              '307':
                $ref: 'TS29122_CommonData.yaml#/components/responses/307'
              '308':
                $ref: 'TS29122_CommonData.yaml#/components/responses/308'
              '400':
                $ref: 'TS29122_CommonData.yaml#/components/responses/400'
              '401':
                $ref: 'TS29122_CommonData.yaml#/components/responses/401'
              '403':
                $ref: 'TS29122_CommonData.yaml#/components/responses/403'
              '404':
                $ref: 'TS29122_CommonData.yaml#/components/responses/404'
              '411':
                $ref: 'TS29122_CommonData.yaml#/components/responses/411'
              '413':
                $ref: 'TS29122_CommonData.yaml#/components/responses/413'
              '415':
                $ref: 'TS29122_CommonData.yaml#/components/responses/415'
              '429':
                $ref: 'TS29122_CommonData.yaml#/components/responses/429'
              '500':
                $ref: 'TS29122_CommonData.yaml#/components/responses/500'
              '503':
                $ref: 'TS29122_CommonData.yaml#/components/responses/503'
              default:
                $ref: 'TS29122_CommonData.yaml#/components/responses/default'
    responses:
      '201':
        description: Successful created.
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ServiceSecurity'
        headers:
          Location:
            description: >
              Contains the URI of the newly created resource, according to the structure
              {apiRoot}/capif-security/v1/trustedInvokers/{apiInvokerId}
            required: true
            schema:
              type: string
      '400':
        $ref: 'TS29122_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29122_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
```

```
        '411':
          $ref: 'TS29122_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29122_CommonData.yaml#/components/responses/413'
        '414':
          $ref: 'TS29122_CommonData.yaml#/components/responses/414'
        '415':
          $ref: 'TS29122_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'
    delete:
      parameters:
        - name: apiInvokerId
          in: path
          description: Identifier of an individual API invoker
          required: true
          schema:
            type: string
      responses:
        '204':
          description: No Content (Successful deletion of the existing subscription)
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'
  /trustedInvokers/{apiInvokerId}/update:
    post:
      parameters:
        - name: apiInvokerId
          in: path
          description: Identifier of an individual API invoker
          required: true
          schema:
            type: string
      requestBody:
        description: Update the security context (e.g. re-negotiate the security methods).
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/ServiceSecurity'
      responses:
        '200':
          description: Successful updated.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/ServiceSecurity'
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
```

```
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29122_CommonData.yaml#/components/responses/404'
      '411':
        $ref: 'TS29122_CommonData.yaml#/components/responses/411'
      '413':
        $ref: 'TS29122_CommonData.yaml#/components/responses/413'
      '415':
        $ref: 'TS29122_CommonData.yaml#/components/responses/415'
      '429':
        $ref: 'TS29122_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29122_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29122_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29122_CommonData.yaml#/components/responses/default'

/trustedInvokers/{apiInvokerId}/delete:
  post:
    parameters:
      - name: apiInvokerId
        in: path
        description: Identifier of an individual API invoker
        required: true
        schema:
          type: string
    requestBody:
      description: Revoke the authorization of the API invoker for APIs.
      required: true
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/SecurityNotification'
    responses:
      '204':
        description: Successful revoked.
      '307':
        $ref: 'TS29122_CommonData.yaml#/components/responses/307'
      '308':
        $ref: 'TS29122_CommonData.yaml#/components/responses/308'
      '400':
        $ref: 'TS29122_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29122_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29122_CommonData.yaml#/components/responses/404'
      '411':
        $ref: 'TS29122_CommonData.yaml#/components/responses/411'
      '413':
        $ref: 'TS29122_CommonData.yaml#/components/responses/413'
      '415':
        $ref: 'TS29122_CommonData.yaml#/components/responses/415'
      '429':
        $ref: 'TS29122_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29122_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29122_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29122_CommonData.yaml#/components/responses/default'

/securities/{securityId}/token:
  post:
    parameters:
      - name: securityId
        in: path
        description: Identifier of an individual API invoker
        required: true
        schema:
          type: string
    requestBody:
      required: true
      content:
        application/x-www-form-urlencoded:
```

```
            schema:
              $ref: '#/components/schemas/AccessTokenReq'
      responses:
        '200':
          description: Successful Access Token Request
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/AccessTokenRsp'
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          description: Error in the Access Token Request
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/AccessTokenErr'
        '401':
          description: Unauthorized
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/AccessTokenErr'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'

components:
  schemas:
    ServiceSecurity:
      type: object
      description: >
        Represents the details of the security method for each service API interface.
        When included by the API invoker, it indicates the preferred method of security.
        When included by the CAPIF core function, it indicates the security method to be
        used for the service API interface.
      properties:
        securityInfo:
          type: array
          items:
            $ref: '#/components/schemas/SecurityInformation'
          minimum: 1
        notificationDestination:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Uri'
        requestTestNotification:
          type: boolean
          description: >
            Set to true by API invoker to request the CAPIF core function to send a
            test notification as defined in in clause 7.6. Set to false or omitted otherwise.
        websockNotifConfig:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/WebsockNotifConfig'
        supportedFeatures:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - securityInfo
        - notificationDestination

    SecurityInformation:
      type: object
      description: Represents the interface details and the security method.
      properties:
```

```
      interfaceDetails:
        $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/InterfaceDescription'
      aefId:
        type: string
        description: Identifier of the API exposing function
      apiId:
        type: string
        description: API identifier
      prefSecurityMethods:
        type: array
        items:
          $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/SecurityMethod'
        minItems: 1
        description: Security methods preferred by the API invoker for the API interface.
      selSecurityMethod:
        $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/SecurityMethod'
      authenticationInfo:
        type: string
        description: Authentication related information
      authorizationInfo:
        type: string
        description: Authorization related information
      grantType:
        type: array
        items:
          $ref: '#/components/schemas/OAuthGrantType'
        minItems: 1
    required:
      - prefSecurityMethods
    oneOf:
      - required: [interfaceDetails]
      - required: [aefId]

  SecurityNotification:
    type: object
    description: Represents the revoked authorization notification details.
    properties:
      apiInvokerId:
        type: string
        description: String identifying the API invoker assigned by the CAPIF core function.
      aefId:
        type: string
        description: String identifying the AEF.
      apiIds:
        type: array
        items:
          type: string
        minItems: 1
        description: Identifier of the service API
      cause:
        $ref: '#/components/schemas/Cause'
    required:
      - apiInvokerId
      - apiIds
      - cause

  AccessTokenReq:
    format: x-www-form-urlencoded
    description: Represents the access token request information.
    properties:
      grant_type:
        type: string
        enum:
          - client_credentials
          - authorization_code
      client_id:
        type: string
      resOwnerId:
        $ref: '#/components/schemas/ResOwnerId'
      client_secret:
        type: string
      scope:
        type: string
      authCode:
        type: string
      redirect_uri:
        type: string
    required:
```

```
      - grant_type
      - client_id

    AccessTokenRsp:
      type: object
      description: Represents the access token response information.
      properties:
        access_token:
          type: string
          description: >
            JWS Compact Serialized representation of JWS signed JSON object (AccessTokenClaims)
        token_type:
          type: string
          enum:
            - Bearer
        expires_in:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/DurationSec'
        scope:
          type: string
      required:
        - access_token
        - token_type
        - expires_in

    AccessTokenClaims:
      type: object
      description: Represents the claims data structure for the access token.
      properties:
        iss:
          type: string
        scope:
          type: string
        exp:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/DurationSec'
        resOwnerId:
          $ref: '#/components/schemas/ResOwnerId'
      required:
        - iss
        - scope
        - exp

    ResOwnerId:
      type: object
      description: >
        Represents the identifier of the resource owner.
      properties:
        gpsi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
      anyOf:
        - required: [gpsi]

    AccessTokenErr:
      type: object
      description: Represents an error in the access token request.
      properties:
        error:
          type: string
          enum:
            - invalid_request
            - invalid_client
            - invalid_grant
            - unauthorized_client
            - unsupported_grant_type
            - invalid_scope
        error_description:
          type: string
        error_uri:
          type: string
      required:
        - error

    Cause:
      anyOf:
      - type: string
        enum:
          - OVERLIMIT_USAGE
          - UNEXPECTED_REASON
          - AUTHORIZATION_ISSUE
```

```
          - OTHER_REASON
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: |
        Indicates the cause for revoking the API invoker's authorization to the service API.
        Possible values are:
        - OVERLIMIT_USAGE:
            The revocation of the authorization of the API invoker is due to the overlimit
            usage of the service API
        - UNEXPECTED_REASON:
            The revocation of the authorization of the API invoker is due to unexpected reason.
        - AUTHORIZATION_ISSUE:
            The revocation of the authorization of the API invoker is due to API Invoker
            not being authorized anymore by the API Provider.
        - OTHER_REASON:
            The revocation of the authorization of the API invoker is due to other reason.

    OAuthGrantType:
      anyOf:
      - type: string
        enum:
          - CLIENT_CREDENTIALS
          - AUTHORIZATION_CODE
          - AUTHORIZATION_CODE_WITH_PKCE
      - type: string
        description: >
          This string provides forward-compatibility with future extensions to the enumeration and
          is not used to encode content defined in the present version of this API.
      description: |
        Indicates the supported authorization flow (e.g. client credentials flow, authorization code
         flow, etc.) to the API invoker.
        Possible values are:
        - CLIENT_CREDENTIALS: Indicate that the grant type is is client credentials flow.
        - AUTHORIZATION_CODE: Indicate that the grant type is authorization code.
        - AUTHORIZATION_CODE_WITH_PKCE: Indicate that the grant type is authorization code with
PKCE.
```

A.7 CAPIF_Access_Control_Policy_API

```
openapi: 3.0.0

info:
  title: CAPIF_Access_Control_Policy_API
  description: |
    API for access control policy.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
  version: "1.3.0"

externalDocs:
  description: 3GPP TS 29.222 V18.6.0 Common API Framework for 3GPP Northbound APIs
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.222/

servers:
  - url: '{apiRoot}/access-control-policy/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 7.5 of 3GPP TS 29.222

paths:
  /accessControlPolicyList/{serviceApiId}:
    get:
      description: Retrieves the access control policy list.
      parameters:
        - name: serviceApiId
          in: path
          description: Identifier of a published service API
          required: true
          schema:
            type: string
        - name: aef-id
```

```
          in: query
          required: true
          description: Identifier of the AEF
          schema:
            type: string
        - name: api-invoker-id
          in: query
          description: Identifier of the API invoker
          schema:
            type: string
        - name: supported-features
          in: query
          description: To filter irrelevant responses related to unsupported features
          schema:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      responses:
        '200':
          description: OK.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/AccessControlPolicyList'
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29122_CommonData.yaml#/components/responses/406'
        '414':
          $ref: 'TS29122_CommonData.yaml#/components/responses/414'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'

components:
  schemas:
    AccessControlPolicyList:
      type: object
      description: Represents the access control policy list for a published service API.
      properties:
        apiInvokerPolicies:
          type: array
          items:
            $ref: '#/components/schemas/ApiInvokerPolicy'
          minItems: 0
          description: Policy of each API invoker.

    ApiInvokerPolicy:
      type: object
      description: Represents the policy of an API Invoker.
      properties:
        apiInvokerId:
          type: string
          description: API invoker ID assigned by the CAPIF core function
        allowedTotalInvocations:
          type: integer
          description: Total number of invocations allowed on the service API by the API invoker.
        allowedInvocationsPerSecond:
          type: integer
          description: Invocations per second allowed on the service API by the API invoker.
        allowedInvocationTimeRangeList:
          type: array
          items:
            $ref: '#/components/schemas/TimeRangeList'
          minItems: 0
```

```
          description: >
            The time ranges during which the invocations are allowed on the service API
            by the API invoker.
      required:
        - apiInvokerId

    TimeRangeList:
      type: object
      description: >
        Represents the time range during which the invocation of a service API is allowed
        by the API invoker.
      properties:
        startTime:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/DateTime'
        stopTime:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/DateTime'
```

A.8 CAPIF_Logging_API_Invocation_API

```
openapi: 3.0.0

info:
  title: CAPIF_Logging_API_Invocation_API
  description: |
    API for invocation logs.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
  version: "1.3.0"

externalDocs:
  description: 3GPP TS 29.222 V18.6.0 Common API Framework for 3GPP Northbound APIs
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.222/

servers:
  - url: '{apiRoot}/api-invocation-logs/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 7.5 of 3GPP TS 29.222

paths:
  /{aefId}/logs:
    post:
      description: Creates a new log entry for service API invocations.
      parameters:
        - name: aefId
          in: path
          description: Identifier of the API exposing function
          required: true
          schema:
            type: string
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/InvocationLog'
      responses:
        '201':
          description: >
            Log of service API invocations provided by API exposing function successfully
            stored on the CAPIF core function.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/InvocationLog'
          headers:
            Location:
              description: >
                Contains the URI of the newly created resource, according to the structure
                {apiRoot}/api-invocation-logs/v1/{aefId}/logs/{logId}
              required: true
              schema:
                type: string
        '400':
```

```
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29122_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29122_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29122_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'
  /{aefId}/logs/{logId}:
    description: Creates a new log entry for service API invocations.
    parameters:
      - name: aefId
        in: path
        description: Identifier of the API exposing function
        required: true
        schema:
          type: string
      - name: logId
        in: path
        description: Identifier of individual log entry
        required: true
        schema:
          type: string
components:
  schemas:
    InvocationLog:
      type: object
      description: >
        Represents a set of Service API invocation logs to be stored in a CAPIF core function.
      properties:
        aefId:
          type: string
          description: >
            Identity information of the API exposing function requesting logging of
            service API invocations
        apiInvokerId:
          type: string
          description: Identity of the API invoker which invoked the service API
        logs:
          type: array
          items:
            $ref: '#/components/schemas/Log'
          minItems: 1
          description: Service API invocation log
        supportedFeatures:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - aefId
        - apiInvokerId
        - logs

    Log:
      type: object
      description: Represents an individual service API invocation log entry.
      properties:
        apiId:
          type: string
          description: String identifying the API invoked.
        apiName:
          type: string
          description: >
            Name of the API which was invoked, it is set as {apiName} part of the URI
            structure as defined in clause 5.2.4 of 3GPP TS 29.122.
        apiVersion:
          type: string
```

```
          description: Version of the API which was invoked
        resourceName:
          type: string
          description: Name of the specific resource invoked
        uri:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Uri'
        protocol:
          $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/Protocol'
        operation:
          $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/Operation'
        result:
          type: string
          description: For HTTP protocol, it contains HTTP status code of the invocation
        invocationTime:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/DateTime'
        invocationLatency:
          $ref: '#/components/schemas/DurationMs'
        inputParameters:
          description: >
            List of input parameters. Can be any value - string, number, boolean, array or object.
        outputParameters:
          description: >
            List of output parameters. Can be any value - string, number, boolean, array or object.
        srcInterface:
          $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/InterfaceDescription'
        destInterface:
          $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/InterfaceDescription'
        fwdInterface:
          type: string
          description: >
            It includes the node identifier (as defined in IETF RFC 7239 of all forwarding
            entities between the API invoker and the AEF, concatenated with comma and space,
            e.g. 192.0.2.43:80, unknown:_OBFport, 203.0.113.60
      required:
        - apiId
        - apiName
        - apiVersion
        - resourceName
        - protocol
        - result

    DurationMs:
      type: integer
      description: Represents a period of time in units of milliseconds.
      minimum: 0
```

A.9 CAPIF_Auditing_API

```
openapi: 3.0.0

info:
  title: CAPIF_Auditing_API
  description: |
    API for auditing.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
  version: "1.3.0"

externalDocs:
  description: 3GPP TS 29.222 V18.6.0 Common API Framework for 3GPP Northbound APIs
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.222/

servers:
  - url: '{apiRoot}/logs/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 7.5 of 3GPP TS 29.222.

paths:
  /apiInvocationLogs:
    get:
      description: Query and retrieve service API invocation logs stored on the CAPIF core function.
      parameters:
        - name: aef-id
```

```
          in: query
          description: String identifying the API exposing function.
          schema:
            type: string
        - name: api-invoker-id
          in: query
          description: String identifying the API invoker which invoked the service API.
          schema:
            type: string
        - name: time-range-start
          in: query
          description: Start time of the invocation time range.
          schema:
            $ref: 'TS29122_CommonData.yaml#/components/schemas/DateTime'
        - name: time-range-end
          in: query
          description: End time of the invocation time range.
          schema:
            $ref: 'TS29122_CommonData.yaml#/components/schemas/DateTime'
        - name: api-id
          in: query
          description: String identifying the API invoked.
          schema:
            type: string
        - name: api-name
          in: query
          description: >
            API name, it is set as {apiName} part of the URI structure as defined in
            clause 5.2.4 of 3GPP TS 29.122.
          schema:
            type: string
        - name: api-version
          in: query
          description: Version of the API which was invoked.
          schema:
            type: string
        - name: protocol
          in: query
          description: Protocol invoked.
          schema:
            $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/Protocol'
        - name: operation
          in: query
          description: Operation that was invoked on the API.
          schema:
            $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/Operation'
        - name: result
          in: query
          description: Result or output of the invocation.
          schema:
            type: string
        - name: resource-name
          in: query
          description: Name of the specific resource invoked.
          schema:
            type: string
        - name: src-interface
          in: query
          description: Interface description of the API invoker.
          content:
            application/json:
              schema:
                $ref:
'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/InterfaceDescription'
        - name: dest-interface
          in: query
          description: Interface description of the API invoked.
          content:
            application/json:
              schema:
                $ref:
'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/InterfaceDescription'
        - name: supported-features
          in: query
          description: To filter irrelevant responses related to unsupported features
          schema:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      responses:
```

```
        '200':
          description: >
            Result of the query operation along with fetched service API invocation log data.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/InvocationLogsRetrieveRes'
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29122_CommonData.yaml#/components/responses/406'
        '414':
          $ref: 'TS29122_CommonData.yaml#/components/responses/414'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'

components:
  schemas:
    InvocationLogs:
      type: object
      description: >
        Represents several (more than one) invocation logs.
      properties:
        multipleInvocationLogs:
          type: array
          items:
            $ref: 'TS29222_CAPIF_Logging_API_Invocation_API.yaml#/components/schemas/InvocationLog'
          minItems: 1
        supportedFeatures:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - multipleInvocationLogs

    InvocationLogsRetrieveRes:
      description: >
        Represents the result of an invocation logs retrieval request.
      oneOf:
        - $ref: 'TS29222_CAPIF_Logging_API_Invocation_API.yaml#/components/schemas/InvocationLog'
        - $ref: '#/components/schemas/InvocationLogs'
```

A.10 AEF_Security_API

```
openapi: 3.0.0

info:
  title: AEF_Security_API
  description: |
    API for AEF security management.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
  version: "1.3.0"

externalDocs:
  description: 3GPP TS 29.222 V18.6.0 Common API Framework for 3GPP Northbound APIs
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.222/

servers:
  - url: '{apiRoot}/aef-security/v1'
```

```
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 7.5 of 3GPP TS 29.222.

paths:
  /check-authentication:
    post:
      summary: Check authentication.
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/CheckAuthenticationReq'
      responses:
        '200':
          description: The request was successful.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/CheckAuthenticationRsp'
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29122_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29122_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29122_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'

  /revoke-authorization:
    post:
      summary: Revoke authorization.
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/RevokeAuthorizationReq'
      responses:
        '200':
          description: The request was successful.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/RevokeAuthorizationRsp'
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '411':
```

```
          $ref: 'TS29122_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29122_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29122_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
         $ref: 'TS29122_CommonData.yaml#/components/responses/default'

components:
  schemas:
    CheckAuthenticationReq:
      type: object
      description: Represents authentication check request data.
      properties:
        apiInvokerId:
          type: string
          description: >
            API invoker ID assigned by the CAPIF core function to the API invoker
            while on-boarding the API invoker.
        supportedFeatures:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - apiInvokerId
        - supportedFeatures

    CheckAuthenticationRsp:
      type: object
      description: Represents authentication check response data.
      properties:
        supportedFeatures:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - supportedFeatures

    RevokeAuthorizationReq:
      type: object
      description: Represents authorization revocation request data.
      properties:
        revokeInfo:
          $ref: 'TS29222_CAPIF_Security_API.yaml#/components/schemas/SecurityNotification'
        supportedFeatures:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - revokeInfo
        - supportedFeatures

    RevokeAuthorizationRsp:
      type: object
      description: Represents authorization revocation response data.
      properties:
        supportedFeatures:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - supportedFeatures
```

A.11 CAPIF_API_Provider_Management_API

```
openapi: 3.0.0

info:
  title: CAPIF_API_Provider_Management_API
  description: |
    API for API provider domain functions management.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
  version: "1.2.0"

externalDocs:
  description: 3GPP TS 29.222 V18.6.0 Common API Framework for 3GPP Northbound APIs
```

```
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.222/

servers:
  - url: '{apiRoot}/api-provider-management/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 7.5 of 3GPP TS 29.222

paths:
  /registrations:
    post:
      description: Registers a new API Provider domain with API provider domain functions profiles.
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/APIProviderEnrolmentDetails'
      responses:
        '201':
          description: API provider domain registered successfully
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/APIProviderEnrolmentDetails'
          headers:
            Location:
              description: >
                Contains the URI of the newly created resource, according to the structure
                {apiRoot}/api-provider-management/v1/registrations/{registrationId}
              required: true
              schema:
                type: string
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29122_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29122_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29122_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'

  /registrations/{registrationId}:
    delete:
      description: Deregisters API provider domain by deleting API provider domain and functions.
      parameters:
        - name: registrationId
          in: path
          description: String identifying an registered API provider domain resource.
          required: true
          schema:
            type: string
      responses:
        '204':
          description: The API provider domain matching registrationId is deleted.
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
```

```
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29122_CommonData.yaml#/components/responses/404'
      '429':
        $ref: 'TS29122_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29122_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29122_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29122_CommonData.yaml#/components/responses/default'
  put:
    description: Updates an API provider domain's registration details.
    parameters:
      - name: registrationId
        in: path
        description: String identifying an registered API provider domain resource.
        required: true
        schema:
          type: string
    requestBody:
      description: >
        Representation of the API provider domain registration details to be updated
        in CAPIF core function.
      required: true
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/APIProviderEnrolmentDetails'
    responses:
      '200':
        description: API provider domain registration details updated successfully.
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/APIProviderEnrolmentDetails'
      '204':
        description: No Content
      '307':
        $ref: 'TS29122_CommonData.yaml#/components/responses/307'
      '308':
        $ref: 'TS29122_CommonData.yaml#/components/responses/308'
      '400':
        $ref: 'TS29122_CommonData.yaml#/components/responses/400'
      '401':
        $ref: 'TS29122_CommonData.yaml#/components/responses/401'
      '403':
        $ref: 'TS29122_CommonData.yaml#/components/responses/403'
      '404':
        $ref: 'TS29122_CommonData.yaml#/components/responses/404'
      '411':
        $ref: 'TS29122_CommonData.yaml#/components/responses/411'
      '413':
        $ref: 'TS29122_CommonData.yaml#/components/responses/413'
      '415':
        $ref: 'TS29122_CommonData.yaml#/components/responses/415'
      '429':
        $ref: 'TS29122_CommonData.yaml#/components/responses/429'
      '500':
        $ref: 'TS29122_CommonData.yaml#/components/responses/500'
      '503':
        $ref: 'TS29122_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29122_CommonData.yaml#/components/responses/default'
  patch:
    description: Modify an individual API provider details.
    operationId: ModifyIndApiProviderEnrolment
    tags:
      - Individual API Provider enrolment details
    parameters:
      - name: registrationId
        in: path
        required: true
        schema:
          type: string
    requestBody:
      required: true
```

```
        content:
          application/merge-patch+json:
            schema:
              $ref: '#/components/schemas/APIProviderEnrolmentDetailsPatch'
      responses:
        '200':
          description: >
            The definition of the service API is modified successfully and a
            representation of the updated service API is returned in the request body.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/APIProviderEnrolmentDetails'
        '204':
          description: No Content. The definition of the service API is modified successfully.
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29122_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29122_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29122_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'

components:
  schemas:
    APIProviderEnrolmentDetails:
      type: object
      description: Represents an API provider domain's enrolment details.
      properties:
        apiProvDomId:
          type: string
          description: >
            API provider domain ID assigned by the CAPIF core function to the API management
            function while registering the API provider domain. Shall not be present in the
            HTTP POST request from the API Management function to the CAPIF core function,
            to on-board itself. Shall be present in all other HTTP requests and responses.
          readOnly: true
        regSec:
          type: string
          description: >
            Security information necessary for the CAPIF core function to validate the
            registration of the API provider domain. Shall be present in HTTP POST request
            from API management function to CAPIF core function for API provider domain
            registration.
        apiProvFuncs:
          type: array
          items:
            $ref: '#/components/schemas/APIProviderFunctionDetails'
          minItems: 1
          description: >
            A list of individual API provider domain functions details. When included by
            the API management function in the HTTP request message, it lists the API
            provider domain functions that the API management function intends to
            register/update in registration or update registration procedure. When
            included by the CAPIF core function in the HTTP response message, it lists
            the API domain functions details that are registered or updated successfully.
        apiProvDomInfo:
          type: string
          description: >
```

```
            Generic information related to the API provider domain such as details
            of the API provider applications.
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
        failReason:
          type: string
          description: >
            Registration or update specific failure information of failed API provider
            domain function registrations.Shall be present in the HTTP response
            body if atleast one of the API provider domain function registration or update
            registration fails.
        apiProvName:
          type: string
          description: Represents the API provider name.
      required:
        - regSec

    APIProviderFunctionDetails:
      type: object
      description: Represents an API provider domain function's details.
      properties:
        apiProvFuncId:
          type: string
          description: >
            API provider domain functionID assigned by the CAPIF core function to the
            API provider domain function while registering/updating the API provider domain.
            Shall not be present in the HTTP POST request from the API management function to
            the CAPIF core function, to register itself. Shall be present in all other HTTP
            requests and responses.
        regInfo:
          $ref: '#/components/schemas/RegistrationInformation'
        apiProvFuncRole:
          $ref: '#/components/schemas/ApiProviderFuncRole'
        apiProvFuncInfo:
          type: string
          description: >
            Generic information related to the API provider domain function such as details
            of the API provider applications.
      required:
        - regInfo
        - apiProvFuncRole

    RegistrationInformation:
      type: object
      description: >
        Represents registration information of an individual API provider domain function.
      properties:
        apiProvPubKey:
          type: string
          description: Public Key of API Provider domain function.
        apiProvCert:
          type: string
          description: API provider domain function's client certificate
      required:
        - apiProvPubKey

    APIProviderEnrolmentDetailsPatch:
      type: object
      description: >
        Represents a list of modifications for the API provider domain's enrolment details.
      properties:
        apiProvFuncs:
          type: array
          items:
            $ref: '#/components/schemas/APIProviderFunctionDetails'
          minItems: 1
          description: >
            A list of individual API provider domain functions details. When included by
            the API management function in the HTTP request message, it lists the API
            provider domain functions that the API management function intends to
            register/update in registration or update registration procedure.
        apiProvDomInfo:
          type: string
          description: >
            Generic information related to the API provider domain such as details
            of the API provider applications.

# Simple data types and enumerations
```

```
    ApiProviderFuncRole:
      anyOf:
      - type: string
        enum:
          - AEF
          - APF
          - AMF
      - type: string
        description: >
          This string provides forward-compatiblity with future extensions to the enumeration
          but is not used to encode content defined in the present version of this API.
      description: |
        Indicates the role (e.g. AEF, APF, etc.) of an API provider domain function.
        Possible values are:
        - AEF: API provider function is API Exposing Function.
        - APF: API provider function is API Publishing Function.
        - AMF: API Provider function is API Management Function.
```

A.12 CAPIF_Routing_Info_API

```
openapi: 3.0.0

info:
  title: CAPIF_Routing_Info_API
  description: |
    API for Routing information.
    © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.
  version: "1.2.0"

externalDocs:
  description: 3GPP TS 29.222 V18.6.0 Common API Framework for 3GPP Northbound APIs
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.222/

servers:
  - url: '{apiRoot}/capif-routing-info/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 7.5 of 3GPP TS 29.222

paths:
  /service-apis/{serviceApiId}:
    get:
      description: Retrieves the API routing information.
      parameters:
        - name: serviceApiId
          in: path
          description: Identifier of a published service API
          required: true
          schema:
            type: string
        - name: aef-id
          in: query
          required: true
          description: Identifier of the AEF
          schema:
            type: string
        - name: supp-feat
          in: query
          required: false
          description: To filter irrelevant responses related to unsupported features
          schema:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      responses:
        '200':
          description: OK.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/RoutingInfo'
        '307':
          $ref: 'TS29122_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29122_CommonData.yaml#/components/responses/308'
```

```
        '400':
          $ref: 'TS29122_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29122_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29122_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29122_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29122_CommonData.yaml#/components/responses/406'
        '414':
          $ref: 'TS29122_CommonData.yaml#/components/responses/414'
        '429':
          $ref: 'TS29122_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29122_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29122_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29122_CommonData.yaml#/components/responses/default'

components:
  schemas:
    RoutingInfo:
      type: object
      description: Represents an API routing information.
      properties:
        routingRules:
          type: array
          items:
            $ref: '#/components/schemas/RoutingRule'
          minItems: 1
      required:
        - routingRules

    RoutingRule:
      type: object
      description: Represents an API routing rule.
      properties:
        ipv4AddrRanges:
          type: array
          items:
            $ref: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/Ipv4AddressRange'
          minItems: 1
        ipv6AddrRanges:
          type: array
          items:
            $ref: '#/components/schemas/Ipv6AddressRange'
          minItems: 1
        aefProfile:
          $ref: 'TS29222_CAPIF_Publish_Service_API.yaml#/components/schemas/AefProfile'
      required:
        - aefProfile

    Ipv6AddressRange:
      type: object
      description: Represents IPv6 address range.
      properties:
        start:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Ipv6Addr'
        end:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Ipv6Addr'
      required:
        - start
        - end
```

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2018-03	CT3#95	C3-181278				TS skeleton of Common API Framework for 3GPP Northbound APIs	0.0.0
2018-03	CT3#95	C3-181378				Inclusion of documents agreed in CT3#95: C3-181281, C3-181282, C3-181283, C3-181284, C3-181285, C3-181286, C3-181287, C3-181321, C3-181322, Rapporteur changes	0.1.0
2018-04	CT3#96	C3-182527				Inclusion of documents agreed in CT3#96: C3-182204, C3-182387, C3-182393, C3-182395, C3-182468, C3-182469, C3-182470, C3-182483, C3-182484, C3-182485	0.2.0
2018-05	CT3#97					Inclusion of documents agreed in CT3#97: C3-183271, C3-183274, C3-183275, C3-183372, C3-183376, C3-183377, C3-183378, C3-183379, C3-183598, C3-183599, C3-183602, C3-183603, C3-183604, C3-183798, C3-183799, C3-183809, C3-183841, C3-183842	0.3.0
2018-06	CT#80	CP-181037				TS sent to plenary for approval	1.0.0
2018-06	CT#80	CP-181037				TS approved by plenary	15.0.0
2018-09	CT#81	CP-182016	0001	1	F	Changes to clause 4 – Overview	15.1.0
2018-09	CT#81	CP-182016	0003	2	F	Changes to CAPIF Publish Service API clause	15.1.0
2018-09	CT#81	CP-182016	0004	2	F	Changes to CAPIF Events API clause	15.1.0
2018-09	CT#81	CP-182016	0005	4	F	Changes to CAPIF API Invoker Management API clause	15.1.0
2018-09	CT#81	CP-182016	0006	4	F	Changes to CAPIF Authentication Authorization API clause	15.1.0
2018-09	CT#81	CP-182016	0007	3	F	Update to data types for ServiceAPIDescription and APIQuery	15.1.0
2018-09	CT#81	CP-182016	0008	5	F	Definition of CAPIF_Access_Control_Policy_API, and OpenAPI schema	15.1.0
2018-09	CT#81	CP-182016	0009	4	F	CAPIF_Events_API OpenAPI schema	15.1.0
2018-09	CT#81	CP-182016	0010	4	F	AEF_Authentication_API OpenAPI schema	15.1.0
2018-09	CT#81	CP-182016	0011	1	F	CAPIF_Discover_Service API - Corrections	15.1.0
2018-09	CT#81	CP-182016	0012	3	F	CAPIF_discovery_service API OpenAPI file	15.1.0
2018-09	CT#81	CP-182016	0013	4	F	CAPIF_Publish_Service API - Corrections and OpenAPI file	15.1.0
2018-09	CT#81	CP-182016	0014	4	F	AEF_Authentication API - Editor's notes	15.1.0
2018-09	CT#81	CP-182016	0015	4	F	Corrections to data type	15.1.0
2018-09	CT#81	CP-182016	0016	1	F	API Invoker's Information in APIInvokerEnrolmentDetails	15.1.0
2018-09	CT#81	CP-182016	0017	1	F	Corrections to OnboardingInformation data type	15.1.0
2018-09	CT#81	CP-182016	0018	2	F	Security method preference	15.1.0
2018-09	CT#81	CP-182016	0019	1	F	Clarifications to Obtain_API_Invoker_Info service operation	15.1.0
2018-09	CT#81	CP-182016	0020	1	F	Subscribed and Subscribing functional entity	15.1.0
2018-09	CT#81	CP-182016	0021	1	F	Miscellaneous corrections	15.1.0
2018-09	CT#81	CP-182016	0023	1	F	Definitions and abbreviations	15.1.0
2018-09	CT#81	CP-182016	0024	1	F	Referenced data types and enumerations	15.1.0
2018-09	CT#81	CP-182016	0025	2	F	CAPIF_Security_API OpenAPI schema	15.1.0
2018-09	CT#81	CP-182016	0026	1	F	CAPIF discovery service API – API invoker retrieves API information using GET	15.1.0
2018-09	CT#81	CP-182016	0028	2	F	CAPIF_Auditing_API – API management function retrieves API information logs using GET – OpenAPI document	15.1.0
2018-09	CT#81	CP-182016	0029	3	F	API Names changes in clause 5	15.1.0
2018-09	CT#81	CP-182016	0030		F	Change security-related API names in clause 8 and 10	15.1.0
2018-09	CT#81	CP-182016	0031	2	F	Describe response code 202 for Onboard_API_Invoker POST method	15.1.0
2018-09	CT#81	CP-182016	0032		F	Correct cardinality for onboardingNotificationDestination	15.1.0
2018-09	CT#81	CP-182016	0033		F	Correct cardinality for securityNotificationDestination	15.1.0
2018-09	CT#81	CP-182016	0034	1	F	Correct protocol type in Interface Description	15.1.0
2018-09	CT#81	CP-182016	0036	1	F	Query parameter in retrieving access control	15.1.0
2018-09	CT#81	CP-182037	0037	1	F	Authorization endpoint and token request	15.1.0
2018-09	CT#81	CP-182016	0038	1	F	CAPIF Events	15.1.0
2018-09	CT#81	CP-182016	0040	1	F	Corrections to resource figures	15.1.0
2018-09	CT#81	CP-182016	0041	1	F	CAPIF_Auditing_API - 'query' custom operation	15.1.0
2018-09	CT#81	CP-182016	0042	2	F	OpenAPI - CAPIF_API_Invoker_Management API	15.1.0
2018-09	CT#81	CP-182016	0043	2	F	OpenAPI - CAPIF_Logging_API_Invocation API	15.1.0
2018-12	CT#82	CP-183109	0047		F	Correct server definition	15.2.0
2018-12	CT#82	CP-183109	0027	2	F	Security adaptation for Nnef northbound APIs with CAPIF	15.2.0
2018-12	CT#82	CP-183109	0045	1	F	Correct security API name in clause 5.6.2.1	15.2.0
2018-12	CT#82	CP-183109	0046	1	F	Remove Event operations from CAPIF_Publish_API	15.2.0
2018-12	CT#82	CP-183109	0048		F	Correct CAPIF services	15.2.0
2018-12	CT#82	CP-183109	0049	2	F	Correct api name and service name for CAPIF_Publish_Service_API	15.2.0
2018-12	CT#82	CP-183109	0050	2	F	Correct api name and service name for CAPIF_Discover_Service_API	15.2.0
2018-12	CT#82	CP-183109	0051	4	F	Correct CAPIF_Publish_Service_API	15.2.0
2018-12	CT#82	CP-183109	0052	1	F	Correct CAPIF_Discover_Service_API	15.2.0
2018-12	CT#82	CP-183109	0053	4	F	Correct CAPIF_Logging_API_Invocation_API	15.2.0

2018-12	CT#82	CP-183109	0054	3	F	Correct CAPIF_Auditing_API	15.2.0
2018-12	CT#82	CP-183109	0055	2	F	Correct CAPIF_Security_API	15.2.0
2018-12	CT#82	CP-183109	0055	3	F	Correct CAPIF_Security_API	15.2.0
2018-12	CT#82	CP-183109	0057		F	Correct CAPIF_Access_Control_Policy_API	15.2.0
2018-12	CT#82	CP-183109	0058	2	F	supportedFeatures - CAPIF_Discover_Service_API	15.2.0
2018-12	CT#82	CP-183109	0059		F	supportedFeatures 002 - CAPIF_Publish_Service_API	15.2.0
2018-12	CT#82	CP-183109	0060	1	F	supportedFeatures 003 - CAPIF_Events_API	15.2.0
2018-12	CT#82	CP-183109	0061		F	supportedFeatures 004 - CAPIF_API_Invoker_Management_API	15.2.0
2018-12	CT#82	CP-183109	0062		F	supportedFeatures 005 - CAPIF_Security_API	15.2.0
2018-12	CT#82	CP-183109	0063	2	F	supportedFeatures - CAPIF_Access_Control_Policy_API	15.2.0
2018-12	CT#82	CP-183109	0064		F	supportedFeatures 007 - CAPIF_Logging_API_Invocation_API	15.2.0
2018-12	CT#82	CP-183109	0065	2	F	supportedFeatures - CAPIF_Auditing_API	15.2.0
2018-12	CT#82	CP-183109	0067		F	Redundant Editor's note	15.2.0
2018-12	CT#82	CP-183109	0068	1	F	Correct CAPIF_API_Invoker_Management_API	15.2.0
2018-12	CT#82	CP-183109	0070		F	Missing general description in A.1	15.2.0
2018-12	CT#82	CP-183109	0071	1	F	Update mandatory error status code	15.2.0
2018-12	CT#82	CP-183109	0072	3	F	Correct resource model and add missing functions in CAPIF_Security_API	15.2.0
2018-12	CT#82	CP-183109	0074	2	F	Correct resource model and add missing function in AEF_Authentication_API	15.2.0
2018-12	CT#82	CP-183109	0075	1	F	externalDocs field in OpenAPI documents	15.2.0
2018-12	CT#82	CP-183109	0076	3	F	location header in OpenAPI documents	15.2.0
2018-12	CT#82	CP-183109	0077	1	F	version number in OpenAPI documents	15.2.0
2018-12	CT#82	CP-183109	0078	2	F	corrections to CAPIF_Access_Control_Policy_API	15.2.0
2018-12	CT#82	CP-183109	0079	1	F	corrections to CAPIF_Logging_API_Invocation_API	15.2.0
2018-12	CT#82	CP-183109	0079	2	F	Security adaptation for T8 APIs with CAPIF	15.2.0
2018-12	CT#82	CP-183109	0080		F	corrections to EventNotification	15.2.0
2018-12	CT#82	CP-183109	0081		F	corrections to theSubscriber	15.2.0
2018-12	CT#82	CP-183109	0082		F	remove 'OnboardingRequestAck' data type	15.2.0
2019-03	CT#83	CP-190119	0083	1	F	Correct GET description for retrieving service API information	15.3.0
2019-03	CT#83	CP-190119	0084	1	F	Correct PUT message for updating service APIs	15.3.0
2019-03	CT#83	CP-190119	0085	2	F	Correct AEF operations related to obtaining security info or revoking API invokers	15.3.0
2019-03	CT#83	CP-190119	0086	1	F	Correction of definition of obtaining the correct resource in Security APIs	15.3.0
2019-03	CT#83	CP-190119	0089	1	F	Correct several descriptions in clause 8 tables	15.3.0
2019-06	CT#84	CP-191088	0090	1	F	Correct CAPIF_Logging_API yaml file	15.4.0
2019-06	CT#84	CP-191221	0091	1	F	Copyright notice in the YAML files	15.4.0
2019-06	CT#84	CP-191222	0092	1	F	API version update	15.4.0
2019-09	CT#85	CP-192158	0093	3	F	Northbound API registeration and discovery	16.0.0
2019-12	CT#86	CP-193194	0095	1	A	Correct cardinality in event API	16.1.0
2019-12	CT#86	CP-193199	0096	4	B	Reference update: RFC 8259	16.1.0
2019-12	CT#86	CP-193199	0097		F	Detailed information in CAPIF event notification	16.1.0
2019-12	CT#86	CP-193195	0101	4	B	Updates to Service Architecture and functional entities	16.1.0
2019-12	CT#86	CP-193194	0103	1	A	Clause reference corrections	16.1.0
2019-12	CT#86	CP-193194	0105	1	A	Conventions for Open API specification files	16.1.0
2019-12	CT#86	CP-193195	0106	1	B	Update-to-Service-Architecture	16.1.0
2019-12	CT#86	CP-193195	0107	2	B	Update-to-Service-API-Publish	16.1.0
2019-12	CT#86	CP-193195	0108	1	B	Interconnection-Service-API-Publish	16.1.0
2019-12	CT#86	CP-193195	0109	2	B	Update-to-Discover-Service-API	16.1.0
2019-12	CT#86	CP-193199	0111	1	B	Supported feature in API publish service	16.1.0
2019-12	CT#86	CP-193195	0112	1	B	API invoker details update – Service Definition	16.1.0
2019-12	CT#86	CP-193195	0113	1	B	API invoker details update – API Definition	16.1.0
2019-12	CT#86	CP-193195	0114	1	B	API Provider Registration and Update – Service Definition	16.1.0
2019-12	CT#86	CP-193195	0115	3	B	API Provider Registration and Update – API Definition	16.1.0
2019-12	CT#86	CP-193195	0116	1	B	Support for 3rd party API provider domain	16.1.0
2019-12	CT#86	CP-193194	0118	1	A	Correct the notificationDestination of ServiceSecurity object in yaml file	16.1.0
2019-12	CT#86	CP-193194	0120	1	A	Align the API name of Initiate_Authentication	16.1.0
2019-12	CT#86	CP-193212	0121		F	Update of API version and TS version in OpenAPI file	16.1.0
2020-03	CT#87e	CP-200205	0123	1	B	Published API path	16.2.0
2020-03	CT#87e	CP-200205	0124		B	API Invoker Udpate – Event Updates	16.2.0
2020-03	CT#87e	CP-200205	0125	2	B	API Provider Management – Open API	16.2.0
2020-03	CT#87e	CP-200216	0126		F	29.222 Rel-16 Update of OpenAPI version and TS version in externalDocs field	16.2.0
2020-06	CT#88e	CP-201277	0128	3	B	Service description and operations for CAPIF_API_Routing_Policy_API	16.3.0
2020-06	CT#88e	CP-201277	0129	3	B	API definition for CAPIF_API_Routing_Policy_API	16.3.0
2020-06	CT#88e	CP-201278	0130	3	B	API Topology hiding	16.3.0
2020-06	CT#88e	CP-201230	0133		A	Correct API publish procedure	16.3.0
2020-06	CT#88e	CP-201231	0131	1	F	API Provider management API attribute name optimization	16.3.0
2020-06	CT#88e	CP-201231	0135	1	F	Correct ServiceAPIDescription	16.3.0

2020-06	CT#88e	CP-201231	0136	2	F	Correct service API discovery in interconnection	16.3.0
2020-06	CT#88e	CP-201231	0137	1	F	Correct shareable information	16.3.0
2020-06	CT#88e	CP-201235	0138	1	F	Correct the supported features in the published API	16.3.0
2020-06	CT#88e	CP-201235	0139	1	F	Update general clause for OpenAPI specification	16.3.0
2020-06	CT#88e	CP-201256	0140	1	F	URI of the CAPIF APIs	16.3.0
2020-06	CT#88e	CP-201231	0141	1	B	Add API category in discovery	16.3.0
2020-06	CT#88e	CP-201235	0142		F	Optionality of ProblemDetails	16.3.0
2020-06	CT#88e	CP-201230	0144	1	A	Clause and reference point correction	16.3.0
2020-06	CT#88e	CP-201231	0145	1	F	Align interface names	16.3.0
2020-06	CT#88e	CP-201235	0146	1	F	Supported headers, Resource Data type, Operation Name and yaml mapping	16.3.0
2020-06	CT#88e	CP-201255	0147		F	Update of OpenAPI version and TS version in externalDocs field	16.3.0
2020-06	CT#88e	CP-201319	0149		A	Required attribute corrections to CAPIF Open APIs	16.3.0
2020-09	CT#89e	CP-202064	0151	1	F	Missing and inconsistent "apiVersion" notations and Location header	16.4.0
2020-09	CT#89e	CP-202064	0152	1	F	CAPIF Routing Info API corrections	16.4.0
2020-09	CT#89e	CP-202064	0153		F	CAPIF topology hiding correction	16.4.0
2020-09	CT#89e	CP-202233	0155	3	A	Correct CAPIF security API	16.4.0
2020-09	CT#89e	CP-202063	0157	1	A	Correct api invoker certificate in onboarding	16.4.0
2020-09	CT#89e	CP-202084	0158		F	Update of OpenAPI version and TS version in externalDocs field	16.4.0
2020-12	CT#90e	CP-203139	0160	1	F	Essential corrections and alignments	16.5.0
2020-12	CT#90e	CP-203126	0162	1	A	Correct inconsistency in SecurityNotification	16.5.0
2020-12	CT#90e	CP-203139	0163	1	F	Storage of YAML files in 3GPP Forge	16.5.0
2021-03	CT#91e	CP-210239	0164	1	F	CAPIF_Security API externalDocs version correction	16.6.0
2021-03	CT#91e	CP-210221	0165	1	F	Corrections to HTTP custom headers handling for Northbound APIs	17.0.0
2021-03	CT#91e	CP-210220	0166		F	OpenAPI reference	17.0.0
2021-06	CT#92e	CP-211239	0177	1	F	Missing data type in the CAPIF_API_Provider_Management_API Data Types tables	17.1.0
2021-06	CT#92e	CP-211239	0178	2	F	Missing data type in the CAPIF_Routing_Info_API Data Types tables	17.1.0
2021-06	CT#92e	CP-211123	0179	1	F	Missing data type in the CAPIF_Security_API Data Types tables	17.1.0
2021-06	CT#92e	CP-211239	0180	1	F	Missing data types in the CAPIF_Access_Control_Policy_API Data Types tables	17.1.0
2021-06	CT#92e	CP-211124	0181	3	F	Missing data types in the CAPIF_Publish_Service_API Data Types tables	17.1.0
2021-06	CT#92e	CP-211216	0185		A	SecurityMethod data type incorrectly written some parts of the CAPIF_Publish_Service_API description clause	17.1.0
2021-06	CT#92e	CP-211241	0186	1	F	DiscoverService: Unbreakable spaces and missing "description" field	17.1.0
2021-06	CT#92e	CP-211241	0187	1	F	PublishService API: Unbreakable spaces and missing "description" fields	17.1.0
2021-06	CT#92e	CP-211241	0188	1	F	Events API: Unbreakable spaces and missing "description" fields	17.1.0
2021-06	CT#92e	CP-211241	0189	1	F	InvokerManagement API: Unbreakable spaces and missing "description" fields	17.1.0
2021-06	CT#92e	CP-211241	0190	1	F	Security API: Unbreakable space and missing "description" fields	17.1.0
2021-06	CT#92e	CP-211241	0191	1	F	AccessControlPolicy API: Unbreakable spaces and missing "description" fields	17.1.0
2021-06	CT#92e	CP-211241	0192	1	F	LoggingAPIInvocation API: Unbreakable spaces and missing "description" fields	17.1.0
2021-06	CT#92e	CP-211241	0193	1	F	Auditing API: Unbreakable spaces	17.1.0
2021-06	CT#92e	CP-211241	0194	1	F	AEFSecurity API: Unbreakable spaces and missing "description" fields	17.1.0
2021-06	CT#92e	CP-211241	0195	1	F	API_Provider_Management API: Missing "description" fields	17.1.0
2021-06	CT#92e	CP-211241	0196	1	F	RoutingInfo API: Unbreakable spaces and missing "description" fields	17.1.0
2021-06	CT#92e	CP-211239	0197		F	Correction of the clause clause terminology	17.1.0
2021-06	CT#92e	CP-211239	0198		F	Corrections to the CAPIF_API_Invoker_Management_API Data Model clause	17.1.0
2021-06	CT#92e	CP-211240	0199	1	F	Corrections to the CAPIF_Auditing_API Data Model clause	17.1.0
2021-06	CT#92e	CP-211239	0200		F	Corrections to the CAPIF_Events_API Data Model clause	17.1.0
2021-06	CT#92e	CP-211239	0201		F	Corrections to the CAPIF_Logging_API_Invocation_API Data Model clause	17.1.0
2021-06	CT#92e	CP-211239	0202		F	Corrections to the CAPIF_Publish_Service_API Data Model clause	17.1.0
2021-06	CT#92e	CP-211239	0203		F	Corrections to the CAPIF_Security_API Data Model clause	17.1.0
2021-06	CT#92e	CP-211240	0204	1	F	Miscellaneous corrections to the CAPIF_Discover_Service_API	17.1.0
2021-06	CT#92e	CP-211240	0205	1	F	Miscellaneous corrections to the AEF_Security_API	17.1.0
2021-06	CT#92e	CP-211240	0206	1	B	Support of 204 No content response code for service API definition update(NBI17)	17.1.0
2021-06	CT#92e	CP-211240	0207	1	F	Support redirection and mandatory error codes for CAPIF APIs	17.1.0
2021-06	CT#92e	CP-211265	0208		F	Update of OpenAPI version and TS version in externalDocs field	17.1.0
2021-09	CT#93e	CP-212224	0209		F	Correction of cardinality of InvocationLogs in POST request	17.2.0
2021-09	CT#93e	CP-212214	0210		F	Resource URI correction on CAPIF APIs	17.2.0

2021-09	CT#93e	CP-212214	0211		F	204 No Content during modification procedure on CAPIF_API_Provider_Management_API	17.2.0
2021-09	CT#93e	CP-212214	0212		F	Correction of some remaining invalid characters in OpenAPI specification files	17.2.0
2021-09	CT#93e	CP-212214	0213		F	Updates 204 No Content in CAPIF_API_Invoker_Management_API	17.2.0
2021-09	CT#93e	CP-212223	0214		F	Update of OpenAPI version and TS version in externalDocs field	17.2.0
2021-12	CT#94e	CP-213221	0215	2	B	AEF location support	17.3.0
2021-12	CT#94e	CP-213220	0216		B	Alignment with SA3 supported TLS profiles	17.3.0
2021-12	CT#94e	CP-213246	0217		F	Update of OpenAPI version and TS version in externalDocs field	17.3.0
2022-03	CT#95e	CP-220203	0218	1	F	Clarify the query logic for API invoker id	17.4.0
2022-03	CT#95e	CP-220168	0221		A	Correct inconsistencies	17.4.0
2022-03	CT#95e	CP-220204	0222	1	B	Obtain security info with API ID	17.4.0
2022-03	CT#95e	CP-220204	0223	1	F	Clarification about building the apiRoot of a discovered API	17.4.0
2022-03	CT#95e	CP-220323	0224	2	B	Support PATCH for the update of an API Provider Domain Registration resource.	17.4.0
2022-03	CT#95e	CP-220350	0225	3	B	Support PATCH for the update of an On-boarded API resource	17.4.0
2022-03	CT#95e	CP-220204	0226		B	Support PATCH for the update of an APF published API resource	17.4.0
2022-03	CT#95e	CP-220194	0227		F	Update of info and externalDocs fields	17.4.0
2022-06	CT#96	CP-221147	0230	3	F	Resolving the naming convention issues	17.5.0
2022-06	CT#96	CP-221275	0231	2	F	Token request error	17.5.0
2022-06	CT#96	CP-221147	0232		F	CAPIF_Discover_Service_API: formatting of preferred-aef-loc query parameter	17.5.0
2022-06	CT#96	CP-221147	0233		F	Resource URI overview and apiVersion placeholder	17.5.0
2022-06	CT#96	CP-221148	0234	1	F	OpenAPI long descriptions	17.5.0
2022-06	CT#96	CP-221124	0237	1	A	Correcting the data type of the APF identifier	17.5.0
2022-06	CT#96	CP-221124	0240	1	A	Correcting the data type of the service API Identifier	17.5.0
2022-06	CT#96	CP-221124	0243		A	Correcting query parameters names in the CAPIF_Security_API	17.5.0
2022-06	CT#96	CP-221263	0244	2	F	Missing definition of the AccessTokenErr data type in the main body	17.5.0
2022-06	CT#96	CP-221124	0247	1	A	Correct token request content type	17.5.0
2022-06	CT#96	CP-221151	0248		F	Update of info and externalDocs fields	17.5.0
2022-09	CT#97e	CP-222118	0251	2	F	Corrections to the references for URI structure from TS 29.501 to TS 29.122.	17.6.0
2022-09	CT#97e	CP-222121	0252		F	Update of info and externalDocs fields	17.6.0
2022-12	CT#98e	CP-223235	0262	2	A	Corrections for CAPIF_API_Invoker_Management_API	17.7.0
2022-12	CT#98e	CP-223184	0266		F	Add the missing status code for CAPIF_API_Invoker_Management_API	17.7.0
2022-12	CT#98e	CP-223169	0267	1	A	Corrections for data type of CAPIF services	17.7.0
2022-12	CT#98e	CP-223169	0270		A	Corrections on Enumeration Protocol for CAPIF_Publish_Service_API	17.7.0
2022-12	CT#98e	CP-223169	0273		A	Corrections on POST request body for CAPIF_Logging_API_Invocation_API	17.7.0
2022-12	CT#98e	CP-223169	0276		A	Corrections on resource URI for CAPIF_Discover_Service_API	17.7.0
2022-12	CT#98e	CP-223169	0279		A	Corrections on Time Range List for CAPIF_Access_Control_Policy_API	17.7.0
2022-12	CT#98e	CP-223188	0284		F	Update of info and externalDocs fields	17.7.0
2022-12	CT#98e	CP-223185	0253	1	B	Completing the interface descriptions	18.0.0
2022-12	CT#98e	CP-223185	0254	1	B	Custom Operations modelling	18.0.0
2022-12	CT#98e	CP-223185	0256	1	F	Correction of the tables for the re-used, API-specific data structures in CAPIF APIs	18.0.0
2022-12	CT#98e	CP-223185	0257		F	Correction of the OpenAPI file formating and descriptions in the CAPIF APIs	18.0.0
2022-12	CT#98e	CP-223185	0258		F	"Error handling" clause: alignment with other NBI and 5GS APIs	18.0.0
2022-12	CT#98e	CP-223185	0259		F	Corrections on CAPIF_API_Provider_Management_API	18.0.0
2022-12	CT#98e	CP-223189	0285		F	Update of info and externalDocs fields	18.0.0
2023-03	CT#99	CP-230156	0286	1	F	Correction of the description fields in enumerations	18.1.0
2023-03	CT#99	CP-230157	0287	1	B	Vendor specific extensions	18.1.0
2023-03	CT#99	CP-230157	0290	1	B	Support of CAPIF extensibility requirements	18.1.0
2023-03	CT#99	CP-230157	0294	1	B	Update for CAPIF_Auditing_API to support carrying multiple invocation logs and feature negotiation	18.1.0
2023-03	CT#99	CP-230156	0295		F	Update the description field of CAPIF_Publish_Service API	18.1.0
2023-03	CT#99	CP-230161	0296		F	Update of info and externalDocs fields	18.1.0
2023-06	CT#100	CP-231140	0297	3	B	Completing the support of CAPIF protocol and data formats extensibility requirements	18.2.0
2023-06	CT#100	CP-231139	0298		F	Corrections on presence of the attributes in CAPIF APIs	18.2.0
2023-06	CT#100	CP-231139	0299		F	Support CAPIF model in SNPN	18.2.0
2023-06	CT#100	CP-231141	0305		F	Update of info and externalDocs fields	18.2.0
2023-09	CT#101	CP-232091	0306	1	F	CAPIF security method clarification	18.3.0
2023-09	CT#101	CP-232091	0307	1	B	Update definitions of CAPIF provider domain and SNPN trust domain	18.3.0
2023-09	CT#101	CP-232091	0308	1	F	Clarify CCF role in service publish	18.3.0
2023-09	CT#101	CP-232086	0309	1	B	CAPIF Events API update subscription	18.3.0

2023-09	CT#101	CP-232091	0310	1	F	Various corrections	18.3.0
2023-09	CT#101	CP-232085	0311		F	Update of info and externalDocs fields	18.3.0
2023-12	CT#102	CP-233231	0300	4	B	Supporting query parameters extensionsibility for the CAPIF_Discover_Service_API	18.4.0
2023-12	CT#102	CP-233261	0312	2	B	Authorization code flow for resource owner-aware northbound api access	18.4.0
2023-12	CT#102	CP-233261	0313	2	B	Update authorization obtaining part to support resource owner-aware northbound API access	18.4.0
2023-12	CT#102	CP-233261	0314	2	B	Update securitymethod data type for Resource owner-aware northbound API access	18.4.0
2023-12	CT#102	CP-233243	0316	1	B	Service API status monitoring in the CAPIF APIs	18.4.0
2023-12	CT#102	CP-233231	0317	2	F	Error handling in the CAPIF layer	18.4.0
2023-12	CT#102	CP-233232	0318	2	F	Update of the CAPIF layer architecture description	18.4.0
2023-12	CT#102	CP-233261	0319	1	B	Discovering of APIs based on the API provider name in the CAPIF_Discover_Service_API	18.4.0
2023-12	CT#102	CP-233231	0320	1	F	HTTP RFC uplifting	18.4.0
2023-12	CT#102	CP-233231	0321	1	F	Correction of the InterfaceDescription data structure	18.4.0
2023-12	CT#102	CP-233261	0322	1	B	Discovering of APIs based on the IP address of UE in the CAPIF_Discover_Service_API	18.4.0
2023-12	CT#102	CP-233232	0325	2	F	Corrections to boolean type definitions	18.4.0
2023-12	CT#102	CP-233231	0326		F	Corrections on the CAPIF service	18.4.0
2023-12	CT#102	CP-233232	0327	1	F	CAPIFEventDetail data type clarification	18.4.0
2023-12	CT#102	CP-233232	0328	1	D	Correcting an incorrect clause number	18.4.0
2023-12	CT#102	CP-233241	0331	1	B	New IE(Service KPI) in Service API publish request	18.4.0
2023-12	CT#102	CP-233261	0332	1	B	CAPIF_Publish_Service_API – Publish the Public IP ranges information	18.4.0
2023-12	CT#102	CP-233237	0333		F	Update of info and externalDocs fields	18.4.0
2024-03	CT#103	CP-240171	0301	9	B	CAPIF Security Methods usage for vendor extensions	18.5.0
2024-03	CT#103	CP-240171	0335		F	CAPIF Security Methods presence condition update	18.5.0
2024-03	CT#103	CP-240193	0336	1	B	Support onboarding expiration in the CAPIF_API_Invoker_Management_API	18.5.0
2024-03	CT#103	CP-240168	0338	1	F	Correction to CAPIF_Publish_Service_API	18.5.0
2024-03	CT#103	CP-240192	0339		F	Correction to CAPIF_Security_API	18.5.0
2024-03	CT#103	CP-240192	0341	1	B	Update CAPIF_Publish_Service_API and CAPIF_API_Provider_Management_API to support RNAA	18.5.0
2024-03	CT#103	CP-240171	0342	1	F	CAPIF Security Method handling	18.5.0
2024-03	CT#103	CP-240192	0344	2	B	Corrections and updates to the RNAA Oauth related provisions	18.5.0
2024-03	CT#103	CP-240166	0345		F	Update of info and externalDocs fields	18.5.0
2024-06	CT#104	CP-241095	0346		F	Subscribed events editors note handling	18.6.0
2024-06	CT#104	CP-241083	0347		F	Several OpenAPI Corrections	18.6.0
2024-06	CT#104	CP-241083	0348		F	Service API category update	18.6.0
2024-06	CT#104	CP-241106	0349	1	F	Service API information update	18.6.0
2024-06	CT#104	CP-241138	0350	1	B	API Invoker authorization	18.6.0
2024-06	CT#104	CP-241084	0351	1	F	Various essential corrections	18.6.0
2024-06	CT#104	CP-241084	0352	1	F	Various essential corrections to the common design aspects for all CAPIF APIs	18.6.0
2024-06	CT#104	CP-241085	0353		F	Update of info and externalDocs fields	18.6.0

History

Document history		
V18.5.0	May 2024	Publication
V18.6.0	July 2024	Publication