

NG.144 E2E-S Slicing B2B User Story
Version 0.1
04 June 2024

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 © 2024 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 has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.34 - Policy and Procedures for Official Documents.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

Table of Contents

1 Introduction 3
1.1 Overview 3
1.2 Scope 3
1.3 Definitions 3
1.4 References 4
1.5 Conventions 4
2 Use case summary 5
3 User story 5
4 Workflow 7
4.1 B2B customer contracts the service with the MNO 8
4.2 Service Feasibility 8
4.3 MNO activates the service in the network 8
4.4 Slice activation response 8
4.5 MNO provision the service to the B2B end user devices 8
4.6 Registration Request by End User 9
4.7 Device Management 9
4.8 Slice Authorisation 9
4.9 Access control and service execution 10
5 Key capabilities to be covered and gap analysis 10
6 Target SDOs and gaps resolution 15
Annex A Document Management 16
A.1 Document History 16
A.2 Other Information 16

1 Introduction

1.1 Overview

The objective of this whitepaper is to describe a detailed end-to-end user story for a slicing-based industry service with the intention of ensuring that the required technical capabilities are supported by current GSMA and other SDOs specifications (mainly, 3GPP and IETF).

Concretely, this document intends to assess whether there are gaps for the user story execution. A gap is typically characterized by an ambiguity or lack of standard definition to fulfil a capability needed for the user story execution.

1.2 Scope

From the slicing-based service request received from the customer to the service execution, the ambition is to identify any potential gap on current standard definitions and address it in the proper SDOs.

Once a gap is identified, the relevant SDOs and corresponding working groups owning relevant specifications will be contacted (via Liaison Statements) to confirm/infirm and validate these gaps and take the appropriate actions as appropriate.

Items that are out of the scope of this initial version of the whitepaper are listed in Section 3.

1.3 Definitions

Term	Description
eMBB	Enhanced Mobile Broadband
GST	Generic Network Slice Template
HMTC	High-Performance Machine-Type Communications
MIoT	Massive IoT
MNO	Mobile Network Operator
NEST	NEtwork Slice Type
OSAppId	OS specific Application Identifier
RSD	Route Selection Descriptor
S-NSSAI	Single Network Slice Selection Assistance Information
S-NEST	Standardized NEtwork Slice Type
SDO	Standards Developing Organizations
MTSI	Multimedia Telephony Service for IM
P-NEST	Private NEtwork Slice Type
UE	User Equipment

1.4 References

Ref	Doc Number	Title
[1]	<e.g. PRD AA.34>	<PRD or document title e.g. “Policy and Procedures for Official Documents”. For documents with no reference entries, this section may be deleted >
[2]	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
[3]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174

1.5 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 RFC 2119 [2] and clarified by RFC8174 [3], when, and only when, they appear in all capitals, as shown here.”

2 Use case summary

In this use case a slice is dedicated to a B2B customer to execute specific applications. A typical example is public authority/safety services where availability of communication and required applications need to be guaranteed for supporting services such as video transmission or voice communication through Push to Talk (PTT). In such a scenario, only authorised applications are allowed to make use of the corresponding B2B slice to guarantee the delivery of the service. It is assumed that noncritical applications such as web browsing use the regular eMBB connection or eMBB slice. Public safety is provided as an example to illustrate the overall flow; the findings apply to other B2B slices.

3 User story

The following main steps are identified for this user story:

1. A B2B customer request the service exposed by the MNO.
2. The MNO proceeds with a Service Feasibility check. The check will span all domains over which the intended service should be delivered (scope).

2.1 Appropriate means to extract and map the feasibility check to individual technology domains must be in place (e.g., RAN, CN, and Transport Network).

3. Once pre-validation checks are successfully passed (e.g., service feasibility checks, authorization), the MNO activates the requested service in the network.

3.1 If feasibility checks fails because some resources can't be reserved, the MNO may make a counter proposal to the customer. If the customer accepts the proposed service, the MNO activates the negotiated service in the network.

4. A response is sent back to the customer confirming the activation of the requested service.
5. The MNO needs to identify the B2B customer end user devices and provision the service into them.
6. Registration request from End User device.
7. The MDM, based on the profile, assigns a slice to the related applications.
8. The network applies access control and delivers the service to the connected B2B end user devices.

The following assumptions are made for the initial version of the paper:

1. This document does not cover considerations related to the activation/provision automation through APIs.
2. The presence of a management and orchestration framework is considered in the network.
3. Device management (MDM) is not a mandatory capability in the B2B space.
4. This document does not consider onboarding deployment and connectivity of the application backend to the network.
5. Charging requirements are not covered.
6. This document does not consider the charging and billing journey for the customer.

7. Currently (2024), there are no mechanisms to identify applications accessed by customers through a web browser. Such traffic will by default be bound to the slice allocated to web browsers.
8. It is assumed that the operator BSS systems has the correlation between B2B customer and its subscriptions (SIMs) to provision the services on the devices.

4 Workflow

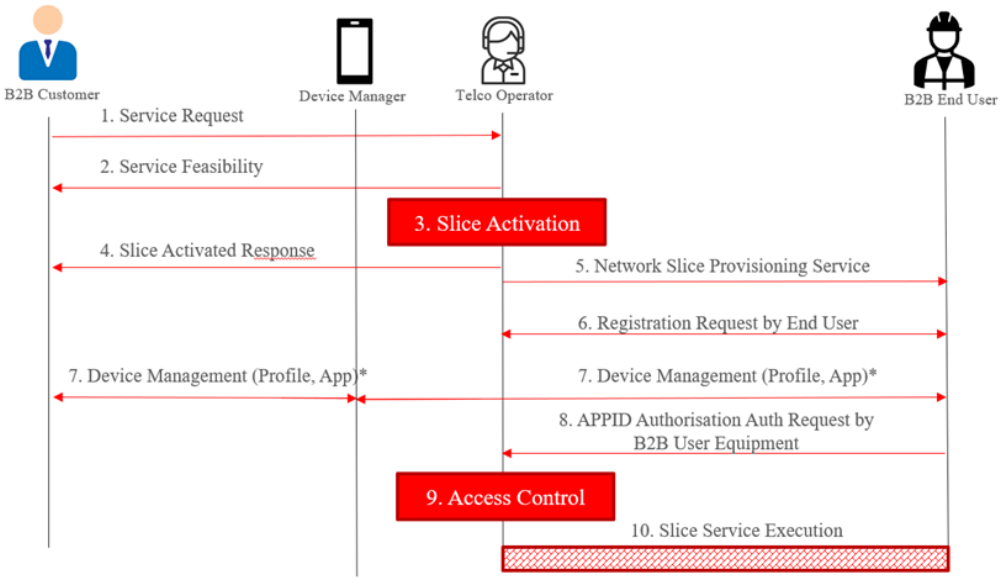

Figure 1: Workflow for B2B customer

Note: The use of the Telco Operator in this case is optional (the MDM platform may or may not be managed by the MNO) so, it can go directly to the end-user terminals.

The following sections describe in more details each of the steps.

4.1 B2B customer rtequest the service with the MNO

At this very first step, the B2B customer, (e.g., a public safety organization), subscribes to a communication service offered by the MNO, and which matches a set of Service Level Agreements/Objectives/Expectations (SLAs/SLOs/SLEs). Those indicators will typically characterize the expected service delivery even in situations where the MNO network might be, overloaded. A slice with the agreed service objectives will be provisioned within the MNO by filling a GST/NEST template defined by GSMA.

The MNO will expose a set of network slice flavours to the B2B customers, allowing them to choose the most suitable option for their needs. The determination of the optimal slice is guided by the specific requirements of each customer/need. Among the key parameters considered are the target geographic area for service delivery, the number of UEs, associated end-user identities, the requested guaranteed bandwidth per UE, maximum permissible latency and/or jitter, and the allowed applications within the UE.

In this context, B2B customers will provide the MNO with a list of devices (identified using reliable identifiers) that will access the service and, have the flexibility to create, accept, or discard a list of applications allowed to access the slice. The applications utilized for the service on the B2B end-user devices encompass a defined set, including voice, video, and multimedia applications. These are referred to as Applications A, B, and C.

4.2 Service Feasibility

The request from the B2B customer is validated as the MNO has verified that the service can be offered from the network and has triggered the activation process.

4.3 MNO activates the service in the network

In this step, the MNO will trigger the provision and activation of the service in the network for this customer. Using as input the NEST template representing the customer request the MNO will configure the network slice dedicated to the service/customer in an existing Network Slice Instance if available (and matching the customer requirements) or will create a new Network Slice Instance for allocating the service if needed.

Those processes may be either manual or automatic, assuming, the service activation does not need to be in place in a very short period of time.

4.4 Slice activation response

B2B customer is informed about the result of the slice activation process.

4.5 MNO provision the service to the B2B end user devices

To complete the provision of the communication service based on network slicing, the MNO needs to provision the proper information to the end user devices. For this use case let´s suppose that the end user devices will be also using other network slices in the MNO for different services (eMBB services).

This is basically a two-step process (3GPP TS 23.501/23.502):

- Provision the S-NSSAI/DNN as allowed for the B2B customer subscriptions.

- Provision of the adequate URSP rules to the end user devices to steer the traffic from applications A, B, and C to the Route Selection Description (RSD) SNSSAI/DNN delivering the communication service.

The URSP Traffic Descriptor (TD) selected will identify uniquely the applications A, B and C, and other traffics from other applications in the end user devices will not use the RSD delivering the service. This is critical because other traffics from other applications not intended to be steered over this S-NSSAI could break the SLAs supposed to be delivered to the B2B customer communication service.

In case of APPID usage, these IDs should be communicated previously by the Application Back End to the MNO to be used in the URSP rule provisioning. At this stage APPIDs cannot be unique as they can be managed through AppStore platforms or directly by the app provider for the service. Therefore, the MNO should have a secure relationship with the app backend to authenticate the APPID provided.

Then, based on the TD OSAppId, only traffics from applications A, B and C will be steered over the RSD delivering the service. Other TDs are discarded since they don´t offer the confidence that only applications A, B and C are placed over that RSD

4.6 Registration Request by End User

The End User needs to register with the network to get authorized to receive services. The End User UE performs a registration procedure and the Allowed NSSAI are provided in the Registration Accept.

If the End User UE indicates its support for Network Slice-Specific Authentication and Authorization, once this procedure is completed for all S-NSSAIs, the AMF will trigger a UE Configuration Update procedure to deliver an Allowed NSSAI also containing the S-NSSAIs for which the Network Slice-Specific Authentication and Authorization was successful and include any rejected NSSAIs with an appropriate rejection cause value.

4.7 Device Management

Through a device management platform, the B2B customer decides of the applications that can be present in the UE and assign a specific user profile to it. Based on the profile a slice is assigned to the related applications.

Note: The use of the Telco Operator in this case is optional (as the MDM platform may or may not be managed by the MNO) so, it can go directly to the end-user terminals.

Note: This step is optional as usage of Device Management platforms for B2B slicing should not be mandatory.

4.8 Slice Authorisation

Based on the assigned slice, the end user makes a request to the MNO to be authorised to access the slice.

This request should be against the MNO, who will provide the necessary mechanism to validate and authenticate the applications identity that have been previously embedded into USRP rules for appropriate routing within the assigned slice.

4.9 Access control and service execution

Once the service is completely provisioned in the MNO's network and the B2B end user devices, the next step is the service execution.

The network authorises or not the App ID requested by the End User to access the slice.

When the applications A, B and C are sending traffic to the network, they need to be properly identified as such by the OS in order the URSP intended policy is properly performed.

Then the UE OS provides the OSAppId information to the URSP implementation to apply the URSP logic defined in the previous section, using the OSAppId [GSMA TS.62].

The device offers the possibility of providing the OSAppId information to execute the URSP logic properly, and matching applications A, B and C to the target RSD. The OS ensures the integrity of the applications identifiers used as A, B and C and that they can be trusted. Indeed, spoofing attacks may happen from applications claiming to be A, B or C in some of the different smartphone OS ecosystems. Then a mechanism allowing the validation and integrity of the identifiers used by the application accessing the slice should be put in place. MNO should be able to authorize only applications A, B and C to be identified as such, and so use the RSD delivering the service.

Once applications A, B and C are successfully identified and authorized by the MNO, they will be able to send traffic to the target RSD delivering the public safety service.

5 Key capabilities to be covered and gap analysis

This section covers key capabilities required to execute the use case and if they are already covered in standards or if specification enhancements are needed.

Capability number	Capability name	Capability description	GAP analysis
1	NEST template	NEST template covering the use case defined in this white paper	There are NEST template types for each of the communication types that are collected as service types to establish global slicing interoperability. This includes: eMBB, URLLC, MIoT, V2X, HMTC, Public Safety. Although there is no specific template for what is described in these use cases, the values of a NEST are assigned to express a given set of requirements to support a network slice customer use case. The MNOs can build their network slice service

			offering based on S-NESTs and/or their P-NESTs. Ref: *NG.116-v.8.0 (Generic Network Slice Template)*
2	Feasibility Check	This allows checking whether the service requirements associated to the requested network slice can be fulfilled with actual network operator capabilities. This feasibility check involves interactions with (domain-specific) managers and inventories, and can be optionally accompanied with resource reservation. A feasibility check is likely to be decomposed into individual checks to cover technology-specific domains (e.g., RAN, Transport Network). Means to easily map the parent Feasibility Check to these child checks should be facilitated.	TMF645 doesn't provide the capacity reservation APIs for resources (Network Resource Models). TMForum Information Framework (SID) resource model for slicing does not exist which means this can be treated and mapped by vendors within existing definitions which may lead to implementation inconsistencies. The service-facing interface of the domain's inventories should be exposed in a standardised model. For this reason, there is a need to add an abstraction layer between the domain managers and the E2E Orchestrator which is compliant with a Slicing specific resource model to ensure correct mapping between inventories northbound and the abstraction layer southbound interfaces. For the transport domain, we do not have sufficient information how reservation and the feasibility to be performed for slice. Need to extend this as a GAP for the IETF Traffic Engineering Architecture and Signalling (TEAS) and OPSAWG to further evaluate. Note, however, that existing IETF specifications covers the followings: • draft-ietf-opsawg-teas-attachment-circuit supports a "test-only" flag which is used to indicate that a service request is only for test and not for setting, even if there are no errors. This is used for feasibility checks of attaching Network Functions to a Network and then called in Network Slice Service. • draft-ietf-teas-ietf-network-slice-nbi-yang includes a "compute-only" parameter which is used to check the feasibility before instantiating a Network Slice Service.

3	APP ID assignment and management	The MNO needs to be made aware of the APP IDs authorised by the B2B customer to access the slice to consider them within the URSP criteria. The network should ensure that only ~~APPs~~applications that granted by the B2B customer can access the slice.	The APP ID should be provided to the MNO by the application backend. Since the Application Identity (APP ID) can be set during the development of the application and is not protected, it is not suitable to uniquely identify the traffic of the application that is to be managed by the operator, nor to be the reference parameter for being the application descriptor in the OS (OS App Id) for URSP rules. The user can spoof the APP ID and install the application directly on the device to bypass the USRP rules. In this case, the network should guarantee that the APP ID received by the OS has been issued by a trusted APP provider.
4	Traffic steering enforcement at OS	Based on the TD OSAppId, only traffics from allowed applications as per URSP rules will be steered by the OS over the RSD delivering the service. Other TDs are discarded.	The Application descriptors provides one or several instances of the OSId and OSAppId combination. It is used by the UE to identify the application traffic for which steering is required based on the Steering Functionality, the Steering Mode, the Steering Mode Indicator and the Threshold Values. Ref: 3GPP TS 23.503
5	Slicing support for Device Management	Device Management platforms allow the assignment of an application to a specific slice.	MDM solutions are increasingly geared towards managing applications and content, allowing enterprises to control and secure corporate data and applications on mobile devices. The MDM can manage different applications to allow connection to specific slices. This is done in a proprietary way by means of APIs provided by the operating systems. The implementation is proprietary to the OS.
6	APP ID integrity and validation	The APP ID provided by the application to the OS is validated and an integrity check mechanism is applied.	There is no mechanism to ensure there is not fraudulent use of APPID. The OS App ID, in its role as an application descriptor within the URSP rules, would also be affected as this mechanism does not exist. Specifically, there is no network-assisted method for strengthening the binding of an application and a Network Slice.

7	APP slice access network enforcement	The network checks that the apps making usage of the slice are authorized to access the service.	Network Slice admission control is defined in Current access control mechanisms within Telco Operators are instrumental in validating end users and applications for service authorization. However, existing standards delegate the responsibility of validating TDs in UE's Subscription Profile URSP rules to local implementations. Now, access control predominantly occurs at the URSP implementation level in UE, introducing certain concerns. One significant issue is the reliance on APPID as the chosen TD for validation. The susceptibility of APPID to hacking, falsification, or unauthorized usage by third parties poses a potential threat to the integrity of access control. Telco Operators may consider implementing additional measures. There is a need to deploy~~ing~~ robust access control mechanisms beyond relying solely on APPIDs such as utilizing operator tokens to provide an extra layer of security. This approach ensures that only applications that are entiteled to access a slice service are actually granted access to ~~a~~ that slice, mitigating the risks associated with potential APPID vulnerabilities such as APPID spoofing.
8	App identity on Web Browsing	Identity checks on applications that run in Web Browsers	Since we could not use URSP rules to identify apps running in Web Browsers, corresponding traffic should go to the default slice assigned to the web browser.

From this analysis, we have therefore identified the following gaps that we will propose to the relevant SDOs.

- Feasibility Check.
- APP ID assignment and management.
- APP ID integrity and validation.
- App Slice Access Network Enforcement.

Note: *App identity in Web Browser will require further analysis and may be addressed in future versions of this document.*

6 Target SDOs and gaps resolution

GAP	Actions	Target SDOs
2. Feasibility Check This allows checking whether the service requirements associated to the requested network slice can be fulfilled with actual network operator capabilities. This feasibility check involves interactions with (domain-specific) managers and inventories, and can be optionally accompanied with resource reservationNetwork	Propose as a GAP	**NaaS TMForum** **3GPP SA5** **IETF Traffic Engineering Architecture and Signaling (TEAS)**
3. APP ID assignment and management The MNO needs to be made aware of the APP IDs authorized by the B2B customer to access the slice to consider them within the URSP criteria. The network should ensure that only applications that granted by the B2B customer can access the slice.	Propose as a GAP	**OPG/OPAG** **Open Gateway** **GSMA Terminal Steering Group (TSG)** **ASAC.01**
6. APP ID integrity and validation The APP ID provided by the application to the OS is validated and an integrity check mechanism is applied.	Propose as a GAP	**GSMA Terminal Steering Group (TSG)** **ASAC.01**
7. App Slice Access Network Enforcement The network checks that the apps making usage of the slice are authorized to access the service.	Propose as a GAP	**3GPP SA3 & CT1** **ASAC.01**
8. App identity on Web Browsing Identity check on applications that run in Web Browsers	We do not see this GAP being resolved in the short term. We propose to route traffic on EMBB's general slide.	-

Figure 2: Resolution Table

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	13/04/2024	New PRD-version 1.0	ISIG-NG/TG	Daniel Doniz, Telefónica daniel.donizaza@telefonica.com Fernando Pascual, Telefónica fernando.pascualblanco@telefonica.com

A.2 Other Information

Type	Description
Document Owner	ISIG-NG
Editor / Company	DANIEL DONIZ AZA daniel.donizaza@telefonica.com FERNANDO PASCUAL BLANCO fernando.pascualblanco@telefonica.com

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.