3GPP TR 29.890 V16.0.0 (2020-07)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Core Network and Terminals;

Study on CT WG3 Aspects of 5G System Phase 1;

(Release 16)

** 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Report is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

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

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword [9](#__RefHeading___Toc517275762)

1 Scope [10](#__RefHeading___Toc517275763)

2 References [10](#__RefHeading___Toc517275764)

3 Definitions and abbreviations [13](#__RefHeading___Toc517275765)

3.1 Definitions [13](#__RefHeading___Toc517275766)

3.2 Abbreviations [13](#__RefHeading___Toc517275767)

4 Requirements [15](#__RefHeading___Toc517275768)

4.1 General Requirements [15](#__RefHeading___Toc517275769)

4.1.1 Architecture Requirements [15](#__RefHeading___Toc517275770)

4.1.2 Requirements for protocol selection for service based interfaces [15](#__RefHeading___Toc517275771)

4.1.3 Additional evaluation criteria for protocol selection for service based interfaces [15](#__RefHeading___Toc517275772)

4.2 Requirements for the 5G Policy Framework [16](#__RefHeading___Toc517275773)

4.3 Requirements for interworking between the 5G System and external Data Networks [17](#__RefHeading___Toc517275774)

4.4 Requirements for Network Capability Exposure of 5G System [17](#__RefHeading___Toc517275775)

5 5G Policy Framework [18](#__RefHeading___Toc517275776)

5.1 Reference Model [18](#__RefHeading___Toc517275777)

5.2 Functional Entities [22](#__RefHeading___Toc517275778)

5.2.1 Policy Control Function (PCF) [22](#__RefHeading___Toc517275779)

5.2.2 Session Management Function (SMF) [23](#__RefHeading___Toc517275780)

5.2.3 Access and Mobility Management Function (AMF) [23](#__RefHeading___Toc517275781)

5.2.4 Application Function (AF) [23](#__RefHeading___Toc517275782)

5.2.5 Network Data Analytics Function (NWDAF) [23](#__RefHeading___Toc517275783)

5.2.6 Network Exposure Function (NEF) [24](#__RefHeading___Toc517275784)

5.2.7 Unified Data Repository (UDR) [24](#__RefHeading___Toc517275785)

5.3 System Procedures [24](#__RefHeading___Toc517275786)

5.3.1 Procedures for Npcf\_AMPolicyControl service [24](#__RefHeading___Toc517275787)

5.3.1.1 Policy request during UE registration [24](#__RefHeading___Toc517275788)

5.3.1.2 Policy update [26](#__RefHeading___Toc517275789)

5.3.1.2.1 Update initiated by the AMF [26](#__RefHeading___Toc517275790)

5.3.1.2.2 Update initiated by the PCF [26](#__RefHeading___Toc517275791)

5.3.1.3 Policy context deletion [27](#__RefHeading___Toc517275792)

5.3.1.3.1 Policy context deletion initiated by the AMF [27](#__RefHeading___Toc517275793)

5.3.1.3.2 Policy context deletion initiated by the PCF [27](#__RefHeading___Toc517275794)

5.3.2 Procedures for Npcf\_SMPolicyControl service [28](#__RefHeading___Toc517275795)

5.3.2.1 Request of Session Management (SM) related policies [28](#__RefHeading___Toc517275796)

5.3.2.2 Update of Session Management (SM) related policies [30](#__RefHeading___Toc517275797)

5.3.2.2.1 PCF initiated update of SM related policies [30](#__RefHeading___Toc517275798)

5.3.2.2.2 SMF triggered update of SM related policies [30](#__RefHeading___Toc517275799)

5.3.2.3 Deletion of the context of SM related policies [31](#__RefHeading___Toc517275800)

5.3.2.3.1 Deletion of the context of SM related policies initiated by the SMF [31](#__RefHeading___Toc517275801)

5.3.2.3.2 Deletion of the context of SM related policies initiated by the PCF [32](#__RefHeading___Toc517275802)

5.3.3 Procedures for Nsmf\_EventExposure service [32](#__RefHeading___Toc517275803)

5.3.3.1 PCF subscription to events [32](#__RefHeading___Toc517275804)

5.3.3.2 SMF Notification about subscribed events [33](#__RefHeading___Toc517275805)

5.3.3.3 PCF unsubscription to events [34](#__RefHeading___Toc517275806)

5.3.4 Procedures over N24 reference point [35](#__RefHeading___Toc517275807)

5.3.5 Procedure for Npcf\_PolicyAuthorization service [35](#__RefHeading___Toc517275808)

5.3.5.1 Initial provisioning of service information [35](#__RefHeading___Toc517275809)

5.3.5.2 Modification of service information [36](#__RefHeading___Toc517275810)

5.3.5.3 AF application session context termination [37](#__RefHeading___Toc517275811)

5.3.5.3.1 Delete the AF application session context initiated by the AF [37](#__RefHeading___Toc517275812)

5.3.5.3.2 Delete the AF application session context initiated by the PCF [37](#__RefHeading___Toc517275813)

5.3.5.4 AF subscription to events [38](#__RefHeading___Toc517275814)

5.3.5.5 AF unsubscription to events [39](#__RefHeading___Toc517275815)

5.3.5.6 PCF notification about application session context events [40](#__RefHeading___Toc517275816)

5.4 Network Function Service Procedures [40](#__RefHeading___Toc517275817)

5.4.1 General [40](#__RefHeading___Toc517275818)

5.4.2 Npcf\_AMPolicyControl service [41](#__RefHeading___Toc517275819)

5.4.2.1 General [41](#__RefHeading___Toc517275820)

5.4.2.2 Operations [42](#__RefHeading___Toc517275821)

5.4.2.3 Encoding Proposal 1: RESTful HTTP with Policy as PCF resource and custom operation to update policy at AMF [43](#__RefHeading___Toc517275822)

5.4.2.4 Encoding Proposal 2: RESTful HTTP with Policy as AMF resource [47](#__RefHeading___Toc517275823)

5.4.2.5 Encoding Proposal 3: RESTful HTTP with Policy as PCF resource and notification to trigger AMF to fetch new policy [52](#__RefHeading___Toc517275824)

5.4.2.5a Encoding Proposal 4: RESTful HTTP with Policy both as PCF resource and as AMF resource and subscription related information only in PCF resource [52](#__RefHeading___Toc517275825)

5.4.2.6 Comparison of Encoding Proposals [53](#__RefHeading___Toc517275826)

5.4.2.7 Conclusions [53](#__RefHeading___Toc517275827)

5.4.3 Npcf\_SMPolicyControl service [53](#__RefHeading___Toc517275828)

5.4.3.1 General [53](#__RefHeading___Toc517275829)

5.4.3.2 Operations [54](#__RefHeading___Toc517275830)

5.4.3.3 Encoding Proposal 1: RESTful HTTP with Policy as PCF resource and custom operation to update policy at SMF [55](#__RefHeading___Toc517275831)

5.4.3.4 Encoding Proposal 2: RESTful HTTP with Policy as SMF resource [59](#__RefHeading___Toc517275832)

5.4.3.5 Encoding Proposal 3: RESTful HTTP with Policy as PCF resource and notification to trigger SMF to fetch new policy [62](#__RefHeading___Toc517275833)

5.4.3.5a Encoding Proposal 4: RESTful HTTP with Policy both as PCF resource and as SMF resource and subscription related information only in PCF resource [63](#__RefHeading___Toc517275834)

5.4.3.6 Comparison of Proposals [63](#__RefHeading___Toc517275835)

5.4.3.7 Conclusions [63](#__RefHeading___Toc517275836)

5.4.4 Npcf\_PolicyAuthorization service [63](#__RefHeading___Toc517275837)

5.4.4.1 General [63](#__RefHeading___Toc517275838)

5.4.4.2 Operations [64](#__RefHeading___Toc517275839)

5.4.4.3 Encoding Proposal 1: RESTful HTTP with event subscriptions as sub-resource [66](#__RefHeading___Toc517275840)

5.4.4.4 Encoding Proposal 2: RESTful HTTP with event subscriptions as a separated sub-resource [70](#__RefHeading___Toc517275841)

5.4.4.5 Comparison of encoding proposals [72](#__RefHeading___Toc517275842)

5.4.4.6 Conclusions [72](#__RefHeading___Toc517275843)

5.4.5 Nsmf\_EventExposure [72](#__RefHeading___Toc517275844)

5.4.5.1 General [72](#__RefHeading___Toc517275845)

5.4.5.2 Operations [73](#__RefHeading___Toc517275846)

5.4.5.3 Encoding Proposal 1: RESTful HTTP [73](#__RefHeading___Toc517275847)

5.4.6 UDR service [77](#__RefHeading___Toc517275848)

5.4.6.1 General [77](#__RefHeading___Toc517275849)

5.4.7 NWDAF services [78](#__RefHeading___Toc517275850)

5.4.7.1 General [78](#__RefHeading___Toc517275851)

5.4.7.2 Nnwdaf\_Events\_Subscription Service [78](#__RefHeading___Toc517275852)

5.4.7.2.1 General [78](#__RefHeading___Toc517275853)

5.4.7.2.2 Operations [78](#__RefHeading___Toc517275854)

5.4.7.3 Nnwdaf\_Analytics\_Info Service [78](#__RefHeading___Toc517275855)

5.4.7.3.1 General [78](#__RefHeading___Toc517275856)

5.4.7.3.2 Operations [78](#__RefHeading___Toc517275857)

5.5 Protocols [79](#__RefHeading___Toc517275858)

5.5.1 Protocol Candidates [79](#__RefHeading___Toc517275859)

5.5.1.1 HTTP2/JSON [79](#__RefHeading___Toc517275860)

5.5.1.1.1 General [79](#__RefHeading___Toc517275861)

5.5.1.1.2 HTTP/1.1 [79](#__RefHeading___Toc517275862)

5.5.1.1.3 HTTP/2 [80](#__RefHeading___Toc517275863)

5.5.1.1.4 Support of Notifications [81](#__RefHeading___Toc517275864)

5.5.1.1.4.1 General [81](#__RefHeading___Toc517275865)

5.5.1.1.4.2 Solution with two client-server pairs [81](#__RefHeading___Toc517275866)

5.5.1.1.4.3 Solutions with a single client-server pair prior to HTTP/2 [82](#__RefHeading___Toc517275867)

5.5.1.1.4.4 Solutions with a single client-server pair: HTTP/2 Server Push [83](#__RefHeading___Toc517275868)

5.5.1.1.4.5 Solution based on Websocket [83](#__RefHeading___Toc517275869)

5.5.1.1.5 Extensibility Mechanisms [84](#__RefHeading___Toc517275870)

5.5.1.1.6 HTTP Proxy [86](#__RefHeading___Toc517275871)

5.5.1.1.7 Protocol Candidate TCP/TLS/HTTP2/JSON [86](#__RefHeading___Toc517275872)

5.5.1.1.8 Protocol Candidate UDP/QUIC/HTTP2/JSON [86](#__RefHeading___Toc517275873)

5.5.1.1.9 Evaluation of HTTP aspects [86](#__RefHeading___Toc517275874)

5.5.1.1.9.1 Selection of HTTP version [86](#__RefHeading___Toc517275875)

5.5.1.1.9.2 Selection of Notification method [87](#__RefHeading___Toc517275876)

5.5.1.2 Diameter [87](#__RefHeading___Toc517275877)

5.5.2 Comparison of RESTful and RPC protocol design [88](#__RefHeading___Toc517275878)

5.5.2.1 Characteristics of RPCs [88](#__RefHeading___Toc517275879)

5.5.2.2 Characteristics of REST [89](#__RefHeading___Toc517275880)

5.5.2.3 Degree of Compliance of the stage 2 requirements with RPC [90](#__RefHeading___Toc517275881)

5.5.2.4 Degree of Compliance of the stage 2 requirements with REST [90](#__RefHeading___Toc517275882)

5.5.2.5 Evaluation of RPC [92](#__RefHeading___Toc517275883)

5.5.2.6 Evaluation of REST [92](#__RefHeading___Toc517275884)

5.5.2.6.1 General [92](#__RefHeading___Toc517275885)

5.5.2.6.2 Level 3 of the Richardson maturity model [92](#__RefHeading___Toc517275886)

5.5.2.7 HTTP APIs types [93](#__RefHeading___Toc517275887)

5.5.2.8 Conclusions [93](#__RefHeading___Toc517275888)

5.5.3 Data Serialization Format [94](#__RefHeading___Toc517275889)

5.5.3.1 Introduction [94](#__RefHeading___Toc517275890)

5.5.3.2 Solution 1 – JSON [94](#__RefHeading___Toc517275891)

5.5.3.2.1 Description [94](#__RefHeading___Toc517275892)

5.5.3.2.2 Evaluation [94](#__RefHeading___Toc517275893)

5.5.3.3 Solution 2 – BSON [94](#__RefHeading___Toc517275894)

5.5.3.3.1 Description [94](#__RefHeading___Toc517275895)

5.5.3.3.2 Evaluation [95](#__RefHeading___Toc517275896)

5.5.3.4 Solution 3 – CBOR [95](#__RefHeading___Toc517275897)

5.5.3.4.1 Description [95](#__RefHeading___Toc517275898)

5.5.3.4.2 Evaluation [95](#__RefHeading___Toc517275899)

5.5.3.5 Conclusion [95](#__RefHeading___Toc517275900)

5.5.4 Transport protocols [96](#__RefHeading___Toc517275901)

5.5.5 Interface Definition Language [96](#__RefHeading___Toc517275902)

5.5.5.1 Introduction [96](#__RefHeading___Toc517275903)

5.5.5.2 Solution 1 – YANG/RESTCONF [97](#__RefHeading___Toc517275904)

5.5.5.2.1 Description [97](#__RefHeading___Toc517275905)

5.5.5.2.2 Evaluation [97](#__RefHeading___Toc517275906)

5.5.5.3 Solution 2 – OpenAPI Specification (Swagger) [97](#__RefHeading___Toc517275907)

5.5.5.3.1 Description [97](#__RefHeading___Toc517275908)

5.5.5.3.2 Evaluation [98](#__RefHeading___Toc517275909)

5.5.5.4 Solution 3 – Protocol Buffers [98](#__RefHeading___Toc517275910)

5.5.5.4.1 Description [98](#__RefHeading___Toc517275911)

5.5.5.4.2 Evaluation [98](#__RefHeading___Toc517275912)

5.5.5.5 Solution 4 – JSON Content Rules [98](#__RefHeading___Toc517275913)

5.5.5.5.1 Description [98](#__RefHeading___Toc517275914)

5.5.5.5.2 Evaluation [99](#__RefHeading___Toc517275915)

5.5.5.6 Solution 5 – JSON Schema [99](#__RefHeading___Toc517275916)

5.5.5.6.1 Description [99](#__RefHeading___Toc517275917)

5.5.5.6.2 Evaluation [99](#__RefHeading___Toc517275918)

5.5.5.7 Solution 6 – CBOR IDL [99](#__RefHeading___Toc517275919)

5.5.5.7.1 Description [99](#__RefHeading___Toc517275920)

5.5.5.7.2 Evaluation [99](#__RefHeading___Toc517275921)

5.5.5.8 Comparison of IDLs [100](#__RefHeading___Toc517275922)

5.5.5.9 Conclusion [101](#__RefHeading___Toc517275923)

5.5.6 Evaluation of candidate protocols for service based interfaces [101](#__RefHeading___Toc517275924)

5.6 AMF Access and Mobility Policy [105](#__RefHeading___Toc517275925)

5.6.1 General [105](#__RefHeading___Toc517275926)

5.6.2 Service Area Restriction [105](#__RefHeading___Toc517275927)

5.6.3 RFSP Index [106](#__RefHeading___Toc517275928)

5.7 Session Management Policy Rules [106](#__RefHeading___Toc517275929)

5.7.1 PCC rule in 5GC [106](#__RefHeading___Toc517275930)

5.7.1.1 General [106](#__RefHeading___Toc517275931)

5.7.1.2 PCC rule operations [110](#__RefHeading___Toc517275932)

5.7.2 5G PDU session related policy information [111](#__RefHeading___Toc517275933)

5.7.3 Packet Filter Set [113](#__RefHeading___Toc517275934)

5.7.3.1 General [113](#__RefHeading___Toc517275935)

5.7.3.2 IP Packet Filter Set [113](#__RefHeading___Toc517275936)

5.7.3.3 Ethernet Packet Filter Set [113](#__RefHeading___Toc517275937)

5.8 UE Policies [114](#__RefHeading___Toc517275938)

5.8.1 General [114](#__RefHeading___Toc517275939)

5.8.2 UE Access Network discovery and selection policies [114](#__RefHeading___Toc517275940)

5.8.3 UE Route Selection Policies (URSP) [114](#__RefHeading___Toc517275941)

5.9 QoS mechanisms [115](#__RefHeading___Toc517275942)

5.9.1 Overview [115](#__RefHeading___Toc517275943)

5.9.2 Policy provisioning for authorized QoS per service data flow [115](#__RefHeading___Toc517275944)

5.9.3 Policy enforcement for authorized QoS per service data flow [115](#__RefHeading___Toc517275945)

5.9.4 Policy provisioning of authorized QoS per PDU Session [116](#__RefHeading___Toc517275946)

5.9.5 Policy enforcement for authorized QoS per PDU session [116](#__RefHeading___Toc517275947)

5.9.6 Reflective QoS [116](#__RefHeading___Toc517275948)

5.9.6.1 General [116](#__RefHeading___Toc517275949)

5.9.6.2 Provisioning of authorized Reflective QoS per service data flow [116](#__RefHeading___Toc517275950)

5.9.6.3 Policy enforcement of authorized Reflective QoS per service data flow [116](#__RefHeading___Toc517275951)

5.9.6.4 Provisioning and Enforcement of authorized Reflective QoS information per PDU session [117](#__RefHeading___Toc517275952)

5.9.7 QoS Information [117](#__RefHeading___Toc517275953)

5.9.7.1 5G QoS Identifier (5QI) [117](#__RefHeading___Toc517275954)

5.9.7.2 QoS Characteristics [117](#__RefHeading___Toc517275955)

5.9.7.3 Allocation Retention Priority [118](#__RefHeading___Toc517275956)

5.9.7.4 Guaranteed Bitrate (DL/UL) [119](#__RefHeading___Toc517275957)

5.9.7.5 Maximum Bitrate (DL/UL) [119](#__RefHeading___Toc517275958)

5.9.7.6 Notification Control [119](#__RefHeading___Toc517275959)

5.9.7.7 PDU Session Aggregate Maximum Bitrate (DL/UL) [119](#__RefHeading___Toc517275960)

5.9.7.8 UE Aggregate Maximum Bitrate (DL/UL) [119](#__RefHeading___Toc517275961)

5.9.8 QoS mapping between Rx and N7 [119](#__RefHeading___Toc517275962)

5.10 Discovery and Selection aspects [119](#__RefHeading___Toc517275963)

5.10.1 General [119](#__RefHeading___Toc517275964)

5.10.2 PCF discovery and selection by the AMF [120](#__RefHeading___Toc517275965)

5.10.3 PCF discovery and selection by the SMF [120](#__RefHeading___Toc517275966)

5.10.4 Network functionality to assist PCF selection by the AF [120](#__RefHeading___Toc517275967)

5.10.4.1 General [120](#__RefHeading___Toc517275968)

5.10.4.2 The PCF Binding Support Functionality (PCF BSF) [120](#__RefHeading___Toc517275969)

5.10.4.3 AF Policy Request to Multiple PCFs [121](#__RefHeading___Toc517275970)

5.11 Roaming scenarios [121](#__RefHeading___Toc517275971)

5.12 Subscription Data Management [122](#__RefHeading___Toc517275972)

5.13 Interworking with EPC [122](#__RefHeading___Toc517275973)

5.14 IMS Aspects [124](#__RefHeading___Toc517275974)

5.14.1 General [124](#__RefHeading___Toc517275975)

5.15 Support of MPS services [124](#__RefHeading___Toc517275976)

5.15.1 General [124](#__RefHeading___Toc517275977)

5.15.2 Invocation/Revocation of Priority PDU connectivity services [125](#__RefHeading___Toc517275978)

5.15.3 Invocation/Revocation of IMS Multimedia Priority Services [126](#__RefHeading___Toc517275979)

5.16 Emergency Services [126](#__RefHeading___Toc517275980)

5.17 Mission Critical Services [126](#__RefHeading___Toc517275981)

5.18 Binding Mechanism [126](#__RefHeading___Toc517275982)

5.18.1 General [126](#__RefHeading___Toc517275983)

5.18.2 Session Binding [127](#__RefHeading___Toc517275984)

5.18.3 PCC Rule Authorization [127](#__RefHeading___Toc517275985)

5.18.4 QoS Flow Binding [128](#__RefHeading___Toc517275986)

5.19 AF influence traffic routing [128](#__RefHeading___Toc517275987)

5.19.1 General [128](#__RefHeading___Toc517275988)

5.19.2 Support of traffic routing request [129](#__RefHeading___Toc517275989)

5.20 Event triggers [131](#__RefHeading___Toc517275990)

5.20.1 General [131](#__RefHeading___Toc517275991)

5.20.2 SMF Event triggers handling [131](#__RefHeading___Toc517275992)

5.20.3 AMF Event triggers handling [133](#__RefHeading___Toc517275993)

6 Interworking between the 5G System and external Data Networks (DN) [134](#__RefHeading___Toc517275994)

6.1 Reference Model [134](#__RefHeading___Toc517275995)

6.1.1 General [134](#__RefHeading___Toc517275996)

6.1.1.1 Interworking with external DN with DHCP service [135](#__RefHeading___Toc517275997)

6.2 Functional entities [135](#__RefHeading___Toc517275998)

6.3 System Procedures [136](#__RefHeading___Toc517275999)

6.3.1 DN Authentication & Authorization [136](#__RefHeading___Toc517276000)

6.3.2 IP Address Management [137](#__RefHeading___Toc517276001)

6.3.2.1 IPv4 Address allocation and IPv4 parameter configuration via DHCPv4 [137](#__RefHeading___Toc517276002)

6.3.2.2 IPv6 Prefix allocation via IPv6 stateless address autoconfiguration via DHCPv6 [139](#__RefHeading___Toc517276003)

6.3.2.3 IPv6 parameter configuration via stateless DHCPv6 [140](#__RefHeading___Toc517276004)

6.3.2.4 IP address/prefix allocation via Diameter or RADIUS [140](#__RefHeading___Toc517276005)

6.3.3 IMS Interworking [140](#__RefHeading___Toc517276006)

6.3.3.1 General [140](#__RefHeading___Toc517276007)

6.3.3.2 IMS Interworking Model [141](#__RefHeading___Toc517276008)

6.3.3.3 IMS Specific Configuration in the SMF [141](#__RefHeading___Toc517276009)

6.3.3.4 IMS Specific Procedures in the SMF [142](#__RefHeading___Toc517276010)

6.3.3.4.1 Provisioning of Signalling Server Address [142](#__RefHeading___Toc517276011)

6.3.4 Unstructured PDU type data transferring over N6 [142](#__RefHeading___Toc517276012)

6.3.4.1 General [142](#__RefHeading___Toc517276013)

6.3.4.2 N6 PtP tunnelling based on UDP/IPv6 [142](#__RefHeading___Toc517276014)

6.3.4.3 Other N6 PtP tunnelling mechanisms [143](#__RefHeading___Toc517276015)

6.4 Network Function Service Procedures [143](#__RefHeading___Toc517276016)

6.5 Protocols [143](#__RefHeading___Toc517276017)

7 Network capability exposure aspects of the 5G system [144](#__RefHeading___Toc517276018)

7.1 Reference Model [144](#__RefHeading___Toc517276019)

7.2 Functional entities [145](#__RefHeading___Toc517276020)

7.2.1 NEF [145](#__RefHeading___Toc517276021)

7.2.2 AF [146](#__RefHeading___Toc517276022)

7.3 System Procedures [146](#__RefHeading___Toc517276023)

7.3.1 Procedures for network external capability exposure [146](#__RefHeading___Toc517276024)

7.3.1.1 General [146](#__RefHeading___Toc517276025)

7.3.1.2 Procedures for event monitoring [146](#__RefHeading___Toc517276026)

7.3.1.2.1 General [146](#__RefHeading___Toc517276027)

7.3.1.2.2 Event Exposure subscription [147](#__RefHeading___Toc517276028)

7.3.1.2.2.1 Event Exposure subscription without NEF pre-subscription [147](#__RefHeading___Toc517276029)

7.3.1.2.2.2 Event Exposure subscription with NEF pre-subscription [148](#__RefHeading___Toc517276030)

7.3.1.2.3 Event Exposure notification [148](#__RefHeading___Toc517276031)

7.3.1.3 Procedures for PFD management [149](#__RefHeading___Toc517276032)

7.3.1.4 Procedures for Background Data Transfer Policy management and activation [149](#__RefHeading___Toc517276033)

7.3.2 Procedures for network internal exposure [149](#__RefHeading___Toc517276034)

7.3.3 Procedures for Application Trigger [149](#__RefHeading___Toc517276035)

7.4 Network Function Service Procedures [150](#__RefHeading___Toc517276036)

7.4.1 General [150](#__RefHeading___Toc517276037)

7.4.2 Nnef\_ApplicationTrigger service [151](#__RefHeading___Toc517276038)

7.4.2.1 General [151](#__RefHeading___Toc517276039)

7.4.2.2 Operations [151](#__RefHeading___Toc517276040)

7.4.3 Nnef\_EventExposure service [151](#__RefHeading___Toc517276041)

7.4.3.1 General [151](#__RefHeading___Toc517276042)

7.4.3.2 Operations [152](#__RefHeading___Toc517276043)

7.5 Protocols [152](#__RefHeading___Toc517276044)

7.5.1 Evaluation of candidate protocols for service based interfaces [152](#__RefHeading___Toc517276045)

8 Conclusions and Recommendations [152](#__RefHeading___Toc517276046)

8.1 5G Policy Framework [152](#__RefHeading___Toc517276047)

8.1.1 Protocol solution for Service Based Interfaces [152](#__RefHeading___Toc517276048)

8.2 Interworking between the 5G System and external Data Networks (DN) [153](#__RefHeading___Toc517276049)

8.2.1 Protocol solution for interworking with external DN [153](#__RefHeading___Toc517276050)

8.3 Network capability exposure aspects of the 5G system [153](#__RefHeading___Toc517276051)

8.3.1 Protocol solution for Service Based Interfaces [153](#__RefHeading___Toc517276052)

Annex A: Impacts to Specifications [154](#__RefHeading___Toc517276053)

A.1 New specifications [154](#__RefHeading___Toc517276054)

A.2 Impacted existing specifications [154](#__RefHeading___Toc517276055)

Annex B: Change history [156](#__RefHeading___Toc517276056)

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# 1 Scope

The present document discusses and describes requirements, procedures, service interfaces (for service-based architecture) and protocols from CT3 aspects of 5G System as specified in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [66].

These CT3 aspects include:

- the 5G Policy Framework definition (including new functionalities such as access and mobility management policy support, UE policy support or applicable functionality related to network slicing). Support for non-3GPP access network, handover between non-3GPP access and 3GPP access, roaming aspects and 5G QoS aspects in the scope of the 5G Policy Framework will be part of the study;

- Inter-working with external networks; and

- Network Capability Exposure scenarios (e.g. monitoring and Policy/Charging Capabilities exposure).

The present document is used as a placeholder for CT3 5G System materials to be moved to appropriate 3GPP technical specifications when it is sufficiently stable. As such, neither all the discussions within this document are finished nor the procedures need to be completed. This TR may also contain some empty clauses. This TR will no longer be updated on a systematic manner and therefore contains information may become outdated.

# 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 23.501: "System Architecture for the 5G System; Stage 2".

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

[4] 3GPP TS 23.203: "Policies and Charging control architecture; Stage 2".

[5] IETF RFC 793: "Transmission Control Protocol".

[6] IETF RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2".

[7] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[8] IETF RFC 7159: "The JavaScript Object Notation (JSON) Data Interchange Format".

[9] IETF RFC 768: "User Datagram Protocol".

[10] IETF draft-ietf-quic-transport-04: " QUIC: A UDP-Based Multiplexed and Secure Transport".

[11] IETF draft-ietf-quic-tls-04: "Using Transport Layer Security (TLS) to Secure QUIC".

[12] IETF draft-ietf-quic-http-04: "Hypertext Transfer Protocol (HTTP) over QUIC".

[13] IETF draft-ietf-quic-recovery-04: "QUIC Loss Detection and Congestion Control".

[14] IETF draft-newton-json-content-rules-08: "A Language for Rules Describing JSON Content".

[15] IETF RFC 4960: "Stream Control Transmission Protocol".

[16] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[17] IETF RFC 6733: "Diameter Base Protocol".

[18] "Architectural Styles and the Design of Network-based Software Architectures", UNIVERSITY OF CALIFORNIA, IRVINE, Dissertation of Roy Thomas Fielding, 2000, Chapter 5 "Representational State Transfer (REST)", <https://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm>.

[19] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[20] IETF RFC 3736: "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6".

[21] IETF RFC 3315: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[22] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[23] IETF RFC 1542: "Clarification and Extensions for the Bootstrap Protocol".

[24] IETF RFC 4039: "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[25] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[26] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[27] IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions".

[28] IETF RFC 3361: "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

[29] IETF RFC 3646: "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[30] IETF RFC 3319: "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[31] IETF RFC 6020: "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)".

[32] IETF RFC 6991: "Common YANG Data Types".

[33] IETF RFC 7950; "The YANG 1.1 Data Modeling Language".

[34] IETF RFC 7951: "JSON Encoding of Data Modeled with YANG".

[35] IETF RFC 8040: "RESTCONF Protocol".

[36] OpenAPI Initiative, "OpenAPI 3.0.0 Specification", <https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md>.

[37] 3GPP TS 29.155: "Traffic steering control; Representational state transfer (REST) over St reference point".

[38] 3GPP TS 29.250: "Nu reference point between SCEF and PFDF for sponsored data connectivity".

[39] 3GPP TS 29.251: "Gw and Gwn reference points for sponsored data connectivity".

[40] 3GPP TS 29.116: "Representational state transfer over xMB reference point between Content Provider and BM-SC".

[41] IETF draft-wright-json-schema-01: "JSON Schema: A Media Type for Describing JSON Documents".

[42] IETF draft-wright-json-schema-validation-01: "JSON Schema Validation: A Vocabulary for Structural Validation of JSON".

[43] IETF draft-ietf-cbor-cddl-00: "Concise data definition language (CDDL): a notational convention to express CBOR data structures".

[44] IETF draft-ietf-core-yang-cbor-04: "CBOR Encoding of Data Modeled with YANG".

[45] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[46] 3GPP TS 29.328: "IP Multimedia (IM) Subsystem Sh interface; Signalling flows and message contents".

[47] IETF RFC 7049: "Concise Binary Object Representation (CBOR)".

[48] Presentation of Leonard Richardson at the QCon Conference. San Francisco (2008): "Justice Will Take Us Millions Of Intricate Moves", Act Three: "The Maturity Heuristic", <https://www.crummy.com/writing/speaking/2008-QCon/act3.html>.

[49] Draft ETSI GS MEC 009 V1.0.1 (2017): "Mobile Edge Computing (MEC); General principles for Mobile Edge Service APIs".

[50] Wikipedia article: "Remote procedure call", <https://en.wikipedia.org/wiki/Remote_procedure_call>.

[51] API Design Guide, Google, "https://cloud.google.com/apis/design/".

[52] IETF RFC 6202: "Known Issues and Best Practices for the Use of Long Polling and Streaming in Bidirectional HTTP".

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

[54] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[55] 3GPP TS 23.379: "Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2".

[56] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[57] 3GPP TS 22.280: "Mission Critical Services Common Requirements".

[58] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[59] IETF RFC 7541: "HPACK: Header Compression for HTTP/2".

[60] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[61] IETF RFC 7232: "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests".

[62] IETF RFC 7233: "Hypertext Transfer Protocol (HTTP/1.1): Range Requests".

[63] IETF RFC 7234: "Hypertext Transfer Protocol (HTTP/1.1): Caching".

[64] IETF RFC 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication".

[65] C4-174201: "GSMA NG Signal LS to 3GPP CT4 on 5G signalling protocol requirements".

[66] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[67] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[68] 3GPP TS 29.213: "Policy and Charging Control signalling flows and Quality of Service (QoS) parameter mapping".

[69] IEEE 802.3: "IEEE Standard for Ethernet".

[70] IEEE 802.1Q: "Local and metropolitan area networks--Bridges and Bridged Networks".

[71] 3GPP TS 29.122: "T8 reference point for Northbound APIs".

[72] 3GPP TS 29.518: "5G System; Access and Mobility Management Services; Stage 3".

[73] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[74] IETF RFC 3576: "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)".

[75] IETF RFC 6733: "Diameter Base Protocol".

# 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].

**Data Network Name**: Data Network Name is defined in 3GPP TS 23.501 [2], and it is equivalent to an APN.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.501 [2], subclause 3.1 apply:

**5G Access Network**

**5G Core Network**

**5G QoS Flow**

**5G QoS Identifier**

**5G System**

**Local Break Out (LBO)**

**Network Function**

**NF service**

**NF service operation**

**PDU Connectivity Service**

**PDU Session**

**PDU Session Type**

**Service based interface**

**Service Data Flow Filter**

**Service Data Flow Template**

## 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].

5GC 5G Core Network

5QI 5G QoS Identifier

AF Application Function

AMBR Aggregate Maximum Bit Rate

AMF Access and Mobility Management Function

AN Access Network

APN Access Point Name

ARP Allocation and Retention Priority

BSF Binding Support Functionality

BSON Binary JSON

CBOR Concise Binary Object Representation

CDDL Concise Data Definition Language

DEI Drop Eligible Indicator

DHCP Dynamic Host Configuration Protocol

DL Downlink

DN Data Network

DNAI Data Network Access Identifier

DNN Data Network Name

DTLS Datagram Transport Layer Security

EPC Evolved Packet Core

GBR Guaranteed Bit Rate

GPSI Generic Public Subscription Identifier

HATEOAS Hypermedia As The Engine Of Application State

HTTP Hypertext Transfer Protocol

IDL Interface Definition Language

JSON JavaScript Object Notation

MAC Media Access Control

MBR Maximum Bit Rate

MPS Multimedia Priority Service

NBIFOM Network Based IP Flow Mobility

NEF Network Exposure Function

NF Network Function

NSSAI Network Slice Selection Assistance Information

NWDAF Network Data Analytics Function

OCS Online Charging System

PCC Policy and Charging Control

PCF Policy Control Function

PCP Priority Code Point

PEI Permanent Equipment Identifier

PFDF Packet Flow Description Function

QFI QoS Flow Identifier

QNC QoS Notification Control

QoS Quality of Service

REST Representational State Transfer

RFSP RAT Frequency Selection Priority

RPC Remote procedure call

RQI Reflective QoS Indicator

SCTP Stream Control Transmission Protocol

SDF Service Data Flow

SMF Session Management Function

S-NSSAI Single Network Slice Selection Assistance Information

SSC Session and Service Continuity

SUPI Subscription Permanent Identifier

TA Tracking Area

TAI Tracking Area Identity

TCP Transmission Control Protocol

TLS Transport Layer Security

UDM Unified Data Management

UDP User Datagram Protocol

UDR Unified Data Repository

UL Uplink

UPF User Plane Function

URSP UE Route Selection Policy

VID VLAN Identifier

VLAN Virtual Local Area Network

# 4 Requirements

## 4.1 General Requirements

### 4.1.1 Architecture Requirements

**Architecture requirement #1**: The proposed solutions shall be aligned with the related functionality as described in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [66].

### 4.1.2 Requirements for protocol selection for service based interfaces

R1. Support of bidirectional communication (Rational: stage 2 requirements that service based interfaces support Request-Response and Subscription-Notification, where subscription can be optional).

R2. Support of reliable communication (in some level of the protocol stack, a reliable message delivery needs to be guaranteed. It appears preferable not to burden the application with that to exploit communalities. Is link-level failover supported?).

R3. Forward compatibility and ease of upgrade (protocol needs to be extensible, also outside standards, and a concept for operation between nodes with different capability levels is required).

R4. Low Response Time. The solution shall also support varying response times, e.g. in roaming and interconnection, latency between 100ms and 5s are usually considered for signalling end-to-end transport (see C4-174201 "GSMA NG Signal LS to 3GPP CT4 on 5G signalling protocol requirements" [65]).

R5. Scalability to large numbers of transactions per service, support long-lived connection and the number of required transport connections should be manageable and not cause hindrance to system performance.

R6. Ease and speed of deployment and instantiation/deinstantiation of network functions and services with minimal impacts on the network.

R7. Time of Availability of used standards.

### 4.1.3 Additional evaluation criteria for protocol selection for service based interfaces

A1. Resource-efficiency (message size and processing requirements?).

A2. Reusability of existing 3GPP implementations (Can existing implementations and deployments be partially reused? How large are the impacts for inter-operator and/or inter-domain interfaces? This includes interworking with legacy networks.).

A3. Minimize number of protocols in network (The overall number of protocols to be supported in a network and at any a given type of network function should be minimized. Selected protocol should be able to support intra- and inter-operator interfaces.).

A4. Congestion, load and overload control.

A5. Support of Security (in particular per service authentication, authorization and possibly encryption, in particular for inter-operator communication).

A6. Ease of troubleshooting and monitoring (Message Traceability and Monitoring). For monitoring and reporting for roaming/interconnection, it is very helpful that an answer follows the same path (i.e. same proxies) as its request (see C4-174201 "GSMA NG Signal LS to 3GPP CT4 on 5G signalling protocol requirements" [65]).

A7. Ease of use of 3GPP services from operator owned application functions (such application function can be used to implement operator-specific services).

A8. Support of service and/or message based failover and failback.

A9. Support of network entity selection based on UE context information (e.g. based on dynamic UE session information).

A10. Ease of traversal of carrier-grade ALG/NAT/firewall.

A11. Impacts to GSMA GRX/IPX.

A12. Open and public Source/Standardization body. (3GPP needs to be able to access SDO sources; this also includes support of the protocol maintenance and ease for 3GPP to extend the protocol).

A13. Protocol enables stateless operation.

A14. Routing support and related mechanisms.

A15. Support of strong error detection and error reporting capabilities.

A16. Support of multiplexing of messages belonging to multiple sessions over a single transport connection.

A17. Support of well-defined schema and unambiguous interpretation of transported data.

## 4.2 Requirements for the 5G Policy Framework

**5GPF requirement #1**: The proposed stage 3 5G Policy Framework shall be aligned with the requirements as described in 3GPP TS 23.503 [66], Annex A.1. That is:

1) A generic PCC framework as defined in 3GPP TS 23.203 [4] including relevant 5G applicable parts for the 5G Policy Framework:

a) The 5G Policy Framework includes the following Functional Elements: The Policy Control Function (PCF), the Session Management Function (SMF), the Application Function (AF), the Online Charging System (OCS), the Unified Data Repository (UDR) and the Network Exposure Function (NEF).

b) The PCF shall be able to evaluate operator policies that are triggered by events received from the SMF, the NEF, the AF, and the OCS.

c) The PCF shall provide Rules for application and service data flow detection, gating, QoS and flow based charging to the SMF.

d) The 5G Policy Framework shall be able to manage the Packet Filter Descriptions (PFDs) in the SMF by the 3rd party AS via the NEF.

e) The 5G Policy Framework shall support to negotiate the background data transfer policy with the 3rd party AS via the NEF.

f) The PCF shall implement a Front End to access subscription information relevant for policy decisions in a Unified Data Repository (UDR) including dynamic profile updates pushed by the UDR.

g) Traffic Steering Control for steering traffic shall be supported for the services on the DN side of the N6 reference point.

h) The 5G Policy Framework shall support IMS Services, Multimedia Priority Services, Emergency Services and Mission critical services.

NOTE: The existing PCC framework is applicable to PDU sessions of IPv4 and IPv6 Types only.

2) Extensions to the PCC framework defined in 3GPP TS 23.203 [4] include:

a) The 5G Policy Framework includes the following additional Functional Elements: the Access and Mobility Management Function (AMF) and the Network Data Analytics Function (NWDAF).

b) The PCF shall be able to provide Access and Mobility Management related policies and UE policies to the AMF.

c) The PCF shall be able to evaluate operator policies that are triggered by events received from the AMF.

d) For a subscriber roaming in a visited PLMN, the visited PLMN shall be able to receive the subscriber's mobility policy data.

e) The PCF shall be able to take input from Network Data Analytics Function (NWDAF) into consideration for policies on assignment of network resources and for traffic steering policies.

Editor's note: The list in bullets 1 and 2 covers the high level requirements that are addressed in the document so far according to the current status of the specification(s). Additional or modified requirements are to be added when the related information is agreed.

Editor's note: Current list of requirements for the Policy Framework are based on an informative Annex in TS 23.503. This has to be updated and has to refer to the proper specification(s) when this information is made normative in stage 2.

**5GPF requirement #2**: The proposed stage 3 5G Policy Framework interfaces shall, in addition to 5G functionality, support the EPC functionality as defined in 3GPP TS 23.203 [4] in order to allow interworking with EPC networks.

**5GPF requirement #3**: The proposed stage 3 5G Policy Framework shall provide a mechanism for PCC network functions discovery and selection.

**5GPF requirement #4**: The proposed stage 3 5G Policy Framework shall be able to provide the QoS mapping mechanisms to apply the proper 5G QoS information based on the relevant QoS information as provided by the Application Function and/or Network Exposure Function.

**5GPF requirement#5**: It shall be possible to apply QoS control at service data flow level, QoS flow level or PDU session level in the SMF.

**5GPF requirement #6:** A PCC rule may be predefined or dynamically provisioned at establishment and during the life time of a PDU session. The latter is referred to as a dynamic PCC rule.

**5GPF requirement#7:** The number of real-time PCC interactions shall be minimized although not significantly increasing the overall system reaction time. This requires optimized interfaces between the PCC nodes.

## 4.3 Requirements for interworking between the 5G System and external Data Networks

**5GDN requirement #1**: The proposed stage 3 solutions shall provide a mechanism for interaction with external DN for transport of signalling PDU session authorization/authentication by external DN as specified in 3GPP TS 23.501 [2].

**5GDN requirement #2**: The proposed stage 3 solutions shall provide a mechanism for interaction with external DN for transport of user plane information by/to external DN as specified in 3GPP TS 23.501 [2].

## 4.4 Requirements for Network Capability Exposure of 5G System

**5GNCE requirement #1**: The proposed stage 3 solution shall comply with the exposure functionality as defined in 3GPP TS 23.501 [2] for Policy/Charging and identified monitoring and provisioning capabilities.

NOTE: External exposure can be categorized as Monitoring capability, Provisioning capability, and Policy/Charging capability. The Monitoring capability is for monitoring of specific event for UE in 5G system and making such monitoring events information available for external exposure via the NEF. The Provisioning capability is for allowing external party to provision of information which can be used for the UE in 5G system. The Policy/Charging capability is for handling QoS and charging policy for the UE based on the request from external party.

**5GNCE requirement #2**: The proposed stage 3 solution shall provide mechanism(s)for both internal and external exposure as defined in 3GPP TS 23.501 [2].

# 5 5G Policy Framework

## 5.1 Reference Model

The policy framework functionality in 5G is comprised by the functions of the Policy Control Function (PCF), the policy and charging enforcement functionality supported by SMF and UPF, the access and mobility policy enforcement functionality supported by the AMF, the Network Data Analytics Function (NWDAF), the Network Exposure Function (NEF), the Online Charging System (OCS), the Unified Data Repository (UDR) and the Application Function (AF). 3GPP TS 23.501 [2] specifies the 5G policy framework stage 2 functionality.



Figure 5.1-1a: Overall non-roaming 5G Policy framework architecture (service based representation)



Figure 5.1-1b: Overall non-roaming 5G Policy framework architecture (reference point representation)

Editor's note: Implications from multiple Slices and its relation to PCF are FFS in stage 2.

NOTE 1: The PCEF functionality defined in 3GPP TS 23.203 [4] corresponds to the functions supported by the SMF and the UPF.

Editor's note: 5GC interfaces corresponding to the PCEF interfaces towards charging system are FFS.

NOTE 2: The N4 interface is not part of the Policy Framework architecture but shown in the figures for completeness.

NOTE 3: The reference point PGw supports equivalent functionality as Gw between PFDF and PCEF in EPC.

NOTE 4: The interactions between the PCF and the AF need to provide the Rx functionalities as defined in 3GPP TS 23.203 [4] to allow the 5GC to interwork with the AFs related to the existing services e.g. IMS based services and Mission critical services.



Figure 5.1-2a: Overall roaming policy framework architecture - local breakout scenario (service based representation)



Figure 5.1-2b: Overall roaming policy framework architecture - local breakout scenario (reference point representation)

NOTE 5: In the local breakout scenario, the PCF in the VPLMN can interact with the AF in order to generate PCC Rules for services delivered via the VPLMN. The PCF in the VPLMN uses locally configured policies according to the roaming agreement with the HPLMN operator as input for PCC Rule generation. The PCF in the VPLMN has no access to subscriber policy information from the HPLMN to retrieve input for PCC Rule generation. The interactions between the PCF in the VPLMN and the PCF in the HPLMN through the Npcf service based interface enables the PCF in the HPLMN to provision access and mobility policy rules and UE policies to the PCF in the VPLMN, as described in 3GPP TS 23.503 [66] subclause 5.2.5.

Editor's note: Position of the NWDAF in 5G roaming policy framework architecture for local breakout scenario is still FFS in SA2.



Figure 5.1-3a: Overall roaming policy framework architecture - home routed scenario (service based representation)



Figure 5.1-3b: Overall roaming policy framework architecture - home routed scenario (reference point representation)

## 5.2 Functional Entities

### 5.2.1 Policy Control Function (PCF)

The PCF is a functional element for policy control decision and flow based charging control functionalities. The PCF provides the following functions:

- policy rules for application and service data flow detection, gating, QoS and flow based charging to the SMF.

- Access and Mobility Management related policies to the AMF. The policies provided from PCF to AMF includes Service Area Restrictions and RFSP index.

- UE policies that include Access Network discovery and selection policies and URSP to the AMF.

The policy decisions made by the PCF may be based on one or more of the following:

- Information obtained from the AF, e.g. the session, media and subscriber related information.

- Information obtained from the UDR. The PCF implements a Front End to access subscription information relevant for policy decisions in a UDR.

- Information obtained from the AMF, e.g. UE related and access related information.

- Information obtained from the SMF.

- Information obtained from the NWDAF.

- Information obtained from the NEF.

- Information obtained from the OCS.

- Information obtained from another PCF in the roaming scenario.

- Own PCF pre-configured information.

### 5.2.2 Session Management Function (SMF)

The 5GC Policy Framework interface corresponding to the PCEF interface is supported by the SMF and corresponds to the N7 reference point.

The SMF is responsible for the enforcement control of policy decisions related to QoS, charging, gating, service flow detection, packet routing and forwarding, traffic usage reporting.

The actual enforcement of QoS, charging, gating, service flow detection, packet routing and forwarding and traffic accounting and reporting policy decisions is distributed among the UPF, RAN and UE depending on the policy type.

The SMF functionality related to policy and charging enforcement control includes:

- creating the context of SM related policies;

- updating the context of SM related policies;

- deleting the context of SM related policies;

- subscribing for event notifications on the specified PDU session; and

- notifying about subscribed events on the PDU session.

Editor's note: It is FFS to consider the related services for policy request and event notification or to explicitly indicate that the modification also includes event reporting.

### 5.2.3 Access and Mobility Management Function (AMF)

The AMF includes the following functionality:

- Handling of UE Context Establishment request sent by the AMF to the PCF as part of UE Registration procedure(s);

- Handling of UE Context Modification request sent by the AMF to the PCF when the conditions related to the access and mobility management decision (e.g. UE location) change.

- Handling of UE Context Modification request sent by the PCF to the AMF when the policy information related to the UE changes.

- Receive the access and mobility management decision from the PCF to the AMF;

- Delivery of network events from the AMF to the PCF;

- Handling of UE Context Termination request sent by the AMF to the PCF as part of UE De-Registration procedure.

### 5.2.4 Application Function (AF)

Within the Policy Framework, the AF is a functional element that communicates to the PCF to transfer dynamic application session information required for the PCF decisions (e.g. service specific information, application influence on traffic routing) as well as to receive PDU service specific information and notifications about PDU events.

If not allowed by the operator to communicate directly with the PCF, the AF shall use the external exposure network to communicate with the PCF via the NEF.

### 5.2.5 Network Data Analytics Function (NWDAF)

The NWDAF is a functional element to provide slice specific network data analytics. NWDAF notifies/publishes slice specific network status analytic information to the PCF(s). PCF(s) can collect directly slice specific network status analytic information from NWDAF. This information may be used for policy decisions.

Load level information of network slice is provided by the NWDAF.

NOTE: How the information is used by the PCF is not standardized in Release 15.

### 5.2.6 Network Exposure Function (NEF)

The NEF is a functional element to support the following functionality in 5G policy framework:

- It provides a means to securely expose the services and capabilities provided by the PCF as described in clause 7.

- It supports management of Packet Filter Descriptions (PFDs) as described in clause 7.

- It supports the negotiation and activation of background data transfer policy as described in clause 7.

### 5.2.7 Unified Data Repository (UDR)

The UDR is a functional element that supports the following PCC related functionalities:

- Storage and retrieval of the policy data by the PCF.

- Retrieval of subscription data by the PCF.

- Storage of the structured data e.g. by the NEF, such as application detection data of the Packet Flow Descriptions and application request information for one or multiple UEs.

Editor's note: The entities that retrieve the structured data are FFS.

## 5.3 System Procedures

Editor's note: The procedures in this clause need to be aligned with the PCF service(s) or procedures defined in stage 2.

### 5.3.1 Procedures for Npcf\_AMPolicyControl service

#### 5.3.1.1 Policy request during UE registration

This procedure is performed when the UE needs to perform initial registration to the 5G system or needs to perform the registration with the AMF relocation.



Figure 5.3.1.1-1: Policy request during UE registration

1. The AMF receives the registration request from the AN. The AMF can obtain Service Area Restrictions, RFSP index, and GPSI from the UDM during the update location procedure. Based on local policy, the AMF selects to contact the PCF. The AMF selects the PCF as described in subclause 5.10.2 and invokes the Npcf\_AMPolicyControl\_Get service operation to request the PCF to create the policy context in the PCF and to retrieve the UE policies and/or Access and Mobility control policies. The request operation provides the SUPI, and if received from the UDM, the Service Area Restrictions, RFSP index, and GPSI, and may provide the access type, the PEI if received in the AMF, the User Location Information if available, the UE Time Zone if available, Serving Network, RAT type, GPSI. The request also includes a Notification URI to indicate to the PCF where to send a notification when the policy/ies is/are updated.

2. If PCF does not have the subscription data for the UE, the PCF invokes the Nudr\_UnifiedDataManagement\_Query service operation and includes in the request to the UDR the PCF Identifier and the Data Identifier which uniquely identifies the requested subscription data within the UDR i.e. SUPI.

The UDR responds to the PCF with the subscription data that may include UE policies and Access and Mobility control policies.

3. The PCF makes the requested policy decision including, e.g. UE policies such as Service Area Restrictions, RAT Frequency Selection Priority (RFSP) Index and UE Route Selection Policy (URSP) and may determine applicable event trigger(s).

4. The PCF responds to the AMF by including requested policy:

- UE policy (see subclause 5.8) including UE Access Network discovery and selection policies and/or UE Route Selection Policies (URSP) of the UE; and/or

- AMF Access and Mobility Policy (see subclause 5.6) including Service Area Restrictions, and/or a RAT Frequency Selection Priority (RFSP) Index,

as determined by the PCF.

5. The PCF can subscribe to the Namf\_EventExposure service.

NOTE: The definition of the Namf\_EventExposure service is out of scope of the present study.

#### 5.3.1.2 Policy update

##### 5.3.1.2.1 Update initiated by the AMF

This procedure is performed when the conditions impacting the access and mobility control policies change, e.g. UE location.

Editor's note: Whether this procedure is needed is FFS. There are no such stage 2 requirements so far.



Figure 5.3.1.2.1-1: Policy update initiated by the AMF event notification

1. The AMF uses the Namf\_EventExposure\_Notify service operation to indicate that an event that requires reporting to the PCF has occurred.

2. Step 1 through step 3 as specified in subclause 5.3.1.2.2 "Update initiated by the PCF".

##### 5.3.1.2.2 Update initiated by the PCF

This procedure is performed when the UE policies and/or Access and Mobility control policies are changed.



Figure 5.3.1.2.2-1: Policy update initiated by the PCF

1. The PCF makes policy decisions to modify the policy context based on the changed condition, the changed UE policies, or Access and Mobility control policies (e.g. subscription update, event notification that triggers the change of Access and Mobility control policy, analytics information received from the NWDAF).

2. The PCF invokes the Npcf\_AMPolicyControl\_UpdateNotify service operation to the AMF that has previously subscribed and includes SUPI in the Npcf\_AMPolicyControl\_UpdateNotify service operation. If this procedure is required to update AMF Access and Mobility policies, the Npcf\_AMPolicyControl\_UpdateNotify service operation also includes Service Area Restrictions and/or RFSP index. If this procedure is required to update the UE policies, the Npcf\_AMPolicyControl\_UpdateNotify service operation includes URSP and/or UE Access Network discovery and selection policies.

3. The AMF enforces the corresponding policies and responds to the PCF, indicating a success or failure of the policy enforcement.

#### 5.3.1.3 Policy context deletion

##### 5.3.1.3.1 Policy context deletion initiated by the AMF

This procedure is performed when the UE deregisters from the network or when the old AMF removes the UE context during handover.



Figure 5.3.1.3.1-1: Policy context deletion initiated by the AMF

1. The AMF sends the Npcf\_AMPolicyControl\_Delete service operation to delete the policy context in the PCF. The request operation includes SUPI.

2. The PCF deletes the policy context for that AMF.

NOTE: The PCF can unsubscribe from data modification notifications from the UDR.

3. The PCF responds to the AMF and in the response the PCF indicates result (success/failure) of the Npcf\_AMPolicyControl\_Delete service operation.

##### 5.3.1.3.2 Policy context deletion initiated by the PCF

This procedure is performed when the PCF decides to terminate the policy context.

Editor's note: Whether this procedure is need is FFS. There are no such stage 2 requirements so far.



Figure 5.3.1.3.2-1: Policy context deletion initiated by the PCF

1. The PCF makes policy decisions to terminate the policy context based on the external trigger, e.g. UE subscription data is deleted, or internal trigger, e.g. operator policy is changed.

2. The PCF sends the Npcf\_AMPolicyControl\_UpdateNotify service operation to the AMF that has previously subscribed.

Editor's note: The parameters sent by the PCF are FFS.

3. The AMF sends the response to the Npcf\_AMPolicyControl\_UpdateNotify service operation to the PCF.

4. Step 1 through step 3 in subclause 5.3.1.3.1 "Policy context deletion initiated by the AMF".

### 5.3.2 Procedures for Npcf\_SMPolicyControl service

#### 5.3.2.1 Request of Session Management (SM) related policies

This procedure is performed when the UE requests to establish a PDU session.



Figure 5.3.2.1-1: Request the SM related policies

1. The SMF receives a PDU session establishment request from the UE. The SMF selects the PCF as described in subclause 5.10.3 and invokes the Npcf\_SMPolicyControl\_Get service operation to request the SM related policies in the PCF and to get the default PCC Rules for the PDU session. The request operation provides the SUPI, the PDU session ID and DNN. The request operation can provide the GPSI, the access type, the IPv4 address and/or the IPv6 network prefix (if available), the PEI if received in the SMF, the User Location Information, the UE Time Zone, Serving Network, RAT type, charging information, the Session-AMBR and the default QoS information, if available. The request operation also includes a Notification URI to indicate to the PCF where to send a notification when the SM related policies are updated.

2. If PCF does not have the subscription data for the SUPI and DNN, the PCF invokes the Nudr\_UnifiedDataManagement\_Query service operation to the UDR and includes the PCF Identifier and the Data Identifier which uniquely identifies the requested subscription data.

The UDR responds to the PCF with the subscription data.

Editor's note: The interaction between the PCF and UDR are FFS.

3. The PCF makes the policy decision to determine the information provided in step 4 and to determine the event trigger to subscribe to event(s) in step 5.

Editor's note: Other policies determined by the PCF are FFS.

4. The PCF responds to the SMF and includes in the response of the Npcf\_SMPolicyControl\_Get service operation the policy determined by the PCF. The policy information provided by the PCF is the PCC rules of the PDU session, the authorized Session-AMBR and the authorized default QoS information.

5. Step 2 through step 3 as specified in subclause 5.3.3.1 "PCF initiated events subscription".

#### 5.3.2.2 Update of Session Management (SM) related policies

##### 5.3.2.2.1 PCF initiated update of SM related policies

This procedure is performed when the PCF decides to modify policy decisions for a PDU session.

Editor's note: Other triggers to initiate the procedure is FFS.



Figure 5.3.2.2.1-1: Update of SM related policies initiated by the PCF

1. The PCF makes policy decisions to modify the information provided for the PDU session based on e.g. the operation policy or upon AF requests or the UE subscription data is modified.

Editor's note: The interaction between the PCF and UDR, and the interaction between the PCF and AF is FFS.

2. The PCF invokes the Npcf\_SMPolicyControl\_UpdateNotify service operation to the SMF that has previously subscribed and includes the PDU session ID and can include the updated PCC Rules of the PDU session, the authorized Session-AMBR and the authorized default QoS information.

3. The SMF provides to the PCF the result (success/failure) of the Npcf\_SMPolicyControl\_UpdateNotify service operation.

4. If the PCF decides to modify the subscribed events, step 2 through step 3 as specified in subclause 5.3.3.1 "PCF initiated events subscription" are executed.

##### 5.3.2.2.2 SMF triggered update of SM related policies

This procedure is performed when the SMF observes some events that the PCF has subscribed to.



Figure 5.3.2.2.2-1: Update of SM related policies triggered by an SMF event

1. Step 2 through step 4 as specified in subclause 5.3.3.2 "SMF Notification about subscribed events".

2. If the PCF decides to modify the policy and/or the subscribed events based on the event information received in step 1, step 1 through step 4 as specified in subclause 5.3.2.2.1 "PCF initiated update of SM related policies" are executed.

#### 5.3.2.3 Deletion of the context of SM related policies

##### 5.3.2.3.1 Deletion of the context of SM related policies initiated by the SMF

This procedure is performed during the PDU session termination.



Figure 5.3.2.3.1-1: Deletion of the context of SM related policies initiated by the SMF

1. The SMF invokes the Npcf\_SMPolicyControl\_Delete service operation to request the PCF to delete the context of the SM related policy. The request operation includes the PDU session ID to identify the context of SM related policies that was initially created and information the SMF received during the PDU session termination that is relevant for the PCF e.g. usage monitoring information (if applicable) or access network information.

Editor's note: The parameters sent to the PCF by the SMF are FFS. Apart from the PDU session ID, Stage 2 only list "Relevant information for the PCF". It also needs to be considered which information is rather provided based on subscription using the Nsmf\_EventExposure\_Notify service operation.

2. The PCF removes the corresponding context of SM related policies.

3. The PCF responds to the SMF and in the response the PCF indicates result (success/failure) of the Npcf\_SMPolicyControl\_Delete service operation.

##### 5.3.2.3.2 Deletion of the context of SM related policies initiated by the PCF

This procedure is performed when the PCF requests to terminate a PDU session based on some external or internal triggers as described in step 1 below.



Figure 5.3.2.3.2-1: Deletion of the context of SM related policies initiated by the PCF

1. The PCF makes policy decisions to terminate a PDU session based on some external trigger, e.g. UE subscription data is deleted, or based on some internal trigger, e.g. operator policy is changed.

2. The PCF sends the Npcf\_SMPolicyControl\_UpdateNotify service operation to trigger the SMF to request the release of the PDU session. The PCF includes the PDU session ID and an indication to terminate the PDU session.

3. The SMF provides to the PCF the result (success/failure) of the Npcf\_SMPolicyControl\_UpdateNotify service operation.

4. Step 1 through step 3: as specified in subclause 5.3.2.3.1 "Deletion of the context of SM related policies initiated by the SMF", as needed.

### 5.3.3 Procedures for Nsmf\_EventExposure service

#### 5.3.3.1 PCF subscription to events

This procedure is performed at PDU session establishment for the PCF to subscribe at least to the events that always require PCF subscription, and at any time during the PDU session lifetime when the PCF decides to subscribe to events for a PDU session. Both, events that always require PCF subscription and events that depend on PCF policy decision can be subscribed with the same Nsmf\_EventExposure\_Subscribe service operation.

Editor's note: Other triggers to initiate the procedure are FFS.



Figure 5.3.3.1-1: Subscription to events by the PCF

1. The PCF makes policy decision to subscribe to events for the PDU session based on e.g. the operator policy or an AF request or when the UE subscription data is modified.

Editor's note: The interaction between the PCF and the UDR, and the interaction between the PCF and the AF is FFS.

2. The PCF may subscribe to events from the SMF by invoking Nsmf\_EventExposure\_Subscribe service operation indicating the PDU Session ID, UE ID (SUPI or GPSI or IP address and DNN), and the subscribed event (including the event filters and the requested notification method (periodic, one time, on event detection) and optionally an immediate one time notification flag and reporting options (e.g. Maximum Number of Reports or Monitoring Duration). The PCF also supplies a Notification URI to indicate where to send notifications.

3. The SMF provides a response to the Nsmf\_EventExposure\_Subscribe service operation. If the request is accepted the SMF returns the Event correlation ID indicating the requested subscription is created.

The Nsmf\_EventExposure\_Subscribe service operation including the Event correlation ID is invoked by the PCF when it needs to modify an existing subscription previously created by itself in the SMF.

#### 5.3.3.2 SMF Notification about subscribed events

This procedure is performed when the SMF notifies the PCF that some PDU session related event(s) occurred for which the PCF has subscribed to event notifications.



Figure 5.3.3.2-1: SMF Notification about the PCF subscribed event

1. An event to which the PCF has subscribed to occurs.

2. The SMF sends the Nsmf\_EventExposure\_Notify service operation to the Notification URI provided by the PCF to indicate that an event previously subscribed by the PCF has occurred. The SMF provides the PDU Session ID, UE ID (SUPI or GPSI or IP address and DNN), the Event correlation ID, and the Event Trigger describing the event.

3. The PCF sends the response to the Nsmf\_EventExposure\_Notify operation.

4. The PCF makes policy decision and if applicable, the PCF may send an event notification to the AF.

#### 5.3.3.3 PCF unsubscription to events

This procedure is performed when the PCF decides to unsubscribe to all previously subscribed events for a PDU session.

Editor's note: Other triggers to initiate the procedure are FFS.



Figure 5.3.3.3-1: Unsubscription to events by the PCF

1. The PCF makes policy decision to unsubscribe to all previously subscribed events for the PDU session based on e.g. operator policy or upon AF requests or when the UE subscription data is modified.

Editor's note: The interaction between the PCF and the UDR, and the interaction between the PCF and the AF is FFS.

2. The PCF may unsubscribe to events from the SMF by sending Nsmf\_EventExposure\_UnSubscribe service operation indicating the Event correlation ID to cancel.

3. The SMF provides the response to the Nsmf\_EventExposure\_UnSubscribe service operation.

### 5.3.4 Procedures over N24 reference point

### 5.3.5 Procedure for Npcf\_PolicyAuthorization service

#### 5.3.5.1 Initial provisioning of service information

This procedure is performed when the AF/NEF requests to create an AF application session context for the requested service.

NOTE: The NEF acts as an AF to support the network exposure functionality.



Figure 5.3.5.1-1: Create the AF application session context

1. The AF receives a AF session establishment request. The AF invokes the Npcf\_PolicyAuthorization\_Create service operation to the PCF including the AF Identifier, the IP address of the UE, the identification of the application session context, the SUPI if available, the DNN if available, Media information (Media type, Media format), bandwidth requirements, sponsored data connectivity if applicable, flow description, AF application identifier, Flow status, Priority indicator, emergency indicator, Application service provider, resource allocation outcome.

Editor's note: The complete set of parameters sent to the PCF by the AF are FFS.

2. If PCF does not have the subscription data for the SUPI and DNN, the PCF invokes the Nudr\_UnifiedDataManagement\_Query service operation to the UDR including the PCF identifier, the SUPI and the requested subscription data.

The UDR responds to the PCF with the subscription data.

3. The PCF processes the received service information according to the operator policy and can decide whether the request is accepted or not.

4. The PCF responds to the AF.

5. If the AF request was accepted in step 3, the PCF determines the PCC Rules to be created and provisioned. Provisioning of PCC rules to the SMF is carried out as described in subclause 5.3.2.2.1 "PCF initiated update of SM related policies".

#### 5.3.5.2 Modification of service information

This procedure is performed when the AF/NEF requests to update an AF application session context for the requested service.

NOTE: The NEF acts as an AF to support the network exposure functionality.



Figure 5.3.5.2-1: Update the AF application session context

1. The AF receives a AF session modification request. The AF invokes the Npcf\_PolicyAuthorization\_Update service operation to the PCF including the modified service information.

Editor's note: The complete set of parameters sent to the PCF by the AF are FFS.

2. If PCF does not have the subscription data for the SUPI and DNN corresponding to the application session context to update, the PCF sends the Nudr\_UnifiedDataManagement\_Query service operation to the UDR including the PCF identifier, the SUPI and the requested subscription data.

The UDR responds to the PCF with the subscription data.

3. The PCF processes the received service information according to the operator policy and can decide whether the request is accepted or not.

4. The PCF responds to the AF.

5. If the AF request was accepted in step 3, the PCF determines the PCC Rules to be created and provisioned. Provisioning of PCC rules to the SMF is carried out as described in subclause 5.3.2.2.1 "PCF initiated update of SM related policies".

#### 5.3.5.3 AF application session context termination

##### 5.3.5.3.1 Delete the AF application session context initiated by the AF

This procedure is performed when the AF/NEF requests to delete the AF application session context.

NOTE: The NEF acts as an AF to support the network exposure functionality.



Figure 5.3.5.3.1-1: Delete the AF application session context initiated by the AF

1. The AF sends the Npcf\_PolicyAuthorization\_Delete request including the information which identifies the AF application session context.

2. The PCF removes the AF application session context and sends the Npcf\_PolicyAuthorization\_Delete Response indicating deletion of the AF application session context in the PCF.

3. The PCF determines the PCC Rules to be removed. Deletion of PCC rules to the SMF is carried out as described in subclause 5.3.2.2.1 "PCF initiated update of SM related policies".

4. The PCF determines the events to unsubscribe for an active PDU session and can invoke an Nsmf\_EventExposure\_Unsubscribe service operation to the SMF.

##### 5.3.5.3.2 Delete the AF application session context initiated by the PCF

This procedure is performed when the PCF requests the AF/NEF to delete the AF application session context.

NOTE: The NEF acts as an AF to support the network exposure functionality for policy/charging capability.



Figure 5.3.5.3.2-1: Delete the AF application session context initiated by the PCF

1. The PCF can determine to terminate an ongoing application session context based on external or internal trigger.

2. The PCF invokes the Npcf\_PolicyAuthorization\_Notify service operation to the AF to indicate the AF application session context is no longer valid. The PCF includes information to identify the AF application session context, and an AF application session context termination cause.

Editor's note: The parameters sent by the PCF are FFS.

3. The AF sends response to the Npcf\_PolicyAuthorization\_Notify service operation.

Editor's note: The parameters sent by the AF are FFS.

4. Step 1 through step 4: as specified in subclause 5.3.5.3.1 "Delete AF application session context initiated by the AF", as needed.

#### 5.3.5.4 AF subscription to events

This procedure is performed when the AF/NEF decides to subscribe to events for an active application session context.

NOTE: The NEF acts as an AF to support the network exposure functionality.



Figure 5.3.5.4-1: Subscription to events by the AF

1. The AF decides to subscribe to events for the active AF application session context in relation to the corresponding PDU session.

2. The AF invokes the Npcf\_PolicyAuthorization\_Subscribe service operation indicating the AF application session context and the events that subscribes. The request also includes a Notification URI to indicate to the PCF where to send the notification of the subscribed events.

Editor's note: The parameters sent by the AF are FFS.

3. The PCF can subscribe to PDU session events as described in subclause 5.3.3.1 "PCF subscription to events".

Editor's note: Whether the PCF provides the response to the Npcf\_PolicyAuthorization\_Subscribe service operation after receiving the outcome in step 3 is FFS.

#### 5.3.5.5 AF unsubscription to events

This procedure is performed when the AF/NEF decides to unsubscribe to previously subscribed events for an active application session context.

NOTE: The NEF acts as an AF to support the network exposure functionality.



Figure 5.3.5.5-1: Unsubscription to events by the AF

1. The AF decides to unsubscribe to events for the active AF application session context in relation to the corresponding PDU session.

2. The AF invokes the Npcf\_PolicyAuthorization\_Unsubscribe service operation indicating the AF application session context and the events that unsubscribes.

Editor's note: The parameters sent by the AF are FFS.

3. The PCF can unsubscribe the related PDU session events using Nsmf\_EventExposure\_Unsubscribe service operation for the active PDU session.

Editor's note: Whether the PCF provides the response to the Npcf\_PolicyAuthorization\_Unsubscribe service operation after receiving the outcome in step 3 is FFS.

#### 5.3.5.6 PCF notification about application session context events

This procedure is performed when the PCF notifies the AF/NEF that the PDU session and/or service related event(s) occurred.

NOTE: The NEF acts as an AF to support the network exposure functionality.



Figure 5.3.5.6-1: PCF notification about application session context events

1. An event to which the AF has subscribed to occurs. E.g. the PCF receives an SMF Notification, as defined in subclause 5.3.3.2 "SMF Notification about events that require reporting".

2. The PCF invokes the Npcf\_PolicyAuthorization\_Notify service operation to the AF to indicate that an event for the active application session has occurred.

Editor's note: The parameters sent to the AF by the PCF are FFS.

3. The AF sends the response to the Npcf\_PolicyAuthorization\_Notify service operation.

## 5.4 Network Function Service Procedures

### 5.4.1 General

The following NF services are specified for PCF:

Table 5.4.1-1: NF Services provided by PCF

| Service Name | Description | Reference | Example Consumer |
| --- | --- | --- | --- |
| Npcf\_AMPolicyControl | This service provides access control, network selection and mobility management related policies to the AMF, UE Route Selection Policy to the UE via the AMF. | 5.4.2 | AMF |
| Npcf\_SMPolicyControl | This service provides session related policies to the SMF. | 5.4.3 | SMF |
| Npcf\_PolicyAuthorization | This service is to authorise an AF request and to create policies as requested by the authorised AF for the PDU-CAN session to which the AF session is bound. | 5.4.4 | AF/NEF |

The following policy control related NF services are specified for the SMF:

Table 5.4.1-2: NF Services provided by SMF

| Service Name | Description | Reference | Example Consumer |
| --- | --- | --- | --- |
| Nsmf\_EventExposure | This service provides events related to PDU sessions towards consumer NF. The service operations exposed by this service allow other NFs to subscribe, unsubscribe and get notified of events happening on the PDU session. | 5.4.5 | PCF, NEF, AMF, AF |

### 5.4.2 Npcf\_AMPolicyControl service

#### 5.4.2.1 General

The Npcf\_AMPolicyControl service provides access control, and mobility management related policies to the AMF, the UE Route Selection Policy to the UE via the AMF, which includes the following functionalities:

- create policies based on the request from the AMF during UE registration;

- notify the AMF of the updated policies which are subscribed; and

- delete policy context for the UE.

#### 5.4.2.2 Operations

Table 5.4.2.2-1: Operations of the Npcf\_AMPolicyControl Service

| Service operation name | Description | Initiated by | Inputs, required | Inputs, optional | Outputs, required | Outputs, optional |
| --- | --- | --- | --- | --- | --- | --- |
| Npcf\_AMPolicyControl\_Get | Provides the requested policy to the NF service consumer | NF service consumer (AMF) | SUPI,  Notification URI (NOTE) | Generic Public Subscription Identifier (GPSI),  Access type,  Permanent Equipment Identifier (PEI),  User Location Information,  UE Time Zone,  Serving Network,  RAT type,  List of Service Area Restriction elements, RAT Frequency Selection Priority (RFSP) Index | The requested policy:  UE policy (see subclause 5.8) including UE Access Network discovery and selection policies and/or UE Route Selection Policies (URSP); and/or,  AMF Access and Mobility Policy (see subclause 5.6) including Service Area Restrictions, and/or RAT Frequency Selection Priority (RFSP) Index | none |
| Npcf\_AMPolicyControl\_UpdateNotify | Provides updated policy to the NF service consumer. | PCF | SUPI,  Updated Policies:  UE policy (see subclause 5.8) and/or,  AMF Access and Mobility Policy (see subclause 5.6) | none | Success or Failure | none |
| Npcf\_AMPolicyControl\_Delete | Provides means for the NF service consumer to delete the policy context. | NF service consumer (AMF) | SUPI | none | Success or Failure | none |
| NOTE: The "Notification URI" corresponds to the "subscription to Notification indicator" in stage 2. | | | | | | |

#### 5.4.2.3 Encoding Proposal 1: RESTful HTTP with Policy as PCF resource and custom operation to update policy at AMF



Figure 5.4.2.3-1: Proposed Resource URI structure of the Npcf\_AMPolicyControl API

Table 5.4.2.3-1: Proposed resources and methods overview for the Npcf\_AMPolicyControl service

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | Resource URI | HTTP method | Request body | Successful response body | Meaning |
| AM Policies | {apiRoot}/ npcf-am-policy-control/ v1/policies/ | POST | NpcfAMPolicyControlRequest | NpcfAMPolicyControl | Create a new Individual AM Policy resource for a supi supplied by the AMF. |
| Individual AM Policy | {apiRoot} /npcf-am-policy-control/ v1/policies/ {policyId} | PUT (FFS) | NpcfAMPolicyControlRequest | NpcfAMPolicyControl | Update an existing Individual AM Policy resource for a supi supplied by the AMF. |
| PATCH (FFS) | FFS | FFS | Update an existing Individual AM Policy resource for a supi supplied by the AMF. |
| GET  (FFS) | none | NpcfAMPolicyControl | Read the Individual AM Policy resource for a supi supplied by the AMF. |
| DELETE | none | none | Delete the Individual AM Policy resource for a supi supplied by the AMF. |

Editor's note: It is also FFS whether to use different data types in the bodies of the related request and response.

Editor's note: It is FFS whether PUT/PATCH methods and the related GET method are required to cover possible resource updates requested by the AMF invoking Npcf\_AMPolicyControl\_Get service operation.

Editor's note: It is FFS if further changes are required in the resource structure.

Table 5.4.2.3-2: Proposed methods overview for the Npcf\_AMPolicyControl\_UpdateNotify service operation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | URI | HTTP method | Request body | Successful response body | Meaning |
| AM Policy Notification | {notificationURI} | POST | Npcf\_AMPolicyControlNotification | none | Notify the AMF about updated policies. |

Editor's note: The HTTP method and body for notifications are still FFS. An efficient encoding of partial Notifications is also FFS.

Table 5.4.2.3-3: Proposed type NpcfAMPolicyControl

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| request | Npcf\_AMPolicyControlRequest | 1 |  |
| policy | Npcf\_AMPolicyControlPolicy | 1 |  |

Table 5.4.2.3-4: Proposed type NpcfAMPolicyControlRequest

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| supi | Supi (FFS) | 1 | Subscription Permanent Identifier |
| notificationURI | Uri (FFS) | 0..1 | Identifies the recipient of Notifications sent by the PCF. |
| gpsi | Gpsi (FFS) | 0..1 | Generic Public Subscription Identifier |
| accessType | AccessType | 0..1 | The Access Type where the served UE is camping. |
| ratType | RatType (FFS) | 0..1 | The RAT Type where the served UE is camping. |
| servingNetwork | NetworkId (FFS) | 0..1 | The serving network where the served UE is camping. |
| userLocationInformation | UserLocationInformation (FFS) | 0..1 | The location of the served UE is camping. |
| ueTimeZone | TimeZone (FFS) | 0..1 | The time zone where the served UE is camping. |
| permanentEquipmentIdentifier | PermanentEquipmentIdentifier (FFS) | 0..1 | The Permanent Equipment Identifier of the served UE. |
| serviceAreaRestriction | ServiceAreaRestriction | 0..1 | Service Area Restriction |

NOTE 1: The Supi, Uri, RatType, AccessType, NetworkId, UserLocationInformation, TimeZone, and PermanentEquipmentIdentifier Data Types should be specified as common data types applicable for multiple APIs.

Table 5.4.2.3-5: Proposed type Npcf\_AMPolicyControlNotification

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| supi | Supi (FFS) | 1 | Subscription Permanent Identifier |
| uePolicy | UePolicy | 0..1 | UE policy (see subclause 5.8). |
| amfAccessAndMobilityManagementControlPolicy | AmfAccessAndMobilityManagementControlPolicy | 0..1 | AMF Access and Mobility Management Control Policy (see subclause 5.6). |

Table 5.4.2.3-6: Proposed type Npcf\_AMPolicyControlPolicy

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| uePolicy | UePolicy | 0..1 | UE policy (see subclause 5.8). |
| amfAccessAndMobilityManagementControlPolicy | AmfAccessAndMobilityManagementControlPolicy | 0..1 | AMF Access and Mobility Management Control Policy (see subclause 5.6). |

Table 5.4.2.3-7: Proposed type UePolicy

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| accessNetworkDiscoverySelectionPolicy | FFS | 0..1 |  |
| urspRules | UrspRule | 0..N | UE Route Selection Policy (URSP) rules |

Table 5.4.2.3-8: Proposed type UrspRule

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| trafficFilter | TrafficFilter (FFS) | 0..1 | Traffic Filter Information. (NOTE) |
| applicationIdentifier | ApplicationIdentifier (FFS) | 0..1 | Application Identifier (NOTE) |
| nonSeamlessOffloadRules | NonSeamlessOffloadRule | 0..N | Non-seamless Offload Rules (more than one rule allowed, one per Non-3GPP access type). |
| slices | SliceInfo | 0..N | Describes the network slices that matching traffic is allowed to use. More than one instance allowed, provided in priority order. |
| continuityTypes | ContinuityType | 0..3 | Describes the required SSC mode(s) as defined in see subclause 5.6.9.2 of 3GPP TS 23.501 [2] for matching traffic. More than one instance allowed, provided in priority order. |
| dnns | Dnn (FFS) | 0..N | The required DNN(s) for the matching traffic (more than one instance allowed, provided in priority order). |
| accessType | AccessType | 1..2 | Indicates the type of access (3GPP or non-3GPP) on which the PDU session should be established for the matching traffic. More than one instance allowed, provided in priority order. |
| NOTE: Either trafficFilter or applicationIdentifier shall be included. | | | |

NOTE 2: The TrafficFilter, ApplicationIdentifier, Dnn, ContinuityType and AccessType Data Types should be specified as common data types applicable for multiple APIs.

Editor's note: The data type TrafficFilter is FFS. If uplink and downlink filters cannot be included together in one instance, the cardinality of trafficFilter needs to be adjusted to "0..2".

Table 5.4.2.3-9: Proposed type NonSeamlessOffloadRule

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| trafficTreatment | TrafficTreatment | 0..1 | Indicated whether matching traffic is Prohibited, Preferred, or Permitted to be offloaded. |
| non3gppAccessType | Non3gppAccessType (FFS) | 0..1 | Optional parameter to indicate the Non-3GPP access network type for which the traffic treatment applies. |

Table 5.4.2.3-10: Proposed Enumeration TrafficTreatment

|  |  |
| --- | --- |
| Enumeration value | Description |
| PROHIBITED | Matching traffic is Prohibited to be offloaded. |
| PREFERRED | Matching traffic is Preferred, to be offloaded. |
| PERMITTED | Matching traffic is Permitted to be offloaded. |

Table 5.4.2.3-11: Proposed type SliceInfo

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| sliceType | integer | 1 | Indicates expected Network Slice behaviour in terms of features and services. Standardised values are "1" for enhanced Mobile Broadband (eMBB), "2" for ultra-reliable low latency communications (URLLC), and "3" for massive IoT (MIoT), but non-standard values can also be used. |
| slice Differentiator | FFS | 0..1 | Optional parameter that complements the Slice/Service type(s) to allow further differentiation for selecting a Network Slice instance from the potentially multiple Network Slice instances that all comply with the indicated Slice/Service type. |

NOTE 3: The SliceInfo Type should be specified as common data type applicable for multiple APIs.

Table 5.4.2.3-12: Proposed Enumeration ContinuityType

|  |  |
| --- | --- |
| Enumeration value | Description |
| SSC\_MODE\_1 | As defined in subclause 5.6.9.2 of 3GPP TS 23.501 [2]. |
| SSC\_MODE\_2 | As defined in subclause 5.6.9.2 of 3GPP TS 23.501 [2]. |
| SSC\_MODE\_3 | As defined in subclause 5.6.9.2 of 3GPP TS 23.501 [2]. |

Table 5.4.2.3-13: Proposed Enumeration AccessType

|  |  |
| --- | --- |
| Enumeration value | Description |
| 3GPP\_ACCESS |  |
| NON\_3GPP\_ACCESS |  |

NOTE 4: The Enumeration AccessType should be specified as common data type applicable for multiple APIs.

Table 5.4.2.3-14: Proposed type AmfAccessAndMobilityManagementControlPolicy

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| serviceAreaRestriction | ServiceAreaRestriction | 0..1 | Service Area Restriction Policy |
| rfspIndex | UInteger (FFS) | 0..1 | RAT/Frequency Selection Priority Index Note: Is encoded as unsigned integer with 256 values in LTE. |

Table 5.4.2.3-15: Proposed type ServiceAreaRestriction

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| allowedTais | Tai (FFS) | 0..N | A list of allowed Tracking Area Identities. (NOTE 2) |
| notAllowedTais | Tai (FFS) | 0..N | A list of not allowed Tracking Area Identities. (NOTE 2) |
| allowedTaNumber | UInteger (FFS) | 0..1 | The maximum number of allowed TAs within a list of allowed TAs defined in the AMF. Default is 0. (NOTE 1, NOTE 2) |
| unlimitedAllowedTa | Boolean | 0..1 | Indicates whether all of the allowed TAs within a list of allowed TAs defined in the AMF are allowed. Default is "FALSE". (NOTE 1, NOTE 2) |
| NOTE 1: If unlimitedAllowedTa with value "TRUE" is provided, this overrides any value of allowedTaNumber including the default "0".  NOTE 2: AllowedTais may be provided in combination with allowedTaNumber or unlimitedAllowedTa. However, notAllowedTAIs shall not be provided in combination with allowedTais, allowedTaNumber or unlimitedAllowedTa with value "TRUE". | | | |

NOTE 5: The UInteger data type (for unsigned integer) and the Tai (for tracking area identity) should be specified as common data type applicable for multiple APIs.

#### 5.4.2.4 Encoding Proposal 2: RESTful HTTP with Policy as AMF resource



Figure 5.4.2.4-1: Proposed Resource URI structure of the Npcf\_AMPolicyControl API

Table 5.4.2.4-1: Proposed resources and methods overview for the Npcf\_AMPolicyControl service

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | Resource URI | HTTP method | Request body | Successful response body | Meaning |
| AM Policies Subscription | {apiRoot}/ npcf-am-policy-control/ v1/subscriptions | POST | NpcfAMPolicyControlSubscription | NpcfAMPolicyControl | Create a new Individual AM Subscription resource for a SUPI supplied by the AMF. |
| Individual AM Policy Subscription | {apiRoot} /npcf-am-policy-control/ v1/subscriptions/ {subscriptionId} | PUT  FFS | Npcf\_AMPolicyControlSubscription | Npcf\_AMPolicyControSubscription | Update an existing Individual AM Policy resource for a SUPI supplied by the AMF. |
| PATCH (FFS) | FFS | FFS | Update an existing Individual AM Policy resource for a SUPI supplied by the AMF. |
| GET | none | Npcf\_AMPolicyControlSubscription | Read the Individual AM Policy resource for a SUPI supplied by the AMF. |
| DELETE | none | none | Delete the Individual AM Policy resource for a SUPI supplied by the AMF. |

Stage 2 requires that Policy information can be provided both as response to a Npcf\_AMPolicyControl\_Get, and as Npcf\_AMPolicyControl\_UpdateNotify request. The information can be quite extensive and includes a possibly high number of USRP rules. Some related issues are:

- How to achieve maximum communality in the implementation of Npcf\_AMPolicyControl\_Get and Npcf\_AMPolicyControl\_UpdateNotify?

- How to enable an effective update for both cases?

The service consumer subscribes to policies by supplying the Individual AM Policy Subscription resource including the notificationURI. The PCF does not return policies in the HTTP response to that subscription. The PCF rather immediately sends an HTTP request towards notificationURI to create or update the policy resource at the service consumer (AMF) as depicted in figure 5.4.2.4-2 and described in table 5.4.2.4-2.



Figure 5.4.2.4-2: Proposed Resource URI structure for resources at the service consumer (AMF) for the Npcf\_AMPolicyControl API

Editor's note: It is FFS whether to introduce resources between the {notificationURI} and the AM Policy that enable the PCF (e.g. for restoration purposes) to read the installed policies for several subscribers. The URI structure could then for instance be {notificationURI}/{sessionID}/policies.

Table 5.4.2.4-2: Proposed resources and methods overview for resources at the service consumer (AMF) of the Npcf\_AMPolicyControl service

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | URI | HTTP method | Request body | Successful response body | Meaning |
| AM Policy | {notificationURI}/ policy | PUT | Npcf\_AMPolicyControlPolicy | FFS | Install new AM policy or replace existing AM policy at the service consumer. |
| PATCH | FFS | FFS | Update existing AM policy at the service consumer. |
| GET | - | Npcf\_AMPolicyControlPolicy | Read existing AM policy. |
| DELETE  (FFS, NOTE) | - | - | Delete existing AM policy at the service consumer. |
| UE Policy | {notificationURI}/ policy/ ue-policy | PUT | UePolicy | FFS | Install new UE policy or replace existing UE policy at the service consumer. |
| PATCH | FFS | FFS | Update existing UE policy at the service consumer. |
| GET | - | UePolicy | Read existing UE policy. |
| DELETE | - | - | Delete existing UE policy at the service consumer. |
| URSP Rules | {notificationURI}/ policy/ ue-policy/ ursp-rules | PUT | 1..N UrspRule | FFS | Install new URSP Rules or replace existing URSP Rules at the service consumer. |
| PATCH | FFS | FFS | Update existing URSP rules at the service consumer. |
| GET | - | 1..N UrspRule | Read existing URSP rules. |
| DELETE | - | - | Delete existing URSP rules at the service consumer. |
| Individual URSP Rule | {notificationURI}/ policy/ ue-policy/ ursp-rules/ {urspRuleId} | PUT | UrspRule | FFS | Install new URSP rule or replace existing URSP rule at the service consumer. |
| PATCH | FFS | FFS | Update existing URSP rule at the service consumer. |
| GET | - | UrspRule | Read existing URSP rule. |
| DELETE | - | - | Delete existing URSP rule at the service consumer. |
| AMF Access and Mobility ManagementControl Policy | {notificationURI}/ amf-policy | PUT | AmfAccessAndMobilityManagementControlPolicy | FFS | Install new or replace existing AMF Access and Mobility ManagementControl Policy at the service consumer. |
| PATCH | FFS | FFS | Update existing AMF Access and Mobility ManagementControl Policy at the service consumer. |
| GET | - | AmfAccessAndMobilityManagementControlPolicy | Read existing AMF Access and Mobility ManagementControl Policy. |
| DELETE | - | - | Delete existing AMF Access and Mobility ManagementControl Policy at the service consumer. |
| NOTE: If the SMF deletes the Individual SM PDUSessioPolicy Subscription resource, the corresponding SM Policies resource is also deleted in the SMF without a DELTE request from the PCF | | | | | |

Table 5.4.2.4-3: Proposed type Npcf\_AMPolicyControlSubscription

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Attribute name | | Data type | | Cardinality | | Description |
| supi | | Supi (FFS) | | 1 | | Subscription Permanent Identifier |
| notificationURI | | Uri (FFS) | | 1 | | Identifies the recipient of Notifications sent by the PCF. |
| gpsi | Gpsi (FFS) | | 0..1 | | Generic Public Subscription Identifier | |
| accessType | | AccessType | | 0..1 | | The Access Type where the served UE is camping. |
| ratType | | RatType (FFS) | | 0..1 | | The RAT Type where the served UE is camping. |
| servingNetwork | | NetworkId (FFS) | | 0..1 | | The serving network where the served UE is camping. |
| userLocationInformation | | UserLocationInformation (FFS) | | 0..1 | | The location of the served UE is camping. |
| ueTimeZone | | TimeZone (FFS) | | 0..1 | | The time zone where the served UE is camping. |
| permanentEquipmentIdentifier | | PermanentEquipmentIdentifier (FFS) | | 0..1 | | The Permanent Equipment Identifier of the served UE. |
| serviceAreaRestriction | | ServiceAreaRestriction | | 0..1 | | Service Area Restriction |

NOTE 1: The Supi, Uri, Gpsi, AccessType, RatType, NetworkId, UserLocationInformation, TimeZone, and PermanentEquipmentIdentifier Data Types should be specified as common data types applicable for multiple APIs.

Table 5.4.2.4-4: Proposed type Npcf\_AMPolicyControlPolicy

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| supi | Supi (FFS) | 1 | Subscription Permanent Identifier |
| uePolicy | UePolicy | 0..1 | UE policy (see subclause 5.8). |
| amfAccessAndMobilityManagementControlPolicy | AmfAccessAndMobilityManagementControlPolicy | 0..1 | AMF Access and Mobility Management Control Policy (see subclause 5.6). |

Table 5.4.2.4-5: Proposed type UePolicy

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| accessNetworkDiscoverySelectionPolicy | FFS | 0..1 |  |
| urspRules | UrspRule | 0..N | UE Route Selection Policy (URSP) rules |

Table 5.4.2.4-6: Proposed type UrspRule

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| urspRuleId | UrspRuleId | 1 |  |
| trafficFilter | TrafficFilter (FFS) | 0..1 | Traffic Filter Information. (NOTE) |
| applicationIdentifier | ApplicationIdentifier (FFS) | 0..1 | Application Identifier (NOTE) |
| nonSeamlessOffloadRules | NonSeamlessOffloadRule | 0..N | Non-seamless Offload Rules (more than one rule allowed, one per Non-3GPP access type). |
| slices | SliceInfo | 0..N | Describes the network slices that matching traffic is allowed to use. |
| continuityTypes | ContinuityType | 0..3 | Describes the required SSC mode(s) as defined in see subclause 5.6.9.2 of 3GPP TS 23.501 [2] for matching traffic. More than one instance allowed, provided in priority order. |
| dnns | Dnn (FFS) | 0..N | The required DNN(s) for the matching traffic (more than one instance allowed, provided in priority order). |
| accessType | AccessType | 1..2 | Indicates the type of access (3GPP or non-3GPP) on which the PDU session should be established for the matching traffic. More than one instance allowed, provided in priority order. |
| NOTE: Either trafficFilter or applicationIdentifier shall be included. | | | |

NOTE 2: The TrafficFilter, ApplicationIdentifier, Dnn and AccessType Data Types should be specified as common data types applicable for multiple APIs.

Editor's note: The data type TrafficFilter is FFS. If uplink and downlink filters cannot be included together in one instance, the cardinality of trafficFilter needs to be adjusted to "0..2".

Table 5.4.2.4-7: Proposed type NonSeamlessOffloadRule

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| trafficTreatment | TrafficTreatment | 0..1 | Indicated whether matching traffic is Prohibited, Preferred, or Permitted to be offloaded. |
| non3gppAccessType | Non3gppAccessType (FFS) | 0..1 | Optional parameter to indicate the Non-3GPP access network type for which the traffic treatment applies. |

Table 5.4.2.4-8: Proposed Enumeration TrafficTreatment

|  |  |
| --- | --- |
| Enumeration value | Description |
| PROHIBITED | Matching traffic is Prohibited to be offloaded. |
| PREFERRED | Matching traffic is Preferred, to be offloaded. |
| PERMITTED | Matching traffic is Permitted to be offloaded. |

Table 5.4.2.4-9: Proposed type SliceInfo

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| sliceType | integer | 1 | Indicates expected Network Slice behaviour in terms of features and services. Standardised values are "1" for enhanced Mobile Broadband (eMBB), "2" for ultra-reliable low latency communications (URLLC), and "3" for massive IoT (MIoT), but non-standard values can also be used. |
| sliceDifferentiator | FFS | 0..1 | Optional parameter that complements the Slice/Service type(s) to allow further differentiation for selecting a Network Slice instance from the potentially multiple Network Slice instances that all comply with the indicated Slice/Service type. |

NOTE 3: The SliceInfo Type should be specified as common data type applicable for multiple APIs.

Table 5.4.2.4-10: Proposed Enumeration ContinuityType

|  |  |
| --- | --- |
| Enumeration value | Description |
| SSC\_MODE\_1 | As defined in subclause 5.6.9.2 of 3GPP TS 23.501 [2]. |
| SSC\_MODE\_2 | As defined in subclause 5.6.9.2 of 3GPP TS 23.501 [2]. |
| SSC\_MODE\_3 | As defined in subclause 5.6.9.2 of 3GPP TS 23.501 [2]. |

Editor's note: It is FFS if the ContinuityType Enumeration Types should be specified as common data type applicable for multiple APIs

Table 5.4.2.4-11: Proposed Enumeration AccessType

|  |  |
| --- | --- |
| Enumeration value | Description |
| 3GPP\_ACCESS |  |
| NON\_3GPP\_ACCESS |  |

NOTE 4: The Enumeration AccessType should be specified as common data type applicable for multiple APIs.

Table 5.4.2.4-12: Proposed type AmfAccessAndMobilityManagementControlPolicy

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| serviceAreaRestriction | ServiceAreaRestriction | 0..1 | Service Area Restriction Policy |
| rfspIndex | UInteger (FFS) | 0..1 | RAT/Frequency Selection Priority Index Note: Is encoded as unsigned integer with 256 values in LTE. |

Table 5.4.2.4-13: Proposed type ServiceAreaRestriction

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| allowedTais | Tai (FFS) | 0..N | A list of allowed Tracking Area Identities. (NOTE 2) |
| notAllowedTais | Tai (FFS) | 0..N | A list of not allowed Tracking Area Identities. (NOTE 2) |
| allowedTaNumber | UInteger (FFS) | 0..1 | The maximum number of allowed TAs within a list of allowed TAs defined in the AMF. Default is 0. (NOTE 1, NOTE 2) |
| unlimitedAllowedTa | Boolean | 0..1 | Indicates whether all of the allowed TAs within a list of allowed TAs defined in the AMF are allowed. Default is "FALSE". (NOTE 1, NOTE 2) |
| NOTE 1: If unlimitedAllowedTa with value "TRUE" is provided, this overrides any value of allowedTaNumber including the default "0".  NOTE 2: AllowedTais may be provided in combination with allowedTaNumber or unlimitedAllowedTa. However, notAllowedTAIs shall not be provided in combination with allowedTais, allowedTaNumber or unlimitedAllowedTa with value "TRUE". | | | |

NOTE 5: The UInteger data type (for unsigned integer) and the Tai (for tracking area identity) should be specified as common data type applicable for multiple APIs.

#### 5.4.2.5 Encoding Proposal 3: RESTful HTTP with Policy as PCF resource and notification to trigger AMF to fetch new policy

This encoding proposal is identical to encoding proposal 1 with the exception that the proposed type Npcf\_AMPolicyControlNotification does not contain policy, but only a trigger to fetch updated policy.

The AMF fetches policy using an HTTP GET when receiving such a notification.

#### 5.4.2.5a Encoding Proposal 4: RESTful HTTP with Policy both as PCF resource and as AMF resource and subscription related information only in PCF resource

The proposal is similat to proposal 2. However, policy related information is also included in the Individual Subscription resource to allow the PCF to return this information in a response to the initial GET.

#### 5.4.2.6 Comparison of Encoding Proposals

Table 5.4.2.6-1: Comparison of Encoding Proposals

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Proposal 1 | Proposal 2 | Proposal 3 | Proposal 4 |
| Communality of policy provisioning between Get (Pull operation) and Notify (Push operation) | No | Yes | Yes | No |
| Efficient policy provisioning for initial GET | Yes | Less efficient, as two HTTP Request response pairs required. | Yes | Yes |
| Efficient policy provisioning for subsequent GET (Pull operation, FFS if this is required) | For HTTP GET only complete policy but no deltas can be provided. Thus most likely custom operation required. | Alternatives:  1. two HTTP interactions, but possibility to provide only deltas in Policy.  2. custom operation. | For HTTP GET only complete policy but no deltas can be provided. Thus most likely custom operation required. | Alternatives:  1. return policies in HTTP GET response:  only complete policy but no deltas can be provided.  2. use two HTTP interactions:  only complete policy but no deltas can be provided.  3. custom operation. |
| Efficient policy provisioning for Notify (Push operation) | Yes (Depends on Custom operation design.) | Yes | No, two HTTP interactions, and no possibility to provide only deltas in policy. | Yes |
| RESTful design | Only small fractions. A substantial part of the functionality (PUSH policy provisioning and most likely also subsequent PULL operation) uses Custom operations. | Yes | Partial:  most likely subsequent PULL operation requires custom operation. | Partial:  duplicated resource is not a usual pattern. |
| Efficient resource deletion | OK | OK (assuming policy resources at SMF are implicitly deleted when SMF deletes subscription resource.) | OK | OK (assuming policy resources at SMF are implicitly deleted when SMF deletes subscription resource.) |

#### 5.4.2.7 Conclusions

Encoding proposal 1 is selected for the normative work.

### 5.4.3 Npcf\_SMPolicyControl service

#### 5.4.3.1 General

The Npcf\_SMPolicyControl service provides session related policies to the SMF, which includes the following functionalities:

- create policies based on the request from the SMF during a PDU session establishment;

- notify the SMF of the updated policies which are subscribed; and

- delete policies for a PDU session.

#### 5.4.3.2 Operations

Table 5.4.3.2-1: Operations of the Npcf\_SMPolicyControl Service

| Service operation name | Description | Initiated by | Inputs, required | Inputs, optional | Outputs, required | Outputs, optional |
| --- | --- | --- | --- | --- | --- | --- |
| Npcf\_SMPolicyControl\_Get | Provides the requested policy to the NF service consumer. | NF service consumer (SMF) | SUPI,  PDU session ID,  DNN,  Notification URI (NOTE) | Access type,  the IPv4 address and/or IPv6 network prefix,  Permanent Equipment Identifier (PEI),  User Location Information,  UE Time Zone, Serving Network,  RAT type,  charging information,  Session-AMBR,  default QoS information | The requested PCC rules of the PDU session,  authorized session-AMBR,  authorized default QoS information | none |
| Npcf\_SMPolicyControl\_UpdateNotify | Provides updated policy to the NF service consumer. | PCF | PDU session ID | Updated PCC Rules of the PDU session,  Session-AMBR,  default QoS information,  PDU session termination request | Success or Failure | none |
| Npcf\_SMPolicyControl\_Delete | Provides means for the NF service consumer to delete the context of SM related policy. | NF service consumer (SMF) | PDU session ID and relevant information to the PCF | none | Success or Failure | none |
| NOTE: The "Notification URI" corresponds to the "subscription to Notification indicator" in stage 2. | | | | | | |

Editor's note: Further stage 2 clarification on "relevant information to the PCF" as mandatory input to the Npcf\_SMPolicyControl\_Delete is required.

Editor's note: The optional "PDU session termination request" input parameter to the Npcf\_SMPolicyControl\_UpdateNotify is not defined in stage 2, but stage 2 says that this procedure can be used to trigger the deletion of a PDU session (see step 1b of figure 4.3.4.2-1 within 3GPP TS 23.502 [3]).

Editor's note: Further stage 2 clarification on "default QoS information" as optional input to the Npcf\_SMPolicyControl\_Get is required.

#### 5.4.3.3 Encoding Proposal 1: RESTful HTTP with Policy as PCF resource and custom operation to update policy at SMF



Figure 5.4.3.3-1: Proposed Resource URI structure of the Npcf\_SMPolicyControl API

Table 5.4.3.3-1: Proposed resources and methods overview for the Npcf\_SMPolicyControl service

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | Resource URI | HTTP method | Request body | Successful response body | Meaning |
| SM Policies | {apiRoot}/ npcf-sm-policy-control/ v1/ policies | POST | NpcfSMPolicyControlRequest | NpcfSMPolicyControl | Create a new Individual SM Policy resource for a SUPI and sessionID. |
| Individual SM Policy | {apiRoot}/ npcf-sm-policy-control/ v1/ policies/ {policyId} | PATCH (FFS) | FFS | FFS | Update an existing Individual SM Policy resource. |
| GET | none | Npcf\_SMPolicyControl | Read the Individual SM Policy resource. |
| DELETE | none | none | Delete the Individual SM Policy resource. |

Editor's note: It is FFS whether the PUT, PATCH, and GET for the Individual SM Policy resource are required.

Editor's note: The GET HTTP method is intended for recovery scenarios only.

Table 5.4.3.3-2: Proposed methods overview for the Npcf\_SMPolicyControl\_UpdateNotify service operation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | URI | HTTP method | Request body | Successful response body | Meaning |
| SM Policy Notification | {notificationURI} | POST | Npcf\_SMPolicyControlPolicy | FFS | Notify the SMF about updated policies. |

Table 5.4.3.3-3: Proposed type Npcf\_SMPolicyControl

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| request | Npcf\_SMPolicyControlRequest | 1 | The input parameters for the policy decision. |
| policy | Npcf\_SMPolicyControlPolicy | 1 | The authorized policies. |

Table 5.4.3.3-4: Proposed type NpcfSMPolicyControlRequest

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| supi | Supi (FFS) | 1 | Subscription Permanent Identifier |
| pduSessionId | PduSessionId (FFS) | 1 | PDU session Id |
| dnn | Dnn (FFS) | 1 | The DNN of the PDU session. |
| notificationUri | Link | 1 | Identifies the recipient of Notifications sent by the PCF. |
| accessType | AccessType | 0..1 | The Access Type where the served UE is camping. |
| ratType | RatType (FFS) | 0..1 | The RAT Type where the served UE is camping. |
| servingNetwork | NetworkId (FFS) | 0..1 | The serving network where the served UE is camping. |
| userLocationInformation | UserLocationInformation (FFS) | 0..1 | The location of the served UE is camping. |
| ueTimeZone | TimeZone (FFS) | 0..1 | The time zone where the served UE is camping. |
| permanentEquipmentIdentifier | PermanentEquipmentIdentifier (FFS) | 0..1 | The Permanent Equipment Identifier of the served UE. |
| ipv4Address | Ipv4Address (FFS) | 0..1 | The IPv4 Address of the served UE. |
| ipv6AddressPrefix | Ipv6AddressPrefix (FFS) | 0..1 | The Ipv6 Address Prefix of the served UE. |
| chargingInformation | ChargingInformation (FFS) | 0..1 |  |
| sessionAmbr | BitRate (FFS) | 0..1 |  |
| defaultQosInformation | defaultQosInformation (FFS) | 0..1 |  |

NOTE: The Supi, PduSessionId, Link, RatType, Dnn, NetworkId, UserLocationInformation, TimeZone, PermanentEquipmentIdentifier, Ipv4Address, Ipv6AddressPrefix, ChargingInformation, BitRate, and defaultQosInformation Data Types should be specified as common data types applicable for multiple APIs.

Table 5.4.3.3-5: Proposed type NpcfSMPolicyControlNotification

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| supi | Supi (FFS) | 1 | Subscription Permanent Identifier |
| pduSessionId | PduSessionId | 1 | PDU session id |
| sessionPolicy | Npcf\_SMPolicyControlPolicy | 1 | Session management policy (see subclause 5.7). |
| terminationRequest | Boolean | 0..1 | Request to terminate the PDU session. Default is "FALSE". |

Table 5.4.3.3-6: Proposed type NpcfSMPolicyControlPolicy

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| pccRules | PccRule | 0..N | List of PCC Rules with content as described in subclause 5.7.1. |
| SessionAmbr | BitRate (FFS) | 0..1 | Session-AMBR |
| defaultQosInformation | defaultQosInformation (FFS) | 0..1 | Default QoS |

Table 5.4.3.3-7: Proposed type PCCRule

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| ruleId | string | 1 | Uniquely identifies the PCC rule, within a PDU session. |
| removeFlag | Boolean | 0..1 | Indicates the PCC rule is remove. |
| partialFlag | Boolean | 0..1 | Indicate to update the PCC rule partially. |
| ruleActivationTime | datatime | 0..1 | The time when the PCC rule shall be activated. |
| ruleDeactivationTime | datatime | 0..1 | The time when the PCC rule shall be deactivated. |
| resourceAllocationNotification | Boolean | 0..1 | Indicates the notification is needed when the resource of the PCC rule is allocated successfully. |
| chargingCorrelationIndicator | Boolean | 0..1 | Indicates the charging id of the PCC rule is required to report. |
| monitoringFlag | Boolean | 0..1 | Indicates the usage of the PCC rule shall not be accumulated to the PDU session level. |
| serviceId | string | 0..1 | Indicates the identifier of the service or service component the service data flow in a PCC rule relates to. |
| rateGroup | string | 0..1 | The charging key for the PCC rule used for rating purposes. |
| defaultFlowIndication | Boolean | 0..1 | Indicates the PCC rule shall be bound to the default Qos flow. |
| applicationIdentifier | string | 0..1 | A reference to the application detection filter configured at the UPF. |
| flowInformation | FlowInformtion | 0..1 | Contains the information from a single IP flow packet filter. |
| flowStaus | FlowStatus (FFS) | 0..1 | Describes whether the IP flow(s) are enabled or disabled. |
| qosInformation | QoSInformation | 0..1 | Describes the QoS information of the PCC rule. |
| reflectiveQoSIndication | Boolean | 0..1 | Indicates the Reflective QoS is applicable to the service data flow. |
| qoSNotificationControl | Boolean | 0..1 | Indicates a request for notification from RAN for the SDF when the QoS targets for a GBR 5QI cannot be fulfilled for a QoS flow during the lifetime of the QoS flow. |
| reportingLevel | ReportingLevel | 0..1 | Indicates the report level of the charging information. |
| online | Boolean | 0..1 | Indicates the online charging is applicable to the PCC rule. |
| offline | Boolean | 0..1 | Indicates the offline charging is applicable to the PCC rule. |
| meteringMethod | MeteringMethod | 0..1 | Defines what parameters shall be metered for offline charging. |
| precedence | Integer | 0..1 | determines the order, in which service data flow templates consisting of service data flow filters are applied at service data flow detection at the UPF. |
| afChargingIdentifier | AFChargingIdentifer | 0..1 | An identifier, provided from the AF, correlating the measurement for the Charging key/Service identifier values in this PCC rule with application level reports. |
| flows | Flows | 0..n | Identifies the flow of the AF charging identifier is related to. |
| monitroingKey | Integer | 0..1 | The PCF uses the monitoring key to group services that share a common allowed usage. |
| redirectInformation | RedirectInformation | 0..1 |  |
| muteNotification | Boolean | 0..1 | Indicates application's start or stop notification is to be muted. |
| afSignallingProtocol | AFSignallingProtocol | 0..1 |  |
| sponsorInformation | Sponsorinformation | 0..1 | Indicates the sponsor information including sponsor id and ASP id. |
| requireAccessInfo | RequiredAccessInfo | 0..1 | Indicates that access network information is required. |
| sharingKeyDl | SharingKeyDL (FFS) | 0..1 | Indicates resource sharing in downlink direction with service data flows having the same value in their PCC rule. |
| sharingKeyUl | SharingKeyUL (FFS) | 0..1 | Indicates resource sharing in uplink direction with service data flows having the same value in their PCC rule. |
| trafficSteeringPolicyIdentifierDl | string | 0..1 | Reference to a pre-configured traffic steering policy in downlink at the SMF. |
| trafficSteeringPolicyIdentifierUl | string | 0..1 | Reference to a pre-configured traffic steering policy in Uplink at the SMF. |
| dataNetworkAccessIdentifier | DataNetworkAccessIdentifier (FFS) | 0..1 | Identifier of the target Data Network Access. |
| dataNetworkAccessCharingReport | dataNetworkAccessCharingReport (FFS) | 0..1 | Indicates whether a notification in case of change of DNAI at addition/change/removal of the UPF is requested, as well as the destination(s) for where to provide the notification. |

Editor's note: It is FFS if the above table need to be updated for common data types.

Editor's note: It is FFS the encoding of the information in the above table is FFS.

Table 5.4.3.3-8: Proposal type QoSInformation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| 5QI | Integer | M | 1 | Identifier for the authorized QoS parameters for the service data flow. |
| maxRequestedBandwidthUl | Bitrates | O | 1 | Indicates the max bandwidth in uplink. |
| maxRequestedBandwidthDl | Bitrates | O | 1 | Indicates the max bandwidth in downlink. |
| guaranteed-BitrateUl | Bitrates | O | 1 | Indicates the guaranteed bandwidth in uplink. |
| guaranteed-BitrateDL | Bitrates | O | 1 | Indicates the max guaranteed in downlink. |
| allocation-RetentionPriority | AllocationRetentionPriority (FFS) | M | 1 | Indicates the allocation and retention priority. |

Table 5.4.3.3-9: Proposal type RedirectInformation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| redirectSupport | Boolean | M | 1 | Indicates the redirect is enable. |
| redirectAddressType | RedirectAddressType | O | 0..1 | Indicates the type of redirect address. |
| redirectServerAddress | string | O | 0..1 | Indicates the address of the redirect server. |

Table 5.4.3.3-10: Proposal type FlowInformation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| flowDescription | FlowDescription | M | 0..n | Contains the packet filters of the IP flow(s). |
| packetFilterUsage | boolean | O | 0..1 | The packet shall be sent to the UE. |
| tosTrafficClass | string | O | 0..1 | Contains the Ipv4 Type-of-Service and mask field or the Ipv6 Traffic-Class field and mask field. |
| spi | string | O | 0..1 | the security parameter index of the IPSec packet. |
| flowLabel | string | O | 0..1 | the Ipv6 flow label header field. |
| flowDirection | FlowDirection | O | 0..1 | indicates the direction/directions that a filter is applicable, downlink only, uplink only or both down- and uplink (bidirectional). |

Table 5.4.3.3-11: Proposal Enumeration FlowStaus

|  |  |
| --- | --- |
| Enumeration value | Description |
| UPSPECIFIED | The corresponding filter applies for traffic to the UE (downlink), but has no specific direction declared. |
| DOWNLINK | The corresponding filter applies for traffic to the UE. |
| UPLINK | The corresponding filter applies for traffic from the UE. |
| BIDIRECTIONAL | The corresponding filter applies for traffic both to and from the UE. |

Table 5.4.3.3-12: Proposal Enumeration ReportingLevel

|  |  |
| --- | --- |
| Enumeration value | Description |
| SERVICE\_IDENTIFIER\_LEVEL | indicates that the usage shall be reported on service id and rating group combination level. |
| RATING\_GROUP\_LEVEL | indicates that the usage shall be reported on rating group level. |
| SPONSORED\_CONNECTIVITY\_LEVEL | indicates that the usage shall be reported on sponsor identity and rating group combination level. |

Table 5.4.3.3-13: Proposal Enumeration MeteringMethod

|  |  |
| --- | --- |
| Enumeration value | Description |
| DURATION | indicates that the duration of the service data flow traffic shall be metered. |
| VOLUME | indicates that volume of the service data flow traffic shall be metered. |
| DURATION\_VOLUME | indicates that the duration and the volume of the service data flow traffic shall be metered. |
| EVENT | indicates that events of the service data flow traffic shall be metered. |

Table 5.4.3.3-14: Proposal Enumeration AFSignallingProtocol

|  |  |
| --- | --- |
| Enumeration value | Description |
| NO\_INFORMATION | Indicate that no information about the AF signalling protocol is being provided. |
| SIP | Indicates that the signalling protocol is Session Initiation Protocol |

Table 5.4.3.3-15: Proposal Enumeration RedirectAddressType

|  |  |
| --- | --- |
| Enumeration value | Description |
| IPv4 | Indicates that the type is in the form of IPv4 |
| IPv6 | Indicates that the type is in the form of IPv6 |
| URL | Indicates that the type is in the form of URL |
| SIP\_URI | Indicates that the type is in the form of SIP URI |

#### 5.4.3.4 Encoding Proposal 2: RESTful HTTP with Policy as SMF resource



Figure 5.4.3.4-1: Proposed Resource URI structure of the Npcf\_SMPolicyControl API

Table 5.4.3.4-1: Proposed resources and methods overview for the Npcf\_SMPolicyControl service

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | Resource URI | HTTP method | Request body | Successful response body | Meaning |
| SM Policies | {apiRoot}/ npcf-sm-policy-control/ v1/ policy\_subscriptions | POST | NpcfSMPolicyControlRequest | NpcfSMPolicyControl | Create a new Individual SM Policy subscription resource for a SUPI and PDU sessionID. |
| Individual SMPolicy Subscription | {apiRoot}/ npcf-sm-policy-control/ v1/ policy\_subscriptions/  {subscriptionID} | PUT (FFS) | Npcf\_SMPolicyControlSubscription | FFS | Update an existing Individual SM Policy Subscription resource for a SUPI and sessionID supplied by the SMF. |
| PATCH (FFS) | FFS | FFS | Update an existing Individual SM Policy Subscription resource. |
| GET | none | Npcf\_SMPolicyControlSubscription | Read the Individual SM PDUSession Policy Subscription resource. |
| DELETE | none | none | Delete the Individual SM PDUSession Policy Subscription resource. |

Editor's note: It is also FFS whether to use different data types in the bodies of the related request and response.

Editor's note: It is FFS whether the DELETE for the Individual SM Subscriber Policy resource is required.

Stage 2 requires that Policy information can be provided both as response to a Npcf\_SMPolicyControl\_Get, and as Npcf\_SMPolicyControl\_UpdateNotify request. The information is quite extensive and includes a possibly high number of PCC rules. Some related issues are

- How to achieve maximum communality in the implementation of Npcf\_SMPolicyControl\_Get and Npcf\_SMPolicyControl\_UpdateNotify?

- How to enable an effective update for both cases?

The service consumer subscribes to policies by supplying the Individual SM PDUSessionPolicy Subscription resource including the notificationURI. The PCF does not return policies in the HTTP response to that subscription. The PCF rather immediately sends an HTTP request towards notificationURI to create or update the policy resource at the SMF as depicted in figure 5.4.3.4-2 and described in table 5.4.3.4-2.



Figure 5.4.3.4-2: Proposed Resource URI structure for resources at the service consumer (SMF) for the Npcf\_SMPolicyControl API

Editor's note: It is FFS whether to introduce resources between the {notificationURI} and the SM Policies that enable the PCF (e.g. for restoration purposes) to read the installed policies for several subscribers and/or the SM Policies for all PDU sessions of one subscriber. The URI structure could then for instance be {notificationURI}/{supi}/{sessionID}/policies.

Table 5.4.3.4-2: Proposed resources and methods overview for resources at the service consumer (SMF) of the Npcf\_SMPolicyControl service

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | URI | HTTP method | Request body | Successful response body | Meaning |
| SM Policies | {notificationURI}/ policy | PUT | Npcf\_SMPolicyControlPolicy | FFS | Install new policies or replace existing SM policies at the service consumer. |
| PATCH | FFS | FFS | Update existing SM policies at the service consumer. |
| GET | - | Npcf\_SMPolicyControlPolicy | Read existing SM policies. |
| DELETE (FFS, NOTE) | - | - | Delete existing SM policies at the service consumer and request termination of corresponding PDU session. |
| PCC Rules | {notificationURI}/ policy/ pcc-rules | PUT | 1..N PccRule | FFS | Install new PCC Rules or replace existing PCC Rules at the service consumer. |
| PATCH | FFS | FFS | Update existing PCC rules at the service consumer. |
| GET | - | 1..N PccRule | Read existing PCC rules. |
| DELETE | - | - | Delete existing PCC rules at the service consumer. |
| Individual PCC Rule | {notificationURI}/ policy/ pcc-rules/ {PCCruleId} | PUT | PCCRule | FFS | Install new PCC rule or replace existing PCC rule at the service consumer. |
| PATCH | FFS | FFS | Update existing PCC rule at the service consumer. |
| GET | - | PCCRule | Read existing PCC rule. |
| DELETE | - | - | Delete existing PCC rule at the service consumer. |
| NOTE: If the SMF deletes the Individual SM PDUSessioPolicy Subscription resource, the corresponding SM Policies resource is also deleted in the SMF without a DELTE request from the PCF | | | | | |

Table 5.4.3.4-3: Proposed type Npcf\_SMPolicyControlSubscription

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| supi | Supi (FFS) | 1 | Subscription Permanent Identifier |
| pduSessionId | PduSessionId (FFS) | 1 | PDU session Id |
| dnn | Dnn (FFS) | 1 | The DNN of the PDU session. |
| notificationUri | Uri | 1 | Identifies the recipient of Notifications sent by the PCF. |
| gpsi | Gpsi (FFS) | 0..1 | Generic Public Subscription Identifier |
| accessType | AccessType | 0..1 | The Access Type where the served UE is camping. |
| ratType | RatType (FFS) | 0..1 | The RAT Type where the served UE is camping. |
| servingNetwork | NetworkId (FFS) | 0..1 | The serving network where the served UE is camping. |
| userLocationInformation | UserLocationInformation (FFS) | 0..1 | The location of the served UE is camping. |
| ueTimeZone | TimeZone (FFS) | 0..1 | The time zone where the served UE is camping. |
| permanentEquipmentIdentifier | PermanentEquipmentIdentifier (FFS) | 0..1 | The Permanent Equipment Identifier of the served UE. |
| ipv4Address | Ipv4Address (FFS) | 0..1 | The IPv4 Address of the served UE. |
| ipv6AddressPrefix | Ipv6AddressPrefix (FFS) | 0..1 | The Ipv6 Address Prefix of the served UE. |
| chargingInformation | ChargingInformation (FFS) | 0..1 |  |
| sessionAmbr | BitRate (FFS) | 0..1 |  |
| defaultQosInformation | DefaultQosInformation (FFS) | 0..1 |  |

NOTE: The Supi, PduSessionId, Gpsi, Uri, AceesType, RatType, Dnn, NetworkId, UserLocationInformation, TimeZone, PermanentEquipmentIdentifier, Ipv4Address, Ipv6AddressPrefix, ChargingInformation, BitRate, and DefaultQosInformation Data Types should be specified as common data types applicable for multiple APIs.

Table 5.4.3.4-4: Proposed type Npcf\_SMPolicyControlPolicy

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| pccRules | PccRule | 0..N | List of PCC Rules with content as described in subclause 5.7.1. |
| activePredefinedPccRules | PccRuleId | 0..N | List of activated predefined PCC Rules. |
| sessionAmbr | BitRate (FFS) | 0..1 |  |
| defaultQosInformation | DefaultQosInformation (FFS) | 0..1 |  |

Editor's note: It is FFS whether supi and PDU session Id are required as additional parameters.

Table 5.4.3.4-5: Proposed type PccRule

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| pccRuleId | PccRuleId(FFS) | 1 | PCC Rule Id |
| FFS |  |  |  |
|  |  |  |  |

Editor's note: FFS. Provide content as described in subclause 5.7.1.

#### 5.4.3.5 Encoding Proposal 3: RESTful HTTP with Policy as PCF resource and notification to trigger SMF to fetch new policy

This encoding proposal is identical to encoding proposal 1 with the exception that the proposed type Npcf\_SMPolicyControlNotification does not contain policy, but only a trigger to fetch updated policy.

The SMF fetches policy using an HTTP GET when receiving such a notification.

#### 5.4.3.5a Encoding Proposal 4: RESTful HTTP with Policy both as PCF resource and as SMF resource and subscription related information only in PCF resource

The proposal is similar to proposal 2. However, policy related information is also included in the Individual SM PDUSessionPolicy Subscription resource to allow the PCF to return this information in a response to the initial GET.

#### 5.4.3.6 Comparison of Proposals

Table 5.4.3.6-1: Comparison of Encoding Proposals

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Proposal 1 | Proposal 2 | Proposal 3 | Proposal 4 |
| Communality of policy provisioning between Get (Pull operation) and Notify (Push operation) | No | Yes | Yes | No |
| Efficient policy provisioning for initial GET | Yes | Less efficient, as two HTTP Request response pairs required. | Yes | Yes |
| Efficient policy provisioning for subsequent GET (Pull operation, FFS if this is required) | For HTTP GET only complete policy but no deltas can be provided. Thus most likely custom operation required. | Alternatives:  1. two HTTP interactions, but possibility to provide only deltas in Policy.  2. custom operation. | For HTTP GET only complete policy but no deltas can be provided. Thus most likely custom operation required. | Alternatives:  1. return policies in HTTP GET response:  only complete policy but no deltas can be provided.  2. use two HTTP interactions:  only complete policy but no deltas can be provided.  3. custom operation. |
| Efficient policy provisioning for Notify (Push operation) | Yes (Depends on custom operation design) | Yes | No, two HTTP interactions, and no possibility to provide only deltas in policy | Yes |
| RESTful design | Only small fractions. A substantial part of the functionality (PUSH policy provisioning and most likely also subsequent PULL operation) uses custom operations. | Yes  (Evolution to combination with event exposure might require custom operation for subsequent GET.) | Partial:  most likely subsequent PULL operation requires custom operation.  (Evolution to combination with event exposure might require custom operation for subsequent GET.) | Partial:  Duplicated resource is not a usual pattern.  (Evolution to combination with event exposure might require custom operation for subsequent GET.) |
| Efficient Deletion | OK | OK (assuming policy resources at SMF are implicitly deleted when SMF deletes subscription resource.) | OK | OK (assuming policy resources at SMF are implicitly deleted when SMF deletes subscription resource.) |

#### 5.4.3.7 Conclusions

Encoding proposal 1 is selected for the normative work.

### 5.4.4 Npcf\_PolicyAuthorization service

#### 5.4.4.1 General

The is service is to authorise an AF request and to create policies as requested by the authorised AF for a PDU session to which the AF session is bound. This service allows the NF consumer to subscribe/unsubscribe the notification of events (e.g. change of access type or RAT type, changes of the PLMN identifier).

#### 5.4.4.2 Operations

Table 5.4.4.2-1: Operations of the Npcf\_PolicyAuthorization Service

| Service operation name | Description | Initiated by | Inputs, required | Inputs, optional | Outputs, required | Outputs, optional |
| --- | --- | --- | --- | --- | --- | --- |
| Npcf\_PolicyAuthorization\_Create | Authorizes the request from the application, and optionally communicates with Npcf\_SessionPolicyControl service to determine and install the policy according to the information provided by the NF Consumer. Creates an application context in the PCF. | NF service consumer (AF/NEF) | IP address of the UE, application session context identifier | SUPI if available,  DNN if available,  Media type, Media format, bandwidth requirements,  sponsored data connectivity if applicable,  flow description, AF application identifier, AF Communication Service Identifier, AF Record Identifier, Flow status, Priority indicator, emergency indicator, Application service provider, resource allocation outcome | Success or Failure | none |
| Npcf\_PolicyAuthorization\_Update | Provides updated application level information and communicates with Npcf\_SessionPolicyControl service to determine and install the policy according to the information provided by the NF Consumer. Updates an application context in the PCF. | NF service consumer (AF/NEF) | application session context identifier | Media type, Media format, bandwidth requirements, sponsored data connectivity if applicable, flow description, AF application identifier, AF Communication Service Identifier, AF Record Identifier, Flow status, Priority indicator, Application service provider, resource allocation outcome | Success or Failure | none |
| Npcf\_PolicyAuthorization\_Delete | Provides means for the NF Consumer to delete the context of application level session information. | NF service consumer (AF/NEF) | application session context identifier | none | none | none |
| Npcf\_PolicyAuthorization\_Notify | Provided by the PCF to notify NF consumers of the subscribed events, such as signalling path status of AF session, access type and RAT type, PLMN identifier, access network information, i.e. User Location Information and/or UE Time Zone, usage report, resource allocation outcome. | PCF | event to notify (signalling path status of AF session, access type and RAT type, PLMN identifier, access network information, i.e. User Location Information and/or UE Time Zone, usage report, resource allocation outcome) | none | The event information for the subscribed event type and event object | none |
| Npcf\_PolicyAuthorization\_Subscribe | Provided by the PCF to enable NF consumers to explicitly subscribe the notification of events, such as change of access type or RAT type, changes of the PLMN identifier. | NF service consumer (AF/NEF) | List of events (including the event type and event object) as specified in Npcf\_PolicyAuthorization\_Notify service operation, application session context identifier,  Notification URI (NOTE) | none | Success or Failure | none |
| Npcf\_PolicyAuthorization\_Unsubscribe | Provided by the PCF to enable NF consumers to explicitly unsubscribe the notification of events as specified for Npcf\_PolicyAuthorization\_Subscribe operation. | NF service consumer (AF/NEF) | List of events (including the event type and event object) as specified in Npcf\_PolicyAuthorization\_Notify service operation, application session context identifier | none | Success or Failure | none |
| NOTE: A Notification URI where to send Notifications is required because support of notification with two HTTP client-server pairs, as specified in subclause 5.5.1.1.9.2, has been selected. This is a stage 3 matter not reflected in stage 2. | | | | | | |

Editor's note: It is FFS whether identification of the application session context is a required input to the Npcf\_PolicyAuthorization\_Notify operation. This parameter is not yet included in stage 2.

Editor's note: It is FFS whether the application session context identifier can be a required output rather than a required input for the Npcf\_PolicyAuthorization\_Create operation and thus be assigned by the PCF. This could enable a resource creation via HTTP POST.

#### 5.4.4.3 Encoding Proposal 1: RESTful HTTP with event subscriptions as sub-resource



Figure 5.4.4.3-1: Proposed Resource URI structure of the Npcf\_PolicyAuthorization API

Table 5.4.4.3-1: Proposed resources and methods overview for the Npcf\_PolicyAuthorization service

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | Resource URI | HTTP method | Request body | Successful response body | Meaning |
| Npcf policy authorization | {apiRoot}/ npcf-policyauthorization/ v1/ sessions | POST (FFS, see editor's note) | SessionRequest | SessionAnswer | Requests that the PCF creates a new session for Npcf policy authorization. |
| Individual Npcf policy authorization | {apiRoot}/ npcf-policyauthorization/ v1/ sessions/ {Sessionid} | PUT  (FFS, see editor's note) | SessionRequest | SessionAnswer | Request that the PCF creates a new session for Npcf policy authorization, if it does not exist or updates an existing session. |
| PATCH (FFS, see editor's note) | FFS | FFS | Partially updates session for Npcf policy authorization |
| GET | none | Session | Provides information about a session for Npcf policy authorization. |
| DELETE | none | DeleteAnswer | Instructs the PCF server to delete a session for Npcf policy authorization. |
| Media Components | {apiRoot}/ npcf-policyauthorization/ v1/ sessions/ {Sessionid}/ media-components | PUT  (FFS) | 1..N MediaComponent | none | Requests that the complete set of media components for a session is added or replaced. |
| GET | none | 1…N, MediaComponent | Gets information about the complete set of media components for a session |
| Individual Media Component | {apiRoot}/ npcf-policyauthorization/ v1/ sessions/ {Sessionid}/ media-components/ {mcNbr} | PUT  (FFS, see editor's note) | MediaComponent | none | Request that the server creates a new media component, if it does not exist or updates an existing media component. |
| PATCH (FFS, see editor's note) | FFS | FFS | Partially updates a media component |
| GET | none | MediaComponent | Provides information about a media component. |
| DELETE | none | none | Instructs the PCF to delete a media component. |
| NPCF policy authorization event subscription  (FFS, see editor's note) | {apiRoot}/ npcf-policyauthorization/ v1/sessions/[Sessionid}/event-subscription | PUT | EventSubscription | none | Allows the NF service consumers to subscribe to the notification of events or modify that subscription. |
| DELETE | none | none | Allows the NF service consumers to unsubscribe to the notification of events. |

Editor's note: It is FFS whether to use PUT or POST or to allow both for the creation of the policy authorization operation. If POST is used the client addresses the resource responsible for service creation at the server. The server allocates the session id (provided in the location header of 201 Created) having a more server centric solution. The advantage of POST is that it is the standard characteristic to create a new resource in RESTful web development, uses a clear server centric solution and service creation and update are distinguished by the methods. The advantage of PUT is that the method is idempotent if the client uses the same session id for following request.

Editor's note: It is FFS whether PATCH should only be supported as an optional method by the PCF. Depending on the selected encoding, PATCH can be not idempotent and not secure. The restriction for the server is that it is not allowed to react on GET request with data not completely patched. Normally PUT is used for service updating with the disadvantage to transport the complete representation of the resource and should normally be supported by the server in any case. Within this usage strategy for PUT the definition of meaningful sub-resources can be helpful (e.g. sub-resources for media component descriptions, sponsored data, etc.).

Editor's note: It is FFS whether the "eventsubscription" should be defined as own subresource or related information only be included in the Individual Npcf policy authorization resource. The "eventsubscription" resource allows to address the DELETE message to the "eventsubscription" resource without a request body and to keep the active service operation with a session id.

Editor's note: It is FFS if the mediacomponent subresource is required or related information only is only included in the Individual Npcf policy authorization resource. In the latter case media components could be updated using PATCH.

Table 5.4.4.3-2: Proposed resources and methods overview for the Npcf\_PolicyAuthorization notification services

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | Resource URI | HTTP method | Request body | Successful response body | Meaning |
| Npcf policy\_notification | {notificationURI}  FFS (see editor's note) | POST | NotificationInformation | none | Informs the client about events. |

Editor's note: It is for FFS whether the notificationURI should be extendable by sub-resources defined. An application can be the event notification service to the resource {notificationURI}/eventid. Another application can be an asynchronous process in which the client waits for a longer time period for service compilation (e.g. a new service creation with POST will be answered with 202 Accepted to the resource {notificationURI}/notificationid) and after final service request compilation with a POST to {notificationURI}/notificationid which has to be answered with 200 OK by the client now.

Table 5.4.4.3-3: Proposed type Session

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| request | ServiceRequest | 1 |  |
| answer | ServiceRequestAnswer | 1 |  |

Table 5.4.4.3-4: Proposed type SessionRequest

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| supi | Supi | 0..1 |  |
| dnn | Dnn | 0..1 |  |
| ipDomainId | IpDomainId | 0..1 |  |
| afAppId | AfAppId | 0..1 |  |
| mediaComponents | MediaComponent | 1..N |  |
| afChargingId | AfChargingId | 0..1 |  |
| subId | SubscriptionId | 0..1 |  |
| resPrio | ResPrio | 0..1 |  |
| ueIpv4 | Ipv4Addr | 0..1 |  |
| ueIpv6 | Ipv6Addr | 0..1 |  |
| svcURN | SvcURN | 0..1 | Service-URN |
| spConnData | SpConnData | 0..1 |  |
| mpsId | MpsId | 0..1 | MPS-Identifier |
| refId | RefId | 0..1 |  |
| eventSubscription | EventSubscription | 0..1 |  |

Table 5.4.4.3-5: Proposed type MediaComponent

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| mcNumber | UInteger | 1 |  |
| FFS |  |  |  |
|  |  |  |  |

Table 5.4.4.3-6: Proposed type SessionAnswer

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| sessionId | SessionId | 1 |  |
| ancId | AncId | 0..1 | Access-Network-Charging-Identifier |
| ancAddr | Address (FFS) | 0..1 | Access-Network-Charging-Address |
| acceptableSvcInfo  FFS if this should rather go to a negative response | AcceptableSvcInfo | 0..1 | Accepable Service Info |
| ipCanType (FFS, needs to cover 5GC) | IpCanType (FFS) | 0..1 |  |
| netLocAccSupp | NetLocAccSupp | 0..1 |  |
| ratType | RatType | 0..1 |  |
| anTrusted | boolean | 0..1 | Indicates whether the access network is trusted or untrusted for the Non-3GPP access network |
| anGWAddr (FFS if this applies for 5GC) | Address (FFS) | 0..1 | Carries the IP address of the ePDG used as IPSec tunnel endpoint with the UE |
| flows | Flows | 0..N |  |
| retryInterval | DurationSec | 0..1 |  |

Table 5.4.4.3-7: Proposed type Flows

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| FFS |  |  |  |
|  |  |  |  |

Table 5.4.4.3-8: Proposed type EventSubscription

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| events | Event (FFS) | 1..N |  |
| notificationURI | Uri | 1 |  |

Table 5.4.4.3-9: Proposed type DeleteAnswer

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| resCode | ResCode | 0..1 |  |
| spConnData | SpConnData | 0..1 |  |
| uli | UserLocationInformation | 0..1 | User-Location-Info |
| uliTime | DateTime | 0..1 |  |
| msTimeZone | TimeZone | 0..1 |  |
| ueLocalIt | DateTime | 0..1 | User-Location-Info-Time |
| ranNasRelCause | RanNasRelCause(FFS) | 0..1 |  |
| sgsnMccMnc | SgsnMccMnc | 0..1 |  |
| twanId | TWANId | 0..1 |  |
| netLocAccSupp | NetLocAccSupp | 0..1 |  |
| tcpSrcPort | Port(FFS) | 0..1 |  |
| udpSrcPort | Port(FFS) | 0..1 |  |

Table 5.4.4.3-10: Proposed type NotificationInformation

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| event | Event (FFS) | 1 |  |
| FFS |  |  |  |

#### 5.4.4.4 Encoding Proposal 2: RESTful HTTP with event subscriptions as a separated sub-resource



Figure 5.4.4.4-1: Proposed Resource URI structure of the Npcf\_PolicyAuthorization API

Table 5.4.4.4-1: Proposed resources and methods overview for the Npcf\_ PolicyAuthorization service

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | Resource URI | HTTP method | Request body | Successful response body | Meaning |
| Application sessions | //{apiRoot}/npcf-policy-authorization/v1/application-sessions | POST | FFS | FFS | Npcf\_PolicyAuthorization\_Create. Creates a new individual Application session context resource. |
| Individual Application session context | //{apiRoot}/npcf-policy- authorization/v1/application-sessions/{appSessionContextId} | PUT (FFS) | FFS | FFS | Npcf\_PolicyAuthorization\_Update. Creates a new or updates an existing individual Application session context resource. |
| PATCH (FFS) | FFS | FFS | Npcf\_PolicyAuthorization\_Update. Updates an existing individual Application session context resource. |
| DELETE | FFS | FFS | Npcf\_PolicyAuthorization\_Delete. Deletes an existing individual Application session context resource. |
| GET | FFS | FFS | Reads an existing individual Application session context resource. |
| Event Subscriptions | //{apiRoot}/npcf-policy-authorization/v1/event-subscriptions | POST | FFS | FFS | Npcf\_PolicyAuthorization\_Subscribe.  Creates a new event subscription resource for a given Application session context identifier. |
| Individual Event Subscription | //{apiRoot}/npcf-policy-authorization/v1/event-subscriptions/{eventSubId} | PUT | FFS | FFS | Npcf\_PolicyAuthorization\_Subscribe. Modifies an existing event subscription resource. |
| DELETE | FFS | FFS | Npcf\_PolicyAuthorization\_Unsubscribe.  Deletes an event subscription. |
| GET | FFS | FFS | Reads an event subscription resource. |

Editor's note: It is FFS whether PUT and/or PATCH should be used for the encoding of the Npcf\_PolicyAuthorization\_Update service operation.

Table 5.4.4.4-2: Proposed methods overview for the Npcf\_PolicyAuthorization\_Notify service operation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | URI | HTTP method | Request body | Successful response body | Meaning |
| Individual Event Subscription | {Notification URI} | POST | FFS | FFS | Npcf\_PolicyAuthorization\_Notify.  Notifies an occurrence of a subscribed event. |

#### 5.4.4.5 Comparison of encoding proposals

Table 5.4.4.5-1: Comparison of encoding proposals

|  |  |  |
| --- | --- | --- |
|  | Proposal 1 | Proposal 2 |
| Separate usage of Event exposure | Yes: all service information related attributes are optional. | Yes |
| Separate Evolution of event exposure to group communication | Possible as long as service information related attributes remain optional. | Yes |
| Combined Evolution of event exposure and service information provisioning to group communication. | Yes | More complex. |
| Support of Events related to particular service media flows (e.g. QoS not available) | Yes | Complicated, e.g. via URL to related resource. |
| Combined operations of event subscriptions and service information provisioning at start of application | Yes | No: two HTTP interactions required. |
| Combined operations of event unsubscriptions and service information revocation at stop of application | Yes | No: two HTTP interactions required. |
| Multiple Event Subscriptions for the same Application session | No | Yes |

NOTE 1: Whether combined operations for service information and event subscription handling are required remains unspecified and the final solution will be covered as part of the normative work.

NOTE 2: Multiple event subscriptions for the same application session is not a stage 2 requirement.

#### 5.4.4.6 Conclusions

The approach defined in Encoding proposal 1 is selected for progressing the normative work.

Resource structure at application session level is left for the normative work.

### 5.4.5 Nsmf\_EventExposure

#### 5.4.5.1 General

This service provides events related to PDU sessions towards consumer NF. The service operations exposed by this service allow other NFs to subscribe, unsubscribe and get notified of events happening on the PDU session. The following are the key functionalities of this NF service.

- Allowing consumer NFs to subscribe and unsubscribe for events on a PDU session; and

- Notifying events on the PDU session to the NFs that require reporting.

The following are the types of events that can be exposed by the SMF:

- UPF change (Addition and/or removal of PDU session anchor);

- SMF change;

- Application traffic detection (start and stop);

- PDU session statistics (for example usage reporting);

- PDU session release; and

- Out of credit.

Editor's note: Stage 2 indicates that it is FFS how this service may be used for online charging.

#### 5.4.5.2 Operations

Table 5.4.5.2-1: Stage 2 requirements for Operations of the Nsmf\_EventExposure service

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Service Operation name | Description | Initiated by | Input, required | Input, optional | Output, required | Output, optional |
| Nsmf\_EventExposure\_Notify | Report UE PDU session related event(s) to the NF which has subscribed to the event report service | SMF | UE ID, PDU Session ID, Event Trigger, Event correlation ID | Event specific parameter list, DNAI | none | none |
| Nsmf\_EventExposure\_Subscribe | This service operation is used by an NF to subscribe for event notifications on a specified PDU session or to modify an existing subscription for event notifications on a specified PDU session. | NF service consumer (PCF, NEF, AMF, or AF) | Notification URI (NOTE), PDU Session ID, Identification of UE(s) (a single UE ID (SUPI or IP address and DNN) or identification for a group of UE(s), or "any UE"), Event correlation ID, Event filter, event notification method (periodic, one time, on event detection) | immediate one time notification flag,  reporting options (e.g. Maximum Number of Reports or Monitoring Duration, Repetition Period for periodic reporting) | none | none |
| Nsmf\_EventExposure\_UnSubscribe | This service operation is used by an NF to cancel a subscription to event notifications. | NF service consumer (PCF, NEF, AMF, or AF) | Event correlation ID | none | none | none |
| NOTE: A Notification URI where to send Notifications is required because support of notification with two HTTP client-server pairs, as specified in subclause 5.5.1.1.9.2, has been selected. It is assumed that the NF ID in stage 2 corresponds to this. | | | | | | |

Editor's note: The Repetition Period for periodic reporting as optional input parameter to the subscribe is not explicitly mentioned in stage 2, but stage 2 only lists examples of reporting options.

Editor's note: The use of the Nsmf\_EventExposure\_UnSubscribe operation to cancel the complete subscription, and thus not requiring other input parameters than the Event correlation ID is not currently covered in stage 2.

#### 5.4.5.3 Encoding Proposal 1: RESTful HTTP



Figure 5.4.5.3-1: Proposed Resource URI structure of the Nsmf\_EventExposure API

Table 5.4.5.3-1: Proposed resources and methods overview for the Nsmf\_EventExposure service

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | Resource URI | HTTP method | Request body | Successful response body | Meaning |
| SMF Notification Subscriptions | {apiRoot}/ nsmf-event-exposure/ v1/ subscriptions/ | POST | Nsmf\_EventExposure | NsmfEventExposure | Create a new Individual SMF Notification Subscription resource. |
| Individual SMF Notification Subscription | {apiRoot }/ nsmf-event-exposure/ v1/ subscriptions / {eventSubId} | GET | none | NsmfEventExposure | Read an Individual SMF Notification Subscription resource. |
| PUT | Nsmf\_EventExposure | NsmfEventExposure | Modify an existing Individual SMF Notification Subscription resource. |
| DELETE | none | none | Delete an Individual SMF Notification Subscription resource and cancel the related subscription. |

Table 5.4.5.3-2: Proposed methods overview for the Nsmf\_EventExposure\_Notify service operation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource name | URI | HTTP method | Request body | Successful response body | Meaning |
| SMF Event Notification | {notificationURI} | POST | Nsmf\_EventExposureNotification | FFS | Notify the NF service consumer about subscribed events |

Table 5.4.5.3-3: Proposed type Nsmf\_EventExposure

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| supi | Supi (FFS) | 0..1 | Subscription Permanent Identifier (NOTE) |
| gpsi | Gpsi (FFS) | 0..1 | Generic Public Subscription Identifier |
| ipv4Address | Ipv4Address (FFS) | 0..1 | The IPv4 Address of the served UE. (NOTE) |
| ipv6AddressPrefix | Ipv6AddressPrefix (FFS) | 0..1 | The Ipv6 Address Prefix of the served UE. (NOTE) |
| dnn | Dnn (FFS) | 0..1 | DNN (NOTE) |
| groupId | GroupId | 0..1 | Identifies a group of UEs. (NOTE) |
| anyUE | Boolean | 0..1 | Default is "FALSE". (NOTE) |
| pduSessionId | PduSessionId (FFS) | 0..1 | PDU session ID (NOTE) |
| eventSubId | EventSubId (FFS) | 0..1 | Event correlation ID. This parameter shall be supplied by the SMF in the body of HTTP requests of Nsmf\_EventExposure\_Notify service operation for reporting events that require subscription. |
| notificationURI | Uri | 0..1 | It identifies the recipient of Notifications sent by the SMF.  This parameter shall be supplied by the NF service consumer in the HTTP requests. |
| eventSubscriptions | EventSubscription | 1..N | Subscribed events |
| NOTE: Either information about a single UE (i.e. supi, gpsi or dnn and IP Address Information (i.e. ipv4Address or ipv6AddressPrefix), all in combination with pduSessionId), or groupId, or anyUE set to "TRUE" shall be included. | | | |

NOTE 1: The Supi, Gpsi, PduSessionId, EventSubId, Uri, Dnn, Ipv4Address, Ipv6AddressPrefix, and GroupId,data types should be specified as common data types applicable for multiple APIs

Table 5.4.5.3-4: Proposed type Nsmf\_EventExposureNotification

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| supi | Supi (FFS) | 1 | Subscription Permanent Identifier (NOTE) |
| ipv4Address | Ipv4Address (FFS) | 0..1 | The IPv4 Address of the served UE. (NOTE) |
| ipv6AddressPrefix | Ipv6AddressPrefix (FFS) | 0..1 | The Ipv6 Address Prefix of the served UE. (NOTE) |
| dnn | Dnn (FFS) | 0..1 | DNN (NOTE) |
| gpsi | Gpsi (FFS) | 0..1 | Generic Public Subscription Identifier (NOTE) |
| pduSessionId | PduSessionId (FFS) | 1 | PDU session ID (NOTE) |
| eventSubId | EventSub (FFS) | 1 | Event correlation ID |
| eventNotifications | EventNotification | 1..N | Notifications about Individual Events |
| NOTE: Information about a specified PDU session (i.e. supi (or gpsi) and pduSessionId, or dnn and IP Address Information (i.e. ipv4Address or ipv6AddressPrefix) and pduSessionId), shall be included. | | | |

Table 5.4.5.3-5: Proposed type EventSubscription

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| event | SmfEvent | 1 | Subscribed events |
| notificationMethod | NotificationMethod | 0..1 | If "notificationMethod" is not supplied, the default value "ON\_EVENT\_DETECTION" applies. |
| immediateNotification | Boolean | 0..1 | Default is "FALSE". |
| maxReportNbr | UInteger (FFS) | 0..1 | If omitted, there is no limit. |
| monitoringDuration | Duration (FFS) | 0..1 | If omitted, there is no limit. |
| repetitionPeriod | Duration (FFS) | 0..1 | Is supplied for notification Method "periodic". |

NOTE 2: The Duration data type and the UInteger (for unsigned integer) should be specified as common data type applicable for multiple APIs.

Table 5.4.5.3-6: Proposed Enumeration SmfEvent

|  |  |
| --- | --- |
| Enumeration value | Description |
| UPF\_CHANGE |  |
| APPLICATION\_TRAFFIC\_START | The start of application traffic has been detected. |
| APPLICATION\_TRAFFIC\_STOP | The stop of application traffic has been detected. |
| PDU\_SESSION\_RELEASE |  |
| OUT\_OF\_CREDIT | Credit is no longer available. |
| PLMN\_CHANGE | The UE has moved to another operator's domain. |
| SESSION\_AMBR\_CHANGE | The subscribed Session-AMBR has changed. |
| DEFAULT\_QOS\_CHANGE | The subscribed Default 5QI/ARP has changed. |
| ACCESS\_TYPE\_CHANGE | The access type of the PDU session has changed. |
| SERVING\_AREA\_CHANGE | The serving area of the UE has changed. |
| USER\_LOCATION\_CHANGE | Triggered upon a change in user location, e.g. change of TA (FFS other possible granularity). |
| CHANGE\_OF\_UE\_PRESENCE\_IN\_ PRESENCE\_REPORTING\_AREA | The UE is entering/leaving a Presence Reporting Area. |
| REVALIDATION\_TIMEOUT | SMF interaction to request PCC rules from the PCF for an established PDU session. This SMF interaction shall take place within the Revalidation time limit set by the PCF in the PDU session related policy information. |
| UE\_IP\_ADDRESS\_ALLOCATE | A UE IP address has been allocated. |
| UE\_IP\_ADDRESS\_RELEASE | A UE IP address has been released. |
| CHARGING\_CORRELATION\_EXCHANGE | Reports the access network charging identifier for the PCC rules that requires it. |
| USAGE\_REPORT | Reports the accumulated usage for one or more monitoring keys. |
| ACCESS\_NETWORK\_INFO\_REPORT | Access information as specified in the Access Network Information Reporting part of a PCC rule. |
| CREDIT\_MANAGEMENT\_SESSION\_ FAILURE | Indicates that a transient/permanent failure has been detected in the OCS. |
| UE\_TIME\_ZONE\_CHANGE | Indicates a change in the time zone the UE is currently located. |
| RAT\_TYPE\_CHANGE | Triggered upon a change in RAT type (FFS). |
| REALLOCATION\_OF\_CREDIT | FFS |
| SUCCESSFUL\_RESOURCE\_ALLOCATION | Indicates that resources have been successfully allocated for a PCC rule. |

Table 5.4.5.3-7: Proposed Enumeration NotificationMethod

|  |  |
| --- | --- |
| Enumeration value | Description |
| PERIODIC |  |
| ONE\_TIME |  |
| ON\_EVENT\_DETECTION |  |

Table 5.4.5.3-8: Proposed type EventNotification

|  |  |  |  |
| --- | --- | --- | --- |
| Attribute name | Data type | Cardinality | Description |
| event | SmfEvent | 1 | Event that is notified |
| dnai | Dnai (FFS) | 0..1 | DN Access Identifier |
| FFS | FFS | 0..1 | Depending on the event type, additional information can be required |

NOTE 3: The Dnai data type should be specified as common data type applicable for multiple APIs.

### 5.4.6 UDR service

#### 5.4.6.1 General

NOTE: Studies on the definition of the UDR service are out of scope of the present TR. The purpose of this subclause is to study the usage of the UDR service for policy control.

Table 5.4.6.1-1: Operations of the Nudr\_Unified\_Data\_Management Service

| Service operation name | Description | NF Consumers | Inputs, required | Inputs, optional | Outputs, required | Outputs, optional |
| --- | --- | --- | --- | --- | --- | --- |
| Nudr\_Unified\_Data\_Management\_Query | NF consumer intends to retrieve user data from UDR. | PCF, NEF | Data ID | None | Requested data | None |
| Nudr\_Unified\_Data\_Management\_Create | NF consumer intends to insert a new user data record into the UDR, e.g. when a provisioning FE consumer creates a profile for a new user, or creates a new service profile for an existing user. | PCF, NEF | Data ID, Data | None | Result | None |
| Nudr\_Unified\_Data\_Management\_Delete | NF consumer intends to delete user data stored in the UDR, e.g. when a provisioning FE deletes a service profile for an existing user, or removes the profile of a user, or NF service consumer intends to delete an application data record. | PCF, NEF | Data ID | None | Result | None |
| Nudr\_Unified\_Data\_Management\_Update | Provisioning FE intends to update stored data in the UDR. | PCF, NEF | Data ID, Data | None | Result | None |
| Nudr\_Unified\_Data\_Management\_Subscribe | NF consumer performs the subscription/un-subscription to notification to data modification in the UDR. The events can be changes on existing data, addition of data. | PCF | Data ID, Subscription Type, Notification Address | None | Result | None |
| Nudr\_Unified\_Data\_Management\_Notify | UDR notifies NF consumer(s) about modification of data, when data in the UDR is added, modified or deleted, and an FE needs to be informed about this, due to a previous subscription to notifications procedure or due to local configuration policy in the UDR. | PCF | Data ID, updated Data | None | Result | None |

Editor's note: The definition of the Data ID is FFS.

### 5.4.7 NWDAF services

#### 5.4.7.1 General

The following NF services are specified for NWDAF:

Table 5.4.7.1-1: NF Services provided by NWDAF

| Service Name | Description | Reference | Example Consumer |
| --- | --- | --- | --- |
| Nnwdaf\_Events\_Subscription | This service enables the consumer to subscribe/unsubscribe to NWDAF slice congestion events notification. Periodic notification and notification upon threshold exceeded can be subscribed to. | 5.4.7.2 | PCF |
| Nnwdaf\_Analytics\_Info | This service enables the consumer to request and retrieve operator specific analytics from NWDAF. | 5.4.7.3 | PCF |

Editor's note: CT3 ask SA2 to confirm the NWDAF operations.

#### 5.4.7.2 Nnwdaf\_Events\_Subscription Service

##### 5.4.7.2.1 General

The Nnwdaf\_Events\_Subscription service enables the NF service consumer to subscribe/unsubscribe to NWDAF slice congestion events notification. Periodic notification and notification upon threshold exceeded can be subscribed to.

##### 5.4.7.2.2 Operations

Table 5.4.7.2.2-1: Operations of the Nnwdaf\_Events\_Subscription Service

| Service operation name | Description | Initiated by | Input,  required | Inputs, optional | Outputs, required | Outputs, optional |
| --- | --- | --- | --- | --- | --- | --- |
| Nnwdaf\_Events\_Subscription\_Subscribe | Subscribes to NWDAF event with specific parameters. | NF service consumer (PCF) | Slice information | FFS | Confirmation of the Subscription | None |
| Nnwdaf\_Events\_Subscription\_Unsubscribe | Unsubscribe to NWDAF event with specific parameters. | NF service consumer (PCF) | Slice information | FFS | Confirmation of the unsubscription | None |
| Nnwdaf\_Events\_Subscription\_Notify | Notifies the consumer instance of the event that has subscribed to the specific NWDAF service. | NWDAF | FFS | FFS | None | FFS |

#### 5.4.7.3 Nnwdaf\_Analytics\_Info Service

##### 5.4.7.3.1 General

The Nnwdaf\_Analytics\_Info service enables the NF service consumer to request and retrieve specific analytics from NWDAF. It represents operator specific analytics that applies only in this network.

##### 5.4.7.3.2 Operations

Editor's note: Format and details of Analytics are FFS.

Table 5.4.7.3.2-1: Operations of the Nnwdaf\_Analytics\_Info Service

| Service operation name | Description | Initiated by | Inputs, required | Inputs, optional | Outputs, required | Outputs, optional |
| --- | --- | --- | --- | --- | --- | --- |
| Nnwdaf\_Analytics\_Info\_Request | The NF service consumer requests NWDAF operator specific analytics. | NF service consumer (PCF) | Analytics ID | None | Requested Analytics (TBC) | None |

## 5.5 Protocols

### 5.5.1 Protocol Candidates

#### 5.5.1.1 HTTP2/JSON

##### 5.5.1.1.1 General

HTTP is protocol that is widely used in the Internet as transport protocol, for instance for Web Browsing or for applications following the Representational State Transfer (REST) or RESTful architectural principles (see Roy T. Fielding`s Dissertation "Architectural Styles and the Design of Network-based Software Architectures" [18]).

REST defines a set of architectural principles on how to design services that focus on a system's resources, RSET uses the create, read, update, and delete (CRUD) operations to handle such resources and HTTP methods can be directly mapped to those operations:

- To create a resource on the server, use HTTP POST;

- To retrieve a resource, use HTTP GET;

- To change the state of a resource or to update it, use HTTP PUT;

- To remove or delete a resource, use HTTP DELETE.

Application data in the HTTP Body can be binary or text encoded. JSON (see IETF RFC 7159 [8] and IETF draft-newton-json-content-rules [14]) is one language to describe the format of such text-based payloads.

The protocol HTTP2 (see IETF RFC 7540 [7]) is in the introduction phase. Compared to HTTP1.1, HTTP2 enables a more efficient use of network resources and a reduced perception of latency by introducing header field compression and allowing multiple concurrent exchanges on the same connection. It also introduces unsolicited push of representations from servers to clients.

##### 5.5.1.1.2 HTTP/1.1

HTTP/1.1 is specified in IETF RFC 7230 [54], IETF RFC 7231 [60], IETF RFC 7232 [61], IETF RFC 7233 [62], IETF RFC 7234 [63] and IETF RFC 7235 [64].

The HTTP/1.1 architecture and routing mechanism are defined in IETF RFC 7230 [54].

Some main characteristics of HTTP/1.1 are listed below:

- Text formatted protocol: text-based framing and text-based HTTP Header;

- Text-based or binary-encoded HTTP Body (see subclause 5.5.3 for further description and assessment of candidate protocols for Serialization);

- Supports HTTP Pipelining: An HTTP client can send multiple HTTP requests to an HTTP server within one HTTP/1.1 connection without having to wait for the HTTP responses of the earlier requests; however the HTTP server shall send the responses in the same order as the corresponding requests, which can result in delayed responses if an earlier request cannot be responded yet (known as HOL blocking at HTTP level);

- Practically requires to open multiple TCP connections towards the same server to mitigate the problem of HOL blocking when it is required to send multiple requests to that server;

- Support of forwarding and routing mechanism, such as redirector, proxy;

- TLS can be applied to provide a transport level security; and

- Extendibility: both HTTP Header and Body can be extended.

##### 5.5.1.1.3 HTTP/2

HTTP/2 is specified in IETF RFC 7540 [7] and IETF RFC 7541 [59].

HTTP/2 does not obsolete the HTTP/1.1 message syntax. HTTP/1.1 semantics remain unchanged.

Some main characteristics of HTTP/2 are listed below:

- Binary formatted protocol: binary framing, binary encoded HTTP Header; HTTP/2 sends binary frames, all with the same layout. Binary framing eases implementations figuring out the start and end of frames.



Figure 5.5.1.1.3-1 HTTP/2 Frame Layout

- Text-based or binary encoded HTTP Body (like supported by HTTP/1.1, see subclause 5.5.3 for further description and assessment of candidate protocols for Serialization);

- Header compression, which enables to encode headers in 1 or 2 octets only (relying on static and/or dynamic tables for header compression);

- Multiplexed streams: A stream is an independent, bi-directional sequence of frames exchanged between the client and server within an HTTP/2 connection. A single HTTP/2 connection can contain multiple concurrently open streams, with either endpoint interleaving frames from multiple streams. This solves the problem of HOL of HTTP/1.1;

- One TCP connection possible per client server pair (a new TCP connection needs to be set up when exhausting the available unused streams ids);

- Server side initiated push, which allows the server to proactively push information to the client that can be used upon subsequent matching requests from the client;

- Stream based transfer with priority and dependency control: each stream has a priority which tells the peer which streams to consider most important in case of resource restraints at the server (e.g. overload); the client can also tell the server which other stream a particular stream depends on, to enable the server to prioritize the completion of the parent stream; and

- Flow control at connection and stream's levels: the HTTP connection and each of its streams have their own advertised flow window that the other end is allowed to send data for.

##### 5.5.1.1.4 Support of Notifications

###### 5.5.1.1.4.1 General

Subclause 7.1.2 of 3GPP TS 23.501 [2] requires support of Subscribe-Notify service operations, where

- a Control Plane NF\_A (NF Service Consumer) subscribes to NF Service offered by another Control Plane NF\_B (NF Service Producer).

- NF\_B notifies the results of this NF service to the interested NF(s) that subscribed to this NF service. The subscription request from consumer may include notification request for periodic updates or notification triggered through certain events (e.g., the information requested gets changed, reaches certain threshold etc.). This mechanism also covers the case where NFs (NF\_B) are subscribed to certain notifications implicitly without explicit subscription request (e.g. due to successful registration procedure).



Figure 5.5.1.1.4.1-1: "Subscribe-Notify" NF Service illustration

A Control Plane NF\_A may also subscribe to NF Service offered by Control Plane NF\_B on behalf of Control Plane NF\_C, i.e. it requests the NF Service Producer to send the event notification to another consumer(s).



Figure 5.5.1.1.4.1-2: "Subscribe-Notify" NF Service on behalf of another NF Service Consumer

Subscribe/Notify service operations require bidirectional communication between the NFs and the support of server-initiated communication from a server to a client, which may occur a long time (e.g. several days) after the client's subscription to the server, when the server needs to communicate information to the client.

With HTTP, a server cannot initiate a connection with a client nor send an unrequested HTTP response to a client; thus the server cannot push asynchronous events to the client. Possible solutions are investigated below.

###### 5.5.1.1.4.2 Solution with two client-server pairs

Subscribe/Notify service operations can be supported with HTTP with two client-server pairs, one per direction, as follows:

- NF A acts as an HTTP client and NF B as an HTTP server when NF A subscribes to NF B's notifications;

- NF B acts as an HTTP client and NF A as an HTTP server when NF B delivers notifications to NF A;

- with RESTful APIs, e.g. like specified in subclause 7.12 of ETSI GS MEC 009 [49]:

- to manage subscriptions, the server exposes a resource under which the client can request the creation/deletion of subscription resources. Those resources define criteria of subscription.

- to receive notifications, the client exposes one or more HTTP endpoints on which the client (or another NF Service Consumer) can receive POST requests. When creating a subscription, the client shall inform the server of the endpoint to which the server will later deliver notifications related to that particular subscription.

- to deliver notifications, the server includes the actual notification payload in the payload body of a POST request, and sends that request to the endpoint it knows from the subscription.

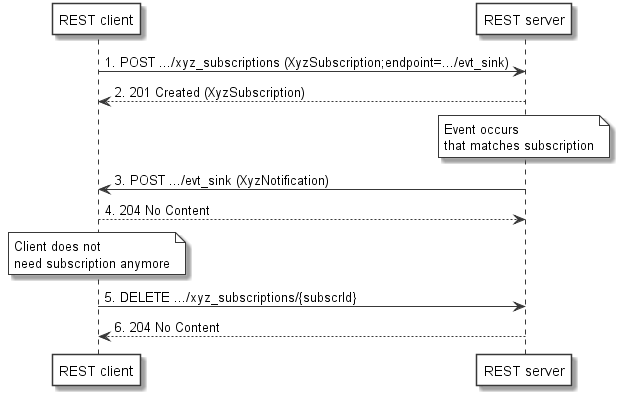


Figure 5.5.1.1.4.2-1: Creation of subscriptions and delivery of a notification

NOTE: A similar approach is also supported in some HTTP-based 3GPP interfaces, e.g. the xMB interface (see 3GPP TS 29.116 [40]), the Gw/Gwn interfaces (see 3GPP TS 29.251 [39]), and the St interface (see 3GPP TS 29.155 [37]).

- with RPC APIs, with different RPC operations for subscribing and delivering notifications respectively.

This solution is transparent to intermediaries.

This mechanism has the following drawbacks:

- overhead of setting up two TCP connections;

- requirement for the NF to act both as HTTP client and HTTP server;

- possible need to configure operator-grade firewalls to pass TCP/TLS/HTTP.

However, most 5G NFs need to support both the roles of client and server regardless of the need to support notifications, which mitigate the above drawbacks. For instance, an SMF acts over N11 as an HTTP server to establish PDU sessions, and as an HTTP client to request the AMF to send N1 or N2 signalling to the UE or RAN.

###### 5.5.1.1.4.3 Solutions with a single client-server pair prior to HTTP/2

IETF RFC 6202 [52] documents existing workarounds and associated issues to enable server push communication on a single HTTP connection, such as

- periodic HTTP polling from the client;

- HTTP Long Polling where the server attempts to hold open (i.e. not immediately reply to) each HTTP request, responding only when there are events to deliver;

- HTTP Streaming where the server keeps a request open indefinitely, i.e. it never terminates the request or close the connection, even after it pushes data to the client.

Due to the issues described in IETF RFC 6202 [52], none of them provides a satisfactory solution for the SBA.

###### 5.5.1.1.4.4 Solutions with a single client-server pair: HTTP/2 Server Push

HTTP/2 supports Server side initiated push (see subclause 8.2 of IETF RFC 7540 [7]), which allows the server to proactively push responses (along with corresponding "promised" requests) to a client in association with a previous client initiated request:

"Promised requests MUST be cacheable (see IETF RFC7231 [60], Section 4.2.3), MUST be safe (see IETF RFC7231 [60], Section 4.2.1), and MUST NOT include a request body. Clients that receive a promised request that is not cacheable, that is not known to be safe, or that indicates the presence of a request body MUST reset the promised stream with a stream error (Section 5.4.2) of type PROTOCOL\_ERROR. Note this could result in the promised stream being reset if the client does not recognize a newly defined method as being safe.

Pushed responses that are cacheable (see IETF RFC 7234 [63], Section 3) can be stored by the client, if it implements an HTTP cache.

Pushed responses are considered successfully validated on the origin server (e.g., if the "no-cache" cache response directive is present (see IETF RFC 7234 [63], Section 5.2.2)) while the stream identified by the promised stream ID is still open. Pushed responses that are not cacheable MUST NOT be stored by any HTTP cache. They MAY be made available to the application separately."

The mechanism is understood to be designed to send proactively responses into client's cache to decrease latency upon subsequent requests from that client matching the pushed responses, and not as a mechanism for the server to send notifications to the application on the client side, although the latter does not seem precluded by the very last sentence of the text quoted above ("They MAY be made available to the application separately") but is not further described (e.g. the use and handling of the promised request is not further described in such a case). Many APIs for HTTP/2, e.g. in browsers, seem to only support making pushed responses available to the application after the application provides the corresponding "promised" request.

This mechanism also has the following drawbacks:

- it is not guaranteed to work in presence of intermediaries:

"An intermediary can receive pushes from the server and choose not to forward them on to the client. In other words, how to make use of the pushed information is up to that intermediary. Equally, the intermediary might choose to make additional pushes to the client, without any action taken by the server."

However, 3GPP standards could address this problem by putting corresponding requirements on intermediaries in their controlled environment.

- it requires the server to generate and send a promised request for every pushes response;  
While this requirement could probably be met by 3GPP standards, it would mean some overhead;

- it requires to keep the stream of the original request of the client to the "open" or "half-closed (remote)" state with respect to the server.

###### 5.5.1.1.4.5 Solution based on Websocket

The Websocket protocol, defined in IETF RFC 6455 [53], provides support for bidirectional communications over a TCP connection that allows the sending of server's notifications to a client.

The main characteristics of Websocket are:

- it relies on the client to open the Websocket;

- Opening handshake based on HTTP/1.1 (HTTP/2 not supported) using HTTP Upgread Header;

- Followed by basic message framing (binary) on top of TCP. This is no more an HTTP connection, but just a transport connection;

- Text or binary data can be sent over a Websocket; and

- Provides 2 ways communication without having to open multiple HTTP connections.

The main intention of Websocket is to enable signaling towards a peer behind a firewall (In a typical Web-browsing scenario, this peer sends the first HTTP requests but may need to be updated with changing contents of a Webpage later on.). However, no such firewalls are expected within the 3GPP core network. Operator grade firewalls between different core networks are expected to be configured anyway but can use security gateways to reduce the number of required connections and related configuration (see 3GPP TS 33.210 [16]).

But as Websocket does not support server-initiated communication from a server to a client, the client and the server would be forced to maintain the websocket (set up after the opening handshake initiated by the client) for a long duration (e.g. several days) to allow the server to push information to the client when required. Keeping connections between all potential clients and servers for long durations when no information needs to be exchanged is not acceptable.

Besides, Websocket just provides a transport connection and is not an HTTP connection.

For the above reasons, this solution is not further considered.

##### 5.5.1.1.5 Extensibility Mechanisms

The Service-Based Architecture applications are likely to evolve, and indeed one of the key characteristics of the new architecture is that it needs to be flexible and allow innovation and development in an easy manner.

There are a number of different aspects in extending the system. These include ability to operate over different IP versions, evolve and change the underlying web protocol framework, and the ability to evolve the application components in Service-Based Architecture itself. Experience with Diameter applications in 3GPP has shown that 3GPP applications are frequently extended.

Examples of extensibility mechanisms:

a) Discover the connectivity options, protocols and possibly features supported by the server via the NRF.

b) HTTP/1.1 contains an upgrade mechanism to change the protocol, which can be used to upgrade e.g. to HTTP/2. However, it is not expected that this mechanism is useful for 3GPP to extend applications on top of HTTP.

c) HTTP/1.1 can be extended by the definition of new header fields; recipients are recommended to ignore unrecognized header fields (see subclause 3.2.1 of IETF RFC 7230 [54]). Such header fields can be, and already have been, defined by 3GPP (see below). In addition, new methods and status codes can be defined.

HTTP/2 continues to allow extensions via new header field, new methods and new status codes, but in addition extensions are permitted to use new frame types, new settings, or new error codes (see subclause 5.5 of IETF RFC 7540 [7]).

d) Whether the JSON payload within HTTP for an application can be extended without defining a new version of the application that is addressed via URL depends on the IDL that describes the payload: Such extensions are possible if information related to optional or added features is expressed in information elements that will be ignored by a recipient not supporting them. Such extensions are supported by some of the IDLs under consideration:

- IETF draft-newton-json-content-rules [14] specifies that additional properties within an object are ignored.

- The "OpenAPI 3.0.0 Specification" [36] specifies that by default, additional properties within an object are ignored; this can be controlled via the "additionalProperties" keyword.

e) It is common practise to express the versions of an application that needs to be addressed in the URL. HTTP routeing will direct the request to a server that supports the URL, and thus also the version. A server can also support different versions of an application and select which version of an application code to invoke based on version information in an URL.

f) Negotiate supported features between client and server: 3GPP CT3 has designed a supported feature mechanism for HTTP based applications and uses this mechanism in 3GPP TS 29.155 [37], 3GPP TS 29.251 [39], 3GPP TS 29.116 [40] and 3GPP TS 29.122 [71]. The mechanism works as follows:

- the "3gpp-Optional-Features" and "3gpp-Required-Features" HTTP header fields defined in 3GPP TS 29.155 [37], allow an HTTP client to express in an HTTP request features it desires or requires using, respectively;

- the "3gpp-Accepted-Features" HTTP header field defined in 3GPP TS 29.155 [37] allows an HTTP client to express in an HTTP responses features it accepts to use;

- those features can be used in subsequent communication between the client and server; and

- the mechanism assumes that an IDL is used where information related to optional or added features is expressed in information elements that will be ignored by a recipient not supporting them.

A versioning of services according to bullet e) influences request routeing (e.g. by versioning services in the request URI). This mechanism seems appropriate in cases where non-backward-compatible changes occur or new features are absolutely required. An example for such changes from past CT4 work is the introduction of new GTP versions. Such a mechanism should be supported by the 5G Service Based Interfaces, but it is expected that version upgrades will not be frequently applied.

Experience with Diameter applications in 3GPP has shown that 3GPP applications are frequently extended (typically in each release and also possibly with several independent optional features within one release). It was considered beneficial not to impact service routeing with those multiple extensions, but rather negotiate supported features between client and server once communication has been established, and 3GPP has designed a Diameter supported feature negotiation for that purpose. (Note that also in Diameter a versioning within application names would have allowed a routeing by DRAs similar to the routeing by http proxies based on versioning in the request URI). Such a fine-granular negotiation mechanism is required for 5G Service Based Interfaces.

To negotiate such fine-granular extensions, the following protocol mechanisms could be used:

1) A mechanism based on the 3gpp-Optional-Features" and "3gpp-Accepted-Features" HTTP custom headers fields similar to the mechanism designed by CT3 (see bullet f) above). Note that the "3gpp-Required-Features" HTTP header field may not be required as extensions with mandatory new feature are rather expected to be handled via URI versioning.

2) A mechanism based on similar information embedded in HTTP bodies.

An advantage of mechanism 2 is that HTTP custom headers can be stripped by some HTTP proxies. However, in the well-controlled environment of a 3GPP core network it is expected that this problem can be avoided. Another possible advantage of mechanism 2 is that HTTP bodies are handled directly by applications rather than the HTTP protocol layer, However, the OpenAPI IDL allows applications to also handle HTTP custom headers and it is also expected that other HTTP custom headers with relevance to applications will be defined, e.g. to indicate the type of HTTP payloads. Another advantage of mechanism 2 is that the scope of negotiation results is defined in a straightforward manner by including attributes used for the negotiation in the definition of a suitable resource for the service associated to or representing the NF Service Consumer (e.g. a top-level resource or a subresource representing the NF Service Consumer): The results apply for that resource and any subordinate resources and remain valid as long as the resource associated to or representing the NF Service Consumer exists. If a service defines multiple resources, the negotiation results would also apply to subordinate resources; it would also apply to custom operations related to that resource and, if the resource is used to subscribe to notifications, for the related notifications.

NOTE: How to negotiate features for APIs that would be designed without any resource (if any) will be clarified during the normative work.

A disadvantage of mechanism 2 is that it is not suitable for HTTP methods that allow no HTTP body, e.g. HTTP GET. However, a capability negotiation within a GET would fail anyway if HTTP responses are cached, and GET request are seldom used as first request when a service is started. Further, as a GET request only returns a resource representation it seems acceptable that a server then also provides information that the client does not understand and simply ignores. Further attributes enabling the mechanism would need to be defined for resource representation of those service operations that can be used as first service operation for a service (apart from HTTP GET) and related responses of each API, typically for the request to create a resource. However, common data types and procedures applicable for all API can still be defined, so the standardisation effort to add the procedures to a given API can be kept very small.

In summary, HTTP offer sufficient extensibility mechanisms to address the needs of 5G Service Based Interface. A versioning of services in the request URI according to bullet e) above will be supported by 3GPP 5G APIs, but it is expected that version upgrades will only be applied for non-backward compatible changes or the introduction of new mandatory features. In addition, a negotiation mechanism embedded in HTTP bodies to negotiate optional features for the upper-level resources of a service will be supported by 3GPP 5G APIs. Further details of those mechanisms will be covered in upcoming 3GPP Technical Specification on Principles and Guidelines for 5G System Services Definition.

Additionally, it should be possible for NF instances to register features (or a subset of the features) they support to the NRF, to enable NF Service Consumers to discover NF Service Producers supporting some specific features. Which features NF instances should register to the NRF will be determined by operator policy.

##### 5.5.1.1.6 HTTP Proxy

The GSMA has requested that the selected protocol provides the following capabilities.

- Use of proxies in the path, especially in the inter-operator networks (IPX) to ease the interconnection between roaming partners and roaming agreement setup.

- Use of proxies at the edge of the network acting as kind of signalling gateways to the rest of the world and performing topology hiding.

As operator will setup roaming agreement with most of the other operators, if the NF in VPLMN connects to the NF in HPLMN directly, there will be lots of long-lived connections. In order to aggregate the number of connections, the HTTP Proxy can be used in the network, especially in the inter-operator networks (IPX).

Operators willing to hide its network topology may deploy reverse HTTP Proxies (for ingress traffic) at the edge of their network.

A client that is configured to use a proxy over HTTP/2 directs requests to that proxy through a single connection. That is, all requests sent via a proxy reuse the connection to the proxy. The proxy performs the URL based routing to forward the received message to the corresponding peer NF.

Editor's note: The detail mechanism of HTTP Proxy will be further clarified.

##### 5.5.1.1.7 Protocol Candidate TCP/TLS/HTTP2/JSON

In current deployments, HTTP is in most cases transported using TCP (see IETF RFC 793 [5]), which provides a reliable transport.

TLS (see IETF RFC 5246 [6]) can be applied to provide transport level security.

##### 5.5.1.1.8 Protocol Candidate UDP/QUIC/HTTP2/JSON

IETF is currently specifying a new alternative transport protocol for HTTP called QUIC (see IETF draft-ietf-quic-transport [10], IETF draft-ietf-quic-tls [11], IETF draft-ietf-quic-http [12], and IETF draft-ietf-quic-recovery [13]).

QUIC is a multiplexed and secure transport protocol that runs on top of UDP. QUIC aims to provide a flexible set of features that allow it to be a general-purpose transport for multiple applications. QUIC implements techniques learned from experience with TCP, SCTP and other transport protocols. Using UDP as the substrate, QUIC seeks to be compatible with legacy clients and middleboxes. QUIC authenticates all of its headers and encrypts most of the data it exchanges, including its signalling. This allows the protocol to evolve without incurring a dependency on upgrades to middleboxes.

##### 5.5.1.1.9 Evaluation of HTTP aspects

###### 5.5.1.1.9.1 Selection of HTTP version

HTTP/1.1 is widely available but HOL blocking at HTTP level is a major concern for its possible use in the 5GC. This would require 5GC NFs acting as HTTP clients to open numerous concurrent TCP connections towards other 5GC NFs acting as HTTP servers. Text-based framing also results in a more complex and inefficient parsing of HTTP frames.

HTTP/2 provides higher performances by supporting:

- the multiplexing of HTTP requests over the same TCP connection without HOL blocking at HTTP level, thus also avoiding the need to open multiple TCP connections towards a same HTTP server;

NOTE: HOL blocking at TCP level still exists with HTTP/2 over TCP.

- binary framing, which allows easier and more efficient parsing of HTTP frames;

- header compression.

Consequently HTTP/2 shall be used if an HTTP solution is adopted for the SBA protocol.

###### 5.5.1.1.9.2 Selection of Notification method

Subscribe/Notify service operations can be supported in the SBA using two client-server pairs between a consumer NF and a provider NF as specified in subclause 5.5.1.1.4.2, without any significant concern, if an HTTP solution is adopted for the SBA protocol.

NOTE: More efficient alternatives might be further investigated for future releases.

#### 5.5.1.2 Diameter

Diameter is an authentication, authorization, and accounting protocol for computer networks. It evolved from and replaces the much less capable RADIUS protocol that preceded it.

The Diameter base protocol is defined by IETF RFC 6733[17], Diameter Applications can extend the base protocol by adding new commands, attributes, or both.

The communication between two diameter peers starts with the establishment of a transport connection (TCP or SCTP). Diameter security is provided by IPsec or TLS/DTLS.

NOTE: For existing 3GPP Diameter interfaces, IPsec is used, see 3GPP TS 33.210 [16].

Diameter is applied for instance by the following reference points in EPC system:

- S9: It provides transfer of (QoS) policy and charging control information between the Home PCRF and the Visited PCRF in order to support local breakout function;

- Gx: It provides transfer of (QoS) policy and charging rules from PCRF to Policy and Charging Enforcement Function (PCEF) in the PDN GW;

- Rx: The Rx reference point resides between the AF and the PCRF.

The protocol stack of Diameter is described in figure 5.5.1.2-1.

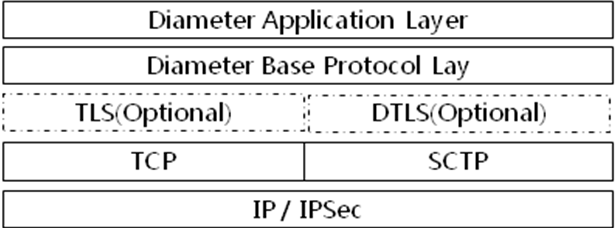


Figure 5.5.1.2-1: Diameter stack

The message format of Diameter is described in figure 5.5.1.2-2.

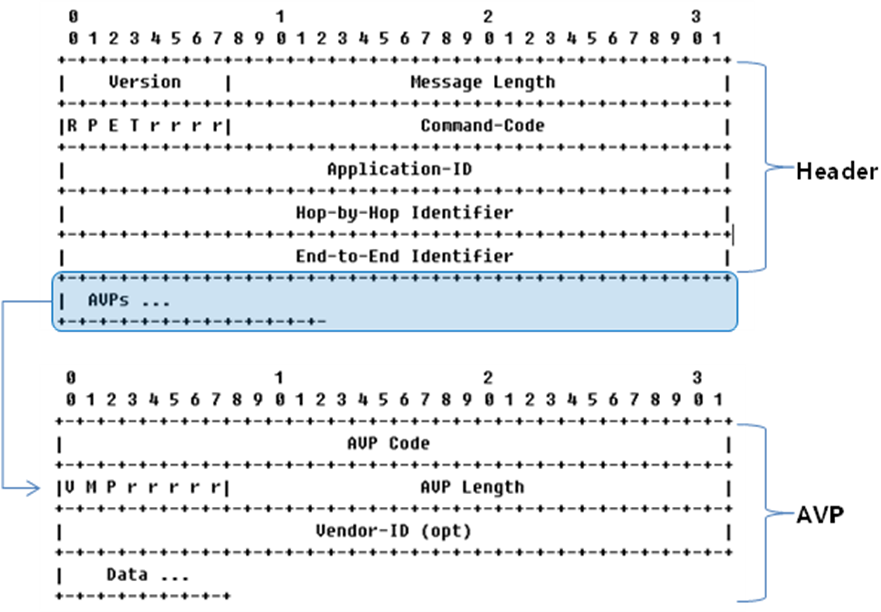


Figure 5.5.1.2-2: Diameter message format

The characters of Diameter protocol set are as follows:

- A pure binary formatted protocol, widely used in Internet and mobile network;

- Session based connection setup and maintenance. Transaction based communication between servers;

- Reliable transport is provided by the underlying transport protocol, e.g. SCTP (see IETF RFC 4960 [15])

- A peer-to-peer communication model that supports relay, proxy and redirect agents and that provide mechanisms for policy decision, message routing and session state maintenance;

- Flexible routing method: Routeing can be based both on Diameter headers and application layer AVPs;

- Enhanced extendibility: operators and vendors are able to define their own commands and AVPs;

- IPSsec, TLS/DTLS can be applied to provide a transport level security.

### 5.5.2 Comparison of RESTful and RPC protocol design

#### 5.5.2.1 Characteristics of RPCs

Remote procedure calls (RPCs) do not have a formal definition, but typical characteristics are described in the related Wikipedia article [50].

RPCs enable inter-process communication where a client entity invokes a certain functionality on a server entity over a network protocol. They typically use a request-response protocol. Unlike the RESTful design, the client typically does not operate on resources, but invokes "functions" or "services".

It should be pointed out that this architectural style is, essentially, how 3GPP has modelled the mobile networks during the last 20 years, with tight coupling of client and servers, and a thorough and detailed protocol specifications mandatory for both ends of each interface.

Many different implementations of RPCs exist that use various protocols for the data transfer and the encoding of the transported data. Among them are also implementations that use HTTP.

Some typical characteristics of RPCs over HTTP are:

- The POST verbs is used in most cases, sometimes also PUT or GET.

- The specific operation (service) to invoke may be included as part of the URI.

- For HTTP GET, the input parameters are coded as URI parameters.

- For HTTP POST or PUT, the input parameters are coded in the HTTP body.

- The result (output parameters) is coded in the body of the HTTP response.

Example of an HTTP request/response interaction following an RPC-style (the example represents an interaction from a well-known S6a protocol in the EPC system, just for the purpose to illustrate how a similar interaction would look like in the 5GC):

POST /operations/S6a:Authentication\_Information\_Request HTTP/1.1  
Host: hss.operator.com  
Content-Type: application/json  
{  
 "S6a:input" : {  
 "IMSI" : "987654321098765",  
 "VPLMNID" : "123456",  
 "RequestedEUTRANAuthenticationInfo" : {  
 "NumberOfRequestedVectors" : 1,  
 "ImmediateResponsePreferred" : true  
 },  
 "Flags" : "Request\_UE\_Usage\_Type"  
 }  
}

HTTP/1.1 200 OK  
Date: Thu, 26 Jan 2017 20:56:30 GMT  
Content-Type: application/json  
{  
 "S6a:output" : {  
 “AuthenticationInfo” : {  
 "EUTRANAuthenticationVectors" : [   
 {  
 "VectorNumber" : 1,  
 "RAND" : "NzA5Mzg0MDI5ODA4NDMyMQ==",  
 "XRES" : "MjA5Mzg0MDU5ODYwMDM4MQ==",  
 "AUTN" : "MTIzNDU2Nzg5MDEyMzQ1Ng==",  
 "KASME" : "OTg3NjU0MzIxMDY1NDMyMQ=="  
 }  
 ]  
 },  
 "UE\_Usage\_Type" : 1  
 }  
}

This style of modelling interactions between network entities is also referred as "Custom API methods" in section 5.5.2.7, as a way to complement a RESTful API with additional methods where it is not easy to find a mapping to a CRUD operation.

#### 5.5.2.2 Characteristics of REST

REST (Representational State Transfer) is a set of architectural principles introduced by Roy T. Fielding`s Dissertation "Architectural Styles and the Design of Network-based Software Architectures" [18]. Those principles are frequently associated to the Service Oriented Architecture. The principles are:

1. **Client/Server:**Split of responsibilities between client and server. A Client sends a request to the server which returns a response. This allows separating different tasks, e.g. the user interface generation from the data storage, which simplifies the single tasks and enhances portability and scalability.

2. **Stateless:**Each request from client to server must contain all the information necessary to understand the request. Session state is therefore kept entirely on the client. The server does not keep history/memory of previous requests. Possible session state can be transferred by the server to another service such as a database to maintain a persistent state for a period. Different request can be served by different servers, improving reliability and scalability.

3. **Cacheable:**If a response is cacheable, then a client cache is given the right to reuse that response data for later, equivalent requests. This allows to eliminate some interactions, improving efficiency, scalability, and average latency.

4. **Uniform interface:**The interface is based on an identification of resources, and allows a manipulation of resources through representations of these resources. Individual resources are identified in requests, for example using URIs. The resources themselves are conceptually separate from the representations that are returned to the client. When a client holds a representation of a resource, including any metadata attached, it should then be able to use server-provided links dynamically to discover all the available actions and has enough information to modify or delete the resource. Messages should be self-descriptive (e.g. indicate format via MIME type.  
The overall system architecture is simplified and the visibility of interactions is improved. Implementations are decoupled from the services they provide, which encourages independent evolvability. The trade-off, though, is that a uniform interface degrades efficiency, since information is transferred in a standardized form rather than one which is specific to an application's needs."

5. **Layered system:**The system is composed of hierarchical layers by constraining component behaviour such that each component cannot "see" beyond the immediate layer with which they are interacting. Intermediary servers may improve system scalability by enabling load balancing and by providing shared caches. The client does not care about how the server provides the response.

6. **Code on Demand** (optional):  
REST allows client functionality to be extended by downloading and executing code in the form of applets or scripts. This simplifies clients by reducing the number of features required to be pre-implemented.

The practise has shown that those principles are adhered to in varying degrees by APIs that claim to be RESTful. The Richardson maturity model for REST APIs (as originally suggested by Leonard Richardson during a conference presentation [48], see also Annex C of ETSI GS MEC 009 [49]) defines the following compliance levels for HTTP-based REST APIs

**Level 0**:  
A single service endpoint (e.g. API) is addressed via URI and HTTP is used as a tunnelling mechanism for remote interaction. RPCs using SOAP are mentioned as an example.

**Level 1**: **Resources**:  
Individual resources are addressed via URIs. Does not make use of the different HTTP methods, but uses HTTP POST only.

**Level 2**: **HTTP Verbs**:  
Using the HTTP verbs or methods as intended (e.g. POST, GET, DELETE, PUT) to keep apart different operations on resources.

**Level 3**: **Hypermedia** **Controls**:  
Hypermedia indicate to the client what is possible to do with a resource. This helps client developers explore the protocol. The links give client developers a hint as to what may be possible next and allow the server to advertise new capabilities.

NOTE: The API design guidelines in ETSI GS MEC 009 [49] recommend compliance with Level 3.

#### 5.5.2.3 Degree of Compliance of the stage 2 requirements with RPC

Stage 2 documents requirements in an RPC-like fashion: It defines "service operations" (i.e. actions described in terms of messages and their parameters).

However, stage 2 also requires that "network functions within the 5GC Control Plane shall only use service-based interfaces for their interactions". General characteristics of those "service based interfaces" are described in clause 7 of 3GPP TS TS 23.501 [2]. Among them are requirements that an NF can expose multiple services and that one service can have several consumers. Stage 3 protocol design for a RPC solution would need to take those requirements into consideration.

In addition to those concrete requirements, stage 2 wording and related argumentation in the preparatory study also signals an intent to align with principles of a service oriented architecture, for which the use of RPCs is prone to result in a proliferation of heterogenous interfaces and methods and lack of reuse.

#### 5.5.2.4 Degree of Compliance of the stage 2 requirements with REST

Table 5.5.2.4-1 analyses the extent to which REST principles according to Roy T. Fielding`s Dissertation "Architectural Styles and the Design of Network-based Software Architectures" [18], as outlined in subclause 5.5.2.2 are met by the stage 2 architecture and procedures of the 5GC Control Plane.

Table 5.5.2.4-1: Compliance of 5G service based architecture with REST principles.

|  |  |
| --- | --- |
| REST Principle | Compliance of 5G Service Based Architecture |
| **1. Client/Server** | ***Mostly met***. Services are defined in such a way that a provider NFs offers services to consumer NFs. However, services can include asynchronous notifications from server to client which may need to be modelled as a separate pair of client and server with reversed roles. |
| **2. Stateless** | ***Not fully met***. Stage 2 requires that a resource at a particular server, rather than a resource at an arbitrary server, is addressed after a separate server selection via the NRF. The server also needs to maintain some state to provide asynchronous notifications.  However, there are no stage 2 requirements to maintain a "session" state at the server on many interfaces (e.g. N8, N10, N12, N13), and other interfaces (e.g. N11, N7) can also be designed as session stateless. |
| **3. Cacheable** | ***Not fully met***. It is anticipated that most interactions will relate to resources for a particular served UE that can be changing frequently. Caching related responses would offer little benefit. However, NFs can cache NRF responses. |
| **4. Uniform interface** | ***Can be met***. It is largely a stage 3 decision how to document interfaces and whether to document service based interface in a uniform fashion. Adherence to level 3 of the Richardson maturity model seems possible. |
| **5. Layered system** | ***Met*.** Consumer NF does not need to be aware of how producer NF provides a response. |
| **6. Code on Demand** (optional) | ***Not met.***  No related stage2 requirements exist. |

Table 5.5.2.4-2 analyses the REST compliance level according to Richardson maturity model, as outlined in subclause 5.5.2.2, that APIs for service based interfaces of the 5GC Control Plane could achieve.

Table 5.5.2.4-2: Achievable Richardson Maturity Levels for RESTful APIs in the 5GC Control Plane.

|  |  |
| --- | --- |
| Level | RESTful APIs in the 5GC Control Plane |
| **Level 1**: **Resources** | ***It is expected that this level can be achieved to a large extent*.**  Stage 2 requirements are not documented in terms of resources, so additional stage 3 analysis will be required to derive resources.  Some services could map easily to resources, e.g. PDU session as resource for SMF services, or stored data as resource for UDM services. Designing resources for some other services may require more discussions, e.g.  • AMF services (N1N2 Message Transfer/Notify, Forward Relocation Request)  • AUSF services (UEAuthentication Request)  • 5G-EIR services (Check ME Identity)  As a possible remedy, RPC-like resources have been defined in previous RESTful APIs, e.g. the "task" resource defined in of ETSI GS MEC 009 [49]. |
| **Level 2**: **HTTP Verbs** | ***It is expected that this level can be achieved to a large extent.***  Once resources are defined in a suitable fashion, in most cases applying suitable HTTP methods should be simple.  However, for some special resources mainly the POST HTTP might be suitable, e.g. • Notifications could be described as resources posted by the client, but there might not be a requirement to subsequently manipulate those resources with other HTTP methods.  • Resources representing transferred messages at the AMF would likely also only be posted.  • There might be a need to pass some parameters when deleting a resource (see e.g. GTP-C DSR/DBR in EPC)  Note: Also for the "task" resource defined in of ETSI GS MEC 009 [49], only the POST method is supported, |
| **Level 3**: **Hypermedia** **Controls** | ***It is expected that this level can be achieved to a large extent.***  Once resources and HTTP verbs are defined in a suitable fashion, Hypermedia can also be provided. |

#### 5.5.2.5 Evaluation of RPC

For 5GC, the SBA definitions in stage-2 follow an architectural style that matches much more closely an RPC style of interaction, rather than a REST approach.

It should be noted that a RESTful or RPC approach is not inherently better or worse, and that several of the advantages present in REST, are also achievable by RPC.

Maybe, one of the advantages where REST is clearly superior is the higher degree of decoupling between client and server (allegedly achieved by the use of the HATEOAS principles). However, this characteristic is expected to bring more benefits in a scenario where the SDO defining an API has no, or little, control over the clients of such API; but this is NOT the case of 3GPP 5GC, where both client and servers are internal network entities fully specified, in all detail (including backwards compatibility across releases, feature negotiation mechanisms, protocol extensibility, etc..), by 3GPP; these criteria, however, may be different for interfaces exposed towards external clients of the 3GPP system.

#### 5.5.2.6 Evaluation of REST

##### 5.5.2.6.1 General

It is evident that the REST architectural style offers remarkable benefits, and that's why its acceptance in the design of web systems has grown exponentially in the last years. However, it should be also noted that the current architectural definition (stage-2) of the 3GPP 5GC has followed a totally opposite paradigm, mainly based on describing interactions between entities by following a procedure/service invocation, or the triggering of a certain action on the server (very much like a Remote Procedure Call), rather than a resource-oriented architectural definition, which would have been desirable in order to achieve a smooth and straightforward stage-3 protocol specification phase.

This fact does not mean that RESTful protocol design cannot be used, since it is often rather straightforward to map the service invocation described in stage-2 to a RESTful resource manipulation operation; when such mapping is easy or straightforward, it is indeed recommended to follow such design approach.

However, in other cases, mapping the stage-2 service invocation style of interaction to a resource operation is quite awkward and totally counter-intuitive, making it very hard and cumbersome the stage-3 protocol definition, which will affect the understanding of the relationship between stage-3 protocol and stage-2 service operations for implementers, making the system prone to inter-operability problems.

##### 5.5.2.6.2 Level 3 of the Richardson maturity model

Level 3 of the Richardson maturity model is supposed to offer the following benefits:

a) Hyperlinks allow developers to explore the possibilities of the API.

b) The structure of resources can be modified and extended by the server at any time and the client automatically adjust to such changes.

However, benefit a) seems not compelling in a 3GPP environment where 3GPP standards provide an open and extensive documentation.

Benefit b) seems to be very hard to achieve in practice, because for each hyperlink the meaning (what type of resource or custom operation does the hyperlink point to?), and possible operations (HTTP verbs, URI query parameters, etc.) would need to be communicated in a clearly standardized and machine readable fashion to allow a client to automatically make use of that hyperlink. Even then, it seems very unrealistic that a client can make automatic use of new API extensions advertised in such a fashion as it would also need the capability to further handle related extensions (e.g. to interwork with similar extensions at other interfaces).

The main drawbacks of adhering to Level 3 of the Richardson maturity model are:

a) Increased message size and computational effort.

b) Increased standardization effort, in particular if a stringent machine-readable format to describe all possible operations on a resource and the semantics associated with a hyperlink to a resource is defined.

It is thus suggested that 5G APIs do not need to support Level 3 of the Richardson maturity.

#### 5.5.2.7 HTTP APIs types

The API Design Guide from Google [51] provides general design guidelines for HTTP-based REST APIs and RPC APIs to design simple, consistent and easy-to-use APIs. Table 5.5.2.5-1 provides an overview of standard and custom API methods described in this document.

Table 5.5.2.7-1: Standard and Custom API methods

|  |  |  |
| --- | --- | --- |
|  | Standard API methods | Custom API methods |
| Usage | API functionality that naturally maps to one of the standard method  (CRUD operations). | API functionality that does not naturally map to one of the standard methods  (non-CRUD operations) |
| Method | Standard method:  List, Get, Create, Update, Delete | Custom methods |
| Resource/Scope | Applies to the resource indicated in the URI | Can be associated with a resource, a collection (see NOTE) or a service |
| HTTP mapping | Standard HTTP method  List: GET <collection URL>  Get: GET <resource URL>  Create: POST <collection URL>  Update: PUT or PATCH <resource URL>  Delete: DELETE <resource URL> | Custom method included in URI.  Mapped to the most suitable HTTP method (POST typically) |
| Parameters | Parameters/objects in Body or URI (e.g. search parameters in URI) | Parameters/objects in Body |
| Properties | Large number of resources, only few methods (CRUD) allowed | Large number of methods permitted |
| API examples | POST /Sessions/  DELETE /sessions/123456 | POST /messages:send  POST /sessions/123456:activate |
| Example use cases | CRUD operations | Cancel an outstanding operation  Move a resource from one parent to another  Activate/Deactivate a resource |
| NOTE: A collection contains a list of resources of the same type. | | |

#### 5.5.2.8 Conclusions

It would be straight forward to design RPCs based on the stage 2 service / service operations documentation, but such a protocol design might not adequately match the expectation motivating the selection of service based interfaces and could also block a future evolution to a larger compliance with a Service Oriented Architecture.

Designing RESTful APIs meeting stage 2 requirements for service based interfaces seems feasible but will require more stage 3 analysis to model resources. RESTful APIs offer the advantage of homogenous, easy to use interfaces, enhanced HTTP visibility (HTTP method accessible e.g. for proxying, logging, monitoring) and a larger decoupling between client and server compared to RPCs. For some operations, an RPC like design might be necessary, but experience exist how to embed such operations in a RESTful framework (see e.g. custom methods associated with a resource in subclause 5.5.2.5).

The 5GC manages resources such as UEs, sessions or database records where large number of instances exist and which can be mapped typically to simple resource operations like CRUD.

It is recommended to apply a RESTful framework for the protocol design as follows:

- service operations should implement the Level 2 of the Richardson maturity model, with standard API methods, whenever it is a good match for the style of interaction to model, e.g. service operations that can naturally map to one of the standard method (CRUD operations); this should be the preferred modelling attempt;

- service operations may use custom API methods (RPC interaction), when it is seen a better fit for the style of interaction to model, e.g. non-CRUD service operations.

### 5.5.3 Data Serialization Format

#### 5.5.3.1 Introduction

There is a huge number of alternatives to encode structured data over-the-wire. As can be seen in <https://en.wikipedia.org/wiki/Comparison_of_data_serialization_formats>, the list is quite exhaustive. Probably the main properties to focus, to select a the most appropriate encoding format would be:

- Standard (defined and backed-up by an SDO)

- Widespread industry adoption

- Performance (related in part to another property: binary vs textual)

So, from the list included in the reference above, the evaluation has been narrowed down to 3 alternatives: JSON (text-based, and being an IETF standard, with the widest adoption), and 2 binary alternatives (BSON and CBOR) to consider other approaches with a potential better performance.

Alternatives such as ASN.1 have not been considered, given the lack of industry acceptance of such format as data serialization over HTTP.

Alternatives such as Protocol Buffers / Apache Avro / MessagePack, etc, have not been considered given that they are not backed up by an SDO (despite the specification being publicly available, and being categorized as "Standardized" in the list of alternatives included in the reference above).

#### 5.5.3.2 Solution 1 – JSON

##### 5.5.3.2.1 Description

JSON is specified in IETF RFC 7159 [8], and it is a lightweight text-based data interchange format, originated from a subset of the JavaScript programming language.

It is the most widespread format, especially in the area of HTTP web services, given its simplicity and ease of use. It has a very simple and straightforward specification, and the tools availability is immense, both from a development perspective (programming language support for code generation to encode/decode documents) and from an application specification perspective (with IDL frameworks such as OpenAPI / Swagger, targeting primarily JSON as data format).

##### 5.5.3.2.2 Evaluation

The main advantage of JSON is its widespread adoption and deployment, being the de-facto industry standard, and also its simplicity (human-readable).

The main drawback is that it is considered as too verbose, with other binary alternatives having better performance, in terms of encoding/decoding and message size.

Given its de-facto industry standard for HTTP web services development, and the tool availability, it is regarded as the primary recommendation for usage in 3GPP 5GC specification. At the same time, it is recommended for further releases to consider a more efficient alternative, which should be assessed once more data regarding expected performance gains are collected by 3GPP members.

Regarding performance, it should be noted that sometimes the critical factor is the usage of a well-optimized encoder/decoder library; this is especially applicable to JSON, where many libraries included by default in a certain software platforms, can be greatly outperformed by specialized libraries (e.g., UltraJson (<https://github.com/esnme/ultrajson>), or Jackson (<https://github.com/FasterXML/jackson>).

#### 5.5.3.3 Solution 2 – BSON

##### 5.5.3.3.1 Description

BSON (short name for Binary JSON) is specified in <http://bsonspec.org/spec.html>. It should be noted that this format is not backed up by a Standards Developing Organization (SDO) and, instead, it was mainly developed as the binary format used in the MongoDB (<https://www.mongodb.com/>) document database to store JSON documents internally.

##### 5.5.3.3.2 Evaluation

The main design goal of BSON is the ease of traversal of documents, given its primary applicability to document databases. It was not designed to be specially more compact of faster than JSON.

BSON offers minimal performance gains (compared with JSON), with some tests claiming that the encoding and decoding might be even slower than a JSON equivalent document. The potential gains are quite dependent on the type of document (numeric fields are encoded/decoded more efficiently than textual fields). Also, when some "native" BSON data types are used during the encoding of the data structures, the performance gains are higher, but the obvious disadvantage is that by using them, the JSON/BSON equivalence is not possible anymore.

Similarly, the gains in message size are minimal, and in some cases, the BSON document may be even larger than the corresponding equivalent JSON document.

Overall, considering its non-standard status, its primary applicability to a "document database" environment, and its questionable performance benefits, BSON is not recommended for 3GPP 5GC protocols.

#### 5.5.3.4 Solution 3 – CBOR

##### 5.5.3.4.1 Description

Concise Binary Object Representation (CBOR) is specified in IETF RFC 7049 [47] and it is a binary serialization format specification developed primarily for constrained devices and applications, such as IoT devices.

The main goal of CBOR is to achieve a higher degree of compactness and efficiency, for both encoder and decoder, at least when compared with other text-based serialization formats such as JSON.

##### 5.5.3.4.2 Evaluation

CBOR is often hyped as being dramatically more efficient than JSON, claiming sometimes an efficiency gain of 2x-3x; however, according to benchmarks run over the Jackson processor (a high-efficiency JSON processor for Java), the efficiency gain in encoding/decoding, is typically around 20-30% (source: [https://groups.google.com/forum/#!topic/jackson-user/OSOnFl2izbo](https://groups.google.com/forum/" \l "!topic/jackson-user/OSOnFl2izbo)). It seems questionable whether a performance gain in this range makes up for some other clear advantages in JSON, such as the widespread industry usage, tools availability, and simplicity.

Another source worth checking is the academic Thesis work "Implementation and evaluation of the CBOR protocol" (<https://is.cuni.cz/webapps/zzp/download/130156104>) where it is stated that, while acknowledging the higher efficiency of CBOR, it is concluded that "while a viable alternative to JSON or MsgPack, CBOR's unique combination of features does not give it a significant competitive edge over these formats in their respective domains".

In addition, using CBOR makes it more difficult to use an IDL such as Open API (Swagger 2.0), which is mainly used along with JSON. There is, in fact, a specification language intended to cover this gap (CDDL – Concise Data Definition Language), currently under definition in IETF, but the status as of today is only an IETF draft (<https://tools.ietf.org/html/draft-ietf-cbor-cddl-00>), probably not mature enough to be used as a basis for specification in 3GPP 5GC.

In any case, CBOR is an alternative worth considering for usage in 3GPP 5GC, mostly because its expected higher efficiency and performance when handling specific data structures, such as byte arrays (octet streams), which are arguably one of the most common data structure expected in 5GC protocols (as they were in EPC protocols). For those, JSON is particularly poorly suited.

#### 5.5.3.5 Conclusion

It is recommended to use JSON as serialization data format for the specification of 3GPP 5GC in Rel-15.

Editor's note: It is FFS to investigate potential performance improvements on the transmission of binary data along with JSON, by using approaches other than a transformation to a text string (typically done with a base64 transform). One of such possibilities is to send large parts of opaque binary data using a multipart/mixed media type, where each part is sent via different media types (e.g. JSON payload with "Content-Type: application/json", and the binary data with "Content-Type: application/octet-stream").

Nonetheless, it is recommended to continue with internal 3GPP research efforts to evaluate the potential performance gain to be expected realistically from other encoding alternatives, for the specific payload types typically used in the 5GC interfaces.

The usage of CBOR (or other binary, more performant alternative) can be re-evaluated for subsequent 3GPP releases, once more detailed benchmark figures are available first-hand from the 3GPP community, and the tools availability is more stable.

It is expected that replacing JSON with a more efficient CBOR alternative can be achieved without impacting the application logic; content types for JSON and CBOR can be indicated by using the respective Media Types (application/json, application/cbor, etc..) allowing client and server to agree (via content negotiation and HTTP "Accept" headers) on the supported serialization format. However, it should be noted that this task would require substantial standardization effort.

### 5.5.4 Transport protocols

### 5.5.5 Interface Definition Language

#### 5.5.5.1 Introduction

An Interface Definition Language (IDL) is a specification language used to describe data models, and interactions between distributed software components.

Ideally, and IDL should have the following characteristics:

- Formal: It has to be machined-parsed, so it allows automatic checking of correctness and consistency

- Abstract: It is not bound to specific realizations, in terms of data modelling, or protocol mechanisms

- Independent of programming language or developing environment

- Independent of protocol or Inter-Process Communication mechanisms

- Independent of the data serialization format

- Provides definitions for frequently required data types

In 3GPP, one of the IDLs with a widest usage, traditionally, has been ASN.1; however, for SBA, and specifically for web technology (RESTful APIs, HTTP/JSON, etc.), there are other approaches with a wider adoption currently in the industry.

A non-exhaustive list of alternatives could be:

- Standards-based

- ITU-T/ETSI: ASN.1

- OASIS: RELAX-NG

- W3C: WSDL / XML Schema

- IETF: ABNF, YANG

- Non-Standard (De-facto Industry standards)

- OpenAPI Specification (Swagger)

- JSON Schema

- JSON Content Rules

- JSON RPC

- RAML

- Protocol Buffers

- Apache Thrift

In particular, for those protocols using a data serialization format such as JSON or CBOR, there is a need to further describe the data that can be transported in the protocol. IDLs typically are supported by tooling that allows to verify if a JSON or CBOR file complies with an interface definition written in the corresponding language, and possibly also to generate APIs and related code in various programming languages to generate or parse conformant JSON or CBOR files. Some of the IDL do not only contain information related to JSON or CBOR bodies, but also related to the underlying transport protocols, and thus allow for tooling with more extensive automation.

The IDL alternatives in the above list have been narrowed down to six alternatives that best characteristics for SBA and specifically for Web technology. An exhaustive and detailed analysis of each and every alternative from the above list is not intended.

#### 5.5.5.2 Solution 1 – YANG/RESTCONF

##### 5.5.5.2.1 Description

YANG is a data modelling language developed by IETF for the NETCONF protocol. It was originally designed for Network Management, as a replacement for the SNMP protocol (and the associated SMI information modelling framework).

It allows the definition of data models (both "configuration" data and "state" data), and also specific interactions between network elements, in the form of "Event Notifications" and "Actions" (associated to data objects), and generic "Remote Procedure Calls" to be invoked in a network entity.

YANG is defined in IETF RFC 6020 [31].

In addition, IETF RFC 8040 [35] defines an HTTP-based protocol (RESTCONF) to access data, and invoke actions, defined in YANG following a REST approach, with standard serialization options based on XML or JSON.

##### 5.5.5.2.2 Evaluation

The main characteristic of this alternative is its capability in terms of abstract data modelling. It shows a higher level of decoupling between the generic data model definition and the actual concrete implementation, in the form of a specific protocol realization and a specific data serialization format.

Additionally, a YANG data model can be used in a standard manner to describe a RESTful type of interaction between client and server, and at the same time, it can also describe RPC (Remote Procedure Call) interactions.

The main issue, from a 3GPP perspective, is that this language was not originally conceived as a general-purpose modeling language and, instead, its primary scope was the Network Management area. In addition, the learning curve is higher than other simpler alternatives.

#### 5.5.5.3 Solution 2 – OpenAPI Specification (Swagger)

##### 5.5.5.3.1 Description

OpenAPI (formerly known as Swagger) defines a standard, programming language-agnostic, interface description for REST APIs. It is specified at:

- <https://github.com/OAI/OpenAPI-Specification>

It consists on a language specification itself, and also on a number of tools intended for specification, documentation and code generation for implementation of client and server sides of the API, together with automation of test cases.

The files describing the RESTful API in accordance with the Swagger specification are represented as JSON objects and conform to the JSON standards. YAML, being a superset of JSON, can be used as well to represent a Swagger specification file.

For the definition of primitive data types, the specification is based on the JSON Schema draft-4 ([https://tools.ietf.org/html/draft-zyp-json-schema-04#section-3.5](https://tools.ietf.org/html/draft-zyp-json-schema-04" \l "section-3.5)).

The last version of OpenAPI Specification, recently approved (June 2017), is version 3.0.0, although the most stable version is 2.0, which has been in production for several years now (since 2014). In version 3.0.0, certain new features have been added, which are expected to be useful in the definition of 5GC interfaces (e.g., language support for adding HATEOAS content, and language support for handling of multipart media types in HTTP bodies).

##### 5.5.5.3.2 Evaluation

The main characteristic of this alternative is its massive and widespread adoption in the industry, for RESTful API design. It can be considered as a de-facto standard (although not backed-up by a formal SDO), and it has the biggest ecosystem of tools (both commercial an Open Source) and community support.

The main criticism to Swagger 2.0 relied on its lack of support for hypermedia, when the framework is mainly targeted for RESTful API specification. This implies that attempting to fulfil the HATEOAS (Hypermedia As The Engine Of Application State) principle, is not straightforward. Sources:

- <http://blog.novatec-gmbh.de/the-problems-with-swagger/>

- <https://jimmybogard.com/swagger-the-rest-kryptonite/>

In addition, given it primary focus on the RESTful architectural style, its support for RPC style of interactions is not so well supported, although there are workarounds to overcome this issue.

#### 5.5.5.4 Solution 3 – Protocol Buffers

##### 5.5.5.4.1 Description

Protocol Buffers is a mechanism, originally developed by Google and then turned to Open Source, to serialize structured data. It defines its own language (proto3, as the last version), to specify the structure of the data (messages, parameters, data types, etc.) so, in that sense, it can be considered as an IDL.

Protocol Buffers documentation can be found in:

- <https://developers.google.com/protocol-buffers/>, and

- https://github.com/google/protobuf/

The encoding of the data over-the-wire is binary and it is very compact and efficient, at the expense of not being self-describing (that is, there is no way to tell the names, meaning, or full datatypes of fields without an external specification).

Protocol Buffers were originally conceived for usage with RPC-style of interactions, internally at Google, and there is a specific protocol (gRPC) designed for high-performance RPC interactions; nevertheless, they can also be used to model RESTful APIs.

##### 5.5.5.4.2 Evaluation

The main characteristic of this alternative is its efficiency and higher performance.

The main drawback is that the language is maintained and evolved by Google, and it is bound to a number of tools (compilers, code generators, runtimes…) also developed and maintained mainly by Google, so it is not a system fully specified by an SDO. Therefore, this option is not considered further.

#### 5.5.5.5 Solution 4 – JSON Content Rules

##### 5.5.5.5.1 Description

IETF draft-newton-json-content-rules [14] is used by 3GPP CT3 in several specifications (3GPP TS 29.155 [37], 3GPP TS 29.250 [38], 3GPP TS 29.251 [39]). An expired version of this draft has been a de-facto standard in the industry for several years. IETF work resumed a while ago with new versions of the draft. The draft provides an IDL for JSON bodies in a relatively simple format.

##### 5.5.5.5.2 Evaluation

The main characteristic of this alternative is its simplicity. As the draft has seen some usage in the industry for several years, tooling support is available. However, the industry seems to have moved towards the more powerful OPenAPI Swagger.

#### 5.5.5.6 Solution 5 – JSON Schema

##### 5.5.5.6.1 Description

IETF draft-wright-json-schema [41] and IETF draft-wright-json-schema-validation [42] are not directly referenced in 3GPP specs, but are used by the "OpenAPI 3.0.0 Specification" [36] (see below). The draft provides an IDL for JSON bodies in a relatively simple format.

##### 5.5.5.6.2 Evaluation

The main characteristic of this alternative is its simplicity. As the draft has seen some usage in the industry for several years, tooling support is available. However, the industry seems to have moved towards the more powerful OpenAPI Swagger.

#### 5.5.5.7 Solution 6 – CBOR IDL

##### 5.5.5.7.1 Description

IETF draft-ietf-cbor-cddl [43] is not used by 3GPP so far. The draft provides an IDL for CBOR bodies.

##### 5.5.5.7.2 Evaluation

For CBOR as serialization language, this draft is typically used as IDL. Only limited tooling is currently available and the draft seems not yet widely used.

#### 5.5.5.8 Comparison of IDLs

Table 5.5.5.8-1: Comparison of IDLs.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | YANG (see IETF RFC 6020 [31], IETF RFC 6991 [32], IETF RFC 7950 [33], IETF RFC 7951 [34], and  IETF draft-ietf-core-yang-cbor [44]) | OpenAPI 3.0.0 Specification [36] | IETF draft-newton-json-content-rules [14] | IETF draft-wright-json-schema [41] and IETF draft-wright-json-schema-validation [42] | IETF draft-ietf-cbor-cddl [43] |
| Supported MIME Formats | JSON, XML, CBOR | JSON, XML | JSON | JSON | CBOR |
| Supported Primitive Data types | Boolean int8, int16, int32, int64, uint8, uint16, uint32, and uint64, optional with range decimal64, optional with range string, optional with length and/or pattern enumeration bits  binary | boolean  Integer with optional int32 or int64 format and/or range  Number with optional float or double format and/or range string with optional byte, binary, date, date-time or password format,  enum | Boolean, integer, integer numbers in a range, float, double, floating point numbers in a range, strings, URI (optionally including URI scheme) regular expressions, Fixed string values (e.g. allowing to define enumerations via groups) | boolean  Integer with optional int32 or int64 format and/or range  Number with optional float or double format and/or range string with optional byte, binary, date, date-time or password format,  enum | Boolean, int, uint. nint float, float16, float32, float64 bytes text choices (allows to describe enumerations), regular expressions |
| Definition of own types supported | yes | yes | yes, via named rules | yes | yes |
| Including external definitions via URI supported | yes | yes | yes | yes | no |
| Support for transport protocol | IETF RFC 8040 [35] defines an HTTP-based protocol that provides a RESTful programmatic interface for accessing data defined in YANG. In addition, RPC-based interactions are also mapped to HTTP-request/response transactions in a standard way. | Extensive HTTP support well aligned with RESTful style: Allows to define HTTP methods applicable to data structures, including parameters and response codes. | no | no | no |
| Stability of reference | RFCs | Webpage by OpenApi Specification, also including reference to outdated version of two individual IETF drafts.  However widely used in the OpenSource community and thus relatively stable. | Individual IETF draft | Individual IETF draft | WG IETF draft |
| Availability of tooling | Tools listed at <http://www.yang-central.org/twiki/bin/view/Main/YangTools> | Tools available at https://swagger.io/ | Some tools available e.g. at http://codalogic.github.io/jcr/ | Tools available at http://json-schema.org/implementations.html | Little tooling at http://cbor.io/tools.html |
| Forward compatibility | It is possible to define optional elements as part of the data definition, via the "mandatory = true/false" statement. | Yes; By default, additional properties within an Object are ignored, This can be controlled via the "additionalProperties" keyword. | Yes: Additional properties within an Object are ignored | Yes; By default, additional properties within an Object are ignored, This can be controlled via the "additionalProperties" keyword. | Yes: "Structs" can be extended with arbitrary key value pairs if a key value pair with wildcarded definition is included in their definition. How the receiver would handle such extensions is nor directly specified. |
| Other aspects | Originally designed for Network Management, not as a general-purpose framework.  Steeper learning curve compared with other simpler approaches. | De-facto industry standard (widest acceptance in industry, at this moment).  Simpler to use than other more formal alternatives.  Powerful enough to address expected needs in 3GPP specifications. | Simplest alternative considered | Simple | Little tooling available. |

#### 5.5.5.9 Conclusion

Given the widest industry acceptance for design of RESTful APIs, and the availability of a big ecosystem of tools and community support, it is recommended to use OpenAPI Specification, version 3.0.0, as the IDL for usage in 5GC.

It is recommended that the definition of each interface is done by including a normative annex, containing the OpenAPI specification file, in each Technical Specification in 5GC, similar to how it has been done is previous TS's in 3GPP (e.g. ASN.1 in 3GPP TS 29.002 [45], XML Schema in 3GPP TS 29.328 [46], Swagger in 3GPP TS 29.116 [40], etc.).

It is also expected that the API/protocol specification will include not only a formal OpenAPI specification file, but also textual and/or tabular format in the main body of the specification describing application-level detailed description handling of parameters (Information Elements) and their mapping to actual protocol structures.

### 5.5.6 Evaluation of candidate protocols for service based interfaces

Table 5.5.6-1 provides a comparison of different candidate protocols based on the requirements and additional evaluation criteria in subclauses 4.1.1 and 4.1.2, respectively. The colours of the cells provide an evaluation how well the criteria are met (Dark green: Criterion well met. Light green: Criterion mostly met. White: Criterion partially met or no substantial differences between candidate protocols. Orange: Criterion not met.)

Table 5.5.6-1: Comparison of candidate protocols.

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement/ Evaluation Criterion | TCP/TLS/HTTP2/JSON  (see IETF RFC 793 [5], IETF RFC 5246 [6], IETF RFC 7540 [7], IETF RFC 7159 [8] and IETF draft-newton-json-content-rules [14]) | UDP/QUIC/HTTP2/JSON  (see IETF RFC 768[9], IETF draft-ietf-quic-transport [10], IETF draft-ietf-quic-tls [11], IETF draft-ietf-quic-http [12], IETF draft-ietf-quic-recovery [13], IETF RFC 5246 [6], IETF RFC 7540 [7], IETF RFC 7159 [8] and IETF draft-newton-json-content-rules [14]) | SCTP/Diameter  (see IETF RFC 4960 [15], 3GPP TS 33.210 [16] and IETF RFC 6733[17]) |
| R1. Support of bidirectional communication | Service communication is unidirectional, i.e. fully bidirectional communication requires 2 client-server pairs - 1 per direction. | Service communication is unidirectional, i.e. fully bidirectional communication requires 2 client-server pairs - 1 per direction. | Diameter support Request-Answer command pairs in both directions. |
| R2. Support of reliable communication | TCP supports packet retransmission for a reliable communication. Failover to alternate paths can be supported by setting up additional TCP connections. | QUIC supports packet retransmission for a reliable communication. Failover to alternate paths can be supported by using additional QUIC connections. | SCTP supports packet retransmission and failover to alternate paths for a reliable communication. |
| R3. Forward compatibility and ease of upgrade | HTTP and JSON payload support versioning of service. New IEs added to JSON schema will be ignored. 3GPP defined supported feature mechanism has already been added also to some HTTP/JSON interfaces. | HTTP and JSON payload support versioning of service. New IEs added to JSON schema will be ignored. 3GPP defined supported feature mechanism has already been added also to some HTTP/JSON interfaces. | Diameter allows to control whether unknown AVPs will be ignored. 3GPP defined supported feature mechanism is well understood and has been proven to work well. |
| R4. Low Response Time | Radical throughput reduction by TCP in overload and TCP head-of-line blocking are potential issues.  See also A1.  TCP is known to work also network conditions with long round-trip times and adjust the retransmission timer accordingly. | UDP based transport avoids head of-line blocking. QUIC support multiple streams.  See also A1.  Avoiding head of line blocking also offers benefits when large jitter and round.trip.times are encountered. | Performance proven to be appropriate for EPC.  See also A1. |
| R5. Scalability | Potentially limited by high number of TCP connections, but HTTP2 streams allows a reuse of TCP connections between service instances. | UDP based  QUIC scales to very high number of transport connections (64-bit identifier) | SCTP associations between Diameter peers can be used for many Diameter sessions.  (3GPP extended Diameter Agent for dynamic UE session information discovery may impact scalability, but this is considered an architectural issue as similar solutions would be required should other protocols be selected) |
| R6. Ease and speed of deployment of network functions and services | If client authentication requires static configuration is ffs. Otherwise dynamic endpoint discovery and connection establishment is supported. | If client authentication requires static configuration is ffs. Otherwise dynamic endpoint discovery and connection establishment is supported. | How well secondary SCTP paths can be supported in dynamic manner (e.g. via DNS) is ffs. Should static configuration be required, Diameter Agents can help. |
| R7. Time of Availability of used standards | Already available. | Planned completion in November 2018 (according to IETF QUIC working group milestones) | Already available. |
| A1. Resource-efficiency | Text encoding of HTTP and JSON brings small processing overhead and increases message size.  (But only a small number of HTTP headers will be needed and HTTP2 provides header compression. HTTP2 also supports binary encoding at the HTTP layer, application still provides a text encoded payload) | Text encoding of HTTP and JSON brings small processing overhead and increases message size.  (But only a small number of HTTP headers will be needed and HTTP2 provides header compression. HTTP2 also supports binary encoding at the HTTP layer, application still provides a text encoded payload) | Binary encoding at the application layer, but message size increase due to AVP header overhead. |
| A2. Reusability of existing 3GPP implementations | Many libraries to choose from for HTTP/JSON layer. But existing application code based on Diameter will require large adaptations. Also, need to implement HTTP equivalent of Diameter Agent with 3GPP extensions. | Many libraries to choose from for HTTP/JSON layer, but QUIC support not yet so widespread. Existing application code based on Diameter will require large adaptations. Also, need to implement HTTP equivalent of Diameter Agent with 3GPP extensions. | Diameter is widely used in EPC  (roaming and non-roaming interfaces |
| A3. Minimize number of protocols in network | Already some limited usage within operators´ networks and for external interfaces at the SCEF (with earlier HTTP versions). HTTP/JSON could be used both for external and internal interfaces.  Legacy interfaces in EPC use different protocols. | No standardised usage of QUIC within operators´ networks up to now.  However already some limited usage of HTTP/JSON (with earlier HTTP versions) within operators´ networks and for external interfaces at the SCEF. HTTP/JSON could be used both for external and internal interfaces. | Already widespread usage in and between operator´s networks.  Diameter not supported on external interfaces. |
| A4. Congestion, load and overload control | HTTP/2: multiple streams, each with priority (weight) and dependency (on another streams)  Only limited possibilities to indicate overload via HTTP errors, but no load feedback.  TCP provides end-to-end congestion control, but with radical throughput reduction. | HTTP/2: multiple streams, each with priority (weight) and dependency (on another streams)  Only limited possibilities to indicate overload via HTTP errors, but no load feedback.  QUIC provides a mechanism for loss detection and overload control, but performance is ffs. | Congestion control supported by SCTP  Application-Level Load/Overload Control supported by Diameter. |
| A5. Support of Security | TLS for transport level.  Support for application-level authentication and authorization via HTTP header. | TLS for transport level.  Support for application-level authentication and authorization via HTTP header. | IPsec for transport level (see 3GPP TS 33.210 [16]). |
| A6. Ease of troubleshooting and Monitoring | Many tools exist to trace/monitor HTTP REST APIs  Distributed logging.  If TLS end-to-end encryption is used, this renders centralized logging at intermediates impossible.  An HTTP response follows the same path as its request as it is sent on the same TCP connection. | Many tools exist to trace/monitor HTTP REST APIs, but no widespread support for QUIC so far.  Distributed logging.  QUIC requires end-to-end encryption that would render centralized logging at intermediates impossible.  An HTTP response follows the same path as its request as it is sent on the same QUIC connection. | Operators likely already have tools for Diameter.  Centralized logging by Diameter Agent or Distributed logging.  Binary decoding required for troubleshooting.  A Diameter answer follows the same path as its command. |
| A7. Ease of use of 3GPP services from operator owned application functions | Largest user community for Web Services. Already supported by some operator owned application functions (with earlier HTTP versions) | Large user community for HTTP/JSON Web Services, but limited experience for QUIC. | Mainly 3GPP user community, but already supported by some operator owned application functions. (P-CSCF acting as AF. GCS AS, SCS) |
| A8. Support of failover | Supported by HTTP error codes and HTTP proxies. | Supported by HTTP error codes and HTTP proxies. | Supported by error codes and Diameter Agent. |
| A9. Support of network entity selection based on UE context information (e.g. based on dynamic UE session information | Supported, if new HTTP proxy extensions required is FFS. | Supported, if new HTTP proxy extensions likely required is FFS. | Supported by Diameter Agent with existing 3GPP extensions. |
| A10. Ease of traversal of carrier-grade ALG/NAT/firewall | Need to configure operator-grade firewalls to pass TCP/TLS/HTTP. For bidirectional communication. configuration for two connection may be required, but security gateways can reduce the number of required connections (see 3GPP TS 33.210 [16]). | Need to configure operator-grade firewalls to pass UDP/QUIC. For bidirectional communication. configuration for two connection may be required, but security gateways can reduce the number of required connections (see 3GPP TS 33.210 [16]). | Need to configure operator-grade firewalls to pass IPSec, but security gateways reduce the number of required connections (see 3GPP TS 33.210 [16]). |
| A11. Impacts to GSMA GRX/IPX | No HTTP support so far. (e.g. GSMA uses home-routed APN for HTTP-based Ut interface). | No HTTP/QUIC support so far. (e.g. GSMA uses home-routed APN for HTTP-based Ut interface). | Existing Diameter support. |
| A12. Open and public Source/Standardization body | yes | yes | yes |
| A13. Protocol enables stateless operation | HTTP is a stateless protocol where each request-response message pair is independent. | HTTP is a stateless protocol where each request-response message pair is independent. | Diameter supports stateless operations with the concept of implicit session termination. An implicitly terminated session is one for which the server does not maintain state information. |
| A14. Routing support and related mechanisms. | HTTP requests are routed based on the request URI. The request URI can point e.g. to a host or a resource (only the later applies for RESTful protocol design)  HTTP supports the use of proxies in the path. | HTTP requests are routed based on the request URI. The request URI can point e.g. to a host or a resource (only the later applies for RESTful protocol design)  HTTP supports the use of proxies in the path. | Diameter supports both routeing based on realm and service and routeing based on a Diameter host Id.  Diameter supports the use of proxies (DA) in the path. |
| A15. Error detection and error reporting capabilities | Many HTTP error codes are defined and own error codes can be defined as extensions by 3GPP (IANA registration requires expert review)  Well defined unambiguous transported data enable an unambiguous interpretation of transported data (see A17) | Many HTTP error codes are defined and own error codes can be defined as extensions by 3GPP (IANA registration requires expert review)  Well defined unambiguous transported data enable an unambiguous interpretation of transported data (see A17) | Many Diameter error codes are defined and own error codes can be defined as extensions by 3GPP.  Well defined unambiguous transported data enable an unambiguous interpretation of transported data (see A17) |
| A.16 Sessions multiplexing over a single transport connection | HTTP/2 supports multiplexing multiple parallel requests in separate streams in a non-blocking fashion at HTTP level) over the same TCP connection.  TCP provides order-of-transmission delivery of data, which can result in HOL blocking within a TCP connection if TCP segments get lost. | QUIC/HTTP/2 supports multiplexing multiple parallel requests in separate streams in a non-blocking fashion over the same UDP connection.  HTTP/2 streams are mapped one to one into QUIC streams and an HTTP request/response consumes a pair of streams ensuring a reliable and in order delivery of request/response without HOL blocking issue. | Diameter supports reuse of SCTP connections for multiple Diameter sessions.  SCTP supports ordered and unordered delivery of data. Head-of-line blocking may occur within an STCP stream using ordered data delivery if SCTP segments get lost. HOL blocking may be mitigated if both Diameter peers support a large number of streams. |
| A17. Well-defined schema and unambiguous interpretation of transported data | IETF RFC 7159 [8] and IETF draft-newton-json-content-rules [14]) provide the framework of schema that enable the unambiguous interpretation of transported data | IETF RFC 7159 [8] and IETF draft-newton-json-content-rules [14]) provide the framework of schema that enable the unambiguous interpretation of transported data | Diameter AVPs allow an encoding that enables the unambiguous interpretation of transported data. |

## 5.6 AMF Access and Mobility Policy

### 5.6.1 General

The PCF may provide AMF Access and Mobility Policy to the AMF via the Npcf\_AMPolicyControl service interface.

The AMF Access and Mobility Policy delivered by the PCF shall consist of:

- Service Area Restrictions; and/or

- RAT Frequency Selection Priority (RFSP Index).

The PCF provides authorized Service Area Restrictions and/or RFSP index to the AMF in the corresponding UE registration. Also, at any time during the life time of the UE registration, the PCF may re-evaluate the applicable Service Area Restrictions and/or RFSP Index due to different events, e.g. change of RAT or change of the serving AMF due to mobility and provide the update Service Area Restrictions and/or RFSP Index to the AMF.

NOTE: The actual enforcement of Service Area Restrictions is executed in the UE, when the UE is in CM-IDLE state or in CM-CONNECTED state when in RRC Inactive, and in the RAN/AMF when the UE is in CM-CONNECTED state, while the enforcement of RAT/Frequency Selection Priority is always performed in the RAN.

### 5.6.2 Service Area Restriction

The Service Area Restriction information consists of:

- either:

- a list of allowed Tracking Area Identities (TAIs); and/or

- the maximum number (that can be unlimited) of allowed TAs within a list of allowed TAs defined in the AMF (and not explicitly provided by the PCF);

- or:

- a list of not allowed Tracking Area Identities (TAIs).

The PCF may determine the Service Area Restriction based on service areas received from the AMF and operator policies. Operator defined policies may take into consideration e.g. UE location, time of day, etc.

When there is no Service Area Restriction to apply, i.e. when the result of Service Area Restriction policy evaluation by the PCF shall determine that the UE is allowed to get service without any restriction in all the Tracking Areas of the PLMN, no Service Area Restriction information shall be included in the service operations Npcf\_AMPolicyControl\_Get response / Npcf\_AMPolicyControl\_UpdateNotify request.

### 5.6.3 RFSP Index

The RFSP Index is an index referring to a UE information used locally by the Access Network in order to apply specific radio resource management strategies.

The PCF may determine the RFSP Index based on an RFSP Index received from the AMF and operator policies that take into consideration e.g. accumulated usage, load level information per network slice instance etc.

## 5.7 Session Management Policy Rules

### 5.7.1 PCC rule in 5GC

#### 5.7.1.1 General

To enable the enforcement in the 5GC of the policy and charging control of a service data flow, the 5GC system shall provide 5G Policy and Charging Control information from the PCF to the SMF.

Two different types of PCC rules exist:

- Dynamic PCC rules: dynamically provisioned by the PCF to the SMF. These PCC rules may be either predefined or dynamically generated in the PCF. Dynamic PCC rules can be installed, modified and removed at any time.

- Predefined PCC rules: preconfigured in the SMF/UPF. Predefined PCC rules can be activated or deactivated by the PCF at any time. Predefined PCC rules may be grouped allowing the PCF to dynamically activate a set of PCC rules.

NOTE 1: The operator can define a predefined PCC rule, to be activated by the SMF. Such a predefined rule is not explicitly known in the PCF.

The purpose of the PCC rule in 5G is to:

- detect a packet belonging to a service data flow;

- identify the service to which the service data flow contributes to;

- provide applicable charging parameters for a service data flow; and

- provide policy control for a service data flow.

The PCC rule information elements in 5GC, as defined in 3GPP TS 23.503 [66], are shown in table 5.7.1.1.-1.

Table 5.7.1.1-1: PCC rule information in 5GC

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Purpose | Information name | Description | Category | PCF permitted to modify dynamically provided information |
| **Rule Identification**  This part uniquely identifies the PCC rule. | Rule identifier | Uniquely identifies the PCC rule, within a PDU session.  It is used between the PCF and the SMF for referencing a PCC rule. | Mandatory | No |
| **Service data flow detection**  This part defines the method for detecting packets belonging to a service data flow. | Service data flow template | For IP PDU traffic: Either a list of service data flow filters or an application identifier that references the corresponding application detection filter for the detection of the service data flow. | Mandatory (NOTE 3) | Conditional (NOTE 4) |
| For Ethernet PDU traffic: Combination of traffic patterns of the Ethernet PDU traffic (packet filters for Ethernet PDU traffic added). |  |
| Precedence | Determines the order, in which the service data flow templates are applied at service data flow detection, enforcement and charging. | Conditional (NOTE 5) | Yes |
| Mute for notification | Defines whether application's start or stop notification is to be muted. | Conditional (NOTE 6) | No |
| **Charging**  This part defines identities and instructions for charging and accounting that is required for an access point where flow based charging is configured. | Charging key | The charging system (OCS or OFCS) uses the charging key to determine the tariff to apply to the service data flow. |  | Yes |
| Service identifier | The identity of the service or service component the service data flow in a rule relates to. |  | Yes |
| Sponsor Identifier | An identifier, provided from the AF which identifies the Sponsor, used for sponsored flows to correlate measurements from different users for accounting purposes. | Conditional (NOTE 7) | Yes |
| Application Service Provider Identifier | An identifier, provided from the AF which identifies the Application Service Provider, used for sponsored flows to correlate measurements from different users for accounting purposes. | Conditional (NOTE 7) | Yes |
| Charging method | Indicates the required charging method for the PCC rule.  Values: online, offline or neither. | Conditional (NOTE 8) | No |
| Measurement method | Indicates whether the service data flow data volume, duration, combined volume/duration or event shall be measured.  This is applicable to reporting, if the charging method is online or offline.  (NOTE 9) |  | Yes |
| Application Function Record Information | An identifier, provided from the AF, correlating the measurement for the Charging key/Service identifier values in this PCC rule with application level reports. |  | No |
| Service identifier level reporting | Indicates that separate usage reports shall be generated for this Service identifier.  Values: mandated or not required. |  | Yes |
| **Policy control**  This part defines the information the PCF shall provide to SMF for policy control for the service data flow. | 5G QoS Identifier (5QI) | Identifier for the authorized QoS parameters, as defined in 3GPP TS 23.501 [2], subclause 5.7.2 | Conditional (NOTE 1) | Yes |
| ARP | The Allocation and Retention Priority for the service data flow consisting of the priority level, the pre-emption capability and the pre-emption vulnerability. | Conditional (NOTE 10) | Yes |
| QoS Notification Control (QNC) | Indicates a request for notification to RAN for the SDF when the QoS targets for a GBR 5QI cannot be fulfilled for a QoS flow during the lifetime of the QoS flow. The QNC is the Notification Control 5G QoS parameter defined in 3GPP TS 23.501 [2], subclause 5.7.2. |  | Yes |
| Bind to QoS flow of the default QoS rule | Indicates that the dynamic PCC rule shall always have its binding with the QoS flow of the default QoS rule. | Conditional (NOTE 2) | Yes |
| Gate status | The gate status indicates whether the service data flow, detected by the service data flow template, may pass (Gate is open) or shall be discarded (Gate is closed). |  | Yes |
| Reflective QoS Control | Indicates to apply reflective QoS for the service data flow. Reflective QoS is defined in 3GPP TS 23.501 [2], subclause 5.7.5. |  | Yes |
| UL-maximum bitrate | The uplink maximum bitrate authorized for the service data flow. |  | Yes |
| DL-maximum bitrate | The downlink maximum bitrate authorized for the service data flow. |  | Yes |
| UL-guaranteed bitrate | The uplink guaranteed bitrate authorized for the service data flow. |  | Yes |
| DL-guaranteed bitrate | The downlink guaranteed bitrate authorized for the service data flow. |  | Yes |
| UL sharing indication | Indicates resource sharing in uplink direction with service data flows having the same value in their PCC rule. |  | No |
| DL sharing indication | Indicates resource sharing in downlink direction with service data flows having the same value in their PCC rule. |  | No |
| Redirect | Redirect state of the service data flow (enabled/disabled). | Conditional (NOTE 6) | Yes |
| Redirect Destination | Controlled Address to which the service data flow is redirected when redirect is enabled. | Conditional  (NOTE 11) | Yes |
| **Access Network Information Reporting**  This part describes access network information to be reported for the PCC rule when the corresponding QoS flow is established, modified or terminated. | User Location Report | The serving cell of the UE is to be reported. When the corresponding QoS flow is deactivated, and if available, information on when the UE was last known to be in that location is also to be reported. |  | Yes |
| UE Timezone Report | The time zone of the UE is to be reported. |  | Yes |
| **Usage Monitoring Control**  This part describes identities required for Usage Monitoring Control. | Monitoring key | The PCF uses the monitoring key to group services that share a common allowed usage. |  | Yes |
| Indication of exclusion from session level monitoring | Indicates that the service data flow shall be excluded from PDU session usage monitoring. |  | Yes |
| **Traffic Steering Enforcement Control**  This part describes identities required for Traffic Steering Enforcement Control. | Traffic Steering Policy Identifier | This part describes identities required for Traffic Steering Enforcement Control. |  | Yes |
| Data Network Access Identifier | Identifier of the target Data Network Access. It is defined in 3GPP TS 23.501 [2], subclause 5.6.7. |  | Yes |
| Data Network Access Change report | Indicates whether a notification in case of change of DNAI is needed. It is defined in 3GPP TS 23.501 [2], subclause 5.6.7 |  | Yes |
| NOTE 1: The 5G QoS Identifier is mandatory for QoS flow binding in the SMF, unless the "Bind to QoS flow of the default QoS rule" is included and set to the value "binding to default QoS rule".  NOTE 2: The presence of this attribute causes the 5QI/ARP/QNC of the rule to be ignored.  NOTE 3: Either service data flow filter(s) or application identifier shall be defined per each rule.  NOTE 4: YES, in case the service data flow template consists of a set of service data flow filters. NO in case the service data flow template consists of an application identifier.  NOTE 5: The Precedence is mandatory for PCC rules with SDF template containing SDF filter(s). For dynamic PCC rules with SDF template containing an application identifier, the precedence is either preconfigured in SMF or provided in the PCC rule from PCF.  NOTE 6: Optional and applicable only if application identifier exists within the rule.  NOTE 7: Applicable to sponsored data connectivity.  NOTE 8: Mandatory if there is no default charging method for the PDU session.  NOTE 9: Event based charging is only applicable to predefined PCC rules and PCC rules used for application detection filter (i.e. with an application identifier).  NOTE 10: Mandatory when policy control on SDF level applies.  NOTE 11: If Redirect is enabled. | | | | |

NOTE 2: The PCC parameters related to NBIFOM, 3GPP PS Data Off, SRVCC and Location change (Serving cell) are not supported, as specified in 3GPP TS 23.503 [66].

Editor's note: It is FFS how it is indicated in the PCC rule the AF subscription to SMF notifications.

Editor's note: Whether to use the access agnostic terminology for the PCC rule is FFS.

Editor's note: It is FFS whether the various constructs (QoS, Charging, Traffic Steering) within the PCC rule will become references to separate rules that are applied/associated with the packet filters, similar to the design on the Sx interface.

The *Service data flow template* may comprise any number of *Service data flow filters* or an *application identifier* for IP PDU traffic as is defined in 3GPP TS 23.503 [66]. Additionally, it may also comprise any combination of traffic patterns of the Ethernet PDU traffic as defined in subclause 5.7.6.3 of 3GPP TS 23.501 [2].

The *5G QoS Identifier*, 5QI, is a scalar that is used as reference to a specific QoS forwarding behaviour (e.g. packet loss rate, packet delay budget) to be provided to a service data flow. It can be a standardized, non-standardized or pre-configured value.

The *Bind to QoS flow of the default QoS rule* indicates that the SDF shall be bound to the default QoS flow of the default QoS rule. The presence of the "Bind to QoS flow of the default QoS rule" parameter attribute causes the 5QI/ARP/QNC of the rule to be ignored by the SMF during the QoS flow binding.

The *QoS Notification Control*, QNC indicates a request for a notification to the access network (RAN) for the SDF when the QoS targets for a GBR 5QI cannot be fulfilled for a QoS flow during the lifetime of the QoS flow. If it is set and QoS targets cannot be fulfilled, RAN sends a notification towards the SMF, which notifies the PCF or other interested receivers. It is indicated by the *QoS Notification Control (QNC)* information element, which is equivalent to the Notification Control 5G QoS parameter described in 3GPP TS 23.501 [2] subclause 5.7.2.

The *Reflective QoS Control* indicates a request to apply reflective QoS for the SDF. The *Reflective QoS Control* is used to control the RQI marking in the DL packets of the service data flow and may trigger the sending of the RQA parameter for the QoS flow the service data flow is bound to. The Reflective QoS is defined in 3GPP TS 23.501 [2] subclause 5.7.5.

NOTE 3: While the UE applies a standardized value for the precedence of all UE derived QoS rules, PCC rules require different precedence values and PCF configuration has to ensure that there is a large enough value range for the precedence of PCC rules corresponding to UE derived QoS rules. To avoid that the precedence of network provided QoS rules need to be changed when Reflective QoS is activated and filters are overlapping, the PCF will take the standardized value for the precedence of UE derived QoS rules into account when setting the precedence value of PCC rules subject to Reflective QoS.

The Target *Data Network Identifier (DNAI)* is a reference to the DNAI the SMF needs to consider for the UPF selection/reselection.

The *Data Network Access Change report* indicates a request for a notification about a change of DNAI for the UPF serving the UE. The subscription can be for an early notification and/or a late notification.

#### 5.7.1.2 PCC rule operations

For dynamic PCC rules, the following operations are available:

- installation: to provision a PCC rule that has not been already provisioned;

- modification: to modify a PCC rule already installed; and

- removal: to remove a PCC rule already installed.

For predefined PCC rules, the following operations are available:

- activation: to activate the PCC rule; and

- deactivation: to deactivate the PCC rule.

The PCF provides PCC rules to the SMF using the Npcf\_SMPolicyControl service. The PCF shall identify each PCC rule with a Rule identifier. The Rule identifier of the PCC rule shall be included for each PCC rule provided in the Npcf\_SMPolicyControl service operations.

Upon reception of the Npcf\_SMPolicyControl\_Get service operation from the SMF the PCF shall decide what PCC rules apply for that PDU session. The PCF shall include the applicable PCC rules in the response of the Npcf\_SMPolicyControl\_Get service operation.

The PCF may use:

- a response to the Npcf\_SMPolicyControl\_Get service operation to:

a) activate a preconfigured PCC rule; and

b) install a dynamic PCC rule; and

- the Npcf\_SMPolicyControl\_UpdateNotify service operation to:

a) activate, modify, or deactivate a preconfigured PCC rule; and

b) install, modify, or remove a dynamic PCC rule.

NOTE 1: For the HTTP methods and resources to realize the Npcf\_SMPolicyControl service operations see subclause 5.4.3.3.

After the PCC rule installation/activation, the PCF may, at any time, remove/deactivate an active PCC rule.

At the PDU session termination when the SMF invokes the Npcf\_SMPolicyControl\_Delete service operation to the PCF, the SMF removes/inactivates all PCC rules associated to that PDU session.

An active PCC rule means that:

- the service data flow template shall be used for service data flow detection;

- the service data flow template shall be used for mapping of downlink packets to the QoS flow determined by the QoS flow binding;

- the service data flow template shall be used for service data flow detection of uplink packets on the PDU session;

- usage data for the service data flow shall be recorded;

- policies associated with the PCC rule, if any, shall be invoked;

- for service data flow detection with an application detection filter, the start or the stop of the application traffic is reported to the PCF, if applicable and requested by the PCF. In that case, the notification for start may include service data flow filters, (if possible to provide) and the application instance identifier associated with the service data flow filters.

A predefined PCC rule is known at least, within the scope of one PDU session.

NOTE 2: The same predefined PCC rule can be activated for multiple QoS flows in multiple PDU sessions.

A predefined PCC rule is bound to one and only one QoS flow per PDU session. For a predefined PCC rule whose service data flow cannot be fully reflected for the uplink direction in terms of traffic mapping information sent to the UE, the SMF may request the UPF to apply the uplink service data flow detection at additional QoS flows with non-GBR 5QI of the same PDU session. The deactivation of such a predefined PCC rule ceases its service data flow detection for the whole PDU session.

When the PCF receives the Nsmf\_EventExposure\_Notify service operation indicating that the QoS flow is terminated, all active PCC rules on that QoS flow are removed/deactivated without sending explicit instruction i.e. the PCF does not need to invoke the Npcf\_SMPolicyControl\_UpdateNotify service operation to the SMF.

PCC rule operations can be also performed in a deferred mode. A PCC rule may have either a single deferred activation time, or a single deferred deactivation time or both. An inactive PCC rule, that has not been activated yet, is still considered to be installed/activated, and may be removed/inactivated by the PCF.

### 5.7.2 5G PDU session related policy information

The PCF may provide 5G PDU session related policy information to the SMF.

The IP-CAN session related policy information defined in 3GPP TS 23.203 [4] is re-used in 5G with the following differences:

- Attributes relate to the PDU session instead of the IP-CAN session.

- Attribute Default NBIFOM access is not applicable to 5G.

- Additional information needed compared to the 3GPP TS 23.203 [4] IP‑CAN session related policy information is described in the table and text below.

Table 5.7.2-1: Additional information needed compared to the 3GPP TS 23.203 [4] IP‑CAN session related policy information

| Attribute | Description | PCF permitted to modify for dynamically provided information | Category | Scope |
| --- | --- | --- | --- | --- |
| PRA Identifier(s) | Defines the Presence Reporting Area(s) to monitor for the UE with respect to entering/leaving | Yes |  | PDU session |
| List(s) of Presence Reporting Area elements | Defines the elements of the Presence Reporting Area(s) | Yes |  | PDU session |
| IP Index | Provided to SMF to assist in determining the IP Address allocation method (e.g. which IP pool to assign from) when a PDU session requires an IP address as defined in 3GPP TS 23.501 [2], subclause 5.8.1.1. | No | Optional | PDU Session |
| Non-standardized QoS Characteristics  (NOTE 5) | Defines a 5QI value (from the non-standardized value range) and the associated 5G QoS characteristics as defined in 3GPP TS 23.501 [2] subclause 5.7.3. | No | Optional | PDU Session |
| Authorized Session-AMBR  (NOTE 3, NOTE 4) | Defines the Aggregate Maximum Bit Rate for the Non-GBR QoS flows of the PDU session. | Yes | Optional | PDU Session |
| Authorized default 5QI/ARP  (NOTE 4) | Defines the default 5QI and ARP of the QoS flow. | Yes | Optional | PDU Session |
| Time Condition  (NOTE 1) | Defines the time at which the corresponding Subsequent Authorized Session-AMBR or Subsequent Authorized default 5QI/ARP shall be applied. | No  (NOTE 2) | Optional | PDU Session |
| Subsequent Authorized Session-AMBR  (NOTE 1, NOTE 3) | Defines the Aggregate Maximum Bit Rate for the Non-GBR QoS flows of the PDU session when the Time Condition is reached. | No  (NOTE 2) | Optional | PDU Session |
| Subsequent Authorized default 5QI/ARP  (NOTE 1) | Defines the default 5QI and ARP of the default QoS flow when the Time Condition is reached. | No  (NOTE 2) | Optional | PDU Session |
| NOTE 1: The Time Condition and Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP are used together. The PCF may provide up to four instances of them. When multiple instances are provided, the values of the associated Time Condition have to be different.  NOTE 2: The PCF may replace all instances that have been provided previously with a new instruction. A previously provided Time Condition and Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP pair cannot be individually modified.  NOTE 3: The Authorized Session-AMBR and the Subsequent Authorized Session-AMBR may be provided together with a list of RAT types.  NOTE 4: There is always an unconditional value for the Authorized Session-AMBR and Authorized default 5QI/ARP available at the SMF. The initial value is received as Subscribed Session-AMBR/Subscribed default 5QI/ARP, and the PCF can overwrite it with these parameters.  NOTE 5: Multiple Non-standardized QoS Characteristics can be provided by the PCF. Operator configuration is assumed to ensure that the non-standardized 5QI to QoS characteristic relation is unique within the PLMN. | | | | |

Editor's note: Whether PRA can be reused as specified in 3GPP TS 23.203 or if there is any PRA equivalent concept in 5G is FFS.

The *Authorized Session-AMBR* defines the UL/DL Aggregate Maximum Bit Rate for the Non-GBR QoS flows of the PDU session, which is enforced in the UPF as defined in subclause 5.9.7. PCF may provide the *Authorized Session-AMBR* in every interaction with the SMF. When SMF receives it from the PDU session policy, it is provided to the UPF over N4 interface for the enforcement.

The *Authorized default 5QI/ARP* defines the default 5QI and ARP of the QoS flow, i.e. the QoS flow corresponding to the default QoS rule as is described in subclause 5.7.2 of 3GPP TS 23.501 [2]. The PCF may provide the authorized default 5QI/ARP in every interaction with the SMF. The SMF shall apply the authorized default 5QI/ARP for the PDU session, including the necessary QoS flow binding actions.

The *Time Condition* and *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* are used together and up to four instances with different values of the *Time Condition* parameter may be provided by the PCF. *Time Condition* indicates that the associated *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* is only applied when the time defined by this attribute is met. When SMF receives a *Time Condition* and *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* pair, it stores it locally. When the time defined by the *Time Condition* parameter is reached, the SMF shall apply (or instruct UPF to apply) *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP*.

NOTE 1: In order to reduce the risk for signalling overload, the PCF should avoid simultaneous provisioning of the *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* for many UEs (e.g. by spreading over time).

NOTE 2: In order to provide further *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* in a timely fashion the PCF can use its own clock to issue the desired changes or use the Revalidation time limit parameter to trigger a SMF request for a policy decision.

NOTE 3: For services that depend on specific Session-AMBR and/or default 5QI/ARP (e.g. MPS session) the PCF is responsible to ensure that no *Subsequent Authorized Session-AMBR* or *Subsequent Authorized default 5QI/ARP* interfere with the service, e.g. by removing the *Subsequent Authorized Session-AMBR* or *Subsequent Authorized default 5QI/ARP* before the respective change time is reached.

### 5.7.3 Packet Filter Set

#### 5.7.3.1 General

Packet Filter Set is used in the QoS rules or SDF template to identify a QoS flow. The Packet Filter Set may contain packet filters for the DL direction, the UL direction or packet filters that are applicable to both directions.

There are two types of Packet Filter Sets (i.e. IP Packet Filter and Ethernet Packet Filter) corresponding to those PDU session types.

#### 5.7.3.2 IP Packet Filter Set

For IP PDU session type, the Packet Filter Set shall support packet filtering based on at least any combination of:

- Source/destination IP address or IPv6 prefix;

- Source / destination port number;

- Protocol ID of the protocol above IP/Next header type;

- Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask;

- Flow Label (IPv6); and

- Security parameter index.

NOTE 1: A value left unspecified in a filter matches any value of the corresponding information in a packet.

NOTE 2: An IP address or Prefix may be combined with a prefix mask.

NOTE 3: Port numbers may be specified as port ranges.

#### 5.7.3.3 Ethernet Packet Filter Set

For Ethernet PDU session type, the Packet Filter Set shall support packet filtering based on at least any combination of:

- Source/destination MAC address;

- Ethertype as defined in IEEE 802.3 [69];

- Customer-VLAN tag (C-TAG) and/or Service-VLAN tag (S-TAG) VID fields as defined in IEEE 802.1Q [70];

- Customer-VLAN tag (C-TAG) and/or Service-VLAN tag (S-TAG) PCP/DEI fields as defined in IEEE 802.1Q [70]; and

- IP Packet Filter Set, in case Ethertype indicates IPv4/IPv6 payload.

NOTE 1: The MAC address may be specified as address ranges.

NOTE 2: A value left unspecified in a filter matches any value of the corresponding information in a packet.

## 5.8 UE Policies

### 5.8.1 General

The PCF will provide UE policies to the AMF via the N15 reference point. Two types of UE policies are defined in 3GPP TS 23.501 [2]:

- UE Access Network discovery and selection policies; and

- UE Route Selection Policies (URSP).

### 5.8.2 UE Access Network discovery and selection policies

These policies are used for the UE to select non-3GPP accesses and to decide how to route traffic between the selected 3GPP and non 3GPP accesses.

Editor's note: The structure of these policies remains unspecified in stage 2.

### 5.8.3 UE Route Selection Policies (URSP)

These policies are used by the UE to determine how to route outgoing traffic.

The following information needs to be provided as part of each UE Route Selection Policy:

- Traffic Filter: Filter information for the traffic (flow information or application identifier). The traffic that matches the traffic filter of an URSP rule is referred to as the "matching traffic" for this URSP rule.

- Non-seamless Offload (more than one instance allowed, one per Non-3GPP access type, provided in priority order). It includes:

a) Traffic-Treatment: Traffic [Prohibited, Preferred, Permitted] to be offloaded to non-3GPP access outside of a PDU session.

b) Non-3GPP Access Type: Optional parameter to indicate the Non-3GPP network for which the traffic treatment applies.

- Slice info (more than one instance allowed, provided in priority order). It includes S-NSSAI information, i.e.:

a) Slice/Service Type: Indicates expected Network Slice behaviour in terms of features and services. Standardised Slice/Service types are "1" for enhanced Mobile Broadband (eMBB)", "2" for ultra- reliable low latency communications (URLLC), and "3" for massive IoT (MIoT), as specified in table 5.15.2.2-1 in 3GPP TS 23.501 [2], but non-standard Slice/Service types can also be used.

b) Slice Differentiator: Optional parameter that complements the Slice/Service type(s) to allow further differentiation for selecting a Network Slice instance from the potentially multiple Network Slice instances that all comply with the indicated Slice/Service type.

Editor's note: What info is provided by the PCF as part of this information remains unspecified in stage 2.

- Continuity Type (more than one instance allowed, provided in priority order). It indicates the required SSC mode(s) as defined in subclause 5.6.9.2 of 3GPP TS 23.501 [2] [SSC Mode 1, SSC Mode 2, SSC Mode 3] for the matching traffic.

- DNN (more than one instance allowed, provided in priority order). It includes the required DNN(s) for the matching traffic. It is used to associate the matching traffic with one or more DNNs.

- Access Type (more than one instance allowed, provided in priority order): It indicates the type of access (3GPP or non-3GPP) on which the PDU session should be established for the matching traffic. If the UE needs to establish a PDU session for the matching traffic, this indicates the type of access (3GPP or non-3GPP) on which the PDU session should be established. It may also indicate a prioritized list of accesses on which the PDU session establishment should be attempted.

Editor's note: It is FFS if the size of the UE policies to be transferred and frequency of the rules update from the PCF to the UE would require additional transport options.

Editor's note: It is FFS if part of the policies can be transferred via UDM.

## 5.9 QoS mechanisms

### 5.9.1 Overview

The PCF may provide authorized QoS to the SMF. The authorized QoS can be the default QoS, the QoS per Service Data Flow and the QoS per PDU session.

The provisioning of the authorized QoS is performed from the PCF to the SMF. The authorized QoS can refer to a policy rule or to a PDU Session.

The authorized QoS provides appropriate values for the resources to be enforced.

The authorized QoS for a policy rule is a request for allocating the corresponding resources.

### 5.9.2 Policy provisioning for authorized QoS per service data flow

The authorized QoS per service data flow shall be provisioned within the corresponding PCC rule by the PCF to the SMF. The PCF shall include the QoS parameters in the authorized QoS as follows:

- When the PCF authorizes the Non-GBR type QoS for the service data flow, the PCF shall include a standardized 5QI or preconfigured 5QI with the non-GBR value or a non-standardized 5QI and the ARP. The PCF may also include the MBR if needed and the Reflective QoS indication if applicable. For the Non-GBR QoS with standardized 5QIs or pre-configured 5QIs the PCF may not provide the ARP as part of the authorized QoS if the default ARP is authorized to the service data flow.

- When the PCF authorizes the GBR type QoS for the service data flow, the PCF shall include a standardized 5QI with GBR value, a preconfigured 5QI or a non-standardized 5QI with the 5G QoS characteristics. The PCF shall also include the ARP, the GBR and the MBR. The PCF may also include the QoS notification control if applicable.

NOTE: The PCF may provide preconfigured 5QI values only when the UE is not roaming.

### 5.9.3 Policy enforcement for authorized QoS per service data flow

Editor's note: Policy enforcement for authorized Qos per service data flow is FFS.

The SMF shall perform a QoS flow binding based on the QoS information provided for the service data flow.

The SMF shall assign the QFI and shall derive, if applicable, the QoS flow information required towards the Access Network and the QoS rule required towards the UE.

NOTE: The 5QI, 5G QoS characteristics if applicable, ARP, MBR and GBR enforcement is performed in the UPF based on the information the SMF sends via N4 interface.

### 5.9.4 Policy provisioning of authorized QoS per PDU Session

Each PDU session of a UE is associated with a Session-AMBR. The PCF shall provision the authorized Session-AMBR for both Uplink and Downlink traffic as part of the PDU session establishment procedure. The SMF may provide an updated Session-AMBR to the PCF when received from UDM and the PCF may modify the Session-AMBR for both Uplink and Downlink traffic at any time as long as there is a PDU session active for that DNN.

The Session-AMBR limits the aggregate bit rate that can be expected to be provided across all Non-GBR QoS flows for a specific PDU session for both Uplink and Downlink traffic.

NOTE: Authorized session-AMBR includes the Session Aggregate Maximum Bit Rate Uplink and/or Downlink.

Each PDU session of a UE is associated with a default QoS. The SMF may provide to the PCF the subscribed default QoS as received from the UDM and the PCF shall provision the authorized default QoS as part of the PDU session establishment procedure. The SMF may provide to the PCF an updated default QoS as provided by the UDM and the PCF may modify the default QoS at any time as long as there is a PDU session active for that DNN.

The default QoS relate to a non-GBR 5QI and includes the 5QI and ARP for the treatment of packets related to the Default QoS flow. The default 5QI shall be from the standardized value range for non-GBR 5QIs.

Editor's note: Handling of errors in the provisioning of the authorized QoS per PDU Session is FFS.

### 5.9.5 Policy enforcement for authorized QoS per PDU session

When the SMF receives an authorized Session-AMBR at PDU session establishment and also at PDU session modification, the SMF shall send the authorized Session-AMBR and/or the default QoS to:

- the UPF via the N4 reference point; and

- the RAN via the AMF.

When the SMF receives an authorized default QoS at PDU Session establishment and also at PDU Session modification, the SMF shall perform the QoS Flow binding as defined in subclause 5.18.4.

Editor's note: Handling of errors at enforcement of the authorized QoS per PDU session is FFS.

### 5.9.6 Reflective QoS

#### 5.9.6.1 General

The Reflective QoS is achieved by creating a derived QoS rule in the UE based on the received downlink traffic, and it applies for IP PDU session and Ethernet PDU session. It shall be possible to apply the Reflective QoS and the non-Reflective QoS concurrently within the same PDU session. For traffic that is subject to the Reflective QoS, the UL packet gets the same QoS marking as the reflected DL packet.

If the 3GPP UE supports Reflective QoS functionality, the UE indicates support of reflective QoS to the network (i.e. SMF) during the PDU session establishment.

#### 5.9.6.2 Provisioning of authorized Reflective QoS per service data flow

When the PCF determines that the Reflective QoS is applied to a non-GBR service data flow, the PCF shall include the related RQI in the corresponding PCC rule and provide the PCC rule to the SMF.

#### 5.9.6.3 Policy enforcement of authorized Reflective QoS per service data flow

When the PCF provides the RQI as part of a PCC rule, and if the PCC rule is the first PCC rule with the RQI bound to a QoS Flow after performing the flow binding, the SMF shall determine if the reflective QoS is applicable to the QoS Flow. If, the SMF shall provide the Reflective QoS Attribute (RQA) in the QoS Flow's QoS profile towards the 5G-RAN, which indicates that some (not necessarily all) traffic carried on this QoS flow is subject to Reflective QoS.

The SMF shall also provide RQI for this SDF as part of the SDF information over N4 interface as described in 3GPP TS 23.501 [2].

When the UPF receives this indication for an SDF, the UPF sets the RQI bit in the encapsulation header on the N3 reference point for every DL packet corresponding to the SDF together with the QFI.

When the PCF removes a PCC rule with the RQI or the PCF removes the RQI from a PCC rule, and if the PCC rule is the last PCC rule with the RQI bound to a QoS Flow, the SMF shall determines that the reflective QoS is no longer applicable to the QoS Flow. In this case, the SMF should signal the removal of the RQA from the QoS Flow QoS profile to the 5G-RAN and remove RQI in the corresponding SDF information provided to the UPF via N4 interface.

When the UPF receives this instruction for the SDF, the UPF will no longer set the RQI bit in the encapsulation header on the N3 reference point.

The UPF continues to accept the UL traffic of the SDF for the originally authorized QoS flow for an operator configurable time.

NOTE 1: This means that the detection and QoS enforcement instructions which were applied before the SMF removed the indication to use reflective QoS remain active in UL direction while the accounting of the UL traffic is done according to the new instructions.

NOTE 2: The operator configurable time has to be at least as long as the RQ Timer value to ensure that no UL packet would be dropped until the UE derived QoS rule is deleted by the UE.

#### 5.9.6.4 Provisioning and Enforcement of authorized Reflective QoS information per PDU session

The Reflective QoS information for the PDU session is provided to the UE as part of the PDU session establishment procedure.

In this case, the Reflective QoS information provided to the UE by the SMF, shall include the RQ Timer indicating the time Reflective QoS applies for all the derived QoS rules related to the non-GBR PCC rules for which Reflective QoS applies via the User Plane for that PDU session.

Editor's note: Whether the PCF provides the Reflective QoS information to the SMF is FFS.

If the Reflective QoS information is provided to the SMF, the SMF shall provide this information following the procedures described in the corresponding NAS Technical Specification.

Editor's note: The identity of the corresponding NAS Technical Specification is FFS.

### 5.9.7 QoS Information

#### 5.9.7.1 5G QoS Identifier (5QI)

A 5QI is a scalar that is used as a reference to 5G QoS characteristics i.e. access node-specific parameters that control QoS forwarding treatment for the QoS flow (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.).

The standardized 5QI values have one-to-one mapping to a standardized combination of 5G QoS characteristics as defined in subclause 5.4.1 in 3GPP TS 23.501 [2].

The 5G QoS characteristics for pre-configured 5QI values are pre-configured in the AN. The 5G QoS characteristics for dynamically assigned 5QI values are signalled as part of the authorized QoS.

#### 5.9.7.2 QoS Characteristics

The following QoS Characteristics are defined for non-standardised 5QI values:

**Resource Type:**

The Resource Type determines if the Service Data Flow is a GBR Service Data Flow, delay critical GBR or a Non-GBR Service Data Flow, i.e. if the resources for the related QoS flow are permanently allocated or not. GBR resource type and delay critical GBR resource type are treated the same, except that the definition of PDB and PER are different.

**Packet Delay Budget:**

The Packet Delay Budget (PDB) defines an upper bound for the time in milliseconds that a packet may be delayed between the UE and the UPF that terminates the N6 interface. For a certain 5QI the value of the PDB is the same in uplink and downlink. In the case of 3GPP access, the PDB is used to support the configuration of scheduling and link layer functions (e.g. the setting of scheduling priority weights and HARQ target operating points). For a delay critical GBR flows, a packet delayed more than the PDB is counted as lost.

**Packet Error Rate:**

The Packet Error Rate (PER) defines an upper bound for the rate of SDUs (e.g. IP packets) that have been processed by the sender of a link layer protocol (e.g. RLC in RAN of a 3GPP access) but that are not successfully delivered by the corresponding receiver to the upper layer (e.g. PDCP in RAN of a 3GPP access). Thus, the PER defines an upper bound for a rate of non-congestion related packet losses. The purpose of the PER is to allow for appropriate link layer protocol configurations (e.g. RLC and HARQ in RAN of a 3GPP access). For a certain 5QI the value of the PER is the same in uplink and downlink. For QoS flows with delay critical GBR resource type, a packet which is delayed more than PDB is counted as lost, and included in the PER.

**Priority Level:**

The Priority level indicate a priority in scheduling resources among QoS flows. The Priority levels shall be used to differentiate between QoS flows of the same UE, and it shall also be used to differentiate between QoS flows from different UEs. Once all QoS requirements are fulfilled for the GBR QoS flows, spare resources can be used for any remaining traffic in an implementation specific manner. The lowest Priority level value corresponds to the highest Priority.

The priority level may be signalled with standardized 5QIs, and if it is received, it overwrites the default value specified in QoS characteristics Table 5.7.4.1 in 3GPP TS 23.501 [2].

**Averaging Window:**

The Averaging window is defined only for GBR QoS flows. The Averaging window represents the duration over which the GFBR and MFBR shall be calculated (e.g. (R)AN, UPF, UE). The averaging window is signalled with 5QIs to the (R)AN and UPF, and if it is not received a standardized default value applies (for standardized 5QIs the value in the QoS characteristics table 5.7.4-1 defined in 3GPP TS 23.501 [2] applies). The Average Windows only applies to GBR flows.

NOTE: For non-standardized combinations of 5G QoS characteristics, a 5QI value from the non-standardized value range together with the 5G QoS characteristics are signalled over N7.

#### 5.9.7.3 Allocation Retention Priority

The ARP is used to indicate the priority of allocation and retention, the pre-emption capability and pre-emption vulnerability for the Service Data Flow.

The Priority Level defines the relative importance of a resource request. This allows deciding whether a new QoS flow may be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). It may also be used to decide which existing QoS flow to pre-empt during resource limitations.

Values 1 to 15 are defined, with value 1 as the highest level of priority.

Values 1 to 8 should only be assigned for services that are authorized to receive prioritized treatment within an operator domain. Values 9 to 15 may be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.

The pre-emption-capability of a Service Data Flow defines whether a service data flow may get resources that were already assigned to another service data flow with a lower priority level.

The pre-emption vulnerability of a Service Data Flow defines whether a service data flow may lose the resources assigned to it in order to admit a service data flow with higher priority level.

The pre-emption capability and the pre-emption vulnerability may be enabled or disabled.

#### 5.9.7.4 Guaranteed Bitrate (DL/UL)

The Guaranteed Bit Rate indicates the guaranteed bitrate in bits per second for a downlink or uplink service data flow. For PDU types IPv4 and IPv6, the bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

#### 5.9.7.5 Maximum Bitrate (DL/UL)

The Maximum Bit Rate indicates the maximum bandwidth in bits per second for a downlink or uplink service data flow. For PDU types IPv4 and IPv6, the bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

#### 5.9.7.6 Notification Control

The Notification control indicates whether notification should be made by the RAN if the GFBR cannot be fulfilled for a Service Data Flow during the lifetime of the Service Data Flow. The RAN shall keep the QoS flow, and should try to fulfil the GFBR. Upon receiving a notification from the RAN that the GFBR cannot be fulfilled, the 5GC may initiate N2 signalling to modify or remove the QoS Flow. Once conditions improve, and the GFBR is fulfilled again, the RAN sends a new notification, informing SMF that the GFBR can be fulfilled again. After a configured time, the RAN may send a subsequent notification that the GFBR cannot be fulfilled.

Notification control is applicable to GBR Service Data Flows.

#### 5.9.7.7 PDU Session Aggregate Maximum Bitrate (DL/UL)

The PDU Session Maximum Bitrate indicates the maximum aggregate bit rate in bits per seconds across all non-GBR QoS flows associated with the same PDU session. The Session-AMBR is measured over an averaging window with a standardized value.

Editor's note: The standardized value of averaging window is to be determined by Stage 2.

#### 5.9.7.8 UE Aggregate Maximum Bitrate (DL/UL)

The UE Maximum Bitrate indicates the maximum aggregate bit rate in bits per seconds across all non-GBR QoS flows associated with a UE. The UE-AMBR is measured over an averaging window with a standardized value.

Editor's note: The standardized value of averaging window is to be determined by Stage 2.

NOTE: This information is not provided by the policy framework.

### 5.9.8 QoS mapping between Rx and N7

When an Rx session is initiated or modified, the PCF may derive Authorized QoS parameters from the service information provided by the AF.

The parameters include 5G QoS Identifier (5QI), Allocation and Retention Priority (ARP), and Maximum/Guaranteed Data Rate UL/DL.

The QoS mapping principles are defined in 3GPP TS 29.213 [68] with the exception that QCI is replaced by 5QI.

Editor's note: If other QoS parameter mappings needs to be aligned with 5G QoS is FFS.

Editor's note: To what extent 5QI characteristics are aligned with QCI characteristics is FFS.

## 5.10 Discovery and Selection aspects

### 5.10.1 General

The PCF discovery and selection procedures are needed when there are multiple and separately addressable PCFs in a PLMN. It is also possible that a PCF may serve only specific DN(s).

These procedures correlate the AF service session establishment over N5 or Rx with the associated PDU session (Session binding) handled over N7.

These procedures enable the AMF and SMF to address the PCF.

These procedures enable the NEF to address the PCF.

### 5.10.2 PCF discovery and selection by the AMF

The AMF selects the PCF for a UE.

The AMF may utilize the Nnrf\_NFDiscovery service of the Network Repository Function to discover the PCF instance(s) unless PCF information is available by other means, e.g. locally configured on AMF. Local operator policies may be considered during the PCF selection.

### 5.10.3 PCF discovery and selection by the SMF

The SMF selects the PCF for a PDU session. The selected PCF may be the same or a different one than the PCF selected by the AMF.

The SMF may utilize the Nnrf\_NFDiscovery service of the Network Repository Function to discover the PCF instance(s) unless PCF information is available by other means, e.g. locally configured on SMF or received from the AMF. The following factors may be considered during the PCF selection.

- Local operator policies.

- Selected Data Network Name (DNN).

- PCF selected by the AMF by signalling PCF addressing information from AMF to SMF. This is to select the same PCF for AMF and SMF.

As an alternative to the PCF selection by the SMF as described above, the SMF may utilize the PCF Binding Support Functionality (PCF BSF) to route the Npcf\_SMPolicyControl service operations to the PCF. In this alternative, the SMF shall route the Npcf\_SMPolicyControl service operations to the PCF BSF.

The PCF BSF may utilize the Nnrf\_NFDiscovery service to discover the PCF instance(s) unless PCF information is available by other means, e.g. locally configured based on operator polices that may use the DNN. The Npcf\_SMPolicyControl\_Get service operation shall contain enough information so that the PCF BSF can utilize the Nnrf\_NFDiscovery service.

### 5.10.4 Network functionality to assist PCF selection by the AF

#### 5.10.4.1 General

When multiple and separately addressable PCFs have been deployed, a network functionality is required in order to ensure that an AF for a certain PDU session reaches over N5/Rx the PCF holding the PDU session information. This network functionality has the following characteristics:

- It has information about the user identity, the DNN, the UE IP address(es) and the selected PCF address for a certain PDU Session. It shall receive information when an IP address is allocated or released for a PDU session.

- It encompasses the ability to determine the selected PCF address, selected by the PCF discovery and selection function described in subclause 5.10.3, according to the information carried by the incoming requests from the AF.

- It encompasses the ability to proxy or redirect N5/Rx requests based on the targeting an IP address of a UE.

Editor's note: Additional information needed by the network functionality, e.g. for network slicing, is FFS.

#### 5.10.4.2 The PCF Binding Support Functionality (PCF BSF)

The PCF BSF has the following characteristics:

a) The PCF BSF has information about the user identity, the DNN, the UE IP address(es) and the selected PCF address for a certain PDU Session. This information is stored internally in the PCF BSF. Optionally, the PCF BSF can store the binding information in the UDR, in the Structured Data for Exposure repository.

Editor's note: It is FFS how the binding information is stored in the UDR.

b) For the storage of binding information, the PCF BSF shall receive the Npcf\_SMPolicyControl service operations when an UE IP address is allocated or released for a PDU session. The PCF BSF obtains the new binding information by acting on the Npcf\_SMPolicyControl\_Get and the Npcf\_SMPolicyControl\_Delete service operations, and the Nsmf\_EventExposure\_Notify service operation.

c) For the retrieval of binding information, the PCF BSF determines the selected PCF address according to the information carried by the incoming requests. The PCF BSF acts on the Npcf\_PolicyAuthorization service operations to get the information carried in the incoming requests and obtains the selected PCF address from the stored binding information.

d) When the PCF BSF stores the binding in a Structured Data for Exposure repository in the UDR, an AF may obtain binding information from the UDR via NEF, and send the AF request towards the PCF without requiring the support of the PCF BSF.

Editor's note: It is FFS how the binding information is retrieved from the UDR.

e) The PCF BSF is able to proxy or redirect N5/Rx requests based on the IP address of a UE.

The PCF BSF may be deployed standalone or may be collocated with other network functions such as the PCF.

#### 5.10.4.3 AF Policy Request to Multiple PCFs

An AF may, via the NEF, provide policy requirements that apply to multiple UE (which, for example, belong to group of UE(s) defined by subscription or to any UE) and hence may apply to multiple PCFs.

The NEF, after validation of the application request and possible parameter mapping shall store the request from the application. When the UDR is deployed, NEF may store the request from the application in the UDR.

Editor's note: The details of NEF and UDR interaction are FFS.

The PCF(s) that need to receive application requests subscribe to receive notifications from the NEF about such group of UE's.

NOTE: The NEF selects the PCF's based on information received from the AF. Such information may include DDN information, network slices information, etc.

Editor's note: It is FFS whether the PCF(s) can subscribe to/receive notification of such application request information from the UDR.

Editor's note: Slicing aspects are FFS.

Editor's note: More detailed information on the procedures need to be added later.

## 5.11 Roaming scenarios

For a subscriber roaming in a visited PLMN, the H-PCF shall provide access and mobility management related policy to V-PCF via the N24 interface. The V-PCF shall authorize the received policy based on the roaming agreement and local policy and then provide to the AMF.

In LBO roaming, the H-PCF shall provide access and mobility management related policies and UE policies to the V-PCF. The V-PCF shall provide access mobility management policies, UE policies and session management policies in the VPLMN. The V-PCF subscribes to AMF related events at the AMF and session related events at the SMF as in the non-roaming case.

In Home Routed roaming, the H-PCF shall provide UE policies to the V-PLMN via the V-PCF. The H-PCF that handles the session related policies subscribes to the events via the H-SMF.

## 5.12 Subscription Data Management

## 5.13 Interworking with EPC

A 3GPP 5G Core Network may interact with an EPC Network (see subclause 4.3 in 3GPP TS 23.501 [2]). In order to do so, the 5G Policy Framework will, in addition to the 5G functionality, provide EPC functionality as defined in 3GPP TS 23.203 [4].

The following figure shows the non-roaming Policy framework for interworking between 5GC and EPC:



Figure 5.13-1: Non-roaming Policy framework for interworking between 5GC and EPC.

The following figure shows the roaming Policy framework for Home Routed case for interworking between 5GC and EPC:



Figure 5.13-2: Home Routed roaming Policy framework for interworking between 5GC and EPC

The following figure shows the roaming Policy framework for Local Breakout for interworking between 5GC and EPC:



Figure 5.13-3: Local breakout roaming Policy framework for interworking between 5GC and EPC

NOTE 1: PCF + PCRF, SMF+ PGW-C and UPF + PGW-U are dedicated for interworking between 5GC and EPC, which are optional and are based on UE and network capabilities. UEs that are not subject to 5GS and EPC interworking may be served by entities not dedicated for interworking, i.e. either by PGW/PCRF or SMF/UPF/PCF.

NOTE 2: N4 interface is shown in the figures for completeness as it is not part of the Policy Framework

Interworking between 5GC and EPC is optional. When supported:

- The PCF+PCRF related functionality shall be offered by the same logical entity.

- The SMF+PGW-C functionality shall be offered by the same logical entity

- N7 interface shall be supported between the PCF-PCRF and the SMF+PGW-C. This interface should be as much transparent as possible to the access network.

- SMF+PGW-C shall be in charge of the applicable attribute derivation when the user accesses via EPC/E-UTRAN.

Editor's note: Reference points and logical entities in the interworking architecture can require further work at stage 2 level.

- The following derivation is required:QoS mapping derivation:

a) 5QI values shall be mapped into QCI values.

b) Notification control different from successful/non-successful resource allocation will be ignored.

c) Session AMBR shall be mapped into the APN-AMBR.

Editor's note: QoS mapping derivation is subject to changes and needs further stage 2 work.

## 5.14 IMS Aspects

### 5.14.1 General

In order to support the IMS service, the PCF shall be able to receive media related information from the IMS and inform the IMS of PDU-CAN events.

In order to support interworking with IMS deployments supporting Rx interface, the PCF shall support Rx interface as specified in 3GPP TS 29.214 [56]. This facilitates the migration from the EPC to the 5GC without requiring these AFs to upgrade to support the Npcf\_PolicyAuthorization service.

## 5.15 Support of MPS services

### 5.15.1 General

To allow the 5G system to support the invocation/revocation of IMS Multimedia Priority services from IMS deployments supporting the Rx interface, the PCF shall support Rx interface as specified in 3GPP TS 29.214 [56]. This facilitates the migration from the EPC to the 5GC without requiring these AFs to upgrade to support the Npcf\_PolicyAuthorization service.

When the PCF derives PCC rules corresponding to the MPS service, the ARP and 5QI (and if applicable, 5G QoS characteristics) shall be set as appropriate for the prioritized service.

When the PCF derives PCC rules corresponding to the non-MPS service, the PCF shall generate the PCC rules as per normal procedures.

At the time the Priority PDU connectivity services is invoked (i.e. MPS EPS Priority and MPS Priority Level are set), the PCF shall upgrade the ARP and/or change 5QI (and if applicable, 5G QoS characteristics) also for the PCC rules corresponding to the non-MPS service. The PCF shall change the ARP and/or 5QI (plus 5G QoS characteristics) modified for the Priority PDU connectivity service to an appropriate value according to the PCF decision.

When the PCF receives the Npcf\_SMPolicyControl\_Get service request from the SMF, the PCF shall check whether any of these parameters is stored in the UDR: MPS EPS Priority, MPS Priority Level and/or IMS Signalling Priority. The PCF shall derive the applicable PCC rules and default QoS flow based on that information. If the IMS Signalling Priority is set and the DNN is dedicated for IMS, the PCF shall assign the ARP corresponding to the MPS for the default QoS flow and for the PCC rules corresponding to the IMS signalling QoS flow. If the DNN is dedicated for IMS, the ARP shall be derived without considering IMS Signalling Priority.

NOTE 1: Subscription data for the MPS is provided to the PCF by the UDR service.

Once the PCF receives a notification of a change in MPS EPS Priority, MPS Priority Level and/or IMS Signalling Priority from the UDR, the PCF shall make the corresponding policy decisions (i.e. the ARP and/or 5QI (and if applicable, 5G QoS characteristics) change) and, if applicable, the PCF shall initiate the Npcf\_SMPolicyControl\_UpdateNotify service to provision the modified data.

NOTE 2: The MPS Priority Level is one among other input data such as operator policy for the PCF to set the ARP.

Whenever one or more AF sessions of the MPS service are active within the same PDU session, the PCF shall ensure that the ARP priority level of the default QoS flow is at least as high as the highest ARP priority level used by any authorized PCC rules belonging to the MPS service. If the ARP pre-emption capability is enabled for any of the authorized PCC rules belonging to the MPS service, the PCF shall also enable the ARP pre-emption capability for the default QoS flow.

NOTE 3: This ensures that services using dedicated QoS flow are not terminated because of default QoS flow with a lower ARP priority level or disabled ARP pre-emption capability being dropped during mobility events.

NOTE 4: This PCF capability does not cover interactions with services other than MPS services.

### 5.15.2 Invocation/Revocation of Priority PDU connectivity services

When a Priority PDU connectivity service is invoked, the PCF shall:

- derive the corresponding PCC rules with the ARP and 5QI (plus 5G QoS characteristics if applicable) set as appropriate for a prioritized service;

- set the ARP of the default QoS flow as appropriate for a Priority PDU connectivity services under consideration of the requirement described in subclause 5.15.1;

- set the 5QI of the default QoS flow as appropriate for the Priority PDU connectivity service;

- set the ARP of PCC rules installed before the activation of the Priority PDU connectivity Service to the ARP as appropriate for the Priority PDU connectivity Service under the consideration of the requirements described in subclause 5.15.1; and

- set the 5QI of the PCC rules installed before the activation of the Priority PDU connectivity Service to the 5QI (plus 5G QoS characteristics if applicable) as appropriate for the Priority PDU connectivity Service if modification of the 5QI (plus 5G QoS characteristics if applicable) of the PCC rules is required.

When a Priority PDU connectivity service is revoked, the PCF shall:

- delete the PCC rules corresponding to the Priority PDU connectivity Service if they were previously provided;

- set the ARP of the default QoS flow to the normal ARP under the consideration of the requirements described in subclause 5.15.1;

- set the 5QI (plus 5G QoS characteristics if applicable) of the default QoS flow as appropriate for the PCF decision;

- set the ARP of all active PCC rules as appropriate for the PCF under the consideration of the requirements described in subclause 5.15.1; and

- set the 5QI (plus 5G QoS characteristics if applicable) to an appropriate value according to the PCF decision if modification of the 5QI (plus 5G QoS characteristics if applicable) of PCC rules is required.

NOTE: The activation/deactivation of the Priority PDU connectivity service requires explicit invocation/revocation via UDR MPS user profile (MPS EPS Priority, MPS Priority Level). The AF for MPS priority service can also be used to provide Priority PDU connectivity services using network-initiated resource allocation procedures (via interaction with PCC) for originating accesses.

### 5.15.3 Invocation/Revocation of IMS Multimedia Priority Services

If the PCF receives service information including an MPS session indication and the service priority level from the P-CSCF or at reception of the indication that IMS Signalling Priority is active for the PDU session, the PCF shall under consideration of the requirements described in subclause 5.15.1.

- set the ARP of the default QoS flow as appropriate for the prioritized service;

- if required, set the ARP of all PCC rules assigned to the IMS signalling bearer as appropriate for IMS Multimedia priority services; and

- derive the PCC rules corresponding to the IMS Multimedia Priority Service and set the ARP of these PCC rules based on the information received over Rx.

If the PCF detects that the P-CSCF released all the MPS session and the IMS Signalling Priority has been deactivated for the PDU session the PCF shall under consideration of the requirements described in subclause 5.15.1:

- delete the PCC rules corresponding to the IMS Multimedia Priority Service;

- set the ARP of the default QoS flow as appropriate for the IMS Multimedia Priority set to inactive; and

- replace the ARP of all PCC rules assigned to the IMS signalling bearer as appropriate when the IMS Multimedia Priority is inactive.

Editor's note: The above procedures may need be updated when the corresponding requirements in 3GPP TS 23.203 [4] are updated.

## 5.16 Emergency Services

The PCF shall be able to identify an emergency PDU session service upon PDU session establishment with an emergency DNN over the Npcf\_SMPolicyControl service based interface.

Editor's note: Further details will be added based on progress in SA2.

## 5.17 Mission Critical Services

To allow the 5G system to interwork with AFs related to the Mission Critical services that support Rx interface as described in 3GPP TS 22.280 [57] and 3GPP TS 23.379 [55], the PCF shall support the corresponding Rx procedures and requirements defined in 3GPP TS 29.214 [56]. This facilitates the migration from the EPC to the 5GC without requiring these AFs to upgrade to support Npcf and Naf service based interfaces.

Editor's note: Further details will be added based on progress in SA2.

## 5.18 Binding Mechanism

### 5.18.1 General

The binding mechanism associates the session information with the QoS flow that is intended to carry the service data flow(s).

The binding mechanism includes three steps:

1. Session binding.

2. PCC rule authorization.

3. QoS flow binding.

The Session binding function receives the AF session information and determines the relevant PDU session. With this information the PCC rule authorization function runs the policy rules and constructs the PCC rule(s), if the authorization is granted. Finally, the QoS flow binding function selects the QoS flow(s) to carry the service data flow (defined in a PCC rule by means of the SDF template), within the PDU session.

The PCC rule authorization function and the QoS flow binding function can take place without the Session binding function at certain PDU session events (e.g. request of SM related policies initiated by the SMF). The PCF may authorize dynamic PCC rules for service data flows without a corresponding AF session.

NOTE: The relation between AF sessions and rules depends only on the operator configuration. An AF session can be covered by one or more PCC rules, if applicable (e.g. one rule per media component of an IMS session).

### 5.18.2 Session Binding

The Session binding is the association of the AF session information to one and only one PDU session.

When the PCF receives the service information from the AF, the PCF shall perform the session binding and shall associate the described service IP flows within the AF session information (and therefore the applicable PCC rules) to one and only one existing PDU session. This association is done comparing the following parameters received from the AF with the corresponding PDU session parameters.

a) The UE IPv4 address or IPv6 network prefix.

b) The UE identity (of the same kind e.g. SUPI), if available.

NOTE: In case the UE identity in the access network and the application level identity for the user are of different kinds, the PCF needs to maintain, or have access to, the mapping between the identities. Such mapping is outside the scope of the present document.

c) The information about the data network (DNN) the user is accessing, if available.

Editor's note: It's FFS that how to solve the following scenario: Within a PLMN, there are several separate IP address domains, with SMF(s) that allocate Ipv4 IP addresses out of the same private address range to UEs for the UPF(s) which located in the different IP address domain. The same IP address can thus be allocated to UEs served by UPFs in different address domains. If one PCF controls several SMFs which has allocated the same Ipv4 address for the UPFs in different IP address domains to the UE, the UE IP address is thus not sufficient for the session binding. An AF can serve UEs in different IP address domains, either by having direct IP interfaces to those domains, or by having interconnections via NATs in the user plane between UPFs and the AF. If a NAT is used, the AF obtains the IP address allocated to the UE via application level signalling and supplies it for the session binding to the PCF. The AF supplies a Domain identifier denoting the IP address domain behind the NAT in addition. The AF can derive the appropriate value from the source address (allocated by the NAT) of incoming user plane packets.

The PCF shall identify the PCC rules affected by the AF session information, including new PCC rules to be installed and existing PCC rules to be modified or removed.

If the PCF is not capable of executing the Session binding, the PCF shall reject the AF request.

Editor's note: Session Binding mechanism for Ethernet PDU session type is FFS.

### 5.18.3 PCC Rule Authorization

The PCC rule authorization is the selection of the 5G QoS parameters for the PCC rules.

The PCF shall perform the PCC rule authorization after successful Session binding for dynamic PCC rules belonging to the AF sessions, as well as for the PCC rules without the corresponding AF sessions. By the authorization process the PCF determines whether the user can have access to the requested services and under what constraints. If so, the PCC rules are created or modified. If the Session information is not authorized, a negative answer shall be issued to the AF.

The PCF shall perform the PCC rule authorization function when the PCF receives the Session information from the AF, when the PCF receives a notification of PDU session events (e.g. establishment, modification) from the SMF, or when the PCF receives a notification from the UDR that calls for a policy decision.

For the authorization of a PCC rule, the PCF shall consider any 5GC specific restrictions, the AF service information and other information available to the PCF (e.g. user's subscription information, operator policies). The PCF assigns appropriate 5G QoS parameters (5QI, QoS characteristics, ARP, GBR, MBR, QNC), that can be supported by the access network, to each PCC rule.

The authorization of a PCC rule associated with an emergency service shall be supported without subscription information (e.g. information stored in the UDR). The PCF shall apply policies configured for the emergency service.

### 5.18.4 QoS Flow Binding

The QoS flow binding is the association of the PCC rule to a QoS flow, identified by the QFI, within a PDU session. The QoS flow binding function resides in the SMF.

The set of 5G QoS parameters assigned by the PCF to the service data flow is the main input for QFI allocation.

When the PCC rule provides an indication for the service data flow(s) to be bound to the QoS flow of the default QoS rule (i.e. the "Bind to QoS flow of the default QoS rule" parameter as defined in subclause 5.7.1), the SMF shall use this indication instead of the set of 5G QoS parameters in the PCC rule for the QoS flow binding and keep the binding as long as this parameter remains set.

When "Bind to Default QoS flow of the default QoS rule" parameter is not received, the allocation of QFI to the service data flow(s) is based on the 5QI, ARP and QNC parameters. When the PCF provisions a PCC Rule, the SMF shall evaluate whether a QoS flow with the same 5QI/ARP/QNC combination exists. If a QoS flow with the same 5QI/ARP/QNC combination exists, the SMF allocates the same QFI to the service data flows that are assigned the same values for of the 5QI, ARP and QNC. If no QoS flow exists, the SMF assigns a QFI for a new QoS flow, derives the QoS parameters for a new QoS flow, using authorized QoS in the PCC Rule, and binds the PCC Rule to the QoS flow.

NOTE 1: For non-GBR QoS flows, QNC is not relevant.

NOTE 2: For non-GBR QoS flows only, and when standardized 5QIs or pre-configured 5QIs are used, the 5QI value can be used as the QFI of the QoS flow. However, the pre-configured 5QI values cannot be used when the UE is roaming.

NOTE 3: For an unstructured PDU session, there is maximum of one QoS flow.

The PCF shall supply the PCC rules to be installed, modified, or removed to the SMF. The SMF shall evaluate whether it is possible to use one of the existing QoS flows or not, and if applicable, shall send the QoS profile to the (R)AN over the N2 interface, the SDF template and the QoS rule information to the UPF over the N4 interface, and the QoS rule to the UE.

If the PCF removes an indication for the service data flow(s) to be bound to the QoS flow of the default QoS rule the binding is created between service data flow(s) and the QoS flow which have the same 5QI, ARP and QNC.

If the PCC rule is removed, the SMF shall remove the association of the PCC rule to the QoS flow. Whenever the authorized QoS of a PCC rule changes, the existing QFI allocation shall be re-evaluated, i.e. the allocation procedure, is performed. The re-evaluation may, for a service data flow, require a new binding with another QoS flow.

NOTE 4: A QoS change of the default 5QI/ARP/QNC values causes the QoS flow binding for PCC rules previously bound to the QoS flow of the default QoS rule set to be re-evaluated. At the end of the re-evaluation of the PCC rules there needs to be at least one PCC rule that successfully binds with the QoS flow of the default QoS rule set.

When a QoS flow is removed the SMF shall report to the PCF that the PCC Rules bound to the corresponding QoS flow are removed.

## 5.19 AF influence traffic routing

### 5.19.1 General

An Application Function (AF) may send requests to influence SMF routing decisions for traffic of PDU session, for event subscription or for both. The AF requests may influence UPF (re)selection and allow routing user traffic to a local access to a Data Network (identified by a DNAI).

### 5.19.2 Support of traffic routing request

Application Function influence on traffic routing only apples to non-roaming and to LBO deployments. Application Function influence on traffic routing does not apply in case of Home Routed deployments. PCF shall not apply AF requests targeting "all users" to PDU sessions established in Home Routed mode.

NOTE 1: The AF can issue requests on behalf of applications not owned by the PLMN serving the UE.

NOTE 2: The AF can be in charge of the (re)selection or relocation of the applications within the local DN. Such functionality is not defined.

The AF requests are sent to the PCF via Npcf. In case of requests regarding on-going PDU sessions of individual UEs the communication can be directly with the PCF or via the NEF. Requests that target multiple UE(s) are sent via the NEF and may target multiple PCF(s). The PCF(s) transform(s) the AF requests into policies that apply to PDU sessions. When the AF has subscribed to UP path management event notifications from SMF, such notifications are sent either directly to the AF or via an NEF (without involving the PCF).

If the AF request targets a specific ongoing session, the AF may send its request directly to the PCF or via the NEF. If the AF request is not for a specific ongoing session, the AF sends its request via NEF.

Editors' note: It is FFS whether the AF Request may correspond to a list IP addresses / IPv6 Prefixed of on-going PDU sessions. If that were the case the request would have to be forked to multiple PCF.

When the AF request is considered as semi-permanent (i.e. does not target an individual IP address / Prefix allocated to a UE) the PCF stores the AF request for usage by future PDU sessions. When the PCF determines if existing PDU sessions are impacted by the AF request, the PCF updates the SMF with corresponding new policy rule(s) via a PDU session modification for each of these PDU sessions.

The AF traffic routing requests may contain at least:

1) Information to identify the traffic to be routed. The traffic can be identified in the AF request by:

- Either a DNN and possibly slicing information (S-NSSAI) or an AF-Service-Identifier.

- When the AF provides an AF-Service-Identifier i.e. an identifier of the service on behalf of which the AF is issuing the request, the 5G Core maps this identifier into a target DNN and slicing information (S-NSSAI).

- When the NEF process the AF request, the AF-Service-Identifier may be used to authorize the AF request.

- An application identifier or traffic filtering information (e.g. 5 Tuple). The application identifier refers to an application handling UP traffic and is used by the UPF to detect the traffic of the application.

2) Information about the N6 traffic routing requirements for traffic identified as defined in bullet 1). This is provided implicitly by reference, in the form of a list of routing profile IDs corresponding each to a DNAI, if the details of the N6 routing requirements are preconfigured in SMF. Otherwise, it is provided explicitly, in the form of a list of DNAIs and associated N6 traffic routing information. Based on the N6 traffic routing information, the PCF determines traffic steering policy IDs sent to SMF that each corresponds to a steering behaviour which is preconfigured on the SMF or UPF.

3) Potential locations of applications towards which the traffic routing should apply. The potential location of application is expressed as a list of DNAI(s). If the AF interacts with the PCF via the NEF, the NEF may map the AF-Service-Identifier information to a list of DNAI(s). The DNAI(s) may be used for UPF (re)selection.

4) Information on the UE(s) whose traffic is to be routed. This may correspond to:

- Individual UEs identified using either an External Identifier or a MSISDN or an IP address/Prefix.

- groups of UEs identified by an External Group Identifier when the AF interacts via the NEF, or Internal-Group Identifier when the AF interacts directly with the PCF.

- any UE the request applies to any UE accessing the combination of DNN, S-NSSAI and DNAI(s).

- In case of PDU type is IPv4/IPv6, when the AF provides an IP address/Prefix this allows the PCF to identify the PDU session for which this request applies and the AF request applies only to the current PDU session of a UE. In this case, additional information such as the UE identity may also be provided to help the PCF to identify the correct PDU session.

- Otherwise the request shall apply to any existing or future PDU session that matches the parameters in the AF request.

- When the AF request targets any UE or a group of UE, the AF request is likely to influence multiple PDU sessions possibly served by multiple SMFs and PCFs.

- When the AF request targets a group of UE it provides one or several identifiers in its request. The group identifiers provided by the AF are mapped to Internal-Group identifiers. Members of the group have this Group Identifier in their subscription. The Internal-Group Identifier is stored in UDM, retrieved by SMF from UDM and passed by SMF to PCF at PDU session set-up. The PCF can then map the AF requests with user subscription and determine whether an AF request targeting a Group of users applies to a PDU session.

5) Information on when (temporal validity condition) the traffic routing is to apply.

NOTE 3: This allows to provide an expiry time for the AF request.

6) Information on where (spatial validity condition) the UE(s) are to be when the traffic routing applies. This is provided in the form of area(s) of interest. If the AF interacts with the PCF via the NEF, it may provide a list of geographic zone identifier(s) and the NEF maps the information to areas of interest based on pre-configuration.

7) AF subscription to following events:

- Early and/or late notifications about UP path management events: A change of DNAI for the UPF serving the UE. The corresponding notification about a change from source DNAI to target DNAI sent by the SMF to the AF shall include the Identity of the target DNAI, the IP address/prefix of the UE, type of notification (i.e. early notification or late notification), the notification may include the UE identity (e.g. an External Identifier or a MSISDN) and N6 routing information.

NOTE 4: The subscription can be for early notification and/or late notification. In case of a subscription for early notification, the SMF sends the notification before executing the UPF (re)selection. In case of a subscription for late notification, the SMF sends the notification when the UPF (re)selection has completed.

8) An AF transaction identifier referring to the AF request. This allows the AF to update or remove the AF influence request.

Based on information received from the AF, operator's policy, etc, the PCF shall authorize the request and determine the traffic steering policy. The traffic steering policy indicates the list of traffic steering policy IDs configured in SMF and if the N6 routing information associated to the application is explicitly provided by the AF, the N6 routing information. The traffic steering policy IDs are related to the mechanism enabling traffic steering to the DN.

NOTE 5: The DNAIs are related to the information considered by SMF for UPF selection, e.g. for diverting (locally) some traffic matching traffic filters provided by the PCF.

Then the PCF shall acknowledge the request either to the AF or to the NEF.

For PDU session that corresponds to the AF request, the PCC rules provided by the PCF to the SMF may contain information about the DNAI(s) towards which the traffic routing should apply and/or a list of traffic steering policy IDs and/or information on AF subscription to SMF events. If the N6 routing information associated to the application is explicitly provided in the AF request, the PCF shall also provide the N6 routing information to the SMF as part of PCC rules. This is done by providing policies at PDU-CAN session establishment or by initiating a PDU-CAN Session Modification procedure.

The PCF evaluates the temporal validity condition of the AF request and informs the SMF to activate or deactivate the corresponding PCC rules according to the evaluation result.

Editor's note: Whether spatial validity conditions are resolved at the PCF or the SMF is FFS.

The SMF receives PCC rules that contain list of DNAI(s) from the PCF. When the PCC rules are activated, the SMF may, based on local policies, take the information in the PCC rules into account to:

- (re)select UPF(s) for PDU sessions. The SMF is responsible for handling the mapping between the UE location (TAI / Cell-Id) and DNAI(s) associated with UPF and applications and of the selection of the UPF(s) that serve a PDU session.

- activate mechanisms for traffic multi-homing or enforcement of an UL Classifier (UL CL).

NOTE 6: Traffic forwarding rules and associated N6 routing information if provided can be provisioned to the UPF.

- inform the Application Function of the (re)selection of the UP path (change of DNAI).

## 5.20 Event triggers

### 5.20.1 General

Event reporting functionality in 5G is realized by the PCF, the SMF and the AMF. The SMF performs PDU session related event triggers detection and reports the occurred events to the PCF using the Nsmf\_EventExposure service. The AMF performs UE mobility related event triggers detection and reports the occurred events to the PCF using the Namf\_EventExposure service.

### 5.20.2 SMF Event triggers handling

The SMF performs PDU session related event trigger detection. When an event matching an armed event trigger occurs, the SMF shall report the occurred event to the PCF by using the Nsmf\_EventExposure\_Notify service operation.

When multiple events occur simultaneously, the SMF may report the occurred events to the PCF within the same Nsmf\_EventExposure\_Notify service operation.

The event triggers define the conditions when the SMF shall interact again with the PCF after an PDU session establishment.

The PCF subscribes to new event triggers with the SMF or removes armed event triggers from the SMF using the Nsmf\_EventExposure service (if applicable). It shall be possible for the SMF to react on the event triggers. The PDU session related event triggers applicable for 5G are listed in table 5.20.2-1.

If the PCF wants to:

- create subscription to one or more SMF detected event triggers; or

- modify previously created subscription to SMF detected event triggers;

the PCF shall send the Nsmf\_EventExposure\_Subscribe service operation to the SMF.

If the PCF wants to delete previously created subscription to SMF detected event triggers the PCF shall send the Nsmf\_EventExposure\_UnSubscribe service operation to the SMF.

When an event matching an event trigger occurs, the SMF shall report the occurred event to the PCF by using the Nsmf\_EventExposure\_Notify service operation.

NOTE: For the HTTP methods and resources to realize the Nsmf\_EventExposure service operations see subclause 5.4.5.3.

Table 5.20.2-1: SMF detected event triggers to be reported to PCF

|  |  |  |
| --- | --- | --- |
| Event trigger  stage 2 definition | Event trigger  stage 3 definition | Description |
| PLMN change | PLMN\_CHANGE | The UE has moved to another operators' domain. |
| Session-AMBR change | SESSION\_AMBR\_CHANGE | The subscribed Session-AMBR has changed.  The Session-AMBR change event trigger shall trigger the PCF interaction for all changes in the data received in the SMF from the UDM. |
| Default QoS change | DEFAULT\_QOS\_CHANGE | The subscribed QoS has changed.  The default QoS change event trigger reports a change in the default 5QI/ARP retrieved by the SMF from the UDM, as explained in subclause 5.7.2.7 of 3GPP TS 23.501 [2].  The default QoS change event trigger shall trigger the PCF interaction for all changes in the data received in the SMF from the UDM. |
| Change in type of Access Type | ACCESS\_TYPE\_CHANGE | The access type of the PDU session has changed. |
| Location change (serving area) | SERVING\_AREA\_CHANGE | The serving area of the UE has changed. |
| Location change (serving CN node) | USER\_LOCATION\_CHANGE | The serving core network node of the UE has changed. |
| Change of UE presence in Presence Reporting Area | CHANGE\_OF\_UE\_PRESENCE\_IN\_ PRESENCE\_REPORTING\_AREA | The UE is entering/leaving a Presence Reporting Area. |
| Out of credit | OUT\_OF\_CREDIT | Credit is no longer available. |
| Enforced PCC rule request | REVALIDATION\_TIMEOUT | SMF is performing a PCC rules request as instructed by the PCF.  The enforced PCC rule request event trigger shall trigger the SMF interaction to request PCC rules from the PCF for an established PDU session. This SMF interaction shall take place within the Revalidation time limit set by the PCF in the PDU session related policy information. |
| UE IP address change | UE\_IP\_ADDRESS\_ALLOCATE | A UE IP address has been allocated/released.  The UE IP address change event trigger shall trigger the SMF interaction with the PCF in case a UE IP address is allocated or released during the lifetime of the IP session. |
| UE\_IP\_ADDRESS\_RELEASE |
| Access Network Charging Correlation Information | CHARGING\_CORRELATION\_ EXCHANGE | Access Network Charging Correlation Information has been assigned.  The Access Network Charging Correlation Information event trigger shall trigger the SMF to report the assigned access network charging identifier for the PCC rules that are accompanied with a request for this event at activation. |
| Usage report | USAGE\_REPORT | The PDU session or the Monitoring key specific resources consumed by a UE either reached the threshold or needs to be reported for other reasons. (NOTE 1) |
| Start of application traffic detection and  Stop of application traffic detection | APPLICATION\_TRAFFIC\_START | The start or the stop of application traffic has been detected.  The Start of application traffic detection and Stop of application traffic detection events shall trigger an interaction with PCF once the requested application traffic is detected (i.e. Start of application traffic detection) or the end of the requested application traffic is detected (i.e. Stop of application traffic detection) unless it is requested within a specific PCC rule to mute such a notification for solicited application reporting or unconditionally in case of unsolicited application reporting. (NOTE 2) |
| APPLICATION\_TRAFFIC\_STOP |
| Access Network Information report | ACCESS\_NETWORK\_INFO\_REPORT | Access information as specified in the Access Network Information Reporting part of a PCC rule.  If the event trigger for Access Network Information reporting is set, the SMF shall check the need for access network information reporting after successful installation/ modification or removal of a PCC rule or upon termination of the PDU session. The SMF shall check the Access Network Information report parameters (User Location Report, UE Timezone Report) of the PCC rules and report the access network information to the PCF. The SMF shall not report any subsequent access network information updates received from the PDU session without any previous updates of related PCC rule unless the associated QoS flow or PDU session has been released.  (NOTE 3, NOTE 4) |
| Credit management session failure | CREDIT\_MANAGEMENT\_SESSION\_FAILURE | Transient/Permanent Failure as specified by the OCS.  The Credit management session failure event trigger shall trigger a SMF interaction with the PCF to inform about a credit management session failure and to indicate the failure reason, and the affected PCC rules. |
| - | UE\_TIME\_ZONE\_CHANGE | Indicates a change in the time zone the UE is currently located. |
| - | RAT\_TYPE\_CHANGE | Triggered upon a change in RAT type (FFS). |
| - | REALLOCATION\_OF\_CREDIT | FFS |
| - | SUCCESSFUL\_RESOURCE\_ ALLOCATION | Indicates that resources have been successfully allocated for a PCC rule. |
| NOTE 1: If the Usage report event trigger is set and the volume or the time thresholds, earlier provided by the PCF, are reached, the SMF shall report this event to the PCF. If both volume and time thresholds were provided and the thresholds, for one of the measurements, are reached, the SMF shall report this event to the PCF and the accumulated usage since last report shall be reported for both measurements.  NOTE 2: The application identifier and service data flow descriptions, if deducible, shall also be included in the report. An application instance identifier shall be included in the report both for Start and for Stop of application traffic detection when service data flow descriptions are deductible. This is done to unambiguously match the Start and the Stop events.  NOTE 3: If the Access Network Information report parameter for the User Location Report is set and the user location (e.g. cell) is not available to the SMF, the SMF shall provide the serving PLMN identifier to the PCF which shall forward it to the AF.  NOTE 4: If the SMF receives a request to install/modify or remove a PCC rule with Access Network Information report parameters (User Location Report, UE Timezone Report) set, the SMF shall initiate a PDU session modification to retrieve the current access network information of the UE and forward it to the PCF afterwards. | | |

Upon reception of the Nsmf\_EventExposure\_Notify service operation:

- if the PCF decides to modify the SMF related policies, then the PCF shall invoke the Npcf\_SMPolicyControl\_UpdateNotify service operation;

- if the PCF decides to modify the subscribed event triggers, then the PCF shall invoke the Nsmf\_EventExposure\_Subscribe service operation to the SMF; or

- if the PCF decides to delete the subscribed event triggers, then the PCF shall invoke the Nsmf\_EventExposure\_Unsubscribe service operation to the SMF.

### 5.20.3 AMF Event triggers handling

The PCF may subscribe to the event triggers at the AMF by invoking the Namf\_EventExposure\_Subscribe service operation.

The Namf\_EventExposure\_Subscribe service operation is initiated if the PCF wants to:

- create subscription to one or more AMF detected event triggers; or

- modify previously created subscription to AMF detected event triggers.

If the PCF wants to delete previously created subscription to AMF detected event triggers the PCF shall send the Namf\_EventExposure\_UnSubscribe service operation to the AMF.

When an event matching an armed event trigger occurs, the AMF shall report the occurred event to the PCF by using the Namf\_EventExposure\_Notify service operation. The AMF shall address the event notification to the Notification URI provided by the PCF in the Namf\_EventExposure\_Subscribe service operation.

When multiple events occur simultaneously, the AMF may report the occurred events to the PCF within the same Namf\_EventExposure\_Notify service operation.

NOTE: For the HTTP methods and resources to realize the Namf\_EventExposure service operations see 3GPP TS 29.518 [72], since the Namf\_EventExposure service is out of scope of this document.

The AMF detected event triggers to be reported to the PCF are listed in table 5.20.3-1 and define the conditions when the AMF shall notify the PCF that a certain event occurred.

Table 5.20.3-1: AMF detected event triggers to be reported to PCF

|  |  |
| --- | --- |
| Event trigger | Description |
| Location change (tracking area) | The tracking area of the UE has changed. |
| Change of UE presence in Area of Interest | The UE is entering/leaving a Presence Reporting Area of interest. |
| Service Area Restriction change | The subscribed service area restriction information has changed. |
| RFSP index change | The subscribed RFSP index has changed. |

Upon reception of the Namf\_EventExposure\_Notify service operation,

- if the PCF decides to modify UE policies, or Access and Mobility policies, then the PCF shall invoke the Npcf\_AMPolicyControl\_UpdateNotify service operation towards the AMF;

- if the PCF decides to modify the subscribed events, then the PCF shall invoke the Namf\_EventExposure\_Subscribe service operation towards the AMF; or

- if the PCF decides to delete the subscribed events, then the PCF shall invoke Namf\_EventExposure\_Unsubscribe service operation towards the AMF.

# 6 Interworking between the 5G System and external Data Networks (DN)

## 6.1 Reference Model

### 6.1.1 General

The PDU-CAN domain can interwork with IP networks and networks handling non-IP data services. When interworking with the IP networks, the PDU-CAN domain can operator IPv4 or IPv6. The interworking point with the external networks is at N6 reference point. This interworking point is shown in the following figure.



Figure 6.1.1-1: External network interworking

The UPF for interworking with the external network is the access point of the PDU-CAN domain. See 3GPP TS 23.501 [2] for further details.

#### 6.1.1.1 Interworking with external DN with DHCP service

The Packet Domain may obtain IP address via external DHCP server during the PDU session establishment procedure in a 5G system. For IPv4, the SMF acts as the DHCP client towards the external DHCP server. For IPv6, the SMF acts as the DHCP server towards the UE and the DHCP client towards the external DHCP server. The UPF does not have any DHCP functionality and just forwards packets between the SMF and external server over the user plane for IPv4 or IPv6, and between the UE and the SMF over the user plane for IPv6.



Figure 6.1.1.1-1: The architecture of 5G System interworking with external netowrk for DHCP

## 6.2 Functional entities

## 6.3 System Procedures

### 6.3.1 DN Authentication & Authorization

The SMF may, depending on DNN configuration, interact with an external DN (AAA server) for transport of signalling for PDU session authorization/authentication by the external DN.

The following system procedure describes the signalling flows for the authentication/authorization procedures with external DN for 5G system. The procedures are based on the descriptions in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3].

1. UE initiates the PDU Session Establishment procedure, including authentication/authorization information.

2. The AMF sends Nsmf\_PDUSession\_CreateSMContext or Nsmf\_PDUSession\_UpdateSMContext Request including the authentication/authorization information to the SMF. And the SMF responds to the service operation.

According to the configuration in the SMF, step 6 to step 9 are executed before step 3 if the SMF needs to send an EAP-Request message to the UE.

3. If the N4 session has not been established before, the SMF triggers the N4 Session Establishment procedure to the UPF.

4. The SMF forwards the Authentication/Authorization request to the DN-AAA via the UPF, the authentication/authorization data is included in N4 user plane message.

5-10. The DN-AAA responds to the UPF. The authentication/authorization information is transferred to UE via N4 user plane message, Namf\_Communication\_N1N2MessageTransfer service and NAS SM Transport message. UE further responds to the received authentication/authorization data and such information is transferred in NAS SM Transport message, Nsmf\_PDUSession\_UpdateSMContext service and N4 user plane message, then finally sent to the DN-AAA by the UPF.

NOTE: Step 5 to step 10 are optional and may be repeated depending on the authentication/authorization mechanism used (e.g. EAP-TLS).

11. The UPF receives final result of authentication/authorization from the DN-AAA and forwards it to the SMF in N4 user plane message.

12. The SMF proceeds with the PDU session establishment procedure and includes the authentication/authorization information in Namf\_Communication\_N1N2MessageTransfer service.

13. The AMF sends the NAS PDU Session Establishment Request with the authentication/authorization information to the UE.

Editor's note: If AAA signalling is tunnelled in N4 user plane will be decided by CT4.



Figure 6.3.1-1: DN Authentication & Authorization

The DN-AAA server may revoke the authorization for a PDU Session or update DN authorization data for a PDU Session by DM or CoA message in RADIUS as defined in IETF RFC 3576 [74] and ASR or RAR message in Diameter as defined in IETF RFC 6733 [75]. According to the request from DN-AAA server, the SMF may release or update the PDU session.

### 6.3.2 IP Address Management

When interworking with IP networks, the SMF may interact with an external Data Network for UE IP Address management. It includes the support of IP address allocation, renewal and release related messages over N6 reference point.

NOTE: The SMF may get an IP index from the PCF to assist in selecting how the IP address is to be allocated when multiple allocation methods or multiple instances of the same method are supported.

The following methods are already considered for UE IP Address management in an external network:

- IPv4 Address allocation and IPv4 parameter configuration using DHCPv4;

- /64 IPv6 prefix allocation via IPv6 stateless address autoconfiguration via DHCPv6 according to IETF RFC 4862 [19];

- IPv6 parameter configuration via stateless DHCPv6 according to IETF RFC 3736 [20]; and

- IPv4 address or IPv6 prefix allocation using Diameter or RADIUS.

#### 6.3.2.1 IPv4 Address allocation and IPv4 parameter configuration via DHCPv4

The UE may obtain the IPv4 address and/or its configuration parameters at or after the initial access signalling (i.e. initial PDU session establishment) to the packet domain. The request for IPv4 address and/or configuration parameters from the UE may trigger the SMF acting as a DHCPv4 client to request the IPv4 address and/or configuration parameters from an external DHCPv4 server and deliver them to the UE. The DHCPv4 functions in the SMF, the UE and the external DHCPv4 server shall be compliant to IETF RFC 2131 [22], IETF RFC 1542 [23] and IETF RFC 4039 [24].

The following system procedure describes the successful IPv4 address allocation and parameter configuration signalling flow between the SMF and the external DHCPv4 server as depicted in figure 6.3.1-1. For a detailed description of the DHCPv4 messages, refer to IETF RFC 2131 [22], IETF RFC 1542 [23] and IETF RFC 4039 [24].

1) The DHCPv4 client function in the SMF sends a DHCPDISCOVER as an IP limited broadcast message, i.e. the destination address 255.255.255.255, towards the external DN. If the SMF has the DHCPv4 server IP addresses configured for the DNN, the DHCPDISCOVER shall be send as unicast (or even multicast) to the external DHCPv4 servers. 2) Upon receiving the DHCPDISCOVER request message, the external DHCPv4 servers reply by sending a DHCPOFFER message including an offered IP address. Several DHCPOFFER messages may be received by the SMF if multiple DHCPv4 servers respond to the DHCPDISCOVER.

3) The DHCPv4 client function in the SMF processes the messages and sends a DHCPREQUEST towards the selected external DHCPv4 server.

NOTE 1: If the optimized signalling (Rapid Commit Option) is used as per IETF RFC 4039 [24], the messages 2-3 can be eliminated.

4) Upon receiving the DHCPREQUEST message, the selected external DHCPv4 server acknowledges the address allocation by sending a DHCPACK containing the lease period (T1), the time-out time (T2) and the configuration information requested in DHCPREQUEST. The SMF stores the allocated IPv4 address, the lease timers and the configuration parameters.

NOTE 2: The SMF will further deliver the IPv4 address and the configuration parameters to the UE by SM NAS message.



Figure 6.3.2.1-1: The signalling flow for IPv4 address allocation and parameter configuration using DHCPv4

Figure 6.3.2.1-2 is a signalling flow for IPv4 address lease renew by using DHCPv4 protocol as specified in IETF RFC 2131 [22].

1) The DHCPv4 client function in the SMF sends a unicast DHCPREQUEST towards the external DHCPv4 server to extend the lease period of the allocated IPv4 address.

2) The external DHCPv4 server replies with a DHCPACK message confirming the renewed lease and the T1 and T2 timers are restarted.



Figure 6.3.2.1-2: The signalling flow for IPv4 address lease renew using DHCPv4

#### 6.3.2.2 IPv6 Prefix allocation via IPv6 stateless address autoconfiguration via DHCPv6

When the IPv6 prefix is allocated from the external DN, the SMF is responsible to obtain the IPv6 prefix for external DN, allocate and release the IPv6 prefix. The SMF may use DHCPv6 to obtain the IPv6 prefix from the external DN. In this context, the SMF shall act as a DHCP client as per IETF RFC 3315 [21] towards the external DHCPv6 server.

The following system procedure describes the signalling flows for the IPv6 Stateless Address Autoconfiguration procedures for 5G system. The procedures are based on the descriptions in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3].

1. UE initiates the PDU Session Establishment procedure, indicating IPv6 address is required.

2. The AMF sends Session Management Request including the PDU Session Establishment Request to the SMF.

3. The SMF may retrieve IPv6 prefix using DHCPv6 mechanism. This procedure is performed when an external DN allocates an IPv6 prefix, the signaling between the SMF and external DN is exchanged via UPF which is omitted in the figure.

4. The SMF sends PDU Session Establishment Accept included in the Session Management Response to the AMF. It includes the IPv6 prefix.

5. The AMF sends PDU Session Establishment Accept message to the UE without the IPv6 prefix. The UE shall ignore the IPv6 prefix if it receives it in the message.

6. The UE may send a Router Solicitation to the SMF via the UPF to solicit a Router Advertisement message.

7. The SMF sends a Router Advertisement message to the UE via the UPF, solicited or unsolicited. It shall include an IPv6 prefix in Prefix Information option field of the message. The prefix is the same as the one in the PDU Session Establishment Accept message, if it is provided during the previous PDU Session Establishment procedure.



Figure 6.3.2.2-2: IPv6 Stateless Address Autoconfiguration

#### 6.3.2.3 IPv6 parameter configuration via stateless DHCPv6

A UE that has obtained an IPv6 address may use stateless DHCP to request other configuration information such as a list of DNS recursive name servers or SIP servers.

For 3GPP networks, when an external DHCPv6 server in a DN is used to obtain the requested parameters, the SMF acts as a DHCPv6 client towards the external DHCPv6 server while acting a DHCPv6 server towards the UE.

The IPv6 parameter configuration via stateless DHCPv6 function in the UE, the SMF and the external DHCPv6 Server shall be compliant to IETF RFC 3736 [20]. The following system procedure describes the signalling flows for the IPv6 parameter configuration via stateless DHCPv6 procedures for 5G system. All messages in the following steps between the UE and the SMF are sent via the UPF.

1) A Router Advertisement with the O-flag set, is sent from SMF to UE to indicate to it to retrieve other configuration information.

2) The UE sends an INFORMATION-REQUEST message with the IP destination address set to the All\_DHCP\_Relay\_Agents\_and\_Servers multicast address defined in the DHCPv6 IETF RFC 3315 [21]. The source address shall be the link-local address of the UE. The DHCP relay agent in the SMF shall forward the message.

3) DHCP servers receiving the forwarded INFORMATION-REQUEST message, reply by sending a RELAY‑REPLY message, with the "Relay Message" option including a REPLY message with the requested configuration parameters.

The UE chooses one of the possibly several REPLY messages and extracts the configuration information.



Figure 6.3.2.3-1: DHCPv6 Other configuration signal flow

#### 6.3.2.4 IP address/prefix allocation via Diameter or RADIUS

The SMF may also request the DN-AAA to allocate IPv4 address or IPv6 prefix by Diameter or RADIUS protocol within the Authentication and Authorization procedure as specified in 3GPP TS 29.061 [67] with the difference that the P-GW is replaced by the SMF (acting as the initiator requesting the IP address/prefix) and the UPF (transparently tranfering AAA messages between the SMF and DN-AAA).

### 6.3.3 IMS Interworking

#### 6.3.3.1 General

Interworking with the IP Multimedia Core Network Subsystem (IMS) puts specific requirements on the SMF.

The SMF shall use the following mechanisms to support the interworking with the IMS:

- the P-CSCF discovery; and

- N7 interface for the policy and charging control of QoS flows for IMS media flows.

Editor's note: Other mechanisms are FFS.

These mechanisms are however not restricted only to the interworking with the IMS and may be used for other services that could benefit from these mechanisms.

#### 6.3.3.2 IMS Interworking Model

The signalling interface between the UE and the P-CSCF is a logical interface, i.e. it uses 5GC as a QoS flow. The Npcf\_SMPolicyControl services, offered via N7 interface, are used for network communication between the SMF and the PCF. For a description of the IMS architecture, refer to 3GPP TS 23.228 [25].

#### 6.3.3.3 IMS Specific Configuration in the SMF

The SMF shall have a list of preconfigured addresses of signalling servers (the P-CSCF servers). This list shall be provided to the UE at PDU session establishment. It shall be possible to preconfigure the list of preconfigured addresses of signalling servers per DNN.

The SMF/UPF may have the locally preconfigured packet filters, and/or the applicable PCC rules, to be applied on the QoS flow. The packet filters shall filter up-link and down-link packets, and shall only allow traffic to/from the signalling servers and to the DNS and the DHCP servers. It shall be possible to locally preconfigure the packet filters per DNN.

It shall be possible to enable/disable the use of the services offered via N7 interface per DNN.

The SMF shall support IPv4 or IPv6 addresses and protocol for IMS signalling and IMS QoS flows.

The methods for the UE to discover the P-CSCF address(es) may vary depending on the access technology that the UE is on. The details of the P-CSCF discovery mechanisms for various accesses are specified in 3GPP TS 23.228 [25] and 3GPP TS 24.229 [26]. The P-CSCF discovery mechanisms are:

- a 5GC procedure for the P-CSCF discovery;

- via DHCP servers i.e. the SMF shall provide the functionality of a DHCP relay agent; and

- if the UE has a P-CSCF FQDN locally configured and request the DNS IP address(es) from the SMF (via 5GC mechanism or DHCP procedures), the SMF shall be able to provide DNS IP address(es) to the UE.

Editor's note: Details for the 5GC discovery and the UE provisioning need to be specified by SA2.

The SMF shall have similar functional support depending on the P-CSCF discovery methods supported by the UE on the access technology. For example, for the UE in 3GPP 5G access network the SMF shall have DHCP server function towards the UE while acting as a DHCP client towards external DHCP server, if the SMF is configured to request DNS and/or P-CSCF IP addresses from the external DHCP servers.

The SMF shall be able to deliver DNS and/or P-CSCF addresses to the UE if requested by the UE via the 5G network or via DHCP procedures using the relevant DHCP options for IPv4/IPv6 DNS and SIP servers (see IETF RFC 2132 [27], IETF RFC 3361 [28], IETF RFC 3646 [29] and IETF RFC 3319 [30]).

On DNNs providing IMS services, the information advertised in Router Advertisements from the SMF to the UEs shall be configured in the same manner as for other DNNs providing IPv6 services except that the "O‑flag" shall be set.

The "O-flag" shall be set in IPv6 Router Advertisement messages sent by the SMF for DNNs used for IMS services. This will trigger a DHCP capable UE to start a DHCPv6 session to retrieve server addresses and other configuration parameters. The UE which doesn't support DHCP shall ignore the "O-flag" and shall request the IMS specific configuration (e.g. the P-CSCF address) via other discovery methods supported in the UE (i.e. via locally configured P-CSCF address/FQDN in the UE or via 5G procedure, if applicable).

Editor's note: Whether this mechanism as defined in EPC remains for 5G is FFS.

The SMF shall have configurable policy rules for controlling QoS flows used for signalling.

#### 6.3.3.4 IMS Specific Procedures in the SMF

##### 6.3.3.4.1 Provisioning of Signalling Server Address

At a PDU Session establishment procedure related to the IMS, the SMF shall support the capability to send the P-CSCF address(es) to the UE. The P-CSCF address information is sent by the visited SMF if LBO is used. For Home routed, the P-CSCF address information is sent by the SMF in the HPLMN. The P-CSCF address(es) shall be sent transparently through the AMF, and in case of Home Routed also through the SMF in the VPLMN.

NOTE 1: The SMF is located in the VPLMN if LBO is used.

NOTE 2: Other options to provide the P-CSCF address(es) to the UE as defined in 3GPP TS 23.228 [25] is not excluded.

NOTE 3: A PDU session for IMS is identified by "APN" or "DNN".

### 6.3.4 Unstructured PDU type data transferring over N6

#### 6.3.4.1 General

When support of unstructured PDU type data is provided at the N6 interface, different Point-to-Point (PtP) tunnelling techniques may be used. When using PtP tunnelling by UDP/IPv6 encapsulation subclause 6.3.4.2 below shall be followed. Other techniques as described in clause 6.3.4.3 below may be used.

#### 6.3.4.2 N6 PtP tunnelling based on UDP/IPv6

N6 PtP tunnelling based on UDP/IPv6 may be used to deliver unstructured PDU type data to an AS.

IP address allocation procedures for the UE (i.e. PDU session) are performed by the SMF as described in subclause 6.3.2, but the IPv6 prefix is not provided to the UE, i.e. Router Advertisements and DHCPv6 are not performed. The SMF assigns a suffix (i.e. IPv6 Interface Identifier) for the PDU session. For the N6 PtP tunnel, the IPv6 prefix allocated for the PDU session plus suffix assigned for the PtP tunnel is used as source address for the uplink data and as destination address for the downlink data.

During the PDU session establishment, the UPF associates the AN tunnel for the PDU session with the N6 PtP tunnel.

The UPF acts as a transparent forwarding node between the UE and the destination in the external DN.

For uplink delivery, if the uplink data is received the UPF shall forward the received data to the external DN over the N6 PtP tunnel associated with the AN tunnel with the destination address in the external DN and the 3GPP defined UDP destination port number for unstructured PDU type data.

For downlink delivery, the external DN shall send the data using UDP/IP encapsulation with the IPv6 prefix plus suffix as destination address and the 3GPP defined UDP destination port number for unstructured PDU type data.

NOTE: The UPF decapsulates the received data (i.e. removes the UDP/IP headers) and forwards the data to AN on the AN tunnel identified by the IPv6 prefix of the UE (i.e. PDU session) for delivery to the UE.



Figure 6.3.4.2-1: Protocol configuration for unstructured PDU type data (user plane) using N6 PtP tunneling

#### 6.3.4.3 Other N6 PtP tunnelling mechanisms

N6 PtP tunnelling mechanisms such as PMIPv6/GRE, L2TP, etc, may be used to deliver unstructured PDU type data to/from AS. The general handling of such delivery mechanisms is as described below.

A PtP tunnel is established by the UPF towards the AS. Depending on the type of protocol employed on the N6 PtP tunnel, the N6 PtP tunnel setup may be done at the time of UE Registration or at the time of first MO datagram being sent by the UE. The UPF selects the AS based on its configuration (e.g. per DNN, or per PtP tunnel type, etc). However, IP address allocation procedures for the UE (according to subclause 6.3.2) are not performed by the SMF.

NOTE: An AS can be dedicated for handling a specific protocol for unstructured PDU type data.

The UPF acts as a transparent forwarding node between the UE and the AS.

For uplink delivery, the UPF forwards the received data to the AS over the established N6 PtP tunnel.

For downlink delivery, the AS locates the right N6 PtP tunnel for the UE (using information such as UE identifiers in the unstructured PDU type protocol itself, etc) to forward the data. The AS sends the data to UPF over the established N6 PtP tunnel. The UPF in turn sends the data on the GTP-U tunnel identified by the associated N6 PtP tunnel for delivery to the UE.

## 6.4 Network Function Service Procedures

## 6.5 Protocols

For 5G network interworking with external DNs, existing protocols in widespread usage in existing DNs (i.e. IP, DHCP, RADIUS and Diameter) as specified in 3GPP TS 29.061 [67] are applicable between the SMF/UPF and the external DNs. The UPF transparently relays the message exchanged between the SMF and the node (e.g. AAA server) of the external DNs.

# 7 Network capability exposure aspects of the 5G system

## 7.1 Reference Model



Figure 7.1-1: 3GPP Architecture for Network Exposure



Figure 7.1-2: 3GPP roaming Architecture for Network Exposure

Editor's note: The overall architecture is assumed to inherit the corresponding one in 3GPP TS 23.682 [58] with service based interface representations and may be subject to change according to 3GPP TS 23.501 [2].

Editor's note: Whether Nnef service is also applicable for south bound interface is FFS (e.g. PFD GET service).

## 7.2 Functional entities

### 7.2.1 NEF

The Network Exposure Function (NEF) supports the following functionality:

- It provides a means to securely expose the services and capabilities provided by 3GPP network functions. The NEF may authenticate, authorize and throttle the Application Functions. In addition, it provides a means for the Application Functions to securely provide information to 3GPP network, e.g. Mobility Pattern, communication pattern.

- It translates between information exchanged with the AF and information exchanged with the internal network function. For example, it translates between an AF-Service-Identifier and internal 5G Core information such as DNN, S-NSSAI, as described in clause 5.6.7 of 3GPP TS 23.501 [2].

- It receives information from other network functions (based on exposed capabilities of other network functions). It may act as a Front End (i.e. NEF-FE) to a Unified Data Repository (UDR) to store the received information as structured data. The stored information can be accessed and "re-exposed" by the NEF to other network functions and Application Functions, and used for other purposes such as analytics.

NOTE: The NEF can access the UDR located in the same PLMN.

Editor's note: It is FFS whether the stored information in the UDR can be exposed directly to other network functions and Application Functions.

### 7.2.2 AF

The Application Function (AF) may interact with the 3GPP Core Network via the NEF in order to access Network Capability Exposure.

If allowed by the operator, the AF may also communicate with the PCF directly.

NOTE: An AS can act as an AF to interact with the NEF.

## 7.3 System Procedures

### 7.3.1 Procedures for network external capability exposure

#### 7.3.1.1 General

The NEF supports external exposure of capabilities of network functions. External exposure can be categorized as follows:

- Monitoring capability: it is for monitoring of specific event for UE in 5G system and making such monitoring events information available for external exposure via the NEF.

- Provisioning capability: it is for allowing external party to provision of information which can be used for the UE in 5G system.

- Policy/Charging capability: it is for handling QoS and charging policy for the UE based on the request from external party.

#### 7.3.1.2 Procedures for event monitoring

##### 7.3.1.2.1 General

The NEF will be in charge to configure/delete the monitoring events in the corresponding NF and report the corresponding monitoring events within the 5GC. It shall support the following events for Event Exposure function as specified in table 7.3.1.2.1-1.

Table 7.3.1.2.1-1: List of events for Event Exposure function

|  |  |  |
| --- | --- | --- |
| Event | Description | Event reporting entity |
| LOSS OF CONNECTIVITY | The AS requests to be notified when the 3GPP network detects that the UE is no longer reachable for signalling or user plane communication. | AMF |
| UE REACHABILITY | The AS requests to be notified when the UE becomes reachable for sending either SMS or downlink data to the UE. | AMF (reachability for data)  UDM (reachability for SMS) |
| LOCATION REPORTING | The AS requests to be notified of the current location or the last known location of the UE. (NOTE 1) | AMF |
| CHANGE OF IMSI IMEI ASSOCIATION | The AS requests to be notified when the association of an ME (IMEI(SV)) that uses a specific subscription (IMSI) is changed | UDM |
| ROAMING STATUS | The AS queries the UE's current roaming status and requests to get notified when the status changes. (NOTE 2) | UDM |
| COMMUNICATION FAILURE | The AS requests to be notified of communication failure events | AMF |
| AVAILABILITY AFTER DDN FAILURE | The AS requests to be notified when the UE has become available after a DL data delivery failure. | AMF |
| NUMBER OF UES PRESENT IN A GEOGRAPHICAL AREA | The AS requests to know how many UEs are in the requested area (last known or current location). | AMF |
| NOTE 1: Location granularity for event request, or event report, or both could be at cell level (Cell ID), TA level or other formats e.g. shapes (e.g. polygons, circles, etc.) or civic addresses (e.g. streets, districts, etc.) which can be mapped by NEF.  NOTE 2: Roaming status means whether the UE is in HPLMN or VPLMN. | | |

Editor's note: Events configuration via the PCF and event reporting by the PCF are FFS.

Editor's note: Whether more events are needed is FFS.

All the identified Monitoring Event Types in previous table (except for the monitoring of the number of UEs present in a geographical area) relate to events on a UE basis for which the configuration of monitoring events is done via the UDM. The UDM may further configure some monitoring events in the AMF depending on the event type and/or event reporting entity. For the monitoring of the number of UEs present in a geographical area, the monitoring event configuration is done via the AMF directly. When the configured event happens, the event reporting NF sends the report directly to the NEF.

##### 7.3.1.2.2 Event Exposure subscription

###### 7.3.1.2.2.1 Event Exposure subscription without NEF pre-subscription



Figure 7.3.1.2.2.1-1: Event Exposure subscription without NEF pre-subcription

1. The AS subscribes to one or several event(s) (identified by Event Id) by Nnef\_EventExposure\_subs service. Reporting options defines the type of reporting requested (e.g. periodic reporting or event based reporting, for Monitoring Events). If the reporting event subscription is authorized by the NEF, the NEF records the association of the event trigger and the requester identity.

2. The NEF subscribes to received event(s) to other NF (e.g. UDM).

3. The NEF acknowledges the event subscription request.

###### 7.3.1.2.2.2 Event Exposure subscription with NEF pre-subscription

The NEF may subscribe to all the NFs that provided the necessary services for one UE, a group of UEs or all of the UEs.



Figure 7.3.1.2.2.2-1: Event Exposure subscription with NEF pre-subcription

1. The NEF subscribes to the serving NF(s) (e.g. AMF) to be notified of the detected event including indication identifying for one UE, a group of UEs or for all of the UEs.

2. Step 1 in subclause 7.3.1.2.2.1.

3. The NEF acknowledges the event subscription request.

##### 7.3.1.2.3 Event Exposure notification



Figure 7.3.1.2.3-1: NEF Event Exposure notification

1. The NF detects the occurred event and sends the event notification to the NEF, which has subscribed to the event before.

2. The NEF further forwards to the AS the reporting event received by Nnef\_EventExposure\_notif service.

3. The AS acknowledges the event notification request.

#### 7.3.1.3 Procedures for PFD management

Editor's note: The procedures are FFS.

#### 7.3.1.4 Procedures for Background Data Transfer Policy management and activation

Editor's note: The procedures are FFS.

### 7.3.2 Procedures for network internal exposure

The NEF may subscribe to the status change of mobility, session, and/or policy data and may store the received data in the UDR if the NEF acts as a Front End. Such data may be exposed to the AF and other NF (e.g. NWDAF), and used for further data process.



Figure 7.3.2-1: Network internal exposure

1. The NEF subscribes to received event(s) to another NF (e.g. AMF).

2. If the event subscription response includes event data, the NEF may store it in the UDR.

3. The NF detects the occurred event and sends the event notification to the NEF, which has subscribed to the event before.

4. The NEF may store the received event data in the UDR.

### 7.3.3 Procedures for Application Trigger

The NEF provides a service for the AS to trigger an application level operation. The application payload is used to instruct the UE a procedure to be executed (e.g. PDU session establishment).



Figure 7.3.3-1: Application Trigger procedure

1. The NEF receives a Nnef\_ApplicationTrigger service request with External Identifier or MSISDN, AS Identifier, validity period, Application Port ID and trigger payload. The Application Port ID is used to identify the receiving application within the UE. The validity period indicates for how long the trigger message is valid. If the trigger message does not reach the UE for the first time (e.g. the UE is temporarily not reachable), the NEF may try to resend the trigger message if it is still valid.

2. The NEF checks whether the AS is authorised to send the Application Trigger based on the AS Identifier. The NEF also check whether the AS has exceeded its quota or rate of trigger submission.

3. The NEF invokes the service provided by the UDM to determine the node (e.g. MSC) which serves the UE and also to get the SUPI of the UE.

4. The NEF sends the Application Trigger to the SMS-C as defined in 3GPP TS 23.040 [73].

5. The NEF sends the Nnef\_ApplicationTrigger response to the AS with trigger result.

Editor's note: Whether the NEF is integrated with MTC-IWF in 5G is FFS.

Editor's note: Nnef\_ApplicationTrigger service needs to be defined by stage 2.

Editor's note: It is FFS that whether a separate service operation for Application Trigger delivery report is needed.

## 7.4 Network Function Service Procedures

### 7.4.1 General

The external exposure network exposes the 3GPP network capabilities to the application consumers via NEF by providing a set of NEF service operations. The following NF services are specified for NEF:

Table 5.4-1: NF Services provided by NEF

| Service Name | Description | Reference | Example Consumer | Mechanism |
| --- | --- | --- | --- | --- |
| Nnef\_ApplicationTrigger | Provides the service of application trigger to the Requester. | 7.4.2 | AS | Request-Response |
| Nnef\_EventExposure | Provides the service of subscribing/unsubscribing/notifying Event Exposure. | 7.4.3 | AS | Subscribe-Notify |

Editor's note: The current NEF services are not stable and could be updated as described in stage 2.

### 7.4.2 Nnef\_ApplicationTrigger service

#### 7.4.2.1 General

This service provides an application level trigger payload towards a UE, in order to trigger the application specific procedure, e.g. start immediate or later communication with the AS by establishing a PDU session if it was not established. The application trigger also includes information for routing the trigger payload to the application in the UE and routing the response of the application back to the Application Server.

#### 7.4.2.2 Operations

Table 7.4.2.2-1: Stage 2 requirements for Operations of the Nnef\_ApplicationTrigger service

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Service Operations | Initiated by | Description | Input (required) | Input (optional) | Output (required) | Output (optional) |
| Request | NF service consumer (AS) | Request to start an application trigger with application specific payload. | UE ID (External Identifier or MSISDN), AS Identifier, validity period, Application Port ID and Trigger Payload. | none | The result of the trigger | none |

### 7.4.3 Nnef\_EventExposure service

#### 7.4.3.1 General

This service provides event exposure towards consumer NF. The service operations exposed by this service allow other NFs to subscribe/unsubscribe and get notified of the subscribed events. The following are the key functionalities of this NF service.

- Allow consumer NFs to Subscribe and unsubscribe for exposure events; and

- Notifying exposure events to the subscribed NFs.

Refer to subclause 7.3.1.2 for the types of events for which a subscription can be made.

#### 7.4.3.2 Operations

Table 7.4.3.2-1: Stage 2 requirements for Operations of the Nnef\_EventExposure service

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Service Operations | Initiated by | Description | Input (required) | Input (optional) | Output (required) | Output (optional) |
| Notify | NEF | Report exposure event(s) to the NF which has subscribed to the event report service. | UE ID (e.g. SUPI or IP address), UE Group ID, Event Trigger, Event correlation ID | none | The consumer is notified of the events it subscribed to | none |
| Subscribe | consumer (AS) | This service operation is used by an NF to subscribe for event notifications. | NF ID, UE ID (e.g. SUPI or IP address), UE Group ID, Event correlation ID, Event filter, event notification method (periodic, one time, on event detection) | none | none | none |
| Unsubscribe | consumer (AS) | This service operation is used by an NF to unsubscribe for event notifications. | NF ID, UE ID (e.g. SUPI or IP address), UE Group ID, Event correlation ID, Event filter, event notification method (periodic, one time, on event detection) | none | none | none |

Editor's note: Other input/output parameters are FFS.

## 7.5 Protocols

### 7.5.1 Evaluation of candidate protocols for service based interfaces

Candidate protocols, serialization protocols, transport protocols, protocol designs and Interface Definition Languages are described in subclauses under subclause 5.5. See the evaluation in subclause 5.5.6 with additional considerations provided in the present subclause (if any).

# 8 Conclusions and Recommendations

## 8.1 5G Policy Framework

### 8.1.1 Protocol solution for Service Based Interfaces

Based on the protocol solutions and evaluations described in subclause 5.5.6, HTTP is preferred for the following reasons:

- allows to design the 5G Service Based Architecture using cloud-native and Web technologies:

a) HTTP based APIs are cloud-friendly, easy to deploy and open;

b) largest user community for Web services. Rich landscape of frameworks, tools and software;

c) HTTP is native to service based architecture;

- use of HTTP is future proof as it is used in large non-telecom ecosystem;

- eases and speeds deployment and continuous integration/delivery of new or upgraded network functions and services;

- eases use of operator owned application functions and interworking with third parties' applications:

a) largest user community for Web services;

b) already supported by some operator owned application functions (e.g. MEC);

c) HTTP REST APIs are supported on northbound NEF interfaces.

It is concluded to standardize the following protocol solution for the Service Based Interfaces under CT3 responsibility identified in subclause 5.5.

- protocol: HTTP/2 (see IETF RFC 7540 [7] and IETF RFC 7541 [59]), as specified in subclause 5.5.1.1.9.1;

- transport: TCP (see IETF RFC 793 [5]);

- serialization protocol: JSON (see IETF RFC 7159 [8]);

- API design style: apply a RESTful framework for the protocol design whenever possible and use custom methods otherwise, as specified in subclause 5.5.2.6;

- support of notification with two HTTP client-server pairs, as specified in subclause 5.5.1.1.9.2;

- Interface Definition Language: OpenAPI Specification, version 3.0.0; each interface will be specified by textual and/or tabular format description in the main body of the Technical Specification and by an OpenAPI specification file in a normative annex, as specified in subclause 5.5.5.

HTTP/2 over QUIC/UDP (see IETF draft-ietf-quic-transport [10]), and other binary encoding alternatives such as CBOR, are regarded as a potential evolution in a later release for enhanced performances and may be subject to further studies and contributions following the normal 3GPP working procedures.

## 8.2 Interworking between the 5G System and external Data Networks (DN)

### 8.2.1 Protocol solution for interworking with external DN

For 5G network interworking with external DNs, based on investigation result in subclause 6.5, IP, DHCP, RADIUS and Diameter protocols as specified in 3GPP TS 29.061 [67] are still applicable between the SMF/UPF and the external DNs with possible adaptation.

## 8.3 Network capability exposure aspects of the 5G system

### 8.3.1 Protocol solution for Service Based Interfaces

The conclusions in subclause 8.1.1 also apply for the Service Based Interfaces under CT3 responsibility identified in subclause 7.5.1 with the following differences:

- protocol: HTTP/1,1 as specified in IETF RFC 7230 [54], IETF RFC 7231 [60], IETF RFC 7232 [61], IETF RFC 7233 [62], IETF RFC 7234 [63] and IETF RFC 7235 [64] is mandatory to support and HTTP/2 (see IETF RFC 7540 [7] and IETF RFC 7541 [59]) is recommended to support.

Annex A:  
Impacts to Specifications

# A.1 New specifications

Table A.1-1 identifies the new specifications that are required to define the CT3 aspects of the 5G System.

Table A.1-1: New specifications for the CT3 aspects of the 5G System

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Series | Title | | Scope |
| TS | 29.507 | 5G System; Access and Mobility Policy Control Service; Stage 3 | | PCF service related to Access and Mobility Policy Control; Stage 3:  includes services supported over N15, N24 (offered by H-PCF). |
| TS | 29.508 | 5G System; Session Management Event Exposure Service; Stage 3 | | Stage 3 details of SM Event Exposure Service |
| TS | 29.512 | 5G System; Session Management Policy Control Service; Stage 3 | | PCF service related to Session Management Policy Control; Stage 3:  includes services supported over N7 interface. |
| TS | 29.514 | 5G System; Policy Authorization Service; Stage 3 | | PCF service related to application policy control; Stage 3:  includes services supported over N5, PNt |
| TS | 29.513 | 5G System; Policy and Charging Control signalling flows and QoS parameter mapping; Stage 3 | | Technical Realization of PCC Service Based Architecture. Includes (to be updated with SA2 progress):  Signalling flows over PCC interfaces  \* includes SBI and p2p defined interfaces  QoS parameter mapping  Binding mechanisms  PCF discovery and selection  Race conditions specifics for PCC. |
| TS | 29.520 | 5G System; Network Data Analytics Services; Stage 3 | | NWDAF services; Stage 3:  includes services supported over N23 |
| TS | 29.594 | 5G System; Spending Limit Control Service; Stage 3 | | Charging Function functionality related to spending limit reporting; Stage 3 |
| TS | 29.561 | 5G System; Interworking between 5G Network and external Data Networks; Stage 3 | | N6 reference point; Stage 3 |
| TS | 29.522 | 5G System; Network Exposure Function Northbound APIs; Stage 3 | | Northbound external capability exposure; Stage 3,  List and reference reused APIs defined in 3GPP TS 29.122. Define nothbound APIs only applicable for 5G. Procedural description of the interactions of the northbound APIs with southbound 5G interfaces. |
| TS | 29.551 | 5G System; Packet Flow Description Management Service; Stage 3 | | Stage 3 details for Sponsored Data Connectivity Service - FFS |
| TS | 29.519 | 5G System; Usage of the Unified Data Repository service for Policy Data, Application Data and Structured Data for exposure; Stage 3 | | Stage 3 details of the usage of the UDR service for Policy Data, Application Data and Structured Data for exposure including data model definition and call flows. |
| TS | 29.521 | 5G System; Binding Support Management Service; Stage 3 | Stage 3 for Binding Support Management Service | |
| TS | 29.554 | 5G System; Background Data Transfer Policy Control Service; Stage 3 | Stage 3 for Background Data Transfer Policy Control Service. | |

# A.2 Impacted existing specifications

Table A.2-1 identifies the impacted existing specifications that are required to define the CT3 aspects of the 5G System.

Table A.2-1: Impacted existing specifications for the CT3 aspects of the 5G System

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Series | Title | Brief description of the impacts |
| TS | 29.213 | Policy and charging Control signalling flows and Quality of Service (QoS) parameter mapping | Possible impacts for Rx interactions |
| TS | 29.214 | Policy and Charging Control over Rx reference point | Possible impacts to support 5G access |
| TS | 29.219 | Policy and charging control: Spending limit reporting over Sy reference point. FFS | Possible impacts to support spending limit report in 5G. FFS |
| TS | 29.122 | T8 reference point for Northbound APIs | Impacts for service exposure interfaces in 5G: Updates to the scope and possible minor updates to existing APIs due to 5G requirements. |

Annex B:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2017-03 | CT#75 | CP-170238 |  |  |  | TR Skeleton | 0.0.0 |
| 2017-04 | CT3#89 | C3-172282 |  |  |  | Inclusion of documents agreed in CT3#89: C3-172169, C3-172273, C3-172277, C3-172252, C3-172264 & C3-172265 | 0.1.0 |
| 2017-05 | CT3#90 | C3-173340 |  |  |  | Inclusion of documents agreed in CT3#90: C3-173317, C3-173209, C3-173211, C3-173208, C3-173212, C3-173300, C3-173206, C3-173213, C3-173283, C3-173301, C3-173207, C3-173214, C3-173216, C3-173217, C3-173218, C3-173284, C3-173285, C3-173210, C3-173286, C3-173302. | 0.2.0 |
| 2017-09 | CT3#91 | C3-174388 |  |  |  | Inclusion of documents agreed in CT3#91: C3-174065, C3-174066, C3-174067, C3-174068,  C3-174202, C3-174206, C3-174208, C3-174209,  C3-174214, C3-174215, C3-174233, C3-174235,  C3-174238, C3-174239, C3-174240, C3-174246,  C3-174247, C3-174249, C3-174253, C3-174317,  C3-174318, C3-174319, C3-174320, C3-174321,  C3-174322, C3-174323, C3-174324, C3-174326,  C3-174327, C3-174350, C3-174363, C3-174364,  C3-174381, C3-174382, C3-174383. | 0.3.0 |
| 2017-09 | CT#77 | CP-172056 |  |  |  | Presentation of TR to plenary for information | 1.0.0 |
| 2017-09 | CT#77 | CP-172125 |  |  |  | Added C3-174346 agreed in CT3#91. | 1.0.1 |
| 2017-11 | CT3#92 | C3-175373 |  |  |  | Inclusion of documents agreed in CT3#92: C3-175033, C3-175034, C3-175039, C3-175063,  C3-175065, C3-175113, C3-175145, C3-175175,  C3-175176, C3-175177, C3-175199, C3-175200,  C3-175203, C3-175206, C3-175208, C3-175213,  C3-175216, C3-175243, C3-175298, C3-175308,  C3-175309, C3-175311, C3-175312, C3-175315,  C3-175316, C3-175320, C3-175321, C3-175340,  C3-175341, C3-175343, C3-175344, C3-175349,  C3-175350, C3-175351, C3-175361, C3-175363,  C3-175367, C3-175371. | 1.1.0 |
| 2017-12 | CT3#93 | C3-176393 |  |  |  | Inclusion of documents agreed in CT3#93: C3-176180, C3-176182, C3-176296, C3-176184,  C3-176297, C3-176344, C3-176345, C3-176188,  C3-176346, C3-176192, C3-176302, C3-176303,  C3-176304, C3-176347, C3-176348, C3-176198,  C3-176197, C3-176349, C3-176307, C3-176308,  C3-176201, C3-176389, C3-176207, C3-176106,  C3-176352, C3-176311, C3-176204, C3-176208,  C3-176331, C3-176210, C3-176211, C3-176213,  C3-176100, C3-176353. | 1.2.0 |
| 2017-12 | CT#78 | CP-173107 |  |  |  | TS sent for approval to plenary | 2.0.0 |
| 2017-12 | CT#78 | CP-173107 |  |  |  | TS approved by plenary | 15.0.0 |
| 2018-03 | CT#79 | CP-180036 | 0002 |  | B | Comparison of Encoding Proposals for Npcf\_PolicyAuthorization service and selection of Encoding Proposal 1. | 15.1.0 |
| 2018-03 | CT#79 | CP-180036 | 0003 | 1 | C | Using HTTP POST to create resources for the Npcf\_SMPolicyControl Service. | 15.1.0 |
| 2018-03 | CT#79 | CP-180036 | 0004 | 1 | B | Comparison of Encoding Proposals for Npcf\_SMPolicyControl Service and selection of Encoding Proposal. | 15.1.0 |
| 2018-03 | CT#79 | CP-180036 | 0005 | 1 | C | Using HTTP POST to create resources for the Npcf\_AMPolicyControl Service. | 15.1.0 |
| 2018-03 | CT#79 | CP-180036 | 0006 | 1 | B | Comparison of Encoding Proposals for Npcf\_AMPolicyControl Service and selection of Encoding Proposal. | 15.1.0 |
| 2018-03 | CT#79 | CP-180036 | 0007 | 1 | B | Reuse of TS 29.221 APIs. | 15.1.0 |
| 2018-03 | CT#79 | CP-180036 | 0008 | 1 | B | Confirmation that TS for the interace charging function is required. | 15.1.0 |
| 2018-06 | CT#80 | CP-181012 | 0009 | - | F | Updates on new specifications | 15.2.0 |
| 2018-06 | CT#80 | CP-181012 | 0010 | - | B | Comparison of Encoding Proposals for Npcf\_AMPolicyControl Service and selection of Encoding Proposa | 15.2.0 |
| 2020-07 | SA#88e | - | - | - | - | Update to Rel-16 version (MCC) | 16.0.0 |