FS_NSCALE KI discussion

CMCC

Shaowen Zheng

Topic

- **Key issue 5: Communication service management exposure**
- **Key issue 12: Network slice capability exposure in the edge data network**

Key issue 5: Communication service management exposure

1. What is Communication service in NSCALE？

NSCE as one of the functionalities of SEAL is responsible to provided the network slice related capability exposure to enable the communication services required by the vertical applications.
In SA1 TS 22.261, several types of communication services provided to the vertical applications are described, e.g., cyber-physical control services, video services, tactile and multi-modal. And the KQIs/QoEs and APIs required by different vertical applications may be diverse.

2. What is Communication service management exposure in NSCALE?

Following requirements related with network capability exposure are described by SA1 TS 22.261**:**

- Based on operator policy, the 5G network shall expose a suitable API to allow an authorized third-party to **define and reconfigure** the properties of the communication services offered to the third-party.
- The 5G system shall support the means for **disengagement (tear down)** of communication services by an authorized third-party.
- The 5G system shall **provide information on the current availability** of a specific communication service in a particular area (e.g. cell ID) upon request of an authorized entity.

3. NSCE is responsible for the following capabilities:

- Communication services availability (e.g.,KQIs/QoEs (resolution, frame freezing for video services)) assurance;
- KQI translations from communications service KQIs to the network KPIs;
- API translations from the APIs invoked by verticals to the APIs provided by NEF or OAM system;
- Lifecycle management of the communication services(e.g., from an order of network slice for a video service, the network slice preparations and operations, until the order cancel) provided to the verticals.

Application enable layer management of slice lifecycle

- What kinds of service APIs are required to be supported for application layer exposure of communication services life cycle management?

Step1: order/registration

The customers propose communication service requirements by ordering the network slice and network slice capability registration

Registration

VAL server sends the registration request to the NSCE server with its identity, and may also include interested service and level of exposure requirement

Step2: preparation

Communication service preparation includes Authorization and authentication, SLA translation, API translation & configuration, subscription (subscribe to OAM and 5GC services to be used by the communication service consumers).

Authorization and authentication

configuration & translation

API configuration and translation Description: Vertical applications requirement => suggested SLA & a bundled or combined API

subscription

Step 3: operation

After the preparation phase, the communication service could be use by communication service consumers. A communication service allows run-time operations includes the slice monitor/exposure and slice adaptation and other basic slice operations (modification etc.).

Slice monitor/ exposure

Based on collected information from 5GS/OAM and collected application layer information from either client or APP server, the function of slice monitor/exposure includes

- QoS verification per slice
- Performance and analytics exposure per slice
- Fault alert and diagnose

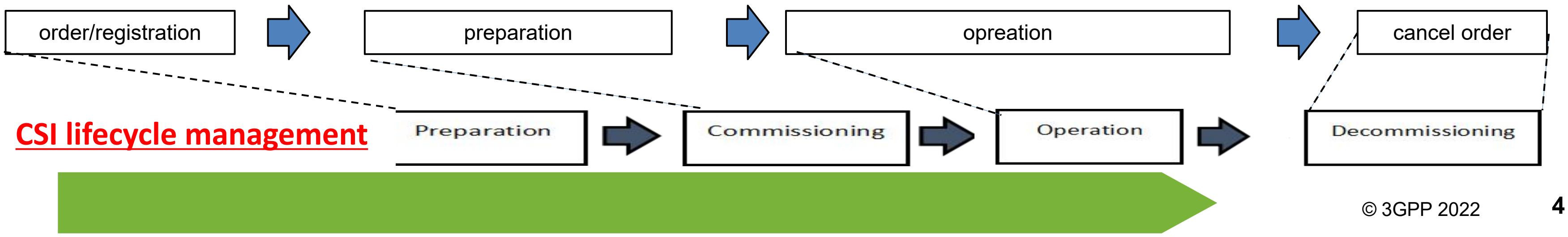
Slice adaption suggestion

Based on slice status info exposure, Slice adaption suggestion could trigger Slice scaling or policy adjustment, like：

- Automatic application layer network slice management
- managing trusted third-party owned application(s)

Step 4: cancel order

When the communication service is no longer needed, the lifecycle of the communication service ends.



order/registration → preparation → opreation → cancel order

CSI lifecycle management

Preparation → Commissioning → Operation → Decommissioning

Key issue 12: Network slice capability exposure in the edge data network

The network slice deployed in the core network has a certain distance from the customer, so the delay will be affected to a certain extent and cannot meet the operation requirements of low latency equipment. Moreover, a variety of service data need to be processed in the core network, the scale of data traffic is large, the backhaul network needs to bear a large load and consume more bandwidth. For example, the differential protection service has strict requirements for latency in power industry.

In order to meet the personalized services requirements of vertical industries, network slices are deployed by using the computing, storage and communication capabilities of the edge date network, so as to realize the localized processing of the service, reduce the service transmission latency and enhance the service performance.

How to expose the network slice capability deployed in the edge data network to the vertical industry or the third parties is worthy of our study.

Open issues:

- How could the NSCE server deployed inside the EDN interact with the NSCE server outside the EDN?
- Whether and how could the NSCE server inside the EDN manage the network slice that has resource outside the EDN?
- Whether and how does SEAL need to be enhanced to support NSCE client to interact with NSCE server in the EDN and NSCE server outside the EDN?

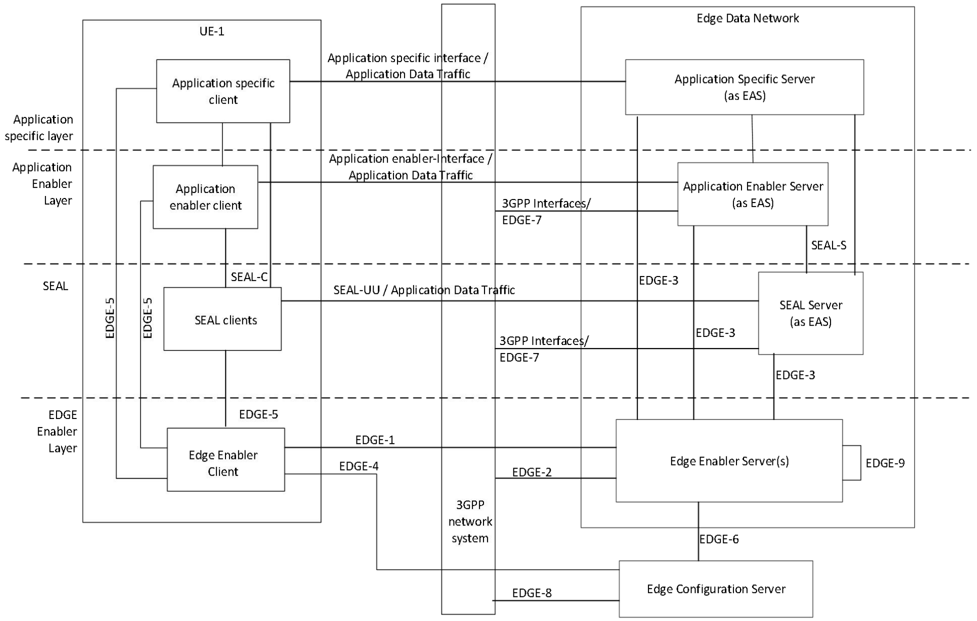

UE-1
Edge Data Network
Application specific layer
Application specific client
Application specific interface / Application Data Traffic
Application Specific Server (as EAS)
Application Enabler Layer
Application enabler client
Application enabler-Interface / Application Data Traffic
Application Enabler Server (as EAS)
3GPP Interfaces/ EDGE-7
SEAL-S
SEAL
SEAL-C
SEAL-UU / Application Data Traffic
EDGE-3
SEAL clients
SEAL Server (as EAS)
EDGE-5
EDGE-5
3GPP Interfaces/ EDGE-7
EDGE-3
EDGE-3
EDGE Enabler Layer
EDGE-5
EDGE-1
Edge Enabler Client
EDGE-4
EDGE-2
Edge Enabler Server(s)
EDGE-9
3GPP network system
EDGE-6
EDGE-8
Edge Configuration Server

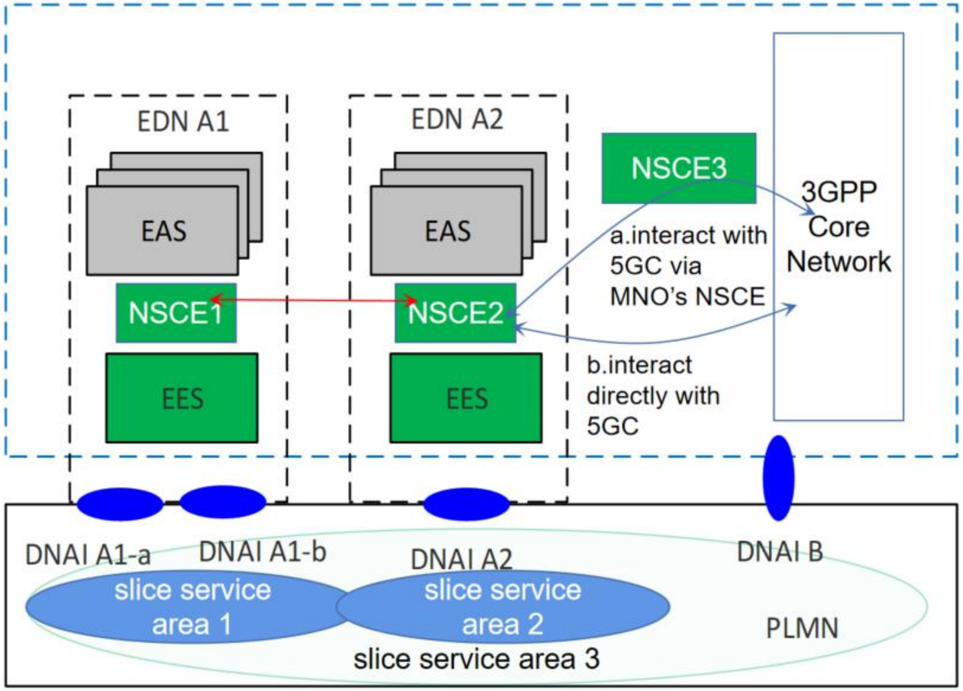
Illustration of layered application architecture with generic SEAL and Application Enabler server functions available in the edge

Similarly, the server functions of an application enabler server can be made available only as an EAS, it is also possible that certain application enabler server functions are available both at the edge and in the cloud. When the server functions of an application are both available at the edge and the cloud, there may be a need for interaction between the two corresponding application servers, which is out of scope of this specification.

KI 12

Considering that users in the EDN 2 need to access slice 3, the NSCE 2 also needs to interact with 5GS to obtain slice 3 information, etc;
Also, when a user moves to EDN 1, the NSCE2 can cooperate with EDN 1to find an alternative slice, if the current slice cannot be supported in EDN 1.

Technically， either the NSCE deployed in the edge or elsewhere can be seen as a trusted AF, as long as it is a trusted third party, so they can interact with 5GS directly.
However, in practice, for MNO, based on some security concerns and management aspect concerns, it is not expected that the NSCE at the edge can interact directly with the 5GC, let alone manage resources directly.



Observation:

- The interface between NSCE servers is needed, the SEAL-E may be enhanced. To distinguish different NSCEs, in addition to the NSCE ID, the service area, location and other attributes of the NSCE may be needed.
- Some procedures need to be updated. some capabilities are needed(e.g, slice continuity)

ANNEX

Lifecycle of a communication service defiend in SA5

- What kinds of service APIs are required to be supported for application layer exposure of communication services life cycle management?

from TS 28535, 28.805

- **Preparation phase:**

Providing a communication service starts with preparation, which includes communication service design, pre-planning, feasibility check, i.e., checking the attainable communication service quality from both resource and service aspects, negotiation of the communication service attributes, preparing communication service and network requirements derived from SLA.

- **Commissioning phase:**

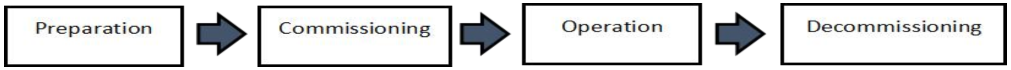
Once a communication service is prepared, it can be established by converting the communication service requirement to network requirements (interaction and use of NF resources including RAN, CN) to be deployed on the network resources and ready to be used by the communication service consumers (subscribers, UEs).

- **Operation phase:**

After the commissioning phase, the communication service is activated for use by all communication service consumers (subscribers, UEs) that are allowed to use the communication service. The initial deployment or trail phase for the training of the communication service assurance algorithms has entered the operation phase. A communication service that is activated allows run-time operations e.g., quality of experience assurance, quality of service assurance,data exposure, CSI modification. The optimization of the utilization by communication services may continue during the operation phase of the communication service.

- **Decommissioning phase:**

When the communication service is no longer needed, after being de-activated, the lifecycle of the communication service ends with termination.

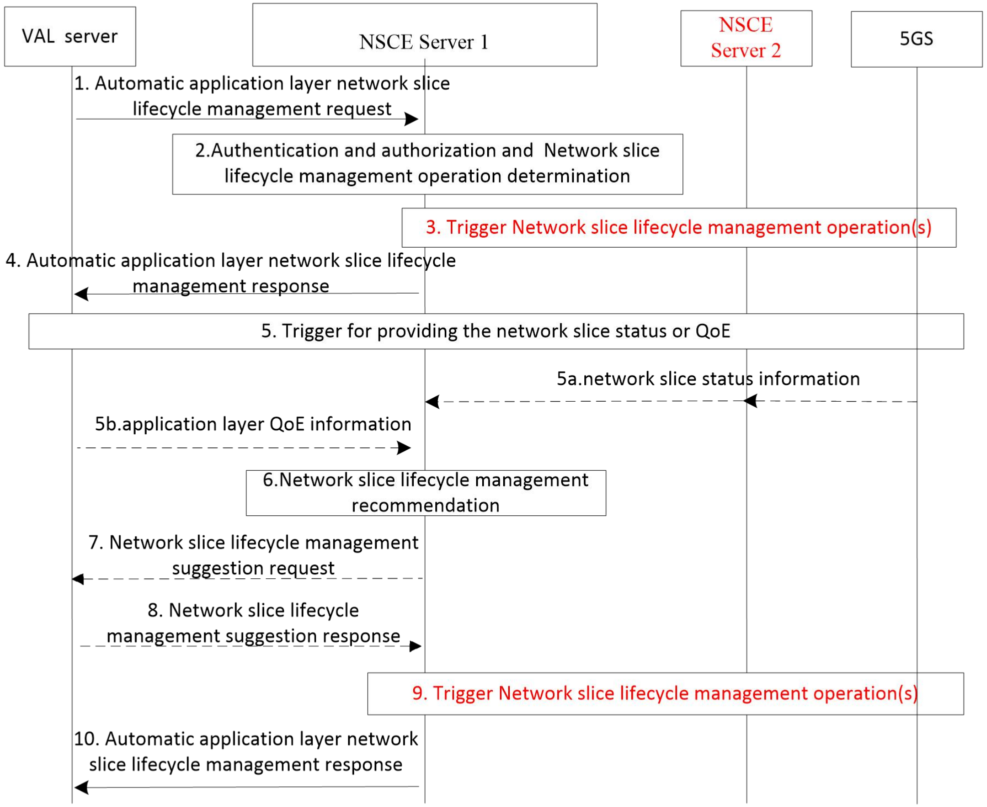


Preparation → Commissioning → Operation → Decommissioning

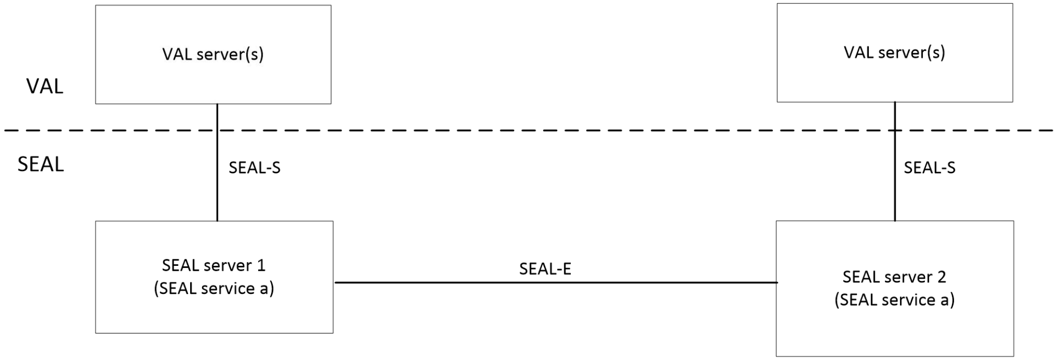
Figure 4.1.1: Lifecycle of a communication service

when the NSCE server inside the EDN wants to manage the network slice that has resource outside the EDN, some solutions would have to be updated, for example

Solution 1: Automatic application layer network slice management


VAL server
NSCE Server 1
NSCE Server 2
5GS
1. Automatic application layer network slice lifecycle management request
2.Authentication and authorization and Network slice lifecycle management operation determination
3. Trigger Network slice lifecycle management operation(s)
4. Automatic application layer network slice lifecycle management response
5. Trigger for providing the network slice status or QoE
5a.network slice status information
5b.application layer QoE information
6.Network slice lifecycle management recommendation
7. Network slice lifecycle management suggestion request
8. Network slice lifecycle management suggestion response
9. Trigger Network slice lifecycle management operation(s)
10. Automatic application layer network slice lifecycle management response

- Whether and how does SEAL need to be enhanced to support NSCE client to interact with NSCE server in the EDN and NSCE server outside the EDN?



The interactions between the SEAL servers of the same type are generically referred to as SEAL-E reference point. The specific SEAL service reference point corresponding to SEAL-E is specified in the specific SEAL service functional model.

solution	SEAL-E may be enhanced to support the functionality such as:
Solution 1: Automatic application layer network slice management	support network slice management operation
Solution 2: Network slice fault management capability	fault management data exposure, fault management operation，
Solution 3: Slice API configuration and translation	transfer requirement and related info
Solution 4: QoS verification capability	PM data exposure, PM operation，
Solution 5: Network slice related performance and analytics exposure	PM data exposure, PM operation，
Solution 6: VAL server authorization and authentication via slice enabler layer	Support NSCE authentication and authorization as a consumer
Solution 7: network slice capability registration	Support NSCE registration as a consumer
Solution 8: Discovery of management service exposure	Depends on MNO’s policy, VAL server could do the management via edge NSCE directly if supported, or through the MNO's NSCE
Solution 9: Support for managing trusted third-party owned application(s)	Depends on MNO’s policy, VAL server could do the management via edge NSCE directly if supported, or through the MNO's NSCE