

Operator Platform: Requirements for Network as a Service

Version 1.0

09 May 2025

Security Classification: Non-Confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2025 GSM Association

Disclaimer

The GSMA makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction 4
1.1 Overview 4
1.1.1 Relationship to existing standards 4
1.2 Scope and Objectives 4
1.3 Definitions 4
1.4 Abbreviations 5
1.5 References 6
1.6 Conventions 7
2 Use Cases 7
3 High-level Requirements for OP to support NaaS services 7
3.1 Functionality offered to OP Ecosystem Party 7
3.1.1 Functionality offered to Application Providers 7
3.1.2 Functionality offered to Aggregators 7
3.1.3 Functionality offered to End-Users/Devices 7
3.1.4 Functionality offered to Operators 8
3.1.5 Functionality offered to other OPs 8
3.2 Network as a Service enabling requirements 8
3.2.1 High-Level requirements 8
3.2.2 Capability Management requirements 8
3.2.3 Service-Specific Requirements 9
3.2.4 Privacy Requirements 10
3.2.5 Mobility Requirements 10
3.3 Security Requirements 10
4 Deployment Scenario using OP Architecture 10
5 Interface Requirements for Enabling NaaS Services 10
5.1 Northbound Interface (NBI) 10
5.1.1 High-level requirements 10
5.1.2 Management Profile 10
5.1.3 Network Capability Exposure Support on the NBI 11
5.1.4 Network Communication Service lifecycle and end user profile 12
5.2 East/Westbound Interface (E/WBI) 12
5.2.1 Application Management 12
5.3 Southbound Interfaces (SBIs) 12
5.3.1 Southbound Interface – Charging Function (SBI-CHF) 12
5.3.2 Southbound Interface – Network Resources (SBI-NR) 12
5.3.3 Southbound Interface – Operation & Maintenance 13
5.3.4 Southbound Interface – Privacy Management (SBI-PrM) 14
6 Requirements on Functional Elements for Enabling NaaS Services 14
6.1 Exposure Functions 14
6.1.1 Exemplary scenarios for Exposure Functions related to NaaS 14
6.2 Federation Functions 14
6.2.1 Exemplary scenarios for Federation Functions related to NaaS 15

6.3 Transformation Functions 15
6.3.1 Exemplary scenarios for Transformation Functions related to NaaS 15
6.4 Integration Functions 15
6.4.1 Network Slice provisioning for an end user 15
Annex A Client-side mechanisms to control QoS 16
A.1 Introduction 16
A.2 URSP traffic categories 16
A.3 L4S 17
A.4 Other mechanisms 18
Annex B Network Communication Service as a Service (NCSaaS) realised with NSaaS 18
B.1 Network Slice lifecycle management 21
B.2 Roaming 22
B.3 Federation 22
B.4 Security 25
B.5 Charging 26
B.6 Provisioning for end user 27
Annex C Document Management 28
C.1 Document History 28
C.2 Other Information 28

1 Introduction

1.1 Overview

The following document details the requirements for exposing network-related Operator Capabilities using the Operator Platform (OP) architecture defined in GSMA PRD OPG.02 [1]. The document utilises the OP architecture and its interfaces [1] to emphasise the delivery of services based on the capabilities of the core network as well as those relying on data and capabilities of other systems in the Operator network (such as the Operation and Business Support Systems).

The requirements for most services will be similar and their realisation may partly rely on proprietary implementations that are specific to each network and realisation is provided already in documents such as GSMA PRD OPG.09 [12] and GSMA PRD OPG.10 [13]. Therefore, this document does not go into specific services and use cases for the more basic scenarios, but instead focusses on the overall approach and on the requirements for delivering more complex services such as Network Communication Service as a Service and how those can be offered within the architecture defined in GSMA PRD OPG.02 [1].

1.1.1 Relationship to existing standards

1.1.1.1 3GPP

Unless otherwise stated, the requirements listed in this document are based on the open and published 3GPP specifications listed in Section 1.5. 3GPP Release 17 is taken as the basis.

1.2 Scope and Objectives

This document outlines the requirements for delivering network-related Operator Capabilities within the OP framework that guide the entire industry ecosystem to define a common solution for exposing network capabilities.

This document covers the following areas:

- Requirements for Operator Platform-based service exposure
    - **Exposure of Network capabilities**: The PRD should define network services integration for the Application Providers, whether within enterprises or independent third parties, to enable a simple and universal way of interacting with networks.

Focusing on network capability exposure, this document provides requirements to enable an end-to-end delivery chain for different services using the architecture defined for the Operator Platform in GSMA PRD OPG.02 [1].

The use-cases covered by the OP concept demonstrate the benefits that access to network capabilities provides, such as low latency interactions between user and application, reduction of network bandwidth.

1.3 Definitions

The definitions provided in GSMA PRD OPG.02 [1] apply to this document.

Term	Description
Communication Service Customer	an entity that uses Communication Services, e.g. enterprise customer, Application Provider

1.4 Abbreviations

Term	Description
3GPP	Third Generation Partnership Project
5G	5th Generation Mobile Network
API	Application Programming Interface
AR	Augmented Reality
CCS	Converged Charging System
CEF	Charging Enablement Function
CHF	Charging Function
CRUD	Create, Read, Update and Delete
CSC	Communication Service Customer
CSP	Communication Service Provider
CTF	Charging Trigger Function
DNN	Data Network Name
DSCP	Differentiated Services Code Point
ECN	Explicit Congestion Notification
EGMF	Exposure Governance Management Function
E/WBI	East/Westbound Interface
eMBB	Enhanced Mobile Broadband
GST	Generic network Slice Template
ID	IDentifier
IETF	Internet Engineering Task Force
IP	Internet Protocol
KPI	Key Performance Indicator
L4S	Low Latency, Low Loss, Scalable Throughput
NBI	Northbound Interface
NCaaS	Network Communication Service as a Service
NEF	Network Exposure Function
NEST	NEtwork Slice Type
NSaaS	Network Slice as a Service
NSI	Network Slice Instance
NSMF	Network Slicing Management Function
NWDAF	Network Data Analytics Function
OP	Operator Platform
PCF	Policy Control Function

Term	Description
PCRF	Policy and Charging Rules Function
PDU	Protocol Data Unit
PRD	(GSMA) Permanent Reference Document
PrM	Privacy Management
QoS	Quality of Service
SBI	Southbound Interface
SBI-CR	Southbound Interface – Cloud Resources
SBI-NR	Southbound Interface – Network Resources
SD	Slice Differentiator
SLA	Service Level Agreement
S-NSSAI	Single Network Slice Selection Assistance Information
SST	Slice/Service Type
UE	User Equipment
URSP	UE Route Selection Policy
VR	Virtual Reality

1.5 References

Ref	Doc Number	Title
[1]	GSMA PRD OPG.02	Operator Platform: Requirements and Architecture
[2]	3GPP TS 23.501	System architecture for the 5G System (5GS) https://www.3gpp.org/DynaReport/23501.htm
[3]	3GPP TS 23.502	Procedures for the 5G System (5GS) https://www.3gpp.org/DynaReport/23502.htm
[4]	GSMA PRD NG.116	Generic Network Slice Template
[5]	GSMA PRD NG.135	E2E Network Slicing Requirements
[6]	3GPP TS 28.530	Management and orchestration; Concepts, use cases and requirements https://www.3gpp.org/DynaReport/28530.htm
[7]	3GPP TS 28.201	Charging management;Network slice performance and analytics charging in the 5G System (5GS);Stage 2 https://www.3gpp.org/DynaReport/28201.htm
[8]	3GPP TS 28.202	Charging management;Network slice management charging in the 5G System (5GS);Stage 2 https://www.3gpp.org/DynaReport/28202.htm
[9]	3GPP TS 28.533	Technical Specification Group Services and System Aspects; Management and orchestration architecture framework https://www.3gpp.org/DynaReport/28533.htm

Ref	Doc Number	Title
[10]	IETF RFC 2119	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
[11]	IG1224 v13	TM Forum NaaS Transformation v13.0.0 https://www.tmforum.org/resources/reference/naas-transformation-v13-0-0-ig1224/
[12]	GSMA PRD OPG.09	NBI APIs Realisation in the SBI
[13]	GSMA PRD OPG.10	Open Gateway Technical Realisation Guidelines

1.6 Conventions

The key words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC2119 [10].

2 Use Cases

No specific use cases are highlighted yet. Those depend heavily on the specific NaaS Service/Capabilities exposed

3 High-level Requirements for OP to support NaaS services

This section defines the requirements that the OP should fulfil to support Network as a Service services beyond the generic platform-related requirements that are defined in GSMA PRD OPG.02 [1].

3.1 Functionality offered to OP Ecosystem Party

3.1.1 Functionality offered to Application Providers

An OP and its architecture shall fulfil the following requirements related to the functionality offered to Application Providers:

1. An OP shall expose network capabilities to the Application Providers, including longer-term managed network services (such as for QoS, i.e. Quality of Service) and shorter-term or transactional style services (such as SIM-derived services, such as location verification).

Note: It is the responsibility of the Application Provider to ensure proper QoS support in the application when making use of end-to-end QoS mechanisms such as Low Latency, Low Loss, Scalable Throughput (L4S), traffic category and Differentiated Services Code Point (DSCP).

3.1.2 Functionality offered to Aggregators

Editor's note: NaaS-specific requirements for further study

3.1.3 Functionality offered to End-Users/Devices

Editor's note: NaaS-specific requirements for further study

3.1.4 Functionality offered to Operators

An OP and its architecture shall fulfil the following requirements related to the functionality offered to Operators:

1. The OP architecture shall allow an OP to influence the quality of service delivered by the network for the interaction between an End-User device and an application.

3.1.5 Functionality offered to other OPs

Editor's note: NaaS-specific requirements for further study

3.2 Network as a Service enabling requirements

This section provides the requirements that an OP's architecture should fulfil for the exposure of Network Capabilities to Application Providers.

3.2.1 High-Level requirements

The following requirements apply for an OP related to the exposure of network capabilities:

1. An OP shall allow an Operator to expose network capabilities within the Operator or a Partner network.
2. An OP shall allow the exposure of Operator network capabilities based on the integration of 3GPP functions like:

    a) Network Exposure Function (NEF)
    b) Network Data Analytics Function (NWDAF)

3. The OP architecture shall allow an Operator to expose, when available, network related Statistics and Analytics to Application roviders regarding different information types (descriptive, predictive and prescriptive ones).
4. The OP architecture shall allow an Operator to expose, when available, network related Statistics and Analytics to Partner OPs, regarding information types (descriptive, predictive and prescriptive ones).
5. The OP architecture shall allow an Operator to expose the end user's profile data to the Application Provider.

Note: This applies to the end users managed by the given Application Provider, and some examples are applicable 5QI, Single Network Slice Selection Assistance Information (S-NSSAI), etc.

3.2.2 Capability Management requirements

Beyond the requirements defined in GSMA PRD OPG.02, an OP shall be able to expose information related with analytics when available (5G core) filtering what information is offered depending on the requester (Application Provider or Partner OP).

An OP shall allow an application to request network capabilities

- for any data session established between any Application Client and Application Instance,

Note: This may be done as part of the application onboarding process, e.g. using the Application Manifest.

- for specific data sessions between a subset of Application Clients or a subset of Application Instances;

Note: This could be, for example, requesting a QoS profile for a specific set of premium users

- for a particular time period of data sessions between Application Client and Application Instance.

Note: This could be, for example, to increase the QoS profile for a video analytic application only while specific events occur.

An OP shall expose the available service access with their QoS options to the Application Provider for the Application Provider to choose the wanted connection options and their priority. An Application Provider must be able to discover which QoS mechanisms are supported in the network where the UE is consuming its service.

3.2.3 Service-Specific Requirements

3.2.3.1 Network Communication Service Enabling Requirements

An OP needs to expose control mechanisms for network connectivity if an Application Provider wants to influence this for their service. This section addresses the high-level requirements on what the OP shall be able to expose to the Application Provider and other OPs for such services. These services address 4G and 5G network connectivity capabilities.

1. An OP architecture shall allow an Operator to expose Network Communication Services.
2. The OP architecture should be able to expose the existence of the Network Communication Service(s) to the Application Provider and other OPs.

Note: In 5G the Network Communication Services can be realised with a Network Slice, and in earlier network generations this could be realised using APNs and/or applying QoS.

3. The OP architecture should be able to access Network Slice lifecycle management and/or other needed capabilities of an Operator and include these in exposed Network Communication Services to the Application Provider.

Note: This capability is dependent on the agreement between the Operator and the Application Provider.

4. An OP should be able to expose Key Performance Indicators (KPIs) to the Application Provider. Network performance attributes such as throughput, latency and reliability could be used to assure that the Application Provider's requirements are met.
5. An OP shall allow an Application Provider to request authorisation for the end user to access the Network Communication Service.
6. The OP architecture shall allow the Application Provider to manage the end user's profile data related to the Network Communication Service.

Note: This applies to the end users managed by the given Application Provider.

7. An OP should be able to request Network Communication Services in federated networks that support the requested Service Level Agreement (SLA) by the Application Provider.

3.2.4 Privacy Requirements

Editor's note: NaaS-specific requirements for further study

3.2.5 Mobility Requirements

Editor's note: NaaS-specific requirements for further study

3.3 Security Requirements

Editor's note: NaaS-specific requirements for further study

4 Deployment Scenario using OP Architecture

Editor's note: specifics of the use of the OP architecture defined in GSMA PRD OPG.02 [1] for NaaS-services are for further study. Some of the OP's interfaces, e.g. SBI-CR or SBI-EIN might not be applicable for this deployment.

5 Interface Requirements for Enabling NaaS Services

This section defines the additional requirements for the delivery of NaaS services on the interfaces in the OP architecture beyond the generic ones that are covered in GSMA PRD OPG.02 [1].

5.1 Northbound Interface (NBI)

5.1.1 High-level requirements

1. The NBI shall offer Network or other Operator Capabilities to Application Providers and Aggregators, in particular:

   a) Network Capabilities Operators agreed to expose
   b) Other Operator Capabilities

5.1.2 Management Profile

An OP shall offer a uniform view of management profile(s) to Application Providers:

1. An OP shall allow an Application Provider to request to be notified about the abstract Service and Session Continuity modes applied for application sessions.
2. An OP shall allow an Application Provider to request to receive application QoS change notifications if the requested Service Levels drops below a threshold
3. An OP shall allow an Application Provider to request to receive UE radio access type change event notifications.
4. An OP shall allow an Application Provider to request to receive UE IP address change event notifications.

5.1.3 Network Capability Exposure Support on the NBI

The NBI shall expose network capabilities towards Application Providers.

An Application Provider may use exposed network capabilities, that is

- Setting network behaviour for the data sessions between the UE and the Application Instance, e.g. QoS;
- Receiving notifications about network events or requesting specific information about UE, network status or information.

The request to use exposed network capabilities may be done dynamically through a dedicated NBI.

5.1.3.1 Requesting network capabilities dynamically

The NBI shall allow the Application Provider to request network capabilities dynamically; that means any or any combination of the following:

- Enabling a specific capability at a specific time (e.g. ‘now’, ‘in 10minutes’) or a time-bound (e.g. ‘for the next 5 minutes’); this also includes the option to stop consuming a capability
- Enabling a specific capability for a particular connection between the Application Client and Application Instance, defined by the source or destination port and protocol, e.g. applying QoS only for the traffic between port range 10000-11000 on the Application Client and port range 12000-13000 on the application instance for UDP
- Enabling a specific capability for a specified subset of data sessions defined by a set of Application Clients
- Enabling a specific capability for a specified subset of Application Instances
- Optionally, requesting new Service Level Objectives

5.1.3.2 Network Event Support

An Application Provider may require to be notified about network events or may want to request specific information about UE, network status or information.

The capabilities, information or services to be provided may be among the following:

- UE location information and events;
- UE network connection events;
- Application to UE connection status;
- UE S-NSSAI.

An OP shall provide through the NBI a publish and notification framework for the Application Provider to request notifications about any network-related events. Events may occur due to an explicit request to receive notifications from an event provider service (e.g. connectivity change events). They may also occur due to a request to use network capabilities affecting the network behaviour. For example, an Application Provider could request QoS and then receive an event notification that the desired QoS level cannot be maintained (e.g. due to a change of the connectivity bearer).

5.1.4 Network Communication Service lifecycle and end user profile

An OP shall be able to support the following requirements:

1. An OP shall allow an Application Provider to manage the lifecycle of the Network Communication Service, optionally with specifying geographical region, timeframe, target Operators, etc..
2. An OP shall allow an Application Provider to request a Network Communication Service lifecycle state change.
3. An OP shall support the notification for the Network Communication Service lifecycle status change.
4. An Application Provider should be able to assign and switch a Network Communication Service for the end user to access the application.

Note: For this action, the Application Provider is expected to know related information such as Network Communication Service ID.

5. An OP shall notify the Application Provider if end user's profile data changes.
6. An OP shall enable the Application Provider to request an end user's profile information.
7. It is essential to provide the UE with the correct network details. The NBI shall allow the Application Provider indicate which UEs shall have access to the specific Network Communication Service.

5.2 East/Westbound Interface (E/WBI)

This section covers specific E/WBI requirements related to NaaS Services.

Editor's note: Specific requirements for the E/WBI related to NaaS services beyond Application Management are further study.

5.2.1 Application Management

Beyond the requirements defined in GSMA PRD OPG.02 [1] for Application Management the following applies when the E/WBI is used for the delivery of NaaS Services:

1. The E/WBI shall forward the network events for use by the Leading OP and the Application that may have requested those from the Leading OP.
2. The E/WBI shall forward the Network Communication Service lifecycle management and related Subscriber information to be shared with the Leading OP of the Application Provider.

5.3 Southbound Interfaces (SBIs)

5.3.1 Southbound Interface – Charging Function (SBI-CHF)

Editor's note: Specific requirements for SBI-CHF related to NaaS services are further study.

5.3.2 Southbound Interface – Network Resources (SBI-NR)

Editor's note: Specific requirements for SBI-NR related to NaaS services are further study.

5.3.3 Southbound Interface – Operation & Maintenance

5.3.3.1 General

The integration with the operation and management APIs on the SBI-OAM allows an OP to expose them to the Application Provider. Depending on the service offerings and the deployment options, the Operator may impose limits on the management capabilities exposed on the SBI-OAM interface.

The OP integration to the operation and management systems should allow:

- The OP to retrieve Network Slice lifecycle notification in a standardised way
- The OP to manage Network Slice lifecycle status in a standardised and secure way.
- The OP to manage and retrieve 4G network characteristics in a standardised way.

An OP's SBI-OAM shall be able to interact with the 5G / 4G system via a slice management function (e.g. NSMF or Exposure Governance Management Function (EGMF)) to access these management capabilities.

Note: The APIs used by an OP to interact with a slice management function can either be TM Forum or 3GPP APIs.

5.3.3.2 Network Slice as a Service (NSaaS) Lifecycle management

Network Communication Services in 5G networks can be realized with NSaaS, in which case the following requirements apply:

1. An OP's SBI-OAM shall be able to interact with the Operator's systems to manage the Network Slice.
1. An OP's SBI-OAM should be able to retrieve information on a Network Slice Instance (NSI).
2. An OP's SBI-OAM shall be able to collect a Network Slice lifecycle status for the Network Slices associated with the services provided by OP.
3. An OP's SBI-OAM should be able to modify the Network Slice lifecycle status.

5.3.3.3 Security requirements

The following security requirements shall be considered:

1. The SBI-OAM shall provide an authentication mechanism to enable access only to authenticated and authorised entities. Therefore, mutual authentication shall be provided between the OP and the OAM system.
2. The SBI-OAM shall support the use of authorisation mechanisms by its endpoints that grant access to only the necessary authorised services and data.
3. The SBI-OAM shall provide security mechanisms to safeguard the confidentiality, integrity and authenticity of the exchanged data.
4. The SBI-OAM shall support the adoption of strong security algorithms that guarantee forward secrecy and prevent intervening attacks such as replay, relay and man-in-the-middle attacks.

5.3.3.4 Network Communication Service management in pre 5G networks

The OP shall be able to manage Network Communication Service characteristics in the networks where NSaaS is not available, or the Operator chooses to use traditional QoS mechanisms.

1. An OP's SBI-OAM shall be able to interact with the Operator's systems to manage the network.
2. If a dedicated APN/Data Network Name (DNN) is provided, the end user's traffic should be treated according to the AP's requirements (e.g. specific QoS). The OP shall provision the Policy and Charging Rules Function (PCRF)/Policy Control Function (PCF) with the rules needed to satisfy the AP request for the APN/DNN.
3. If a dedicated APN/DNN is not available, end user's traffic detection is required in the network, and the end user's traffic should be treated according to the AP's requirements (e.g. specific QoS). The OP shall provision the PCRF/PCF with the rules needed to satisfy the AP request.
4. An OP's SBI-OAM shall be able to collect performance metrics for the APN/DNN associated with the services provided by OP.
5. An OP's SBI-OAM should be able to modify the network characteristics related to QoS/APN/DNN.

5.3.4 Southbound Interface – Privacy Management (SBI-PrM)

Editor's note: Specific requirements for the SBI-PrM related to NaaS services are further study.

6 Requirements on Functional Elements for Enabling NaaS Services

This section defines the additional requirements related to the delivery of NaaS Services on functional elements that make up the OP architecture beyond the generic ones that are covered in GSMA PRD OPG.02 [1].

6.1 Exposure Functions

Editor's note: Specific requirements for Exposure Functions related to NaaS are further study.

6.1.1 Exemplary scenarios for Exposure Functions related to NaaS

Based on the aforementioned capabilities, the NBI is expected to enable the following non-exhaustive list of scenarios:

- Network Communication Service capabilities: the Application Provider directly or via the Aggregator observes and can manage the lifecycle of a Network Communication Service or the resources allocated to the Network Communication Service.

6.2 Federation Functions

Editor's note: Specific requirements for Federation Functions related to NaaS are further study.

6.2.1 Exemplary scenarios for Federation Functions related to NaaS

Typical scenarios enabled by the Federation Functions across the E/WBI role are:

- Network and Analytics Capabilities Exposure towards Partner OPs;

6.3 Transformation Functions

No specific requirement have been identified so far for the Transformation Functions for the delivery of NaaS services.

Note: Future general requirements for the Transformation Functions (e.g., identified in other groups), may be transposed into this document.

6.3.1 Exemplary scenarios for Transformation Functions related to NaaS

Typical scenarios enabled by the Transformation Functions in the context of offering NaaS services are:

- SBI:
  - Configuring UE traffic management policies through the OP to accomplish the application's requirements, e.g. as described in 3GPP TS 23.502 [3], or the UE's IP address shall be maintained;

Note: UE Route Selection Policy (URSP) rules influenced by the OP may also be considered a solution.

  - Interaction with the mobile network via the Southbound Interface – Network Resources (SBI-NR), for example to:
    - Receive information related to the network capabilities, such as QoS, policy, network information, etc.
    - Receive the end user’s profile data (e.g. S-NSSAI, DNN, etc.)
  - Management of Network Slice lifecycle via SouthBound Interface – Operation and Maintenance (SBI-OAM)

6.4 Integration Functions

6.4.1 Network Slice provisioning for an end user

An OP shall offer a centralised management plane for the Operator to manage end user’s profile data and to map it to the corresponding AP ID and Application ID.

Note: S-NSSAI, DNN list and NSI are Network Slice related information associated with the end user managed by the OP in the case of a 5G network.

Annex A Client-side mechanisms to control QoS

A.1 Introduction

Applications often need low latency and jitter to function properly. For this QoS can be applied from the network by calling QoS APIs for each IP flow where the application needs the traffic to be treated with priority. On top of the network-initiated QoS, additional mechanisms that allow an application to ask for priority from the client side exist, such as URSP traffic categories, L4S tagging or DSCP tagging. This can be done by the application supporting URSP traffic categories, L4S tagging or DSCP tagging. Applications can tag priority IP flows using these mechanisms and depending on the network, support and Operator settings might benefit from a better treatment then.

The Application Provider is informed about the supported mechanisms so that the client-server connection between the Application Client and the Application backend or edge instance can select a mechanism that is supported.

A.2 URSP traffic categories

The Operator can provide the end user (UE/device) with the URSP configuration. A UE application can indicate traffic categories for selected flows that will be mapped by the UE to active URSP configurations. It is up to the UE Operating System implementation how a Network Slice is selected or access to the network is done. It is important to associate standardised categories of application traffic with the specific connectivity defined by the Operator.

GSMA PRD NG.135 [5] has listed a range of traffic categories that can be applicable to OP services that require specific traffic treatment for specialised services. The categories would allow to separate normal internet traffic from application-specific traffic. Figure 1 shows an Application Client that utilises 2 different traffic categories, PDU session A and PDU session B are treated separately with different characteristics according to the traffic category applied. Here e.g. Session A could be for normal priority and session B for real-time interactive traffic flows.

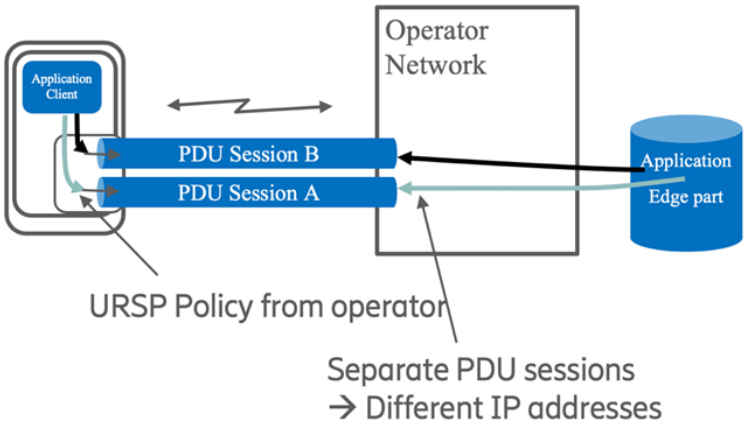


Figure 1: URSP mapping to Operator services

A.3 L4S

L4S is a new technology based on an Internet Engineering Task Force (IETF) standardisation, which provides high throughput and low latency for IP traffic, resulting in improved, fast rate adaption management, and reduced network congestion, queuing and packet loss.

L4S relies on ECN (Explicit Congestion Notification) in the IP header to indicate queue build-up in the radio access network to the application. The congestion signals are then managed at the sender and receiver side thanks to scalable congestion control algorithms. In turn, the technology signals to the application server to adjust the application bit rate to meet the capacity of the established communication link. As a result, L4S is effective in delivering a seamless user experience even with variable traffic load and radio conditions. The application tags the communication handle (socket) according to desired QoS treatment (L4S or no tag)

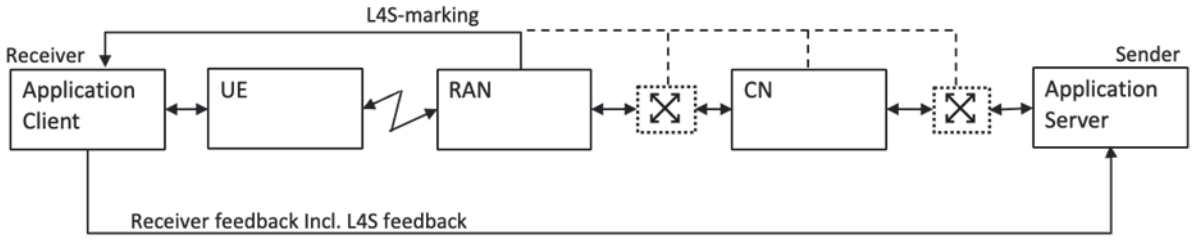


Figure 2: L4S handling

The Operator determines how L4S traffic is handled. When the Subscriber is allowed to use this mechanism from their subscription, the Operator can support L4S using packet filters and prioritise L4S-tagged traffic; see also Figure 3 where the black optimised queue handles only L4S-tagged traffic. The application is expected to respect the ECN bits that indicate congestion and take measures when congestion is detected. This can e.g. by reducing bit-rates for streaming or other measures.

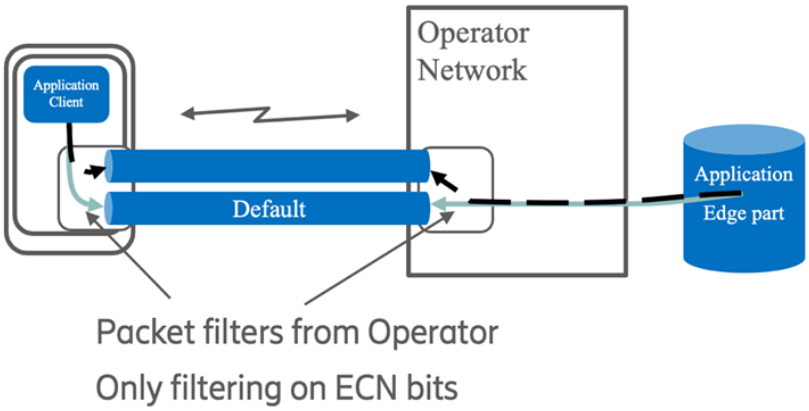


Figure 3: L4S based queue selection

A.4 Other mechanisms

Note: Other client-side QoS mechanisms are for further study. These could include DSCP or other relevant mechanisms.

Annex B Network Communication Service as a Service (NCSaaS) realised with NSaaS

This annex explains the relation between the Network Communication Services and Network Slice as a Service (NSaaS).

From the OP point of view, the Application Provider acts as a Communication Service Customer (CSC), while the Operator takes the role of Communication Service Provider (CSP).

Depending on actual scenarios, the Operators and the Application Providers can play one or several roles simultaneously, as depicted in Figure 4.

Note: The OP is assumed to be in the Operator's domain.

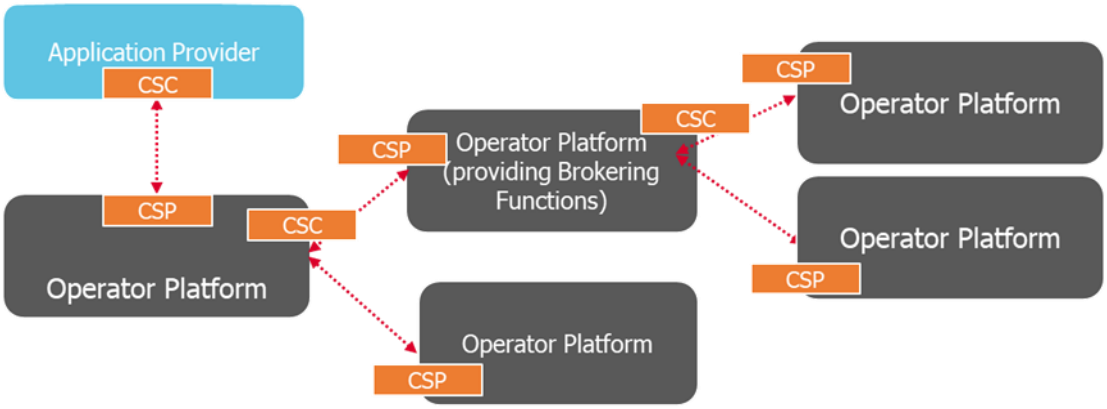


Figure 4: OP and AP roles

A CSP may offer a Network Communication Service to its CSC(s) where they can ask for special treatment of traffic for devices. This service can be realised with the CSP's network via different mechanisms as long as the special treatment can be applied for CSC's device traffic.

In a 5G network, this can be realised using 3GPP Network Slice mechanism which can be offered in the form of a service [6]. This can also be realized via specific QoS flows in both 5G / 4G network. In 4G networks, a Network Slice is typically not available in which case the Operator can revert to other mechanisms such as dedicated APNs combined with QoS flow mechanisms. In the latter case also charging, lifecycle management, etc will need to fallback to traditional mechanisms.

A Network Slice is defined as a logical network that provides specific network capabilities and characteristics [10]. 3GPP has defined standardised Network Slice /Service Types (SSTs) in Section 5.15.2.2 of 3GPP TS 23.501 [10].

The CSC communicates its needs by specifying the Network Communication Service that they need. If that needs to be mapped to a Network Slice in the CSP's south bound, the OP will make use of Network Slice as a Service (NSaaS).

Using NSaaS, Network Slice characteristics and capabilities created by CSP are tailored to satisfy the agreed Network Communication Service needs i.e., the Network Slice is still offered in terms of a Network Communication Service which satisfy certain network characteristics as needed by CSC. Note that the performance requirements of the Network Slice are based on characteristics of the network i.e.

- Radio access technology
- Location
- Bandwidth
- End to end latency
- Reliability
- QOS
- Security, etc.

There are many ways of creation and management of the Network Slices using NSaaS. One option is to leverage GSMA-defined Generic network Slice Template (GST) and several NEtwork Slice Types (NESTs) in GSMA PRD NG.116 [4]. GST contains a list of attributes that can be used to characterise a type of Network Slice/service. A NEST is a selection of GST attributes filled with values. A Network Slice can be tailored to provide a specific service. Figure 5 below shows GST and NEST in the context of the Network Slice lifecycle. A CSP can leverage NEST for the SBI realisation of a Network Communication Service. That way they can hide the technical values and complexity of a Network Slice from the CSC.

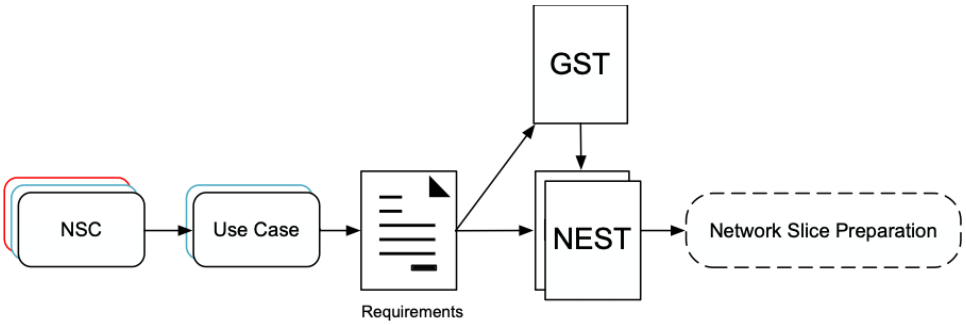


Figure 5: GST and NEST in context of the Network Slice lifecycle [5]

A Network Slice could span across multiple domains – access network (or Radio Access Network), core network and transport network. A variety of Network Communication Services can be supported by a Network Slice (see Figure 6 below). The Network Communication Services using a Network Slice may include 5G eMBB service, AR/VR service, V2X services and many others.

Figure 6 below shows that there can be various combinations of how an NSI can be deployed in a network. How the NSIs are deployed will depend on the Operator's decision and the service level requirements of each Application Provider. It is also possible for the Operator to make use of APN/DNN to realize a Communication Service.

- An NSI can share (or not at all) a certain level of infrastructure resources with other NSIs. Depending on the service level requirements to be delivered by the NSI, it is an Operator decision how and where to allocate (and/or dedicate) resources for the network functions serving the NSI.
- An NSI can be shared by different Application Providers. In that case, all the Application Providers using the same NSI will experience the same service level requirements for their services. A single S-NSSAI will be used by all of them.

In both cases, the OP may be able to trigger various operations from commissioning to decommissioning, together with the other lifecycle operations in between (e.g., configuration, activation, modification, and deactivation). It is an Operator decision how to land the service level requirements from an Application Provider to a concrete NSI, for example if it needs to deploy a dedicated NSI with a certain service level requirements or it can reuse an existing NSI because the service level requirements from the Application Provider can be delivered with an existing NSI.

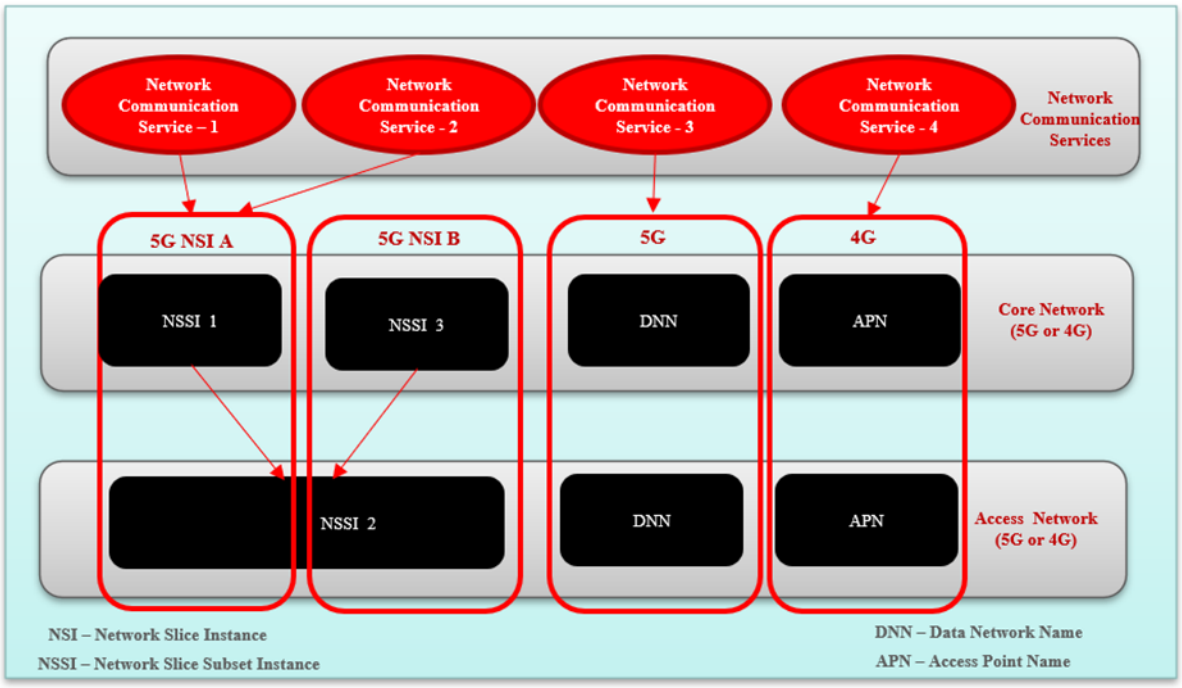


Figure 6: A variety of services provided by multiple Network Slices [6]

A Network Slice Instance (NSI) is a set of Network Function (NFs) instances and the required resources (e.g. compute, storage and networking resources) which form a deployed Network Slice.

An S-NSSAI identifies a Network Slice/service [2] and comprises of:

- **Slice/Service type (SST)**, which refers to the expected Network Slice behaviour in terms of features and services;
- **Slice Differentiator (SD)** which is optional information that complements the SST(s) to differentiate amongst multiple Network Slices of the same SST.

B.1 Network Slice lifecycle management

A Network Slice, like any other network, has various cycles of its life. The Operator needs to understand the Application Provider's requirements to fulfil them correctly (e.g. using a GST as described above). Once the requirements are well defined and captured in a NEST a new Network Slice can be created, or an existing Network Slice will be updated whenever there is a requirement for a new Network Communication Service in form of a Network Slice from a CSC.

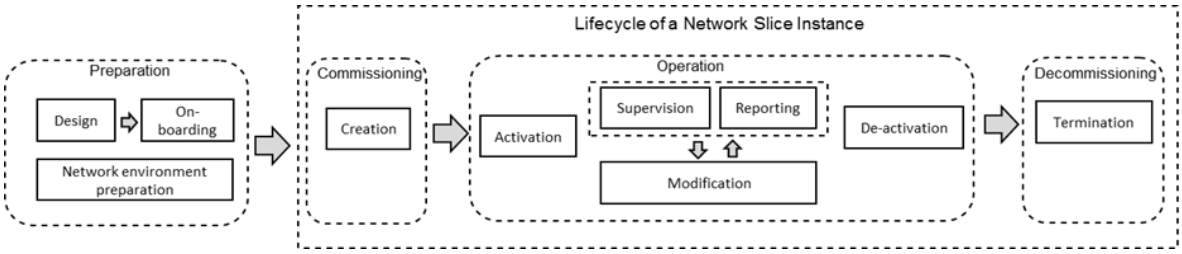


Figure 7: Management aspects of network slicing [6]

There are multiple ways an Operator can manage the preparation and operation of Network Slices. 3GPP has defined four phases of the Network Slice lifecycle in TS 28.530 Section 4.3 [6] , wheras TM Forum has documented similar in NaaS Transformation IG1224 V13 [11]. It is depending on the Operator's deployment architecture what level of integration is best suited.

- **Preparation, also known as Service Qualification and Service feasibility in TM Forum**: This phase includes Network Slice design, Network Slice capacity planning, on-boarding and evaluation of the network functions, list of Network Communication Services supported by the Network Slice, preparing the network environment and other necessary preparations required to be done before the creation of an NSI. In this phase, the NSI does not exist.

  The Operator will decide on what elements to use in each domain for a particular Network Slice. It could be possible that two different Network Slices share some elements (radio, transport, part of the core) but also have other elements that are dedicated to this Network Slice to meet the requirements of that Network Slice (as shown in Figure 6).

- **Commissioning or Service Provisioning**: In this phase, the NSI is created. During NSI creation, all needed resources are allocated and configured to satisfy the Network Slice requirements.
- **Operation**: This phase includes the activation, supervision, performance reporting (e.g. for KPI monitoring), resource capacity planning, testing, problem management, modification, and de-activation of an NSI.
- **Decommissioning**: includes decommissioning of non-shared constituents if required and removing the NSI specific configuration from the shared constituents. After this phase the NSI, does not exist anymore.

Depending on the service offering, the Operator may impose limits on the NSaaS management capabilities exposed to the Application Provider. There may be various levels of the NSaaS management capabilities, from managing only specific characteristics (e.g.

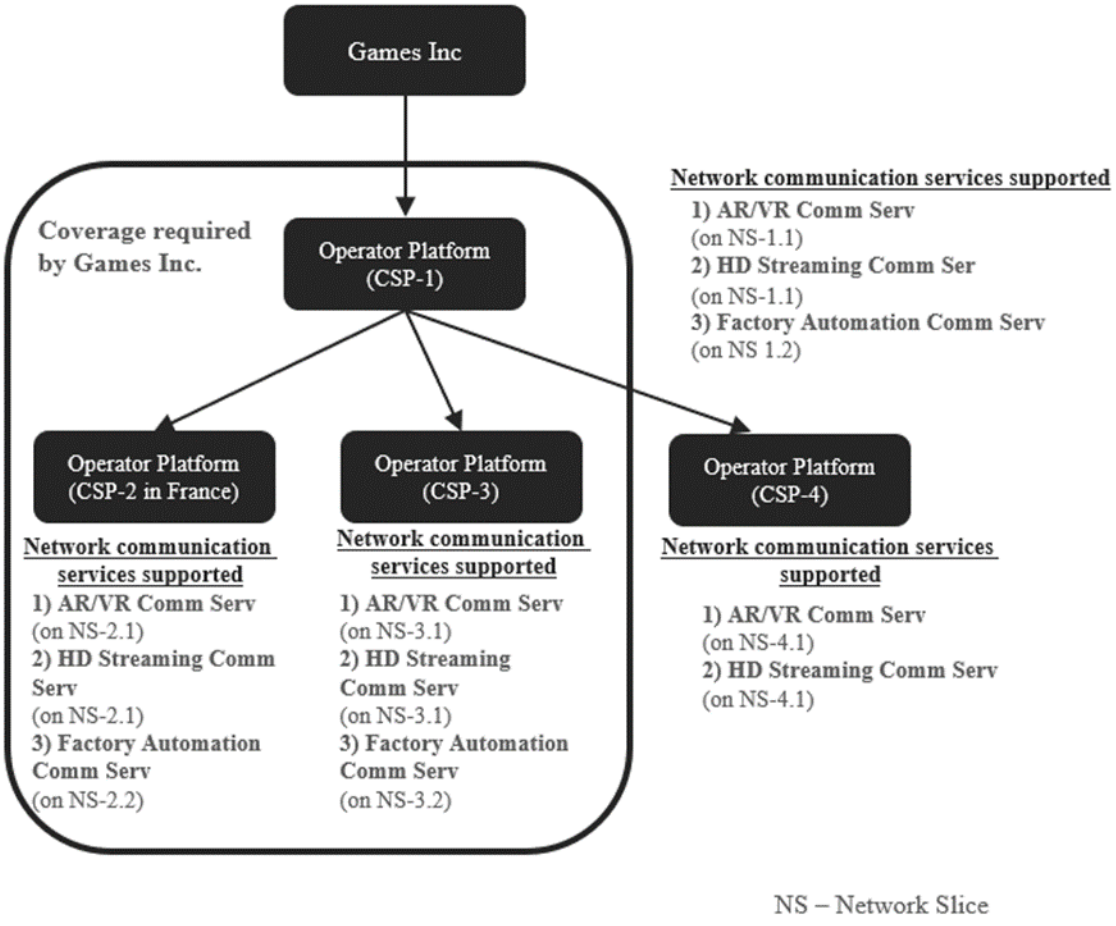
bandwidth, end-to-end latency, QCI) to managing the Network Slice lifecycle (e.g. activation, decommissioning).

B.2 Roaming

Note: Roaming is for further study.

B.3 Federation

For the federation scenario, one of the CSPs acts as Leading CSP/OP, providing a single point of contact to the Application Provider for interaction with all involved CSPs. Thus, the Application Providers do not need to have a direct relation with all the CSPs. Whenever they need to have access to a Network Communication Service, they specify that Network Communication Service's needs and the location needs (e.g., coverage in France, or coverage in a stadium) to their Leading CSP. The Leading CSP will identify the target CSPs and distribute the Network Communication Service needs provided by the Application Provider to them. The figure below provides an example use case depending on this approach.



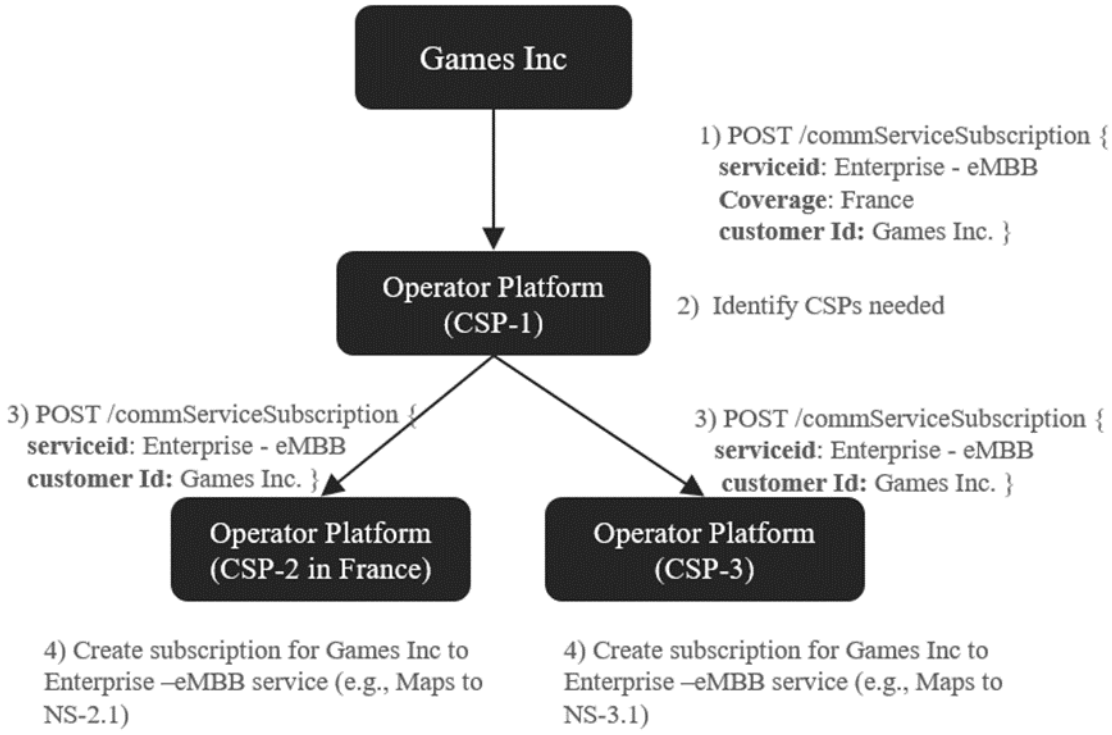
In this use case, Games Inc has an AR/VR game which requires low latency connectivity (Network Communication Service) to provide a good experience to their premium game End-Users. Their game End-Users have subscriptions that span across multiple CSPs (CSP-1, CSP-2, CSP-3), but not CSP-4 which serves a different geographical area that is not covered by Games Inc. They intend to operate only in France which is covered by CSP-1, CSP-2 and CSP-3 whereas. CSP-4 may be operating in the UK for example.

To have this special low latency connectivity for their gaming end users, Games Inc. need all the CSPs in France to support a low latency Network Communication Service. They sign-up with CSP-1 as their primary contact (Leading OP) to have the nation-wide Network Communication Service setup in France. They put a request to CSP-1 for such Network Communication Service to be setup passing these key parameters (ignoring all commercial aspects for now):

- **Network Communication Service characteristics**: LOW_LATENCY (Traffic Category)
- **Network Communication Service Coverage area**: France

As a simplification, the solution proposed leverages the concept of an agreed set of Network Communication Services (with identifiers) among all the CSPs. In this case, the Network Communication Services and their characteristics are agreed with all the CSPs and then published to all the Application Providers. Application Providers do not need to discover any specific Network Communication Service based on some network characteristics. Instead, they can leverage the agreed set of Network Communication Services provided by the involved CSPs' Operator Platforms.

Whenever an Application Providers needs to get the Network Communication Services access, they send out the request to the Leading OP as shown in the figure below (using the Games Inc use case introduced earlier).



Continuing the earlier use case, Games Inc triggers the Network Communication Service subscription in France by giving a POST request passing the Network Communication Service id which is required (Enterprise - eMBB) and coverage area (France).

CSP-1's OP validates the requests and identifies the required target CSPs (in France, CSP-2, CSP-3). Note that as explained earlier CSP-4 is not required since the request relates to France only. CSP1's OP forwards the request to all the required CSPs' OPs. All CSPs' OPs validate the request and create a subscription for Games Inc. to this shared Network Communication Service. They may just forward the request to each of the target CSPs using an E/WBI API similar to the NBI API that the Leading OP exposes to Games Inc. In this example also CSP-1 checks if they offer this Network Communication Service (given that they are based in France themselves). If available, they create / add Games Inc. to that Network Communication Service.

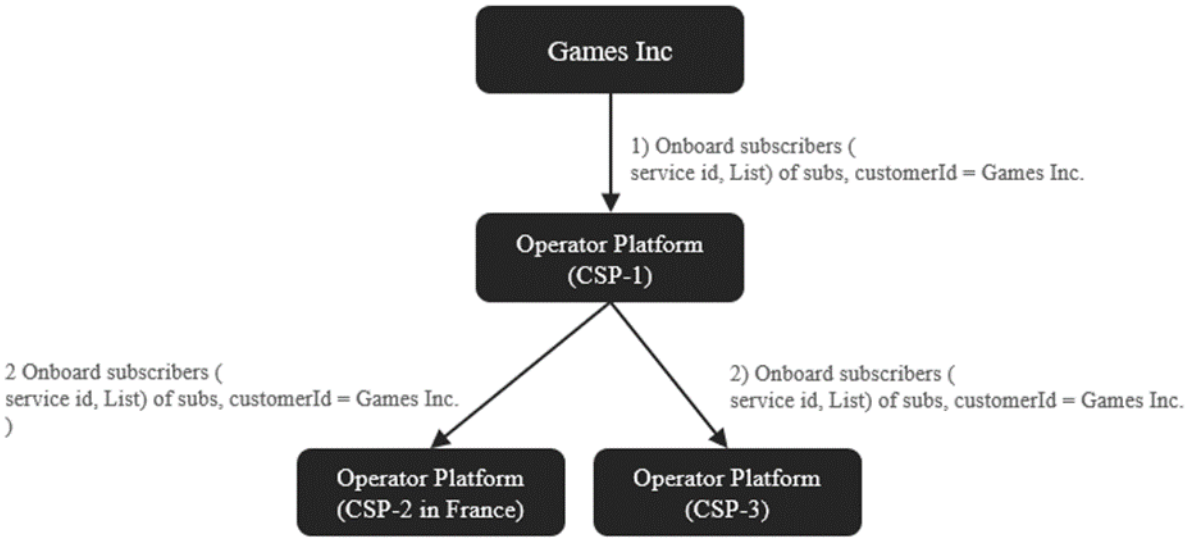
Note: It is possible for each CSP to decide how they want to realize a Network Communication Service as long as the Network Communication Service characteristics can be assured.

In this simplified solution, all the CSPs are aware of the Network Communication Service needed by Games Inc. So, there is no need for any Shared Catalog / inventory between the CSPs. It might still happen that some CSPs cannot offer that Network Communication Service for any reason. In that scenario they will respond with an error message to the Leading OP. The Leading OP can report that error back to the Application Provider (Games Inc) so that they can act accordingly.

Once the Network Communication Services are setup, the Application Provider (Games Inc) can trigger onboarding of their devices (or PDU sessions etc.) on to the Network Communication Service.

Note: This is just one of the options with another one being that the Subscriber might trigger getting onboarded to the Network Communication Service themselves, for example by buying add-on subscriptions.

The figure below shows what the onboarding flow triggered by Application Provider looks like:



Note: Simplistic view shown for easy understanding

As shown in the figure, once the Network Communication Service is setup, Games Inc can send the list of their Subscribers/devices to be onboarded to this Network Communication Service (identified by a service id) to CSP-1.

Note: Rather than a list, Games Inc. might provide also a single Subscriber/device in the request if they would loop around all their Subscribers.

CSP-1's OP identifies the CSP for each of Subscribers provided by Games Inc and prepares a sub-list of Subscribers for CSP-2 and CSP-3. Next to triggering the onboarding requests to CSP-2 and CSP-3 with these sub-lists of Subscribers, CSP-1 triggers onboarding of their own Subscribers from the list provided by Games Inc to the Network Communication Service that was set up.

The Leading OP is responsible to distribute this request to the downstream CSPs with a filtered list of devices. Each CSP then decides how to onboard the devices to the Network Communication Service offered on their network (e.g. by subscription in network, URSP provisioning, QoS flows etc.).

B.4 Security

NSaaS provides on-demand requirements based on the needs of the Application Provider for specific Network Slices. The OP and the Application Provider use appropriate security control policies to be able to protect against unauthorised access and inappropriate use of the E2E Network Slice. Moreover, the capabilities for authentication of management service requests for allocating, deallocating, or modifying an NSI are expected to be supported by the OP or Application Provider either explicitly (directly) or implicitly(indirectly), as per 28.533 section 4.9 [9].

Authorised services allow a CSP to provide management capabilities and grant provisioning permission to the CSC. Once the CSC has provisioning permission, it will manage the

Network Slice Instance lifecycle (allocating, deallocating, or modifying an NSI) and its services.

Authorised services can either be explicit or implicit. Explicit authorisation of a token is obtained from a CSP so that the CSC can interact with a CSP. A CSP can enforce access control and verify the access token. Implicit authorisation is when the CSP enforces access control based on local policies and synchronises the policies across a centralised authorisation service.

B.5 Charging

3GPP has produced a set of technical specifications that define the architecture and protocols that enable Network Slice charging using the Operator's Converged Charging System (CCS). In the context of this Annex, the most relevant ones are:

- TS 28.202 "Charging management; Network Slice management Charging in the 5G System (5GS);Stage 2" [8]
- TS 28.201 "Charging management; Network Slice performance and analytics charging in the 5G System (5GS); Stage 2" [7]

As explained in section B.1 of this Annex, 3GPP has defined the Network Slice lifecycle, which optionally can be managed by the CSC/Application Provider if supported by the MNO/CSP/OP. If this capability is allowed, 3GPP has defined in 3GPP TS 28.202 [8] the protocol that allows doing the rating and charging associated with the following operations related to the Network Slice lifecycle management:

- Network Slice Instance creation.
- Network Slice Instance modification.
- Network Slice Instance termination

When a CSC/Application Provider invokes one of the lifecycle management operations included above, and the operation is successfully completed, the OP triggers a charging request to the Converged Charging System (using the SBI-CHF) to ask for the rating and charging associated with that particular operation.

It is important to note that to enable the rating and charging process, a provisioning in the Operator's BSS and CCS may also be needed.

3GPP has defined different potential architectures for this charging integration, where the charging requests could be triggered:

- Directly from the element managing the lifecycle management operation (embedded charging trigger function -CTF- in 3GPP terminology).
- By the CEF (Charging Enablement Function), an element defined by 3GPP that gets the notifications about an operation's completion and triggers the charging request to the CCS.

Note: The architecture to be used will be dependent on the capabilities available in the Operator and is for further study.

The Charging dialogue with the CCS is based on a Request/Response pattern where:

- The charging requests will include all the information elements that could be relevant for the CCS to calculate the appropriate tariff and do the charging (the commercial model used in the Operator is out of the scope of this document). As a reference, the following elements should be included in the charging request:

  - CSC/Application Provider/Operator Platform identifiers that are invoking the operations
  - Operation type invoked (creation/update/termination)
  - Network Slice Instance identifiers
  - Set of parameters related to the service profile associated with that Network Slice Instance (e.g. latency, resource sharing level, Jitter, reliability …)

- The Charging request responses from the CCS will inform about the outcome of the charging operation.

As a result of this charging operation, the CCS will generate a CDR (Call Details Record) including all the details about the charging operation (parameters used in the charging request, price, balances after doing the charging, etc.).

Note: The potential use of this CDR is for further study.

Besides the charging scenarios associated with Network Slice management operations, 3GPP has also defined the following charging integration scenarios that are for further study [7], [8] :

- Charging based on a device's 5G data usage using a particular Network Slice Instance. This charging scenario is enabled by the information provided by the 5G Packet core in the charging requests sent to the CCS that are associated with the device's data usage.
- Charging based on the performance of a particular Network Slice (based on the SLA commitment for a particular Network Slice Instance).

  In this particular case, the charging integration is defined in 3GPP TS 28.201 [7] and - as in the case of Network Slice management charging scenarios - the charging dialogue is also based on a request/response pattern where charging requests will include information about the analytics for that Network Slice that are periodically collected by the Operator (in the NWDAF). Potential examples of these analytics are the Network Slice load, the device observed service experience, etc.

B.6 Provisioning for end user

Note: It is for further study if the subscription will be managed by the OP directly or if the Application Provider needs to communicate with the Operator's BSS directly.

To enable a UE to select the appropriate Network Communication Service, it is essential to provide the UE with the correct network details. This is done during the provisioning when the end user profile is updated with the service and Network Slice or APN/DNN information. The end user profile includes but is not limited to S-NSSAI, DNN, APN, URSP rules, and location information.

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	09 May 2025	New PRD OPG.12 based on requirements in OPG.02 V8.0	ISAG	Tom Van Pelt / GSMA

C.2 Other Information

Type	Description
Document Owner	Operator Platform Group
Editor / Company	Tom Van Pelt / GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.