SLICE AND EXPOSE

Enhancing Network Slicing Applications by Means of Capability Exposure

Jose Ordonez-Lucena, Telefónica I+D
Berlin, 7th November 2019
Introduction

- NSaaS is a future-proof service delivery model
  - NSI on demand, as a service.
  - NSaaS provider and NSaaS customer roles

- Two complementary service views on an NSI:
  - Resource-facing (NSI deployment details) VS Customer-facing (NSI exposed capabilities)
  - Abstraction to preserve the required demarcation point between the provider and the customer.
First Proof of Concepts on NSaaS carried out in the context of 5GPPP Phase 3 projects

- **ICT-17 projects**: design and deploy a large-scale, E2E facility infrastructure with in-built orchestration and testing tools for KPI validation in realistic 5G scenarios.

- **ICT-19 projects**: deploy, configure and test **vertical use cases** using ICT-17 facilities, assessing the readiness of these use cases and validating their KPIs under different load conditions.

**ICT-17 facilities** offers ICT-19 industry verticals tailored service platforms for use case trialling activities.

**NSaaS roles and projects**
Some lessons learned from experimentation

• A vertical use case may involve the combination of public networks and NPNs.
  ➡ Not only connectivity, but also interworking

• A vertical typically want to retain some control over the NSI provided as a service
  ➡ Get involved beyond passive monitoring
  ➡ Means for 3rd party VNF hosting

• Tailored customer-facing view of the NSI -> SLICE CAPABILITY EXPOSURE
  ➡ Allows NSaaS provider to grant each NSaaS customer with necessary control capabilities over the NSI.
Reference architectural framework in NSaaS

This project has received funding from the EU’s Horizon 2020 research and innovation programme under grant agreement No 815279.
This project has received funding from the EU’s Horizon 2020 research and innovation programme under grant agreement No 815279.

NSaaS phases

• Two main phases

Network Slice (aaS) Request

The NSaaS customer issues a service order towards NSaaS provider, requesting the deployment of a tailored network slice.

Network Slice (aaS) Operation

The NSaaS customer monitors and takes (some) control over the network slice, deployed and made available by the NSaaS provider.

Slice Topology + Slice Requirements

NSI is deployed and activated

Slice performance assurance and fault supervision + Slice Management & Control
Network Slice (aaS) request

- Templates

This project has received funding from the EU’s Horizon 2020 research and innovation programme under grant agreement No 815279.
Network Slice (aaS) request

- Templates with information on
  - Default slice topology, e.g. 3GPP NST.
  - Supported service requirements, e.g. GSMA NEST.

- Default topology can be extended by attaching 3rd party service functions to slice service access points
  - 3rd party PNFs/VNFs, MEC apps and app servers
  - Vertical-driven activity
  - Allows going from a baseline topology to a vertical, service-tailored topology.

This project has received funding from the EU’s Horizon 2020 research and innovation programme under grant agreement No 815279.
Network Slice (aaS) operation – Exposure levels

- In NSaaS scenarios, different verticals may want to take a more or less proactive role in the operation of their slices.

- Exposure levels -> levels of control the vertical can take over the provided slice.

<table>
<thead>
<tr>
<th>Customer is able to consume operations related to…</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>E2E network slice application layer config &amp; management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Network slice subnet (and NF) application layer config &amp; management -&gt; 3GPP scope for RAN and CN, IETF scope for TN.</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Network slice subnet (and NF) virtualized resource layer config &amp; management -&gt; ETSI NFV network service (and VNF) orchestration</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Resource control and management at the virtual infrastructure layer -&gt; NFVI with optional EPA capabilities and infrastructural SDN control</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
</tr>
</tbody>
</table>
Network Slice (aaS) operation – Exposure levels

- Token-based authentication
The next moves

• Explore the feasibility of exposure levels in open source environments like OSM and OpenStack
  ➔ Leveraging the multi-tenancy support capabilities that OSM and OpenStack claim to have

• Integration of non-repudiation mechanisms to allow secure and verifiable interactions between the NSaaS providers and customers
  ➔ Ensure system auditability
  ➔ Relevant in public network integrated NPNs.
This project has received funding from the EU’s Horizon 2020 research and innovation programme under grant agreement No 815279.