

ITU-T Technical Report

(02/2025)

QSTR-UCFTBS

Use cases for federated testbeds and business scenarios



Technical Report ITU-T QSTR-UCFTBS

Use cases for federated testbeds and business scenarios

Summary

This Technical Report lists use cases for federated testbeds covering domains, scope, verticals, technologies and business scenarios. It focuses on synergies and commonalities. Recent technological developments require more realistic testing and new use cases to be validated in real conditions (making testbeds increasingly important).

Keywords

Business scenarios, federated testbeds, use cases.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Change Log

This document contains Version 1.0 of the ITU-T Technical Report QSTR-UCFTBS "Use cases for federated testbeds and business scenarios" approved at ITU-T SG11 meeting held in Geneva from 19 to 28 February 2025.

Editor: Martin Brand
A1 Telekom Austria
Austria

Email: martin.brand@a1.at

Editor: Dr Sébastien Ziegler
Mandat International
Switzerland

E-mail: sziegler@mandint.org

Editor: Cédric Crettaz,
Mandat International
Switzerland

E-mail: ccretgaz@mandint.org

© ITU 2025

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope.....	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Technical Report	1
4 Abbreviations and acronyms	1
5 Introduction.....	4
6 Template for testbeds and their federations	4
7 Federated testbeds use cases	4
Appendix I – Template for use cases related to testbeds and their federations	5
Appendix II – Use cases on testbed federations	7
UC01: Testbed on roaming scenarios (IMS interconnection)	7
UC02: Testing IMS emergency calling	11
UC03: Rapid network resources deployment for disaster scenarios	14
UC04: Testbed for smart cities	16
UC05: Automated construction and demolition waste management using digital twin for buildings	18
UC06: testing of open architecture systems	20
UC07: Federated testbed for cybersecurity	23
UC08: Blockchain based methodology for zero trust modelling and quantification for IMT-2020 networks	25
UC09: Federation of smart city services	27
UC10: Federated testbed for cloud and networking research.....	31
UC11: Federation of smart city water treatment and distribution services	34
UC12: End-to-end design, development of IMT-2020 testbed	37
UC13: continuous integration/continuous deployment framework.....	40
UC14: Integration testing with any commercial RAN and UE	42
UC15: Large scale UE testing	43
UC16: Orchestration	45
UC17: Standards version compliance check for error-free interoperability between RAN and 5GC testbeds	46
UC18: Support for zero trust architecture in federated testbeds.....	48
Appendix III – End-to-end UE registration in IMT-2020 networks	50
Appendix IV – End-to-end network slicing for IMT-2020.....	51
Bibliography.....	52

Technical Report ITU-T QSTR-UCFTBS

Use cases for federated testbeds and business scenarios

1 Scope

This Technical Report serves as a guide for extracting target functionality of available use cases on testbeds and its federations and mapping them to different segments (e.g., network segments as multi-access edge computing (MEC), core, radio access network (RAN), transport). The use cases descriptions (e.g., requirements, features, challenges, key performance indicators (KPIs), etc.) are used for developing general requirements for application program interfaces (APIs) to be used in testbed federations.

2 References

- [[ITU-T Q.3640](#)] Recommendation ITU-T Q.3640 (2018), *Framework of interconnection of VoLTE/ViLTE-based networks*.
- [[ITU-T Q.4068](#)] Recommendation ITU-T Q.4068 (2021), *Open application program interfaces (APIs) for interoperable testbed federations*.
- [[ITU-T Y.4459](#)] Recommendation ITU-T Y.4459 (2020), *Digital entity architecture framework for Internet of things interoperability*.
- [[ITU-T Y.4472](#)] Recommendation ITU-T Y.4472 (2020), *Open data application programming interfaces (APIs) for IoT data in smart cities and communities*.
- [3GPP TS 23.502] 3GPP TS 23.502 (2016), *Procedures for the 5G System (5GS)*.
- [ETSI TS 103 194] ETSI TS 103 194 v.1.1.1 (2014-10), *Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet*.

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following term defined elsewhere:

3.1.1 testbeds federation [b-ITU-T QSTR.FTT]: The method of integrating multiple testbeds into a unified platform that enhances their collective capabilities, creating a seamless and efficient testing environment.

NOTE – This integration allows users to execute tests without needing to interact with individual testbeds separately, simplifying access and improving usability. Simultaneously, each testbed retains its independence, ensuring it can continue to operate as a standalone entity while contributing to the broader, more powerful distributed platform.

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

2G Second Generation

3G	Third Generation
3GPP	Third Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
5GC	5G Core
5GS	5G System
6G	Sixth Generation
AM	Aggregate Manager
AMF	Access and Mobility Management Function
API	Application Program Interface
AuSF	Authentication Server Function
AWS	Amazon Web Services
CD	Continuous Deployment
CDW	Construction and Demolition Waste
CI	Continuous Integration
CPS	Cyber-Physical Systems
CS	Circuit Switched
CSP	Communication Service Provider
E2E	End to End
EPC	Enhanced Packet Core
ETSI	European Telecommunication Standardization Institute
FCTaaS	Federated Cybersecurity Testbed as a Service
FTaaS	Federated Testbed as a Service
GPRS	General Packet Radio Service
GPU	Graphics Processing Unit
GSMA	GSM Association
GTP	GPRS Tunnelling Protocol
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Subsystem
IMT-2020	International Mobile Telecommunications 2020
KPI	Key Performance Indicator
LBO	Local Break Out
LTE	Long Term Evolution
MANO	Management and Network Orchestration
MEC	Multi-Access Edge Computing
MME	Mobility Management Entity

MM-NAS	Mobility Management NAS
MNO	Mobile Network Operator
NAS	Non-Access Stratum
NF	Network Function
NFV	Network Function Virtualization
NGAP	Next Generation Application Protocol
NR	New Radio
NRF	Network Repository Function
NSSAI	Network Slice Selection Assistance Information
OAuth	Open Authorization
OEM	Original Equipment Manufacture
OS	Operational System
OTT	Over-the-Top
P-CSCF	Proxy Call Signalling Control Function
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
PS	Packet Switched
PSAP	Public Safety Answering Point
RAN	Radio Access Network
SBI	Service-Based Interface
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMF	Session Management Function
SST	Slice Service Type
TEID	Tunnel Endpoint Identifiers
UAV	Unmanned Air Vehicle
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UPF	User Plane Function
UTAI	Universal Testbed Access Interface
VM	Virtual Machine
VNF	Virtual Network Function
VoLTE	Voice over LTE
VoNR	Voice over New Radio
VPMN	Visited Public Mobile Network
XML-RPC	Extensible Markup Language-Remote Procedure Call

5 Introduction

There is a need to standardize a generic International Mobile Telecommunications 2020 (IMT-2020) and beyond application testing and validation framework which verifies the vertical application in a systematic manner under different IMT-2020 technology choices. In this regard, there is a need to develop a structured classification of use cases for federated testbeds and assets to cover verticals, scenarios, and capture commonalities in a reference blueprint and highlight differences.

6 Template for testbeds and their federations

To set the scene for the use cases, along with their definitions and specifications, it is important to note that each testbed operates as a standalone entity, offering its regular services. It can also connect via federation to other testbeds to extend its set of assets and enhance the scope of services it offers. It follows a use-case-driven approach in capturing the requirements, dynamics, and commonalities of federated testbeds. Each use case establishes the scene and the frame within which federation is possible, including aspects like scope, type of federation, limitations, and so on.

A template, which is partially aligned with [ETSI TS 103 194], for soliciting use cases as part of the use case pool related to testbeds and their federations, can be found in Appendix II.

7 Federated testbeds use cases

The detailed descriptions of the use cases are available in Appendix II, as follows:

Use case #	Title
UC01	Testbed on roaming scenarios (IP multimedia subsystem (IMS) interconnection)
UC02	Testing IMS emergency calling
UC03	Rapid deployment of network resources for disaster scenarios
UC04	Testbed for smart cities
UC05	Automated construction and demolition waste management using digital twin for buildings
UC06	Testing of open-architecture systems
UC07	Federated testbed for cybersecurity
UC08	Blockchain-based methodology for zero trust modelling and quantification for IMT-2020 networks
UC09	Federation of smart city services
UC10	Federated testbed for cloud and networking research
UC11	Federation of smart city water treatment and distribution services
UC12	End-to-end design, development of IMT-2020 testbed
UC13	Continuous integration/continues deployment framework
UC14	Integration testing with any commercial radio access network (RAN) and user equipment (UE)
UC15	Large-scale UE testing
UC16	Orchestration
UC17	Standards version compliance check for error-free interoperability between RAN and 5G core (5GC) testbeds
UC18	Support for zero trust architecture (ZTA) in federated testbeds

Appendix I

Template for use cases related to testbeds and their federations

1	Use case name/title		
2	Use case short description		
	2.a	Current practice in testbeds, federation, and testbeds federations	
	2.b	Gaps and problems solved via the use case	
	2.c	Rationale and objective/purpose of the use case	
3	Use case high-level technical specification		
	3.a	Type of use case	
	3.b	Types of stakeholders, their roles, demarcations, interactions. Types of roles for actors within each stakeholder	
	3.c	Scope:	
	i	Domain: inter- or intra-stakeholder span [e.g., for a communication service provider (CSP) stakeholder, within the same CSP/Operator or spanning multiple operators]	
	ii	Intra-stakeholder segments (e.g., CSP Core, Transport, RAN, edge, multi-access edge computing (MEC), or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...)	
	iii	Logistical scope <ul style="list-style-type: none"> Location: (countries, states, locations, sites) Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group) 	
4	Involved testbeds specifications		
	4.a	Testbed type	
	4.b	Application program interfaces (APIs) requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain) APIs. Internal and external APIs have different implementation and design requirements in terms of security, rights, certification, interfaces, etc.)</i>	

	4.c	Reference points	
5	Use case detailed technical specifications		
	5.a	Architecture/architectural framework	

Appendix II

Use cases on testbed federations

UC01: Testbed on roaming scenarios (IMS interconnection)

1	Use case name/title	End to end (E2E) testing involving interconnection among CSPs' networks and roaming
2	Use case short description	
2.a	Current practice in testbeds, federation, and testbeds federations	<p>Current practices in E2E testing involving interconnection among CSPs' networks and roaming involve, in most cases, some basic connectivity between the testbeds of CSPs being setup manually, and being limited to only a few CSPs that have certain agreements for such setups. Current practices show that E2E testing involving interconnection among CSPs' networks and roaming increasingly requires connectivity at large scale, and automation through federated testbeds. This is because networks and interconnection scenarios and service delivery requirements (including network slices delivery requirements) across multiple CSPs are on the rise. Even when considering service delivery across multiple operators, benchmarking of the service performance in such E2E environments needs to be carried out through automated federated testing to help operators dimension their network resources accordingly. Emergency call testing, performance and scalability testing and security may need to be carried out across multiple network operator networks. Hence, when testbeds of various operators are interconnected and federated to form distributed test platforms for use in testing various E2E aspects, this helps multiple operators. Some network slices are expected to span multiple operators and hence require E2E testing across the operators. Federation of CSPs' testbeds enables acceleration in E2E testing activities. The following aspects concerning roaming benefit from testing using CSPs' federated testbeds when established at large scale:</p> <ul style="list-style-type: none"> • Network slicing • UE support of network slicing when roaming • 5G core (5GC) support of network slicing when roaming • Voice, video and messaging • Short message service (SMS) over non-access stratum (NAS) • IMS voice roaming architecture • Location support

	2.b	Gaps and problems solved via the use case	There is a need for an E2E testing framework and procedures that should be implemented by operators for establishing an interconnection between voice over new radio (VoNR)-based networks to achieve worldwide interoperability. Voice over long-term evolution (VoLTE) and voice over new radio (VoNR) utilize the same IMS (IP Multimedia Subsystem) as defined in third generation partnership project (3GPP) standards. While the IP IMS framework remains the same, technological improvements in radio, core and devices are expected to provide superior user experience in VoNR compared to VoLTE. Therefore, the VoLTE E2E scenarios in terms of interconnection and roaming, described in [ITU-T Q.3640], are still valid.
	2.c	Rationale and objective/purpose of the use case	The E2E testing framework required by CSPs is intended to be based on leveraging the testbeds of the various CSPs. The CSPs' testbeds need to be interconnected and federated to support various kinds of test scenarios across network operator testing, like in the case of E2E testing of roaming.
3	Use case high-level technical specification		
	3.a	Type of use case	Testing in E2E CSPs interconnection environments using federated testbeds of the CSPs
	3.b	Types of stakeholders, their roles, demarcations, interactions	Network operators and transit network providers (in the case of roaming)
	i	Types of roles for actors within each stakeholder	Testbeds administrators in each CSP involved; test executors
	3.c	Scope:	
	i	Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)	Inter-Domain – spanning multiple operators (covering national and international roaming)
	ii	Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...)	All these network segments may play a role in the roaming scenarios, and multiple vendors may be involved in the infrastructure network segments and management and control layer
	iii	Logistical scope	
		– Location: (countries, states, locations, sites)	Globally applicable, nationally and across country borders

		<ul style="list-style-type: none"> – Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group) 	If the full E2E test scenarios can be covered through the federated testbeds of the operators, then there may not be any time constraints in the use of the testbeds. However, if part of the assets required for the E2E test scenarios can only be provided through a production network, then such tests are likely to be conducted during the non-busy hours of the production network.
4	Involved testbeds specifications		
	4.a	Testbed type	CSP core network, transport networks, RAN, edge, MEC
	4.b	APIs requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same eco-system or value chain) APIs. Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	APIs for the testbeds federation would need to be developed and implemented as outlined in [ITU-T Q.4068].
	4.c	Reference points	The relevant reference points that would need to be implemented should be those specified in [ITU-T Q.4068].

**5.a Architecture/
architectural
framework**

Figures II.1 to II.4 show an example of a multi-operator environment for a roaming scenario in which corresponding testbeds of CSPs need to be federated in order to execute various E2E test scenarios.

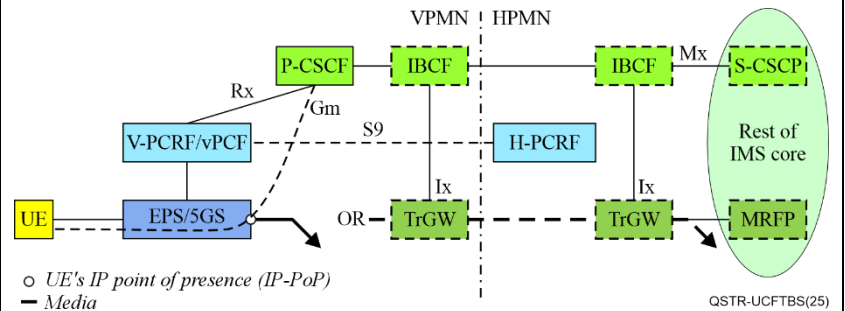


Figure II.1 – Local break out (LBO) roaming with proxy call signalling control function (P-CSCF) in visited public mobile network (VPMN) using 5G system (5GS) to support IMS services [b-GSMA PRD IR.65]

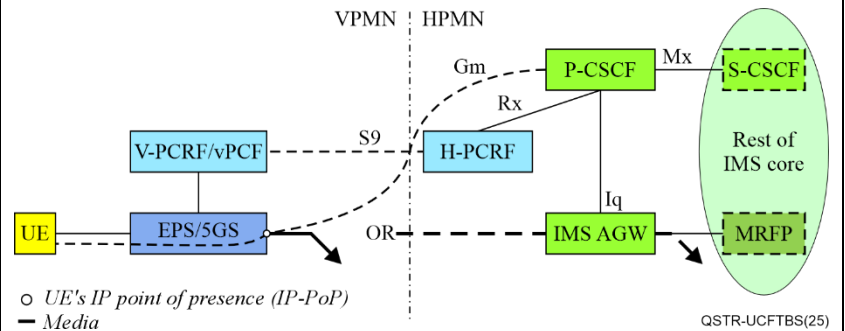


Figure II.2 – LBO roaming with P-CSCF in HPMN using 5GS to support IMS services [b-GSMA PRD IR.65]

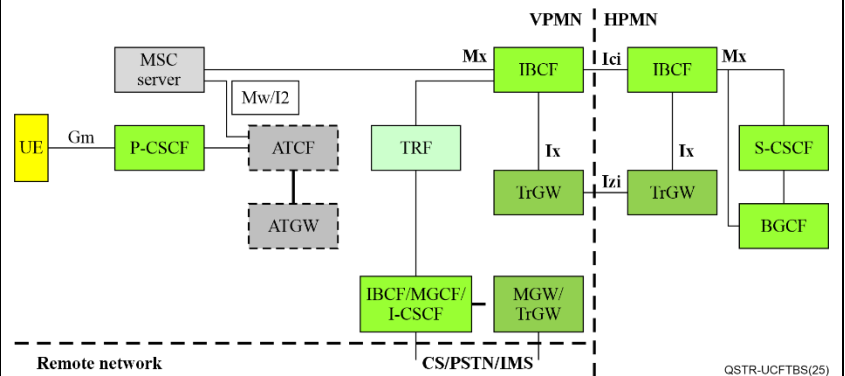
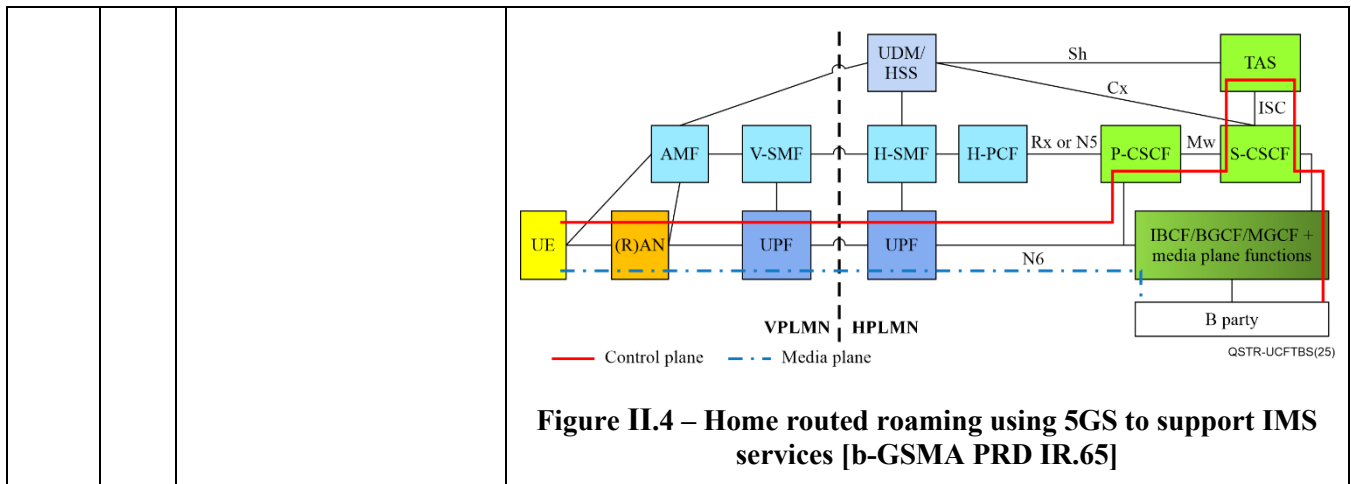


Figure II.3 – LBO with P-CSCF in VPMN with loopback possibility using 5GS to support IMS services [b-GSMA PRD IR.65]



UC02: Testing IMS emergency calling

1	Use case name/title	Testing IMS emergency calling
2	Use case short description	
2.a	Current practice in testbeds, federation, and testbeds federations	<p>Media interest in mid-2022 highlighted issues with VoLTE interoperability, including an inability to complete an IMS emergency call. This becomes a major issue if circuit switched (CS) emergency call is not available due to second generation (2G) / third generation (3G) sunset.</p> <p>Investigations by the GSM association (GSMA) with a number of original equipment manufacturers (OEMs) showed that there was a mixed landscape of some devices attempting an IMS Emergency call when "normal" VoLTE unavailable and others not. The differences were seen between manufacturers, between different models of a single manufacturer and even between the same model dependent on Android operational system (OS) version (an overall very unpredictable landscape).</p> <p>The GSMA board initiated a task force to clarify the requirements for a device for IMS emergency call and to engage with the GSMA Working Groups (WGs) to ensure that the related technical documentation was modified to provide further clarity as required.</p> <p>One of the changes related to the tests conducted on a VoLTE device for IMS emergency call handling. It was noted that the GSMA roaming test specification [b-GSMA IR.25] covered only UE-detected and non-UE detected emergency call, with no consideration for UEs that have reduced/limited voice capabilities or are in a limited service state. IR.25 has recently been modified to include these additional test cases. It is likely that other test specifications external to the GSMA also require enhancement to cover these cited additional use cases.</p>
2.b	Gaps and problems solved via the use case	<p>In addition to the use case U01 defined above, there is a need to consider additional test cases when testing IMS emergency call on a UE. These test cases include the following:</p> <ul style="list-style-type: none"> • UE with reduced/limited voice capabilities, e.g., a roaming UE with no VoLTE roaming agreement in place • A UE without a subscriber identity module (SIM) • A UE with an unauthenticated SIM (e.g., a roaming UE without an LTE data roaming agreement)

			<ul style="list-style-type: none"> Upon detecting an emergency call request, a UE in a limited service state shall (in the general case) check the support for packet switched (PS) and CS emergency in the cell in which the UE is camped If the cell supports PS emergency service, the UE shall initiate an IMS emergency call set-up If the cell supports CS Emergency service, the UE shall initiate a CS emergency call set-up If the cell does not support any emergency service, the UE shall initiate a public land mobile network (PLMN) scan <p>Since this issue mainly concerns IMS emergency call, the additional tests should be targeted accordingly.</p>
	2.c	Rationale and objective/purpose of the use case	To ensure that devices behave correctly on detecting an emergency call as described above. This will ensure that a device shall attempt a PS emergency call irrespective of whether a normal voice service is available.
3	Use case high-level technical specification		
	3.a	Type of use case	<p>Testing of both UEs and mobile network operator (MNO) networks.</p> <p>To ensure that IMS emergency calls are always attempted by the UE when in a limited service state or with reduced voice capabilities, provided PS emergency is available in the cell in which the UE is camped.</p> <p>To ensure that the network handles the IMS emergency call correctly in line with local policy/regulations. In some countries, this currently means the call attempt may be rejected.</p>
	3.b	Types of stakeholders, their roles, demarcations, interactions. <ul style="list-style-type: none"> i Types of roles for actors within each stakeholder 	MNOs and OEMs. Test equipment vendors and test executors.
	3.c	Scope:	
		<ul style="list-style-type: none"> i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators) 	Scope is between the UE and serving network. Depending on the use case, the serving network can be a visited network (e.g., a UE with a SIM and without a VoLTE roaming agreement). Conversely, for a UE without a SIM, there is no concept of a home/visited network.
		<ul style="list-style-type: none"> ii Intra-stakeholder Segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...) iii Logistical scope <ul style="list-style-type: none"> – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the 	<p>Multiple vendors are involved for the UE and network infrastructure. It is also possible for multiple vendors to be involved in the different nodes/elements comprising the network.</p> <p>Globally applicable to any network where IMS emergency calling is deployed – and most importantly, where there is no CS emergency fallback.</p> <p>In terms of timing, this needs to be done as soon as possible as 2G/3G stop operating and countries are starting to deploy IMS emergency calling and switch off CS-emergency calling.</p>

		federation of specific assets (per asset/asset group)	
4	Involved testbeds specifications		
	4.a	Testbed type	Testing equipment needs to mimic the UE (to test a real network) and mimic the network to test a device. In the former case, the call will terminate to a real public safety answering point (PSAP), and so necessary permissions must be obtained. In the latter case, the network will also provide a virtual PSAP to terminate the call.
	4.b	API requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same eco-system or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	
	4.c	Reference points	The relevant 3GPP reference points cover all interfaces between the device and the fourth generation (4G) network, but are mainly concerned with NAS (S1 - mobility management entity (MME)) for emergency attach, etc. and session initiation protocol (SIP) (Gm) for emergency call without registration.

5	Use case detailed technical specifications	
	<div data-bbox="236 210 678 309"> 5.a Architecture/architectural framework (Figures II.5 and II.6) </div>	<div data-bbox="719 232 1489 539"> </div> <div data-bbox="751 568 1458 636"> <p>Figure II.5 – Enhanced packet core (EPC) non-roaming architecture and reference points</p> </div> <div data-bbox="719 665 1489 1099"> </div> <div data-bbox="751 1137 1458 1171"> <p>Figure II.6 – UE/IMS architecture and reference points</p> </div>

UC03: Rapid network resources deployment for disaster scenarios

1	Use case name/title	Rapid network resources deployment for disaster scenarios
2	Use case short description	
	<div data-bbox="236 1415 678 1514"> 2.a Current practice in testbeds, federation, and testbeds federations </div>	<p>During a disaster, the fixed communication infrastructure could be destroyed or unavailable. Computing and network resources have to be deployed during the rescue operations for robots or unmanned air vehicles (UAVs). Furthermore, communicating devices owned by the survivors can be located through the remaining network infrastructure to rescue them. This requires the deployment of edge services at a given place and at a given time, taking into account the limited number of resources such as robots. Reduction of unnecessary communication should be handled to prioritize the rescue operations. Several parameters should be calculated on the network to ensure the efficient deployment of all the available resources. Such parameters are for instance, estimation of workload in terms of quantity, time and space, the allocation of resources and the path trajectory of each robot.</p>
	<div data-bbox="236 1930 678 1998"> 2.b Gaps and problems solved via the use case </div>	<p>Robot self-deployments, data routing and distributed coordination can be tested on existing platforms, but there is currently a lack of edge and mobile services to enable a single experimentation of the whole use case.</p>

	2.c	Rationale and objective/purpose of the use case	<p>The purpose of the use case is to measure several key performance indicators (KPIs):</p> <ul style="list-style-type: none"> • Accuracy in prediction of required resources • Fair allocation of mobile devices • Improvement in using mobile devices • Time to instantiate a network in an end-to-end manner • Time needed for processing data in real time • Edge-core cloud communication latency
3	Use case high-level technical specification		
	3.a	Type of use case	Creation of a complex experimentation using different testbeds within the research infrastructure.
	3.b	Types of stakeholders, their roles, demarcations, interactions i Types of roles for actors within each stakeholder	Fifth generation (5G) services providers, governmental organizations, civil and military rescue services. Researchers, testbed managers.
	3.c	Scope:	
		i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)	Inter-domain, spanning multiple organizations.
		ii Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, etc. iii Logistical scope <ul style="list-style-type: none"> – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group) 	Multiple organizations can be involved in the different segments of the infrastructure network, worldwide and in different locations. Time plays a crucial role in this use case.

4	Involved testbeds specifications		
	4.a	Testbed type	Public and global 5G networks, edge, RAN and MEC.
	4.b	APIs requirements for Testbed Federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	APIs for the "testbeds federation" would need to be developed and implemented as outlined in [ITU-T Q.4068].
	4.c	Reference points	The relevant reference points that would need to be implemented should be those specified in [ITU-T Q.4068].
5	Use case detailed technical specifications		
	5.a	Architecture/architectural framework	<p>Figure II.7 presents the network architecture for a physical disaster scenario, which should be available for the research infrastructure.</p> <p style="text-align: right;">QSTR-UCFTBS(25)</p> <p>Figure II.7 – Network architecture for a physical disaster scenario [b-SLICES-DS D2.5] Figure 1</p>

UC04: Testbed for smart cities

1	Use case name/title	Testbed for smart cities
2	Use case short description	
	2.a	Current practice in testbeds, federation, and testbeds federations A typical smart city contains a large number of sensors and actuators, generating a huge amount of heterogeneous data to store, analyse and compute. This requires various software and services. The main challenge is the multi-dimensional

			heterogeneity such data type, computation type, software type, etc. Other challenges are, for instance, the security and the energy consumption. All the components of a smart city deployment should be tested in real conditions in a research infrastructure composed of several testbeds.
	2.b	Gaps and problems solved via the use case	There are few testbeds that allow researchers to investigate some of the above-mentioned challenges. For example, distributed decision support system can be evaluated on an existing testbed, but there is currently no testbed capable of executing and validating a complete and complex scenario encountered in smart cities.
	2.c	Rationale and objective/purpose of the use case	<p>This use case intends to analyse the interactions between IoT devices and cloud resources where the applications are executed. It will determine the concrete needs in terms of computation, storage and networks. The scalability and the responsiveness of the building blocks used in a smart city deployment can be evaluated in a controlled environment such as the research infrastructure. Several KPIs can be measured through experimentation:</p> <ul style="list-style-type: none"> • Time needed for event handling • Accuracy on successful event detection • Time to instantiate a network • Time needed for processing data in real time • Edge communication latency
3	Use case high-level technical specification		
	3.a	Type of use case	Creation of a whole experimentation using different testbeds of the research infrastructure.
	3.b	Types of stakeholders, their roles, demarcations, interactions i Types of roles for actors within each stakeholder	5G services providers, Internet of things (IoT) services providers, city authorities and services. Researchers, testbeds managers.
	3.c	Scope:	
		i Domain: inter- or intra-stakeholder span [e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators]	Inter-domain, spanning multiple organizations.
		ii Intra-Stakeholder segments (e.g., CSP core, transport, ran, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...) iii Logistical scope <ul style="list-style-type: none"> – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the federation of specific 	Multiple vendors, companies and organizations can be involved in the different segments of the infrastructure network. Worldwide, this may include different testbeds. Time is crucial in this use case, particularly for event detection. The experiment should have a sufficient duration to determine if all the events are effectively detected.

		assets (per asset/asset group)	
4	Involved testbeds specifications		
	4.a	Testbed type	Public and global 5G networks, IoT networks, edge, RAN and MEC.
	4.b	APIs requirements for Testbed Federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same eco-system or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	APIs for the "testbeds federation" would need to be developed and implemented as outlined in [ITU-T Q.4068].
	4.c	Reference points	The relevant reference points that would need to be implemented should be those specified in [ITU-T Q.4068].
5	Use case detailed technical specifications		
	5.a	Architecture/architectural framework	N/A

UC05: Automated construction and demolition waste management using digital twin for buildings

1	Use case name/title		Automated construction and demolition waste management using digital twin for buildings
2	Use case short description		
	2.a	Current practice in testbeds, federation, and testbeds federations	In the context of construction and demolition waste (CDW), a digital twin is established to trace waste generated during the construction and demolition of a building. This approach, using a digital twin, permits an efficient waste management through an information management workflow which should be tested and validated with the help of testbeds.
	2.b	Gaps and problems solved via the use case	In this use case, several aspects should be implemented and tested such as: <ul style="list-style-type: none"> • Cloud-based collaboration solution • Digital twin implementation • Conformance with standards and protocols

			<ul style="list-style-type: none"> • Interoperability between software components • Security and privacy • Data analytics <p>To realise a whole experiment involving all the above-mentioned aspects, testbeds with specific features should be available.</p>
	2.c	Rationale and objective/purpose of the use case	<p>The utilization of different testbeds for a single, complete experiment permits to measure several KPIs:</p> <ul style="list-style-type: none"> • Reduction in time required for estimating produced waste • Waste reduction percentage • End-end network instantiation • Time required for virtual network function (VNF) deployment • Digital twin communication latency • Time required for processing data in real time
3	Use case high-level technical specification		
	3.a	Type of use case	Complete experiment using different testbeds from research infrastructure.
	3.b	Types of stakeholders, their roles, demarcations, interactions i Types of roles for actors within each stakeholder	5G services providers, IoT services providers, city authorities, civil engineering companies, building construction companies Researchers, testbeds managers, civil engineers.
	3.c	Scope:	
		i Domain: inter- or intra-stakeholder span [e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators]	Inter-domain, spanning multiple organizations.
		ii Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...) iii Logistical scope <ul style="list-style-type: none"> – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group) 	Multiple vendors, companies and organizations can be involved in the different segments of the infrastructure network. Worldwide, this may include different testbeds. A long duration of the experiment is expected.
4	Involved testbeds specifications		
	4.a	Testbed type	Public and global 5G networks, IoT networks, cloud, edge, RAN and MEC.

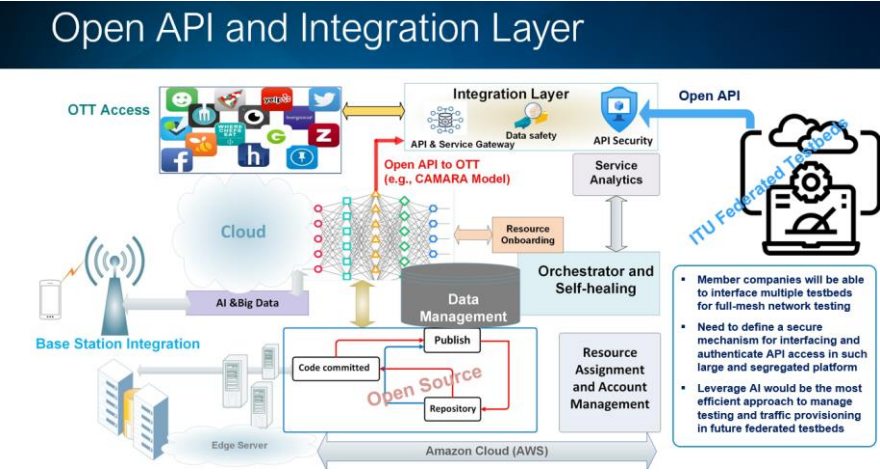
	4.b	APIs requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	APIs for the "testbeds federation" would need to be developed and implemented as outlined in [ITU-T Q.4068].
	4.c	Reference points	The relevant reference points that would need to be implemented should be those specified in [ITU-T Q.4068].
5	Use case detailed technical specifications		
	5.a	Architecture/architectural framework	N/A

UC06: testing of open architecture systems

1	Use case name/title		Testing of open architecture systems
2	Use case short description		
	2.a	Current practice in testbeds, federation, and testbeds federations	<p>Open architecture is a system where different software and hardware components communicate through open standards and interfaces. Testing open architecture systems is essential to ensure that these components are interoperable and compatible with each other, and to guarantee that the overall system meets the desired performance criteria.</p> <p>On the other hand, testbeds are built using commodity software and hardware components, which are readily available and affordable. However, building and using testbeds for open architecture emulations can be a complex and challenging task. The development of a testbed requires specialized expertise in different areas such as networking, software engineering, and system administration.</p> <p>Furthermore, open architecture systems are typically composed of a large number of components, making it difficult to emulate the entire system in a single testbed. The complexity of the system and the need for inter-component communication can make it hard to configure and control the testbed. As a result, the use of testbeds for open architecture emulation requires either investment in developing the necessary expertise, resources, and effort or the development of a new approach through federated testbeds, where one testbed can be built using open-source and open APIs, with messages and connectivity are being evaluated collaboratively through federated testbed dashboards.</p> <p>Among the benefits of federated testbeds is that one or many testbeds are connected through open standards and interfaces to form a larger, distributed testing environment. This allows for the testing of systems that span multiple domains and geographic locations and enables the evaluation of the interactions between different components in a realistic setting.</p>
	2.b	Gaps and problems solved via the use case	An open architecture testing problem can be effectively solved by utilizing an open-source and open API-enabled

			testbed platform. Such a platform provides a flexible and modular environment for testing, which can be easily customized and adapted to meet the needs of any given software application. This Institute of Electrical and Electronics Engineers (IEEE) 5G / sixth generation (6G) innovation tested platform is built using open-source technologies, allowing developers to freely access and modify the source code as needed. Additionally, an open-source testbed platform provides a collaborative environment for testing, enabling developers to work together to identify and solve problems more efficiently. By leveraging open API interfaces according to [ITU-T Q.4068], developers can benefit from the latest testing tools and technologies, while also being able to customize and extend the platform to meet their specific needs. This can help improve the quality and efficiency of software testing, while also reducing the time and resources required.
	2.c	Rationale and objective/purpose of the use case	The rationale behind adopting open source and open APIs in the IEEE 5G/6G innovation testbed is to foster collaboration and innovation across the industry by providing a common platform for researchers, developers, and vendors to experiment, test and validate their solutions. The objective/purpose of adopting open APIs is to ensure interoperability and seamless integration between different systems and components within the testbed, thereby enabling researchers to easily combine and test various solutions. Additionally, open APIs promote transparency and flexibility, enabling researchers to adapt and modify the testbed as needed to support open architecture and measuring/monitoring open API traffic. The latter would gain more and more attention as operators try to find ways to monetize their infrastructure. The goal is to provide platform available to test the concepts of open architecture and enabling technologies as well as open API for over-the-top (OTT) services. Finally, the platform may also be used for developing monitoring and charging tools for monetization.
3	Use case high-level technical specification		
	3.a	Type of use case	Open architecture, Open API, 5G Core, monitoring
	3.b	Types of stakeholders, their roles, demarcations, interactions i Types of roles for actors within each stakeholder	Network operators, OTT, and cloud service providers Testbeds administrators in each CSP involved; test executors
	3.c	Scope:	
		i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)	Inter-domain – spanning multiple operators or multiple clouds for conformity testing. This also involves OTT.
		ii Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry)	All these network segments may play a role in the traffic exchange and measurement as part of open architecture modelling and open API analysis for OTT monetization approaches.

		player/organization/enterprise closed domain, local domain, private network, ...) iii Logistical Scope <ul style="list-style-type: none"> – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group) 	Worldwide, platform is accessed over the cloud (Amazon web services (AWS)).
4	Involved testbeds specifications		
	4.a	Testbed type	Open architecture, open API, 5G Core, monitoring open source.
	4.b	APIs requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	APIs for the testbeds federation would need to be developed and implemented as outlined in [ITU-T Q.4068], APIs for IoT data in smart cities and communities [ITU-T Y.4472], and digital entity architecture framework for Internet of things interoperability [ITU-T Y.4459].
	4.c	Reference points	Relevant reference points that would need to be implemented should be those specified in [ITU-T Q.4068], APIs for IoT data [ITU-T Y.4472], and digital entity architecture framework [ITU-T Y.4459].

5	Use case detailed technical specifications	
	5.a	<p>Architecture/architectural framework</p> <p>Figure II.8 [b-WSHP-ITU-ETSI-IEEE] shows an example of integration layer that consist of API & service gateway and API security module. The gateway will allow API access for OTT or federated testbed to access IEEE innovation testbed elements. The API security module will be used for authenticating APIs. The integration layer would be part of mid/long term evolution to support open architecture branch for IEEE 5G/6G innovation tested as well as federated testbed access.</p>  <p style="text-align: center;">Figure II.8 – Open AI and integration layer</p>

UC07: Federated testbed for cybersecurity

1	Use case name/title	Federated testbed for cybersecurity
2		
Use case short description		
2.a	Current practice in testbeds, federation, and testbeds federations	<p>This federation is composed of the following testbeds experimented with at [b-AICCSA-1] [b-AICCSA-2] [b-AICCSA-3]:</p> <ul style="list-style-type: none"> • IoT testbed • Unified data management (UDM) smart car testbed • Virtual cybersecurity testbed • Wireless cybersecurity testbed <p>The different users, such as researchers, students and trainees, can access these four testbeds by a common interface named universal testbed access interface (UTAI).</p>
2.b	Gaps and problems solved via the use case	<p>Each testbed is handled by a testbed manager. In the cloud, a shared repository of the current state of has been established to collect information concerning the operational state of each testbed. As this repository is shared among different organizations or entities, it is possible to know the operational state of each testbed, independently of the testbed provider. Furthermore, a web portal connected to all the federated testbeds allows users to configure the testbeds, execute the experiments and obtain the results. The configuration of the testbeds includes access control, the specific setup of each testbed and time management. By leveraging the web portal and the information provided in the shared repository of testbeds states, it is possible for the end-users to set up experiments in the federated testbed as a service (FTaaS).</p>

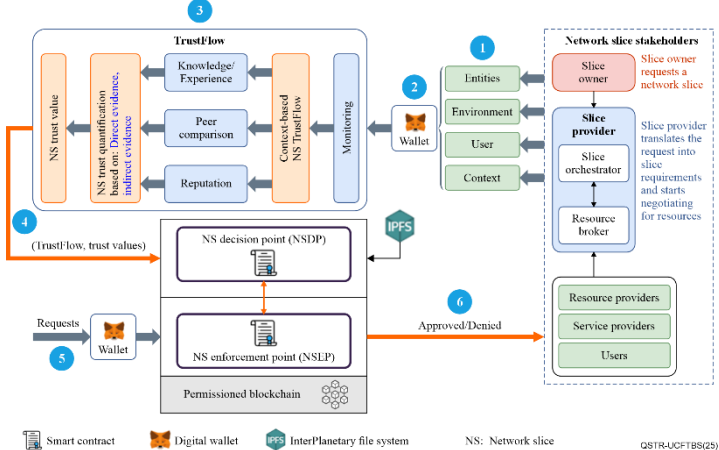
	2.c	Rationale and objective/purpose of the use case	The FTaaS enables the creation of experiments using resources available in different testbeds, not only within the same organization but also in others. It allows the experimentation in different domains, taking advantage of the specific features of each federated testbed.
3	Use case high-level technical specification		
	3.a	Type of use case	Creation of experiments using federated testbeds from different test providers.
	3.b	Types of stakeholders, their roles, demarcations, interactions i Types of roles for actors within each stakeholder	Universities, 5G services providers, governmental organizations. Researchers, students, trainees, testbeds managers.
	3.c	Scope:	
		i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)	Inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators): Inter-domain, spanning multiple organizations.
		ii Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...) iii Logistical scope – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group)	Multiple vendors, organizations and enterprises may be involved in the different segments of the research infrastructure network. 1 Location (countries, states, locations, sites): United States of America. 2 Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group): Time management is carried out through the web portal of the FTaaS. This is an important aspect to consider when setting up an experiment and retrieving its results.
4	Involved testbeds specifications		
	4.a	Testbed type	Public and global 5G networks, edge, RAN and MEC
	4.b	APIs requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding</i>	The FTaaS is based on the APIs, notably those provided by the European Telecommunication Standardization Institute (ETSI) - network function virtualization (NFV) management and network orchestration (MANO) framework.

		<i>security, rights, certification, interfaces, etc.</i>	
	4.c	Reference points	The ETSI-NFV MANO framework.
5	Use case detailed technical specifications		
	5.a	Architecture/architectural framework	<p>Figure II.9 illustrates the architecture at high level of a federated 5G testbed accessible notably through the 5G federated testbed as a service:</p> <p>Figure II.9 – 5G open architecture testbed [b-ARXIV]</p>

UC08: Blockchain based methodology for zero trust modelling and quantification for IMT-2020 networks

1	Use case name/title		Blockchain based methodology for zero trust modelling and quantification for IMT-2020 networks
2	Use case short description		
	2.a	Current practice in testbeds, federation, and testbeds federations	<ul style="list-style-type: none"> Implementing a data collection tool to gather relevant data from the network slice/system. Developing the TrustFlow module that processes real-time data and quantifies the trust of an entity using: deterministic-based quantification and machine learning-based quantification. Developing a zero-trust architecture using blockchain technology with two smart contracts.
	2.b	Gaps and problems solved via the use case	<p>One challenge in the context of IMT-2020 networks and their associated services is the ability to establish accurate trust between the stakeholders. There is a need for a systematic process to continuously evaluate the trustworthiness of an entity which could be a user, application, slice owner, slice provider, or resource provider and enforce zero trust requirements at runtime. Having an accurately measured trust value in such an ecosystem helps a trustor to make an informed decision about whether place itself in a potentially vulnerable position, in case the trustee turns out to have malicious intent.</p>

	2.c	Rationale and objective/purpose of the use case	In IMT-2020 networks, a network slice is defined as a logical network created by partitioning a shared physical infrastructure. Each slice is customized and optimized to meet customers' needs. Network slicing introduces unprecedented security challenges due to its dynamic and diverse structure. Trust in the IMT-2020 ecosystem is a cornerstone for global adaptation and tackling security and privacy risks. In this research, we shed light on the zero trust concept in IMT-2020 using distributed ledger (blockchain). Establishing trust between network slice stakeholders (i.e., slice owners, users, slice resource providers, and service providers).
3	Use case high-level technical specification		
	3.a	Type of use case	Establishing zero trust between stockholders involved in IMT-2020 network slicing.
	3.b	Types of stakeholders, their roles, demarcations, interactions i Types of roles for actors within each stakeholder	
	3.c	Scope:	
		i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)	Inter-domain. Spanning multiple operators.
		ii Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...) iii Logistical scope – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group)	All of these segments will play a role in the blockchain based zero trust. National level. The blockchain based zero trust can operate 24/7 to keep the environment trusted.

4	Involved testbeds specifications		
	4.a	Testbed type	
	4.b	APIs requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	Kafka APIs [b-kafka]
	4.c	Reference points	
5	Use case detailed technical specifications		
	5.a	Architecture/architectural framework	<p>Figure II.10 shows the blockchain-based zero trust architecture for IMT-2020 network slicing [b-AICCSA-4] [b-AICCSA-5] [b-AICCSA-6] [b-AICCSA-8].</p>  <p>Figure II.10 – Blockchain-based zero trust architecture</p>

UC09: Federation of smart city services

1	Use case name/title	Federation of smart city services
2	Use case short description	
	2.a	Current practice in testbeds, federation, and testbeds federations <p>Current practices in most industrial control system adapted for city services are often limited to central control units deployed locally or remotely to manage the water supply infrastructure. This traditional approach increases the risk of cyber-attacks and reduces the resiliency of such critical infrastructure systems. The communication mediums and protocols employed between control systems and remote devices are often inadequate in terms of security as they were not originally designed to address such concerns. This can result in the dissemination of incorrect information to human operators, potentially leading to incorrect actions and a lack of awareness of ongoing attacks. Thus, integrating smart city services across multiple federated services is essential for</p>

			achieving sustainable urban development leading to end-to-end resiliency. A federated approach to smart city services can integrate different critical systems across dispersed locations regardless of implementations techniques, yielding better-coordinated efforts in sharing critical resources and information to optimize overall city resilience. By implementing a federated approach, cities can benefit from increased redundancy, higher flexibility in resource allocation, and improved resilience against potential threats. Further, researchers and advocates can utilize the federation to gather valuable data generated for real-world or simulated scenarios, which can lead to the development of innovative strategies and solutions for enhanced management systems in urban environments.
	2.b	Gaps and problems solved via the use case	The exceptional need for federated smart city services arises from the lack of a unified approach to integrated diverse systems, which limits the understanding of the full potential for futuristic city services. A federated system can address such challenges by enabling the integration of diverse sensors, data sources, and communication protocols, allowing the use of resources beyond the control of a single entity. As such, further development of traditional systems could be investigated through collaboration among multiple stakeholders, deployment of advanced solutions across different levels, and by addressing the complexities that emerge from different operational domains.
	2.c	Rationale and objective/purpose of the use case	The framework for federated smart city services should allow the integration of various cyber-physical systems (CPSs) into a single federation, thereby enabling seamless communication and interoperability among the different entities. As a result, the implementation of different testing scenarios and evaluation of the performance of various CPSs becomes more accessible and efficient.
3	Use case high-level technical specification		
	3.a	Type of use case	Enabling cross-domain communication and interoperability of heterogeneous CPSs through a unified federation platform.
	3.b	Types of stakeholders, their roles, demarcations, interactions i Types of roles for actors within each stakeholder	Government entities, facilities owners, researchers and academia. Testbeds administrators in each CSP involved; test executors.
	3.c	Scope: i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)	Inter-domain – spanning multiple operators (covering multiple sites owing CPS).

		<ul style="list-style-type: none"> ii Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...) iii Logistical scope <ul style="list-style-type: none"> – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group) 	<p>All these network segments may play a role in the smart city services scenarios, and multiple vendors may be involved in the infrastructure network segments and management and control layer.</p> <p>This applies globally, nationally and across country borders. If the full E2E test scenarios can be covered through the federated testbeds of the operators, then there may not be any time constraints in the use of the testbeds. However, if part of the assets required for the E2E test scenarios can only be provided through a production network, then it is likely that such tests can only be conducted during the non-busy hours of the production network (e.g., in the night).</p>
4	Involved testbeds specifications		
	4.a	Testbed type	CSP core network, transport networks, edge
	4.b	APIs requirements for Testbed Federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	APIs for the testbeds federation would need to be developed and implemented internally.
	4.c	Reference points	The relevant reference points that would need to be implemented should be: testbed manager, shared testbed current status, FCTaaS.
5	Use case detailed technical specifications		
	5.a	Architecture/architectural framework	Figures II.11 and II.12 show the steps required to establish the federation of any smart services CPS into a single shared status, enabling data exchange and real-time experimentation. [b-AICCSA-6] [b-AICCSA-7]. Figure II.11 illustrates how user access and the establishment of federated connections among heterogeneous testbeds are enabled.

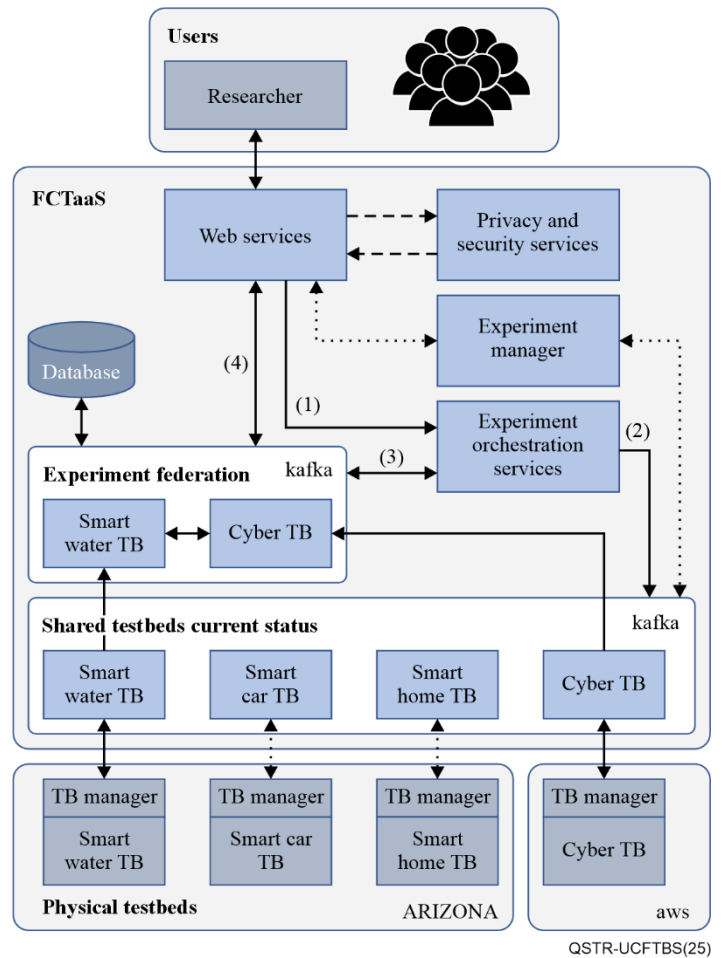


Figure II.11 – General architecture for the federation connecting different user to dispersed CPSs

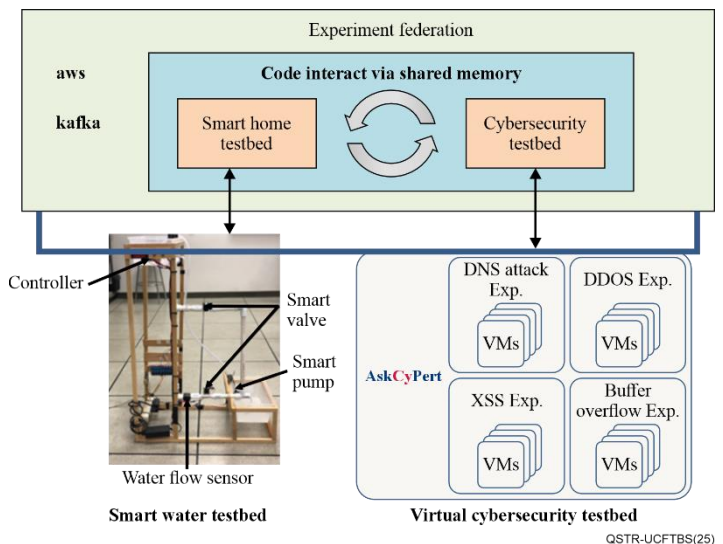


Figure II.12 – Real-time data exchange and communication in the federated CPS experiment

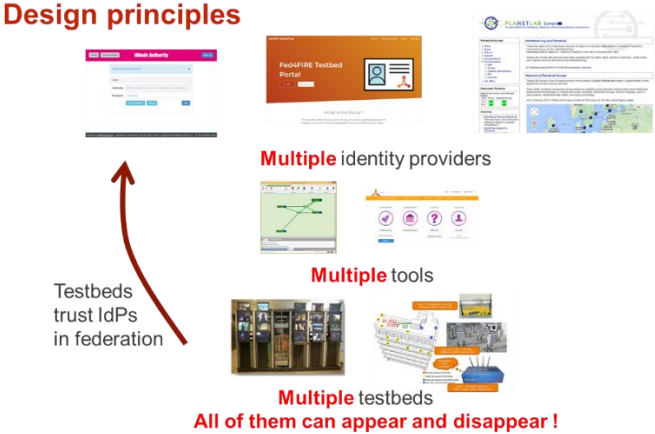
Figure II.12 shows how, after the establishment of the experiment, data are shared in real-time through the federation. Current sensors and actuators data are exchanged through the shared current status implemented in the FCTaaS [b-AICCSA-6] [b-AICCSA-7] [b-AICCSA-9]. The

			federation allows both entities to communicate, enhancing performance according to customers' needs and facilitating further improvements to urban city infrastructure. Further, it enables a deeper understanding of the system's cybersecurity resilience and facilitate the development of advanced security measures.
--	--	--	---

UC10: Federated testbed for cloud and networking research

1	Use case name/title	Federated testbed for cloud and networking research [b-Imec] [b-Fed4FIRE]
2	Use case short description	
	2.a Current practice in testbeds, federation, and testbeds federations	<p>The experimental validation of wired network research (ATM with connected servers) and wireless network research (Wi-Fi based) started in 1998. Each researcher had his own 'testbed' of 5-10 nodes which made it very expensive and very limited in scale.</p> <p>From 2005 onwards, all hardware was combined into a single testbed (one for wired networking research, one for wireless networking research) [b-Imec] which made it possible to have bigger scale experiments. However, it emerged that some researchers needed both testbeds (for related research), which had different toolsets, creating a problem they tried to (ab)use one testbed for a use case more typical of the other. It evolved also that people wanted to use both testbeds at the same time (e.g., core wired network with wireless clients).</p> <p>At that moment the Fed4FIRE (Federation for Future Internet Research and Experimentation) project [b-Fed4FIRE] was started to federate similar testbeds across Europe. With a single tool and account, researchers could now easily use multiple testbeds and even interconnect them with layer 2 connections.</p>
	2.b Gaps and problems solved via the use case	<p>It was made easier for experimenters to use or combine multiple testbeds by providing:</p> <ul style="list-style-type: none"> – A single account – A single tool <p>Multiple testbeds are useful to:</p> <ul style="list-style-type: none"> – Scale up experimenters – Use/combine special resources only available in specific testbeds – Redundancy: e.g., if a testbed is down or in maintenance or fully in use, you can use another one – Re-use experiments/classes: ideal for repeatability – To compare different environments or hardware <p>Some of the things are possible with multiple accounts/tools, but if you want to combine (e.g., with interconnectivity) or repeat experiments, then it is not possible without a federation.</p>
	2.c Rationale and objective/purpose of the use case	Make it easier to use multiple testbeds and enable specific experiments that would require significant manual interventions (e.g., to set up interconnectivity or to repeat the same experiment using different tools)

3	Use case high-level technical specification		
	3.a	Type of use case	Federation of testbeds that are remotely usable
	3.b	Types of stakeholders, their roles, demarcations, interactions i Types of roles for actors within each stakeholder	Testbed administrators, network administrators for interconnectivity, experimenters
	3.c	Scope:	
		i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)	Not applicable
ii Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...) iii Logistical scope – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group)		Not applicable Globally applicable (e.g., Fed4FIRE federation in Europe, GENI/Cloudlab federation in US, are federated) No time constraints	
4	Involved testbeds specifications		
	4.a	Testbed type	Cloud, wireless, IoT, graphics processing unit (GPU) testbeds
	4.b	APIs requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	The current APIs used for federation are the GENI aggregate manager and federation APIs [b-GENI]

	<p>4.c</p> <p>Reference points (Figure II.13)</p>	<p>Design principles</p>  <p>Multiple identity providers</p> <p>Multiple tools</p> <p>Multiple testbeds</p> <p>All of them can appear and disappear !</p> <p>Figure II.13 – Reference points for UC10 [b-IoT-week-2021]</p>
<p>5</p>	<p>Use case detailed technical specifications</p>	<p>5.a</p> <p>Architecture/architectural framework</p> <p>See Figure II.13. The technology used is extensible markup language-remote procedure call (XML-RPC) with client-based authentication (Figure II.14). The testbeds implement the aggregate manager (AM) API, while the identity provider(s) implement the user and slice APIs. The tool used by the user calls all APIs (identity provider + one or more testbeds). A federation consists of testbeds which trust one or more identity providers.</p> <p>The resource specification (RSpec) is used to describe resources. (https://fed4fire-testbeds.ilabt.iminds.be/asciidoc/rspec.html).</p> <p>A light federation model is to federate through Open Authorization (OAuth) which only shares the account, no APIs. (https://doc.fed4fire.eu/testbed_owner/oauth.html)</p> <p>We use active monitoring (setting up end-to-end experiments) to verify the health of the testbeds and federation (https://fedmon.fed4fire.eu/overview/). We offer tools to test the APIs easily.</p>

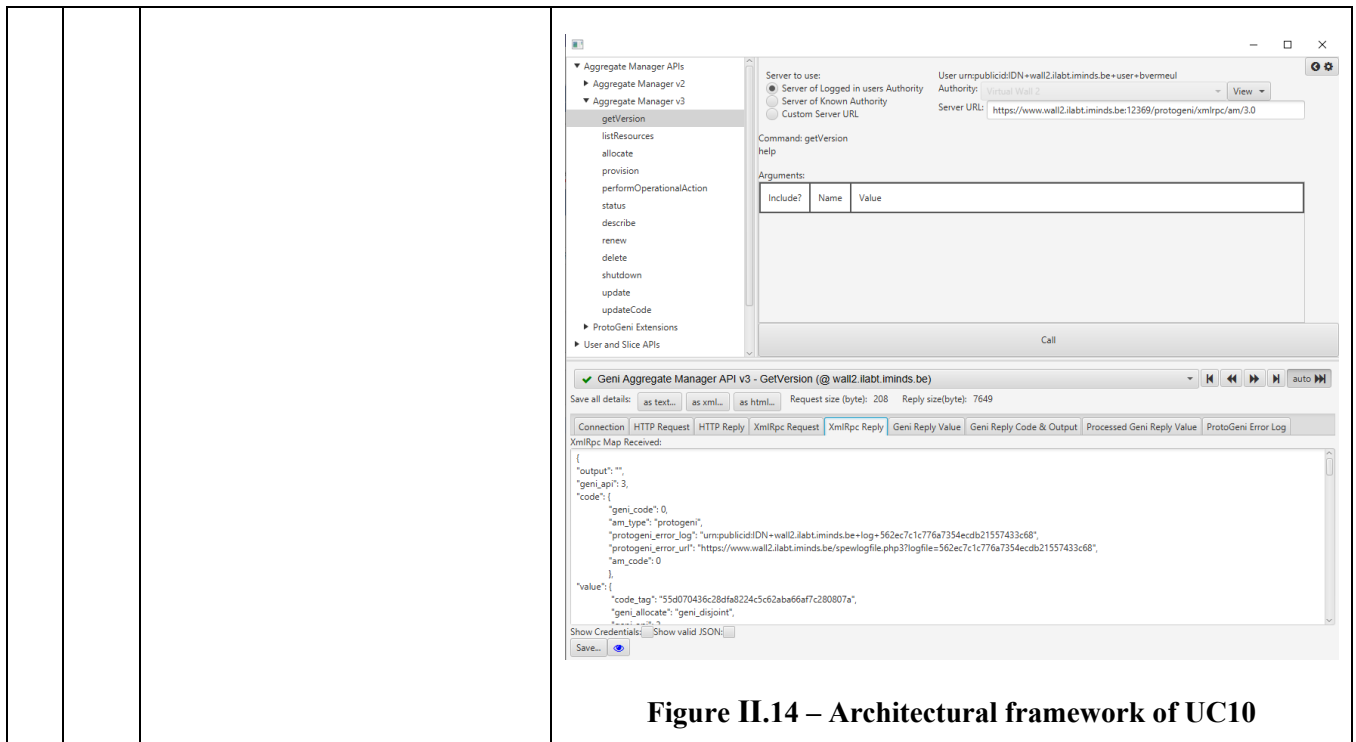


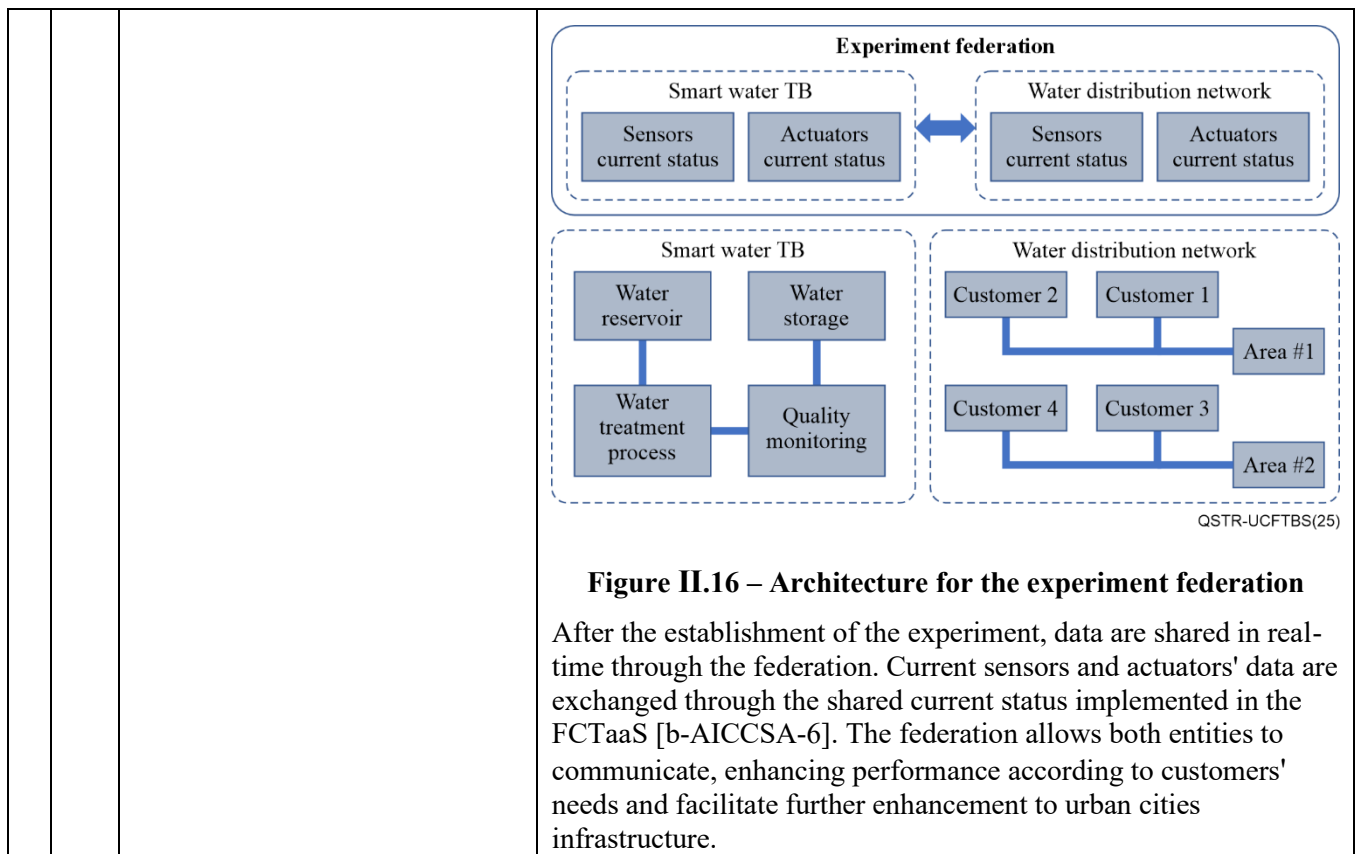
Figure II.14 – Architectural framework of UC10

UC11: Federation of smart city water treatment and distribution services

1	Use case name/title	Federation of smart city water treatment and distribution services
2	Use case short description	
2.a	Current practice in testbeds, federation, and testbeds federations	Current practices in water management are often limited to central control units deployed locally or remotely to manage the water supply infrastructure. This traditional approach increases the risk of cyber-attacks and reduces the resilience of such critical infrastructure systems. Thus, integrating smart city water treatment and distribution across multiple federated services is essential for achieving sustainable urban development. A federated approach to smart city water treatment and distribution services can integrate diverse sensors and actuators from dispersed locations while adapting different implementations techniques yielding better-coordinated efforts in sharing critical resources and information to optimize overall system resilience. By implementing a federated approach, cities can benefit from increased redundancy, higher flexibility in resource allocation, and improved resilience against potential threats. Further, researchers and advocates can utilize the federation to gather valuable data generated for real-world or simulated scenarios, which can lead to the development of innovative strategies and solutions for enhanced water management in urban environments.
2.b	Gaps and problems solved via the use case	The exceptional need for federated smart city water treatment and distribution services arises from the lack of a unified approach to integrating diverse systems, which limits the understanding of the full potential for futuristic city services. A federated system can address such challenges by enabling the integration of diverse sensors, data sources, and communication protocols allowing the use of resources beyond a single entity. As such, further development of traditional systems could be investigated through collaboration among multiple stakeholders, deployment of

			advanced solutions across different levels, and addressing the complexities that emerge from different operational domains.
	2.c	Rationale and objective/purpose of the use case	The framework for federated smart city water treatment and distribution services should allow the integration of various cyber-physical systems (CPSs) into a single federation, enabling seamless communication and interoperability among the different entities. As a result, enabling the implementation of different testing scenarios and evaluation of the performance of various CPSs becomes more accessible and efficient.
3	Use case high-level technical specification		
	3.a	Type of use case	Enabling cross-domain communication and interoperability of heterogeneous CPSs through a unified federation platform.
	3.b	Types of stakeholders, their roles, demarcations, interactions i Types of roles for actors within each stakeholder	Government entities, facility owners, researchers and academia Testbeds administrators in each CSP involved; test executors
	3.c	Scope: i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators) ii Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...) iii Logistical scope – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group)	inter-domain – spanning multiple operators (covering multiple sites owing CPS) All these network segments may play a role in the smart water treatment scenarios, and multiple vendors may be involved in the infrastructure network segments and management and control layer. Worldwide, nationally and across country borders. If the full E2E test scenarios can be covered through the federated testbeds of the operators then there may not be any time constraints in the use of the testbeds, but if part of the assets required for the E2E test scenarios can only be provided through a production network then it may likely be that such tests can only be conducted during the non-busy hours of the production network (e.g., in the night).
4	Involved testbeds specifications		
	4.a	Testbed type	CSP core network, transport networks, edge

4.b	APIs requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	APIs for the testbeds federation would need to be developed and implemented internally.
4.c	Reference points	The relevant reference points that would need to be implemented should be: testbed manager, shared testbed current status, FCTaaS
5	Use case detailed technical specifications 5.a Architecture/architectural framework	<p>Figure II.15 shows the steps required to establish the federation of the smart water treatment and distribution network, which contains multiple disrupted sensors [b-AICCSA-6].</p> <p>QSTR-UCFTBS(25)</p> <p>Figure II.15 – The general architecture for the federation connecting different user to dispersed CPSs</p>



UC12: End-to-end design, development of IMT-2020 testbed

1	Use case name/title	End-to-end design, development of IMT-2020 testbed [b-IITH]	
2	Use case short description		
	2.a	Current practice in testbeds, federation, and testbeds federations	
	2.b	Gaps and problems solved via the use case	
	2.c	Rationale and objective/purpose of the use case	End-to-end features like UE registration, protocol data unit (PDU) session establishment for successfully supporting the data plane services covering a UE+RAN emulator and the 5GC. End-to-end UE registration in IMT-2020 networks is highlighted in Appendix III.
3	Use case high-level technical specification		
	3.a	Type of use case	
	3.b	Types of stakeholders, their roles, demarcations, interactions	
		i Types of roles for actors within each stakeholder	
	3.c	Scope:	

		i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)	Not known
		ii Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...)	Core
		iii Logistical scope <ul style="list-style-type: none">– Location: (countries, states, locations, sites)– Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group)	Not known
4	Involved testbeds specifications		
	4.a	Testbed type	
	4.b	APIs requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	
	4.c	Reference points	

5	Use case detailed technical specifications	
5.a	Architecture/ architectural framework	<p>Multiple domains and parts are involved specifically, RAN+UE emulator and 5GC.</p> <p>Dependency on the RAN and UE side changes at the RAN+UE emulator for end-to-end integration testing.</p> <p>Inter-NF dependency: Multiple network functions (NFs) are involved like access and mobility management function (AMF), which depends on the authentication server function (AuSF) to complete the UE registration.</p> <p>Relevant design and implementation have to be done on all the dependent NFs.</p> <p>The figure in Appendix III depicts the end-to-end call flow from [3GPP TS 23.502] for implementing the UE registration across UE, RAN, and the different NFs of 5GC.</p> <p>Figure II.17 depicts the design of AMF with various layers in the implementation of the protocol stack on N1-N2 interfaces, service-based interfaces (SBIs), and the respective modules. Similar designs and implementations are incorporated at other NFs such as AuSF, UDM, unified data repository (UDR), session management function (SMF), network repository function (NRF), etc.</p> <div data-bbox="762 869 1347 1323"> </div> <p>Figure II.17– High-level view of AMF design</p> <p>Logging and tracing features are helpful for large-scale testing. This is enabled or disabled based on the severity of the specific feature tested.</p> <p>Error handling code must be present – not everything we assume works smoothly. For example, to check if the memory allocation is successful for a certain function to be decoded or to be encoded. If not release any memory previously allocated so far in that function.</p> <p>Security requirements should not be ignored (like marking them as 'for further study') but should be incorporated for every feature added to the 5GC design. This is applicable to all the NFs as appropriate.</p> <p>Code coverage testing – Test cases shall be developed with a static code analysis tool to check if a block of code is needed or simply placed as a dead code.</p>

UC13: continuous integration/continuous deployment framework

1	Use case name/title	continuous integration/continuous deployment (CI/CD) framework
2	Use case short description	
	2.a	Current practice in testbeds, federation, and testbeds federations
	2.b	Gaps and problems solved via the use case
	2.c	Rationale and objective / purpose of the use case
3	Use case high-level technical specification	
	3.a	Type of use case
	3.b	Types of stakeholders, their roles, demarcations, interactions
	3.c	Scope:
	i	Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)
	ii	Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...)
	iii	Logistical scope
		– Location: (countries, states, locations, sites)
		– Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group)
4	Involved testbeds specifications	
	4.a	Testbed type

	<p>4.b APIs requirements for testbed federations (if known)</p> <p><i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i></p>	
	<p>4.c Reference points</p>	
5	<p>Use case detailed technical specifications</p>	
	<p>5.a Architecture/architectural framework</p>	<p>CI/CD must be built from the beginning.</p> <p>Adding new features in the testbed requires changes in the CI/CD.</p> <p>Developing new features may be across NFs of the 5GC. For example, supporting end-to-end network slicing requires changes on AMF, UDM, SMF and user plane function (UPF). The end-to-end sequence diagram of network slicing is shown in Appendix IV.</p> <ol style="list-style-type: none"> 1 Changes at the AMF <p>AMF should decode the "Requested network slice selection assistance information (NSSAI)" information element (IE) from the "NAS UE registration" message to interpret its value. It should encode adding allowed NSSAI IE to send towards the UE in the NAS registration accept. In the process, it should store the allowed slices for the corresponding UE, so that when the UE further requests to establish the PDU session, it can verify if the UE is making the request for the slice which it is allowed to.</p> 2 Changes at the RAN+UE Emulator <ol style="list-style-type: none"> a Here, the UE should send the requested NSSAI IE in the NAS registration message. Therefore, this IE had to be additionally encoded to fit in this message before sending it to the AMF. b Decoding the allowed NSSAI field from the initial context setup next generation application protocol (NGAP) message and NAS registration accept message. c Correct slice service type (SST) value has to be placed in the mobility management NAS (MM-NAS) transport for the corresponding PDU session establishment message. d New run-time configuration field to indicate the value for the requested NSSAI IE. <p>Additionally, this new feature demands changes in the CI/CD framework by adding a new test case in the automation script for precondition testing. Integration must occur with existing testbed code.</p> <p>Hence, adding new features consists of two parts: (1) product CI/CD and (2) scripting and automation. There are challenges in synchronizing the CI/CD-based regression with the corresponding changes in the testbed. As more complex features evolved in the 3GPP NFs, we had to plug in the corresponding</p>

			changed NFs in the testbed. Additionally, we also had to make automated, scripted changes in the testbed test cases. Additionally, to ease the debugging and performance benchmarking, corresponding changes had to be made in the logging, tracing, and configuration management modules.
--	--	--	--

UC14: Integration testing with any commercial RAN and UE

1	Use case name/title	Integration testing with any commercial RAN and UE	
2	Use case short description		
	2.a	Current practice in testbeds, federation, and testbeds federations	
	2.b	Gaps and problems solved via the use case	<div>1 Parameters Configuration<ul style="list-style-type: none">PLMNSlicing supportApplications-specific configurations</div> <div>2 3GPP Release version mismatch<ul style="list-style-type: none">For example: Separate registration accept message instead of inside the initial context setup request message from AMF to RANMismatch in the IEs of the NGAP messages between AMF and RAN, and general packet radio service (GPRS) tunnelling protocol (GTP) messages between UPF and RAN.</div> <div>Simultaneous multi-version handling of 3GPP TS, vendor-specific extensions, handled with runtime configuration control and build-time control macros.</div>
	2.c	Rationale and objective/purpose of the use case	End-to-end integration. This is very much required for testing the end-to-end call flows of UE procedures on the control plane and data plane services, with multiple stakeholders interoperating across UE, RAN, and the 5GC.
3	Use case high-level technical specification		
	3.a	Type of use case	
	3.b	Types of stakeholders, their roles, demarcations, interactions <div>i Types of roles for actors within each stakeholder</div>	
	3.c	Scope:	
i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)		Not known	

	3.b	Types of stakeholders, their roles, demarcations, interactions i Types of roles for actors within each stakeholder	
	3.c	Scope:	
		i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)	Not known
		ii Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...) iii Logistical scope – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group)	Core Not known
4	Involved testbeds specifications		
	4.a	Testbed type	
	4.b	APIs requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	
	4.c	Reference points	
5	Use case detailed technical specifications		
	5.a	Architecture/architectural framework	For large-scale UE testing [b-UERANSIM-1] instantiates a new docker container for each UE. This is not suitable for testing thousands of UEs in a single host. Therefore, changes to the RAN+UE emulator are needed. The following are key takeaways: 1 Some open-source codebases can be useful for end-to-end functional testing but not for non-functional testing (e.g., load, stress testing as described above).

			2 Moreover, an open-source codebase can impose hardware resources/test setup limitations or mandate more resources overall. Hence, it is important to ensure the compatible emulator (like RAN+UE) is built to support large-scale UE testing.
--	--	--	--

UC16: Orchestration

1	Use case name/title	Orchestration
2	Use case short description	
	2.a Current practice in testbeds, federation, and testbeds federations	
	2.b Gaps and problems solved via the use case	Leveraging open-source software. The open-source MANO (OSM) [b-OSM] release is upgraded regularly. As a result, dependency on the previous version, which the testbed was previously deployed, becomes a challenge to resolve any related issues on the OSM. It is also difficult to make changes and get support on the previous versions.
	2.c Rationale and objective/purpose of the use case	Orchestration is needed to support auto-scaling, high availability monitoring, and to leverage it further for analytics and building cognitive autonomous networks. Open source MANO – An ETSI -compliant NFV-based orchestrator for network services and containers.
3	Use case high-level technical specification	
	3.a Type of use case	
	3.b Types of stakeholders, their roles, demarcations, interactions i Types of roles for actors within each stakeholder	
	3.c Scope:	
	i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)	Not known
	ii Intra-stakeholder segments (e.g., CSP core, transport, RAN, edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...)	Core
	iii Logistical scope – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the	Not known

		federation of specific assets (per asset/asset group)	
4	Involved testbeds specifications		
	4.a	Testbed type	
	4.b	APIs requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	
	4.c	Reference points	
5	Use case detailed technical specifications		
	5.a	Architecture/architectural framework	Dependency on the open-source software for smooth integration with the testbed. Dedicated setup has to include orchestration for both virtual machine (VM) or container-based deployments. This will help in regular updates and upgrades whenever any changes in the releases of the open-source software (OSM orchestrator) [b-OSM], being used. Additionally, intent-based handling can be considered to evaluate the influence of it on the orchestration and deployment of the needed architecture.

UC17: Standards version compliance check for error-free interoperability between RAN and 5GC testbeds

1	Use case name/title	Standards version compliance check for error-free interoperability between RAN and 5GC testbeds
2	Use case short description	
	2.a	Current practice in testbeds, federation, and testbeds federations
	2.b	Gaps and problems solved via the use case Message structure misinterpretation and feature availability issues arising due to standards release version mismatch.
	2.c	Rationale and objective/purpose of the use case A solution for checking standards version compliance between the RAN and 5GC testbeds to avoid issues such as:

			For example: Adding run-time configuration parameters to enable/disable GTP extension header support at the core and RAN sides, enable/disable separate registration accept message instead of inside the initial context setup request msg from AMF to RAN
--	--	--	---

UC18: Support for zero trust architecture in federated testbeds

1	Use case name/title	Support for zero trust architecture in federated testbeds
2	Use case short description	
	2.a Current practice in testbeds, federation, and testbeds federations	
	2.b Gaps and problems solved via the use case	<p>Security issues that may arise due to testbeds (e.g., RAN and 5GC) with no mutual trust between each other participating in the federated testbed setup, such as:</p> <ul style="list-style-type: none"> • Exploitation of testbed resources due to access by a malicious testbed user/other compromised testbed. • Increased attack surface of a testbed due to vulnerabilities present in other testbeds in a federated setup.
	2.c Rationale and objective/purpose of the use case	To provide a secure environment in case of federated testbed setup, implementing zero trust architecture.
3	Use case high-level technical specification	
	3.a Type of use case	
	3.b Types of stakeholders, their roles, demarcations, interactions	
	i Types of roles for actors within each stakeholder	
	3.c Scope:	
	i Domain: inter- or intra-stakeholder span (e.g., for a CSP stakeholder, within the same CSP/operator or spanning multiple operators)	Not known
	ii Intra-stakeholder segments (e.g., CSP core, transport, RAN, Edge, MEC, or vendor/industry player/organization/enterprise closed domain, local domain, private network, ...)	RAN, Core
	iii Logistical scope <ul style="list-style-type: none"> – Location: (countries, states, locations, sites) – Time: time constraints and windows (when known and where applicable) for the federation of specific assets (per asset/asset group) 	Not known
4	Involved testbeds specifications	

	4.a	Testbed type	
	4.b	APIs requirements for testbed federations (if known) <i>NOTE – It is necessary to differentiate between internal and third-party (within the same ecosystem or value chain). Internal and external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.</i>	
	4.c	Reference points	
5	Use case detailed technical specifications		
	5.a	Architecture/architectural framework	<p>A Zero Trust Architecture (ZTA) should be incorporated to prevent security breaches [b-NIST-ZTA]. ZTA is a cybersecurity framework designed to prevent data breaches by eliminating the assumption that entities within a network can be trusted. Instead of relying on traditional perimeter-based security measures, ZTA focuses on strict access controls and continuous authentication. It mandates the verification of every request for resources, regardless of the user's location or the network from which the request originates. By adopting the principle of "never trust, always verify," ZTA helps organizations enhance their security posture in an increasingly complex and dynamic threat landscape.</p> <p>These changes need to be made at the testbeds participating in the federated setup to make them secure against unauthorised access to protect the testbed resources.</p> <p>For instance, a scenario where slicing is supported by the RAN and the core testbeds, was considered. If the SMF within the 5GC is compromised in such a way that it causes cross-slice disruption by improperly sharing tunnel endpoint identifiers (TEIDs) between the RAN and UPF, it might lead to a data flooding attack towards the RAN/UPF Instance initiated from either of the sides.</p> <p>There was a scenario suggested by [b-IEEE-netsoft-2023]. The preventive measures considered in this scenario can be incorporated within the testbeds involved.</p> <p>Additionally, following operations can be incorporated within the federated testbed framework using the principles of ZTA:</p> <ul style="list-style-type: none"> • Defining policies for controlled access to the RAN/5GC testbed resources to prevent their misuse in an unauthorised manner. • Verifying the authenticity of the RAN/5GC testbed before granting it permission to establish connection with the other testbed in the federated setup. • Remote attestation can be used to verify that the RAN/5GC testbed incorporates the required security measures in its runtime environment. <p>NOTE – Remote attestation is a method by which a host (client) authenticates its hardware and software configuration to a remote host (server).</p>

Appendix III

End-to-end UE registration in IMT-2020 networks

Figure III.1 depicts the end-to-end call flow of the UE registration (as given in [3GPP TS 23.502]) implemented in IMT-2020 testbed.

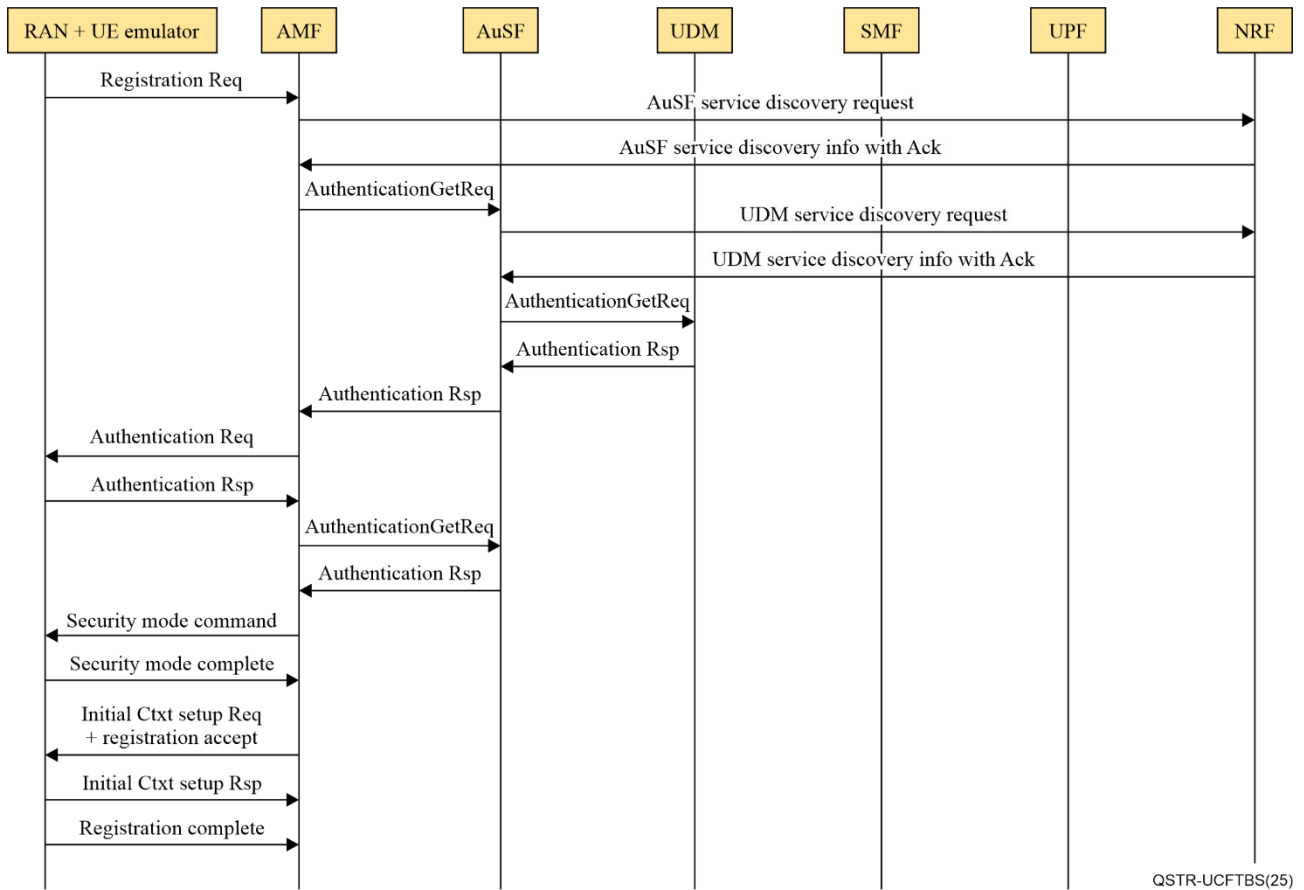


Figure III.1– End-to-end call flow of the UE registration

Appendix IV

End-to-end network slicing for IMT-2020

Figure IV.1 depicts the end-to-end call flow of the slice selection procedure during UE registration where the UE requests for slice services using requested NSSAI(s).

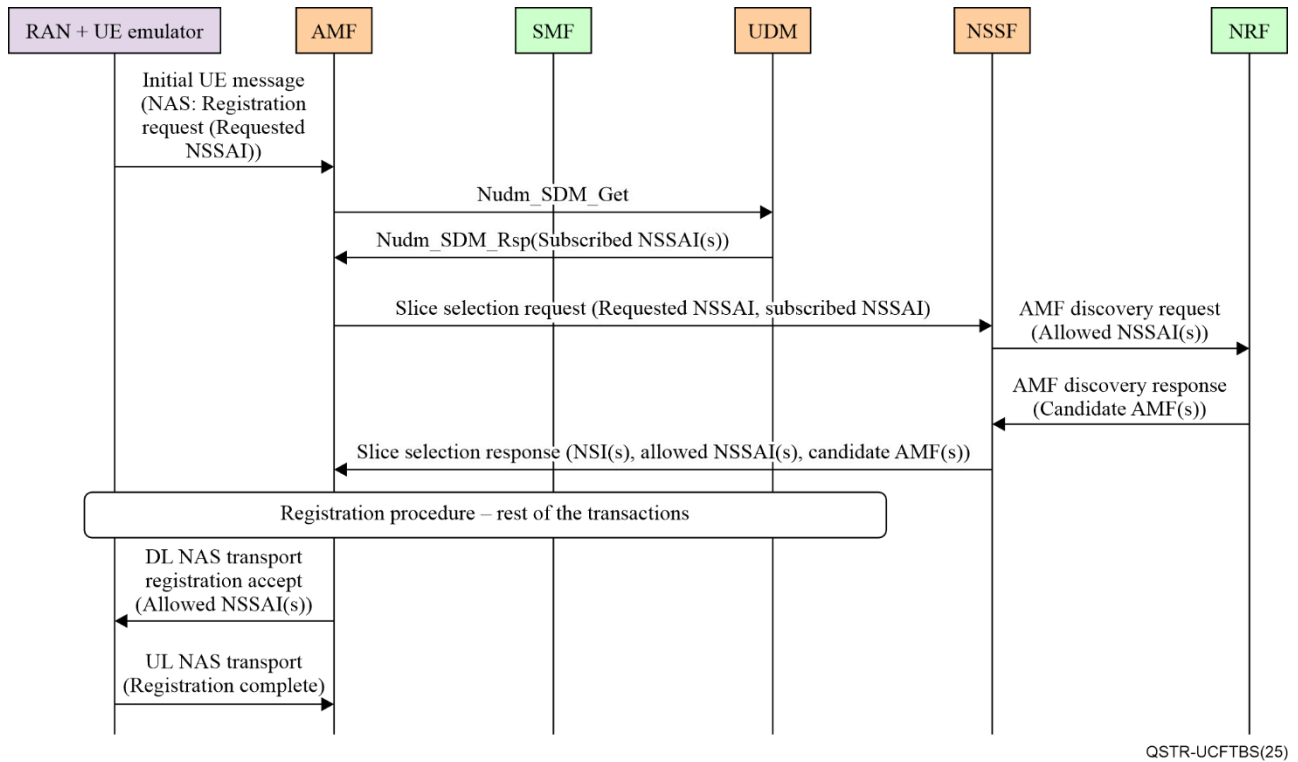


Figure IV.1– End-to-end call flow of the slice selection procedure during UE registration

Bibliography

- [b-AICCSA-1] H. A. Kholidy, A. Berrouachedi, E. Benkhelifa and R. Jaziri (2023), *Enhancing Security in 5G Networks: A Hybrid Machine Learning Approach for Attack Classification*, 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Giza, Egypt, 2023, pp. 1-8, doi: 10.1109/AICCSA59173.2023.10479294.
- [b-AICCSA-2] A. Boualem, A. Berrouachedi, M. Ayaida, H. Kholidy and E. Benkhelifa (2023), *A New Hybrid Cipher based on Prime Numbers Generation Complexity: Application in Securing 5G Networks*, 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Giza, Egypt, pp. 1-8, doi: 10.1109/AICCSA59173.2023.10479316.
- [b-AICCSA-3] H. A. Kholidy (2023), *A Smart Network Slicing Provisioning Framework for 5G-based IoT Networks*, 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), San Antonio, TX, USA, pp. 104-110, doi: 10.1109/IOTSMS59855.2023.10325712.
- [b-AICCSA-4] H. A. Kholidy et al. (2023), *Secure the 5G and Beyond Networks with Zero Trust and Access Control Systems for Cloud Native Architectures*, 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Giza, Egypt, 2023, pp. 1-8, doi: 10.1109/AICCSA59173.10479308.
- [b-AICCSA-5] A. A. Abushgra, H. A. Kholidy, A. Berrouachedi and R. Jaziri (2023), *Innovative Routing Solutions: Centralized Hypercube Routing Among Multiple Clusters in 5G Networks*, 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Giza, Egypt, pp. 1-7, doi: 10.1109/AICCSA59173.2023.10479277.
- [b-AICCSA-6] I. Almazyad, S. Shao, S. Hariri and H. A. Kholidy (2023), *Anomaly Behavior Analysis of Smart Water Treatment Facility Service: Design, Analysis, and Evaluation*, 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Giza, Egypt, pp. 1-7, doi: 10.1109/AICCSA59173.2023.10479312.
- [b-AICCSA-7] H. A. Kholidy (2023), *A Smart Network Slicing Provisioning Framework for 5G-based IoT Networks*, 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), San Antonio, TX, USA, pp. 104-110, doi: 10.1109/IOTSMS59855.2023.10325712.
- [b-AICCSA-8] Elmadani, S., Hariri, S., & Shao, S. (2022). *Blockchain Based Methodology for Zero Trust Modeling and Quantification for 5G Networks*. In 2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA) December, (pp. 1-9). IEEE.

- [b-AICCSA-9] Mamun, M., Lin, Y. Z., Almazyad, I., Shao, S., Satam, S., Hariri, S., & Satam, P. *Federated Cybersecurity Testbed as a Service (Fctaas): A Framework to Federate Cybersecurity Testbeds*. Available at SSRN 4643053.
- [b-ARXIV] <<https://arxiv.org/pdf/2112.13072>> [Accessed: 30 July 2025].
- [b-Fed4FIRE] <<https://www.fed4fire.eu/>> [Accessed: 30 July 2025].
- [b-GENI] <<https://geni-nsf.github.io/CommonFederationAPI/CommonFederationAPIv2.html>> [Accessed: 30 July 2025].
- [b-GSMA IR.25] GSMA, *IR.25 VoLTE Roaming Testing, version 8.0*.
- [b-GSMA PRD IR.65] GSMA, *IR.65 IMS Roaming and Interworking Guidelines v34.0*.
- [b-IEEE-netsoft-2023] S. Vittal, U. Dixit, S. P. Sovitkar, K. Sowjanya and A. Antony Franklin (2023), *Preventing Cross Network Slice Disruptions in a Zero-Trust and Multi-Tenant Future 5G Networks*, IEEE 9th International Conference on Network Softwarization (NetSoft), Madrid, Spain, pp. 227-231.
- [b-IITH] Indian Institute of Technology, Hyderabad, <<https://newslab.iith.ac.in/5gtest-bed.html>> [Accessed: 30 July 2025].
- [b-Imec] Imec iLab.t testbeds (Virtual Wall, w-iLab.t and GPULab), <<https://doc.ilabt.imec.be/>> [Accessed: 30 July 2025].
- [b-IoT-week-2021] IoT week 2021, Aug 30-Sep 3, online, Brecht Vermeulen, *Federated testbeds in Fed4FIRE*, <<https://iotweek.blob.core.windows.net/iotweek2021friday/1-%20MAKING%20TESTBEDS%20INTEROPERABLE.mp4>> [Accessed: 30 July 2025].
- [b-ITU-T QSTR.FTT] ITU-T QSTR.FTT (ex. Q.FTT) (2025), *Federated testbeds taxonomy*.
- [b-kafka] <<https://kafka.apache.org/>> [Accessed: 30 July 2025].
- [b-NIST-ZTA] <<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>> [Accessed: 30 July 2025].
- [b-OSM] <<https://osm.etsi.org/>> [Accessed: 30 July 2025].
- [b-SLICES-DS D2.5 Figure 1] SLICES-DS D2.5, *Use cases validated* <https://www.slices-ds.eu/wp-content/uploads/2022/12/SLICES-DS_D2.5_approval_disclaimer.pdf> [Accessed: 30 July 2025].
- [b-UERANSIM-1] <<https://github.com/algungr/UERANSIM>> [Accessed: 30 July 2025].
- [b-UERANSIM-2] <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20210316/Documents/Anwer%20AI%20Dulaimi_Future%20Networks%20Industry%20Consortium_ITU_Workshop.pdf> [Accessed: 30 July 2025].