ITUPublications

International Telecommunication Union
Standardization Sector

ITU Focus Group Technical Report

(04/2024)

Focus Group on Testbeds Federations for IMT-2020 and beyond

(FG-TBFxG)

FG-TBFxG-TR-D1.1

Use cases for federated testbeds and business scenarios

Technical Report ITU FG-TBFxG-TR-D1.1

Use cases for federated testbeds and business scenarios

Summary

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

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 FG-TBFxG D1.1 Technical Report "Use cases for federated testbeds and business scenarios" approved at FG-TBFxG eighth meeting held in Sophia Antipolis, France from 10 to 12 April 2024.

Acknowledgement

This Technical Report was prepared under the leadership of Dr.-Ing. Giulio Maggiore (Telecom Italia, Italy) and Dr.-Ing. Muslim Elkotob (Vodafone, Germany), who served as the FG-TBFxG chair and FG-TBFxG vice-chair/WG1 chair respectively.

It is based on the contributions of various authors who participated in the Focus Group activities. FG-TBFxG appreciates Prof. Salim Hariri (University of Arizona, US), Dr. Hisham Kholidy (State University of New York Polytechnic Institute, College of Engineering, US), Dr. Shao Sicong (Arizona University, US), Dr.-Ing. Ranganai Chaparadza (Capgemini Engineering, Germany) and Dr.-Ing. Tayeb Ben Meriem (IPv6 Forum, France) for their inputs to this Technical Report.

Dr.-Ing. Muslim Elkotob (Vodafone, Germany) served as the main Editor of this Technical Report.

Mr Denis Andreev (FG-TBFxG Advisor) and Ms Emmanuelle Labare (FG-TBFxG Assistant) served as the FG-TBFxG Secretariat.

Editor: Dr.-Ing. Muslim Elkotob, Vodafone, Germany — Email: muslim.elkotob@vodafone.com

Table of Contents

Technical Report ITU FG-TBFxG-TR-D1.1

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 MEC, Core, RAN, Transport). The use cases descriptions (e.g., requirements, features, challenges, KPIs, etc.) are used for developing general requirements for APIs to be used in testbed federations.

2 References

[ITU-T Q.3060] Recommendation ITU-T Q.3060 (2020), *Signalling architecture of fast deployment emergency telecommunication networks to be used in a natural disaster.*

[ITU-T Q.3647] Recommendation ITU-T Q.3647 (2023), *Signalling requirements for emergency services in an Internet protocol multimedia subsystem roaming environment.*

[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.*

[ETSI TS 103 194] ETSI TS 103 194 v.1.1.1 (2014), *Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet.*

[3GPP TS 23.502] 3GPP TS 23.502 (2016), *Procedures for the 5G System (5GS).*

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following term defined elsewhere:

3.1.1 Testbeds Federation [FG-TBFxG D0.1]: The interconnection of Testbeds is a way that the testbeds are seamlessly viewed as a distributed platform that presents more aggregated capabilities from the diverse testbeds, such that user (test executor) can execute tests on the platform without having to approach each testbed individually to request for testbed service, while each testbed can still offer testbed services even as a standalone entity.

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
AMF	Access and Mobility Management Function
API	Application Program Interface
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
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
NGAP	Next Generation Application Protocol
NR	New Radio
NSSAI	Network Slice Selection Assistance Information
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
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
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
ZTA	Zero Trust Architecture

5 Introduction

There is a need to standardize a generic 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

Setting the scene for the use cases and their definitions and specifications there is a need to note that each testbed operates standalone offering its regular services and it can also connect via federation to other testbeds to extend its set of assets and enhance the scope of services it is offering. It follows a use-case driven approach in capturing the requirements, dynamics, and commonalities of federated testbeds. Each use case sets the scene and the frame in which federation is possible, including aspects like scope, type of federation, limitations, etc.

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 Annex 1.

7 Federated testbeds use cases

The detailed description of the use cases are available in Annex 2, as follows:

Use case #	Title
UC01	Testbed on roaming scenarios (IMS interconnection)
UC02	Testing IMS emergency calling
UC03	Rapid network resources deployment 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	Continues Integration/Continues Deployment Framework
UC14	Integration testing with any commercial RAN and UE
UC15	Large scale UE testing
UC16	Orchestration
UC17	Standards version compliance check for error-free interoperability between RAN and 5GC testbeds
UC18	Support for Zero Trust Architecture in Federated Testbeds

Annex 1

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&Problems solved via the Use Case**	
	2.c	**Rationale and Objective/Purpose of the Use Cased**	
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]	
		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 & windows (when known and where applicable) for 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)** *NOTE – Need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	
	4.c	**Reference Points**	
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	

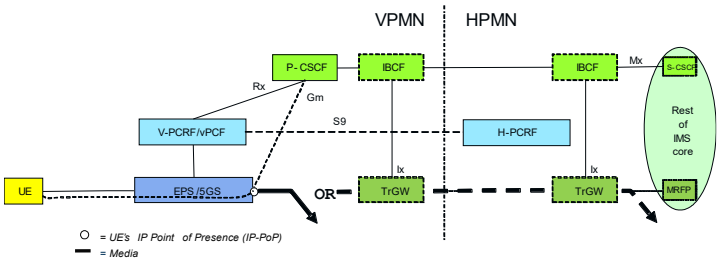
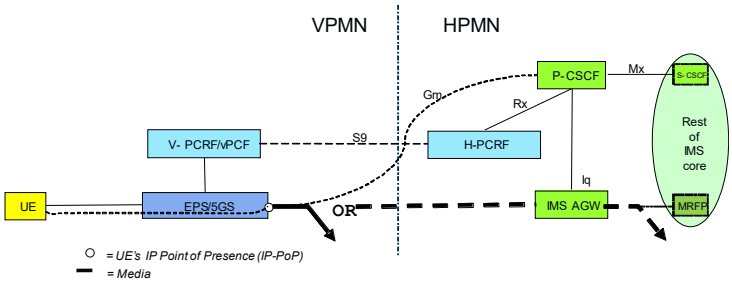
Annex 2

Use cases on testbed federations

UC01: Testbed on roaming scenarios (IMS interconnection)

1	**Use Case Name/Title**		E2E Testing involving Interconnection among CSPs' Networks and Roaming
2	**Use Case Short Description**		
	2.a	**Current Practice in Testbeds, Federation, and Testbeds Federations**	Current practices in E2E testing involving interconnection among CSPs' networks and roaming, involves in most cases some basic connectivity between 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. It 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 dimensioning their network resources accordingly. Emergency Call testing, performance & scalability testing and security may require to be carried out across multiple network operator networks. Hence when testbeds of various operators are interconnected and federated for form distributed test platforms for use in testing various E2E aspects, this helps multiple operators. Some network slices are expected 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: • 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 NAS • IMS voice roaming architecture • Location support
	2.b	**Gaps&Problems solved via the Use Case**	There is need for a 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 LTE (VoLTE) and Voice over New Radio (VoNR) utilize the same IMS (IP Multimedia Subsystem) as defined in 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 supposed 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 boarders
		• Time: time constraints & windows (when known and where applicable) for 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, 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.
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)**	APIs for the testbeds federation would need to be developed and implemented as outlined in the Recommendation ITU-T Q.4068 "Open application program interfaces (APIs) for interoperable testbed federations".

		Note: need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated	
	4.c	**Reference Points**	The relevant reference points that would need to be implemented should be those specified in [ITU-T Q.4068] "Open application program interfaces (APIs) for interoperable testbed federations".
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	The Diagrams below show an example of a multi-operator environment for roaming scenario of which corresponding testbeds of CSPs need to be federated in order to execute various E2E test scenarios.  **Figure 1 – LBO Roaming with P-CSCF in VPMN using 5GS to support IMS Services [b-GSMA PRD IR.65]**  **Figure 2 – LBO Roaming with P-CSCF in HPMN using 5GS to support IMS Services [GSMA PRD IR.65]**

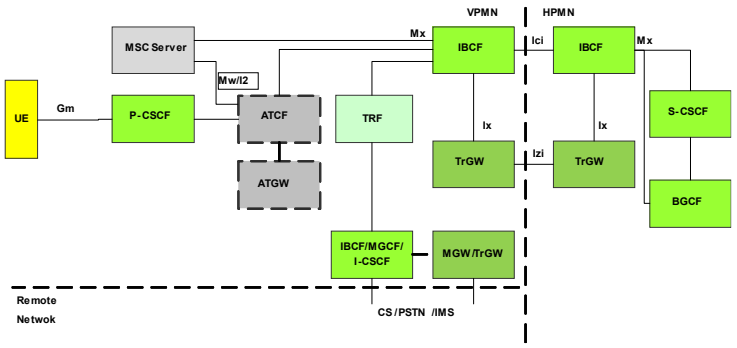


Figure 3 – LBO with P-CSCF in VPMN with Loopback possibility using 5GS to support IMS Services [GSMA PRD IR.65]

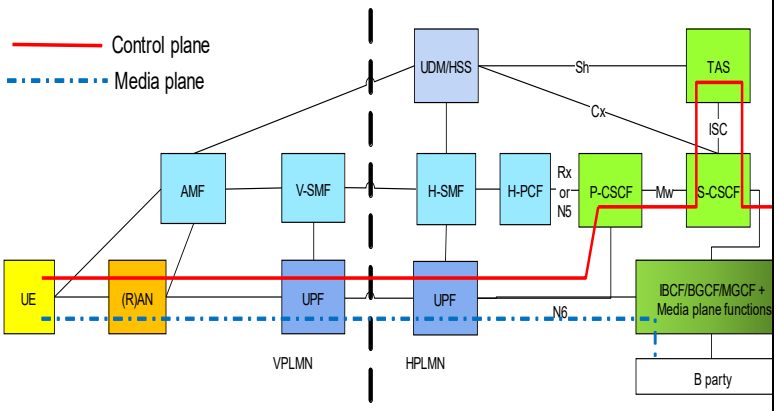
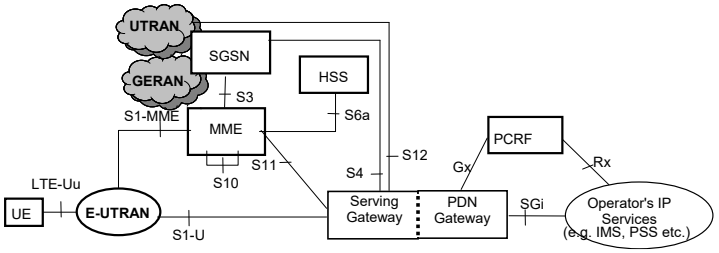


Figure 4 – Home Routed Roaming using 5GS to support IMS Services [GSMA PRD IR.65]

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**	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 CS emergency call is not available due to 2G/3G Sunset. Investigations by the GSMA with a number of 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 OS version. All in all, a very unpredictable landscape. The GSMA Board initiated a Task Force to clarify the requirements on 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. One of the changes was with regard to the tests that are run 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 need to be enhanced to cover these cited additional use cases.
	2.b	**Gaps&Problems solved via the Use Case**	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: • UE with reduced/limited voice capabilities, e.g., a roaming UE with no VoLTE roaming agreement in place, • A UE without a SIM, • A UE with an unauthenticated SIM (e.g., a roaming UE without a LTE data roaming agreement) Upon detecting an Emergency Call request, a UE in limited service state shall (in the general case) check the support for 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 PLMN scan. Since this issue is mainly concerned with IMS Emergency Call, the additional tests should be targeted at IMS Emergency Calling.
	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**	Testing of both UEs and MNO networks. To ensure that IMS Emergency Calls are always attempted by the UE when in limited service state or with reduced voice capabilities when PS Emergency is available in the cell in which the UE is camped. To ensure that the network handles the IMS Emergency Call correctly in line with local policy/regulations. In some countries, at the moment, this would mean the call attempt being rejected.
	3.b	**Types of Stakeholders, their Roles, Demarcations, Interactions.** i) Types of Roles for actors within each stakeholder	MNOs and OEMs. Test equipment vendors and test executors.
	3.c	**Scope:**	
		i) Domain: inter or intra stakeholder span [e.g., for a	Scope is between the UE and serving network. Dependent on the use case, the serving network can be a visited

		CSP stakeholder, within the same CSP/Operator or spanning multiple operators]	network (e.g., a UE with a SIM and without a VoLTE roaming agreement). On the other hand, for a UE without a SIM, there is no concept of a Home/Visited network.
		ii) Intra-Stakeholder Segments (e.g., CSP Core, Transport, RAN, Edge, MEC, or Vendor/Industry Player/Organization/Enterprise closed domain, local domain, private network, …)	Multiple vendors are involved for the UE and network infrastructure. It is also possible for there to be multiple vendors to be involved in the different nodes/elements comprising the Network.
		iii) Logistical Scope • Location: (countries, states, locations, sites) • Time: time constraints & windows (when known and where applicable) for Federation of specific assets (per asset/asset group)	Globally applicable to any network where IMS Emergency Calling is deployed – and most importantly when there is no CS Emergency to fall back on. 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.
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 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	**APIs requirements for Testbed Federations (if known)** *Note: need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	
	4.c	**Reference Points**	The relevant 3GPP reference points cover all interfaces between the device and the 4G network, but are mainly concerned with NAS (S1-MME) for emergency attach etc. and SIP (Gm) for Emergency Call without registration.
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	 **Figure 1 – EPC Non-Roaming Architecture and reference points**

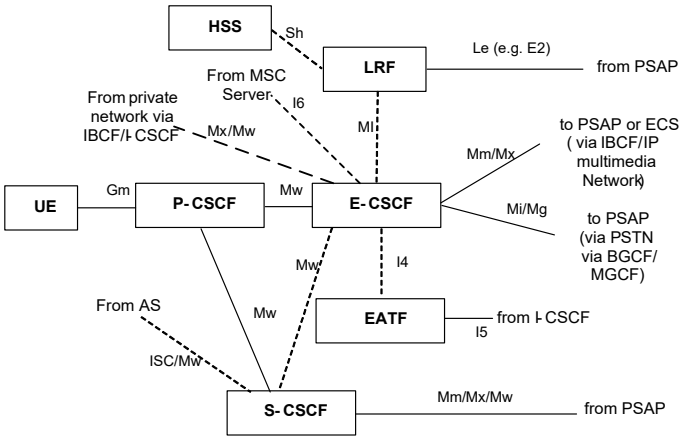
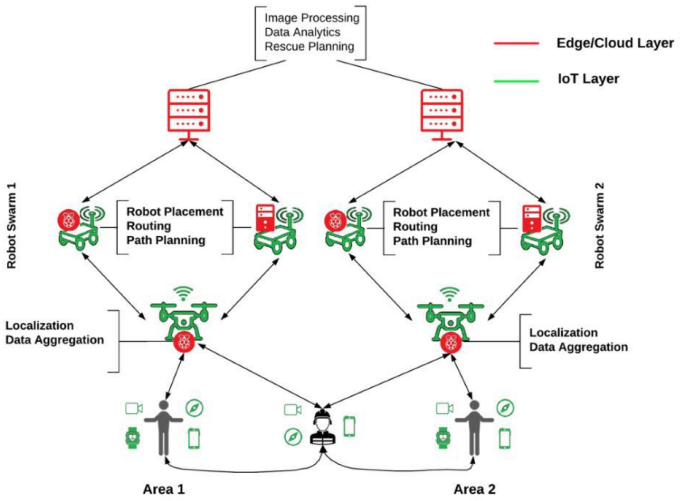


Figure 2 – UE/IMS Architecture and reference points

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**		
	2.a	**Current Practice in Testbeds, Federation, and Testbeds Federations**	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 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, taken 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 an 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.
	2.b	**Gaps & Problems solved via the Use Case**	Robot self-deployments, data routing and distributed coordination can be experimented in existing platforms, but there is currently a lack of edge and mobile services to realise a single experimentation of the whole use case.
	2.c	**Rationale and Objective/Purpose of the Use Case**	The purpose of the use case is to measure several KPIs: • Accuracy on prediction of required resources. • Fair allocation of mobile devices. • Improvement on 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 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, governmental organisations, civil and military rescue 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 organisations.
		ii) Intra-Stakeholder Segments (e.g., CSP Core, Transport, RAN, Edge, MEC, or Vendor/Industry Player/Organization/Enterprise closed domain, local domain, private network, …)	Multiple organisations can be involved in the different segments of the infrastructure network.
		iii) Logistical Scope • Location: (countries, states, locations, sites) • Time: time constraints & windows (when known and where applicable) for Federation of specific assets (per asset/asset group)	Worldwide, in different locations. The time is playing 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)** *NOTE – Need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	APIs for the "Testbeds Federation" would need to be developed and implemented as outlined in [ITU-T Q.4068] "Open application program interfaces (APIs) for interoperable testbed federations".
	4.c	**Reference Points**	The relevant reference points that would need to be implemented should be those specified in [ITU-T Q.4068] "Open application program interfaces (APIs) for interoperable testbed federations".

5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	The following diagram presents the network architecture for a physical disaster scenario should be available for the research infrastructure:  **Figure 1 – Network architecture for a physical disaster scenario [b-SLICES-DS D2.5 Figure 1]**

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 by several testbeds.
	2.b	**Gaps & 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 existing testbed, but there is currently no testbed able to execute and validate a complete and complex scenario encountered in smart cities.
	2.c	**Rationale and Objective/Purpose of the Use Case**	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: • 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, 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 organisations.
		ii) Intra-Stakeholder Segments (e.g., CSP Core, Transport, RAN, Edge, MEC, or Vendor/Industry Player/Organization/Enterprise closed domain, local domain, private network, …)	Multiple vendors, companies and organisations can be involved in the different segments of the infrastructure network.
		iii) Logistical Scope • Location: (countries, states, locations, sites) • Time: time constraints & windows (when known and where applicable) for Federation of specific assets (per asset/asset group)	Worldwide, in different testbeds. The time is crucial in this use case, in particular for event detection. The experiment should have a sufficient duration to determine if all the events were effectively detected.
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)** *NOTE – Need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	APIs for the "Testbeds Federation" would need to be developed and implemented as outlined in [ITU-T Q.4068] "Open application program interfaces (APIs) for interoperable testbed federations".
	4.c	**Reference Points**	The relevant reference points that would need to be implemented should be those specified in [ITU-T Q.4068] "Open application program interfaces (APIs) for interoperable testbed federations".

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 the demolition of a building. This approach with 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 & Problems solved via the Use Case**	In this use case, several aspects should be implemented and tested such as: • Cloud-based collaboration solution • Digital twin implementation • Conformance with standards and protocols • Interoperability between software components • Security and privacy • Data analytics To realise a whole experiment involving all the above-mentioned aspects, testbeds with specific features should be available.
	2.c	**Rationale and Objective/Purpose of the Use Case**	The utilisation of different testbeds for a single complete experiment permits to measure several KPIs: • Reduction in time needed for estimation of produced waste. • Waste reduction percentage. • Network instantiation in an end-to-end manner. • Time needed for VNF deployment. • Digital twin communication latency. • Time needed 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 organisations.

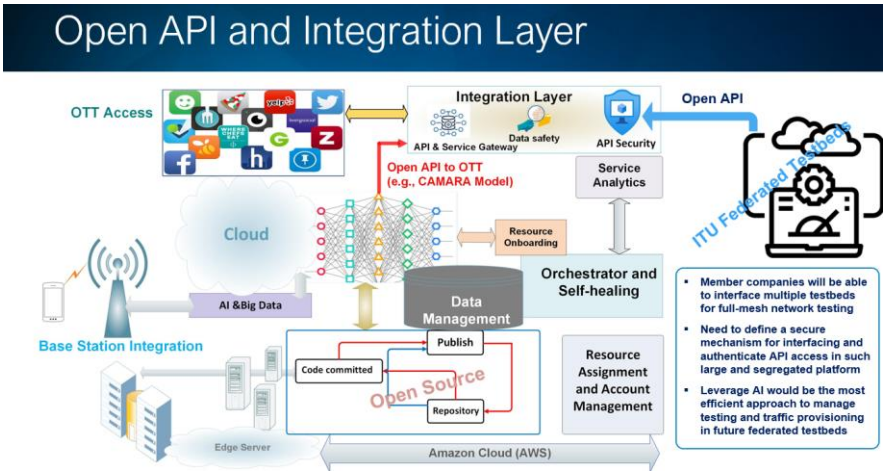
		ii) Intra-Stakeholder Segments (e.g., CSP Core, Transport, RAN, Edge, MEC, or Vendor/Industry Player/Organization/Enterprise closed domain, local domain, private network, ...)	Multiple vendors, companies and organisations can be involved in the different segments of the infrastructure network.
		iii) Logistical Scope • Location: (countries, states, locations, sites) • Time: time constraints & windows (when known and where applicable) for Federation of specific assets (per asset/asset group)	Worldwide, in 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)** *Note: need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	APIs for the "Testbeds Federation" would need to be developed and implemented as outlined in the Recommendation ITU-T Q.4068 "Open application program interfaces (APIs) for interoperable testbed federations".
	4.c	**Reference Points**	The relevant reference points that would need to be implemented should be those specified in the Recommendation ITU-T Q.4068 "Open application program interfaces (APIs) for interoperable testbed federations".
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**	Open architecture is a system where different software and hardware components communicate through open standards and interfaces. The testing of 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. 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. 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 to develop the necessary expertise, resources, and effort or develop new approach to through federated testbeds where one testbed can be built using opensource and open APIs with messages and connectivity are being evaluated collaboratively through federated testbed dashboards. 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 testing of systems that span multiple domains and geographic locations and enables the evaluation of the interactions between different components in a realistic setting.
	2.b	**Gaps&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. An open source/API testbed platform provides a flexible and modular platform for testing, which can be easily customized and adapted to meet the needs of any given software application. This IEEE 5G/6G Innovation Tested platform is built using open-source technologies, which allows developers to freely access and modify the source code as needed. Additionally, an open-source testbed platform provides a collaborative environment for testing, which allows 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 to improve the quality and efficiency of software testing, while also reducing the time and resources required for testing.
	2.c	**Rationale and Objective/Purpose of the Use Case**	The rationale behind adopting open source and open API 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 API 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 API promotes transparency and flexibility, enabling researchers to adapt and modify the testbed as needed to support open architecture and measuring/monitoring

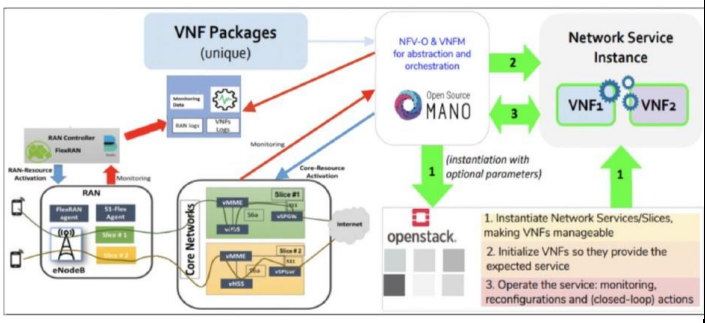
			open API traffic. The latter would gain more and mor attention as operators try to find ways to monetize their infrastructure. The goal is to provide platform available to test the concepts of open architecture and enabling technologies as well as open API for OTT. Finally, to sue the platform for developing monitoring/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 Player/Organization/Enterprise closed domain, local domain, private network, …)	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 approach.
		iii) Logistical Scope • Location: (countries, states, locations, sites) • Time: time constraints & windows (when known and where applicable) for Federation of specific assets (per asset/asset group)	Worldwide, platform is accessed over the cloud (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)** *NOTE – Need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	APIs for the testbeds federation would need to be developed and implemented as outlined in [ITU-T Q.4068] "Open application program interfaces (APIs) for interoperable testbed federations", 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] "Open application program interfaces (APIs) for interoperable testbed federations", 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	**Architecture/Architectural Framework** The Diagram below [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. 

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**	This federation is composed of the following testbeds experimented with at [b-AICCSA-1] [b-AICCSA-2] [b-AICCSA-3]: • IoT Testbed • UDM Smart Car Testbed • Virtual Cybersecurity Testbed • Wireless Cybersecurity Testbed The different users, such as researchers, students and trainees, can access these four testbeds by a common interface named Universal Testbed Access Interface (UTAI).
	2.b	**Gaps&Problems solved via the Use Case**	Each testbed is handled by a testbed manager. On the cloud, a shared testbeds current state repository was put in place to collect the information concerning the current operational state of each testbed. As this repository is shared among different organisations 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 permits to configure the testbeds, to execute the experiments and to get the results of the experiments. The configuration of the testbeds encompasses the access control to the testbeds, the specific setup of each testbed and the time management. Leveraging the Web portal and the information provided in the shared testbeds current state

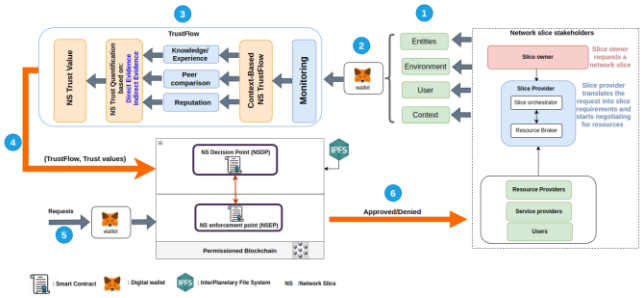
			repository, it is possible for the end-users to set up experiments in the Federated Testbed as a Service (FTaaS).
	2.c	**Rationale and Objective/Purpose of the Use Case**	The Federated Testbed as a Service (FTaaS) permits to create experiments using resources available in different testbeds, not only in the same organisation, but also in other organisations. 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 organisations. 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 organisations.
		ii) Intra-Stakeholder Segments (e.g., CSP Core, Transport, RAN, Edge, MEC, or Vendor/Industry Player/Organization/Enterprise closed domain, local domain, private network, …)	Multiple vendors, organisations and enterprises may be involved in the different segments of the research infrastructure network.
		iii) Logistical Scope • Location: (countries, states, locations, sites) • Time: time constraints & windows (when known and where applicable) for Federation of specific assets (per asset/asset group)	1) Location (countries, states, locations, sites): United States of America. 2) Time: time constraints & windows (when known and where applicable) for Federation of specific assets (per asset/asset group): The time management is realised through the Web portal of the FTaaS. This is an important aspect to be taken into account when setting up an experiment and retrieving the results of this experiment.
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)** *NOTE – Need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security,*	The FTaaS is based on the APIs notably provided by the ETSI-NFV MANO framework.

		rights, certification, interfaces, etc.) ToBeCompleted/Elaborated	
	4.c	**Reference Points**	The ETSI-NFV MANO framework.
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	The following figure illustrates the architecture at high level of a federated 5G testbed accessible notably through the 5G Federated Testbed as a Service:  **Figure 1 – 5G open architecture testbed [b-ARXIV]**

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**	• Implementing a data collection tool to gather relevant data from the network slice/system. • Developing the TrustFlow module that processes real-time date 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&Problems solved via the Use Case**	One challenge in the context of IMT-2020 networks and their services is the ability to establish an 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 accurate measured trust value in such ecosystem helps a trustor to make an informed decision on whether it should put itself in a vulnerable position if it turns out that the trustee has malicious intents.
	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 brings unprecedented security challenges because of its dynamic and diverse structure. Trust in the IMT-2020 ecosystem is a cornerstone for global adaptation and

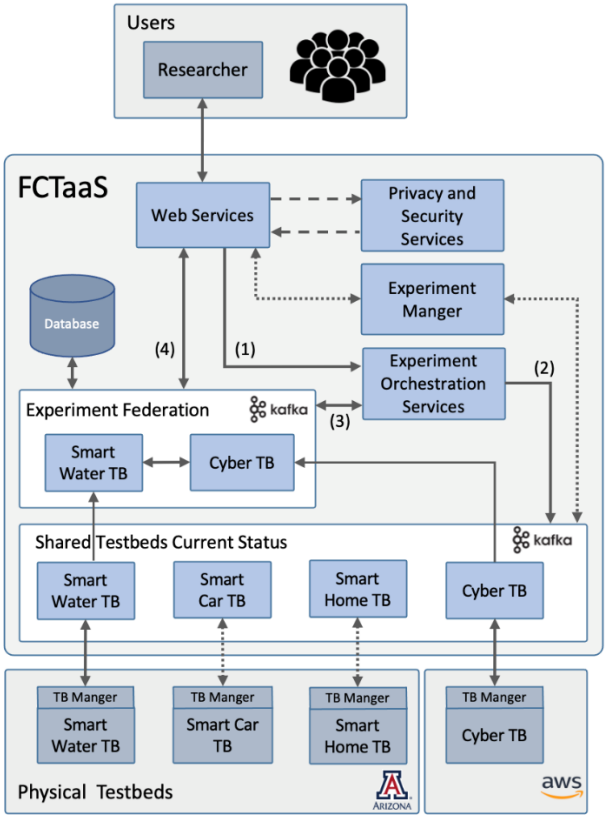
			tackling security and privacy risks. In this research, we shed light on the zero trust concept in IMT-2020 using distributed ledger (blockchain). Establishing trust between network slice stakeholders (i.e., slice owners, users, slice resource providers, and service providers).
3	**Use Case High-Level 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, …)	All of these segments will play a role in the blockchain based zero trust.
		iii) Logistical Scope • Location: (countries, states, locations, sites) • Time: time constraints & windows (when known and where applicable) for Federation of specific assets (per asset/asset group)	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)** *NOTE – Need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	Kafka APIs [b-kafka]
	4.c	**Reference Points**	
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	The diagram below shows the blockchain based zero trust architecture for IMT-2020 network slicing [b-AICCSA-4] [b-AICCSA-5] [b-AICCSA-6] [b-AICCSA-8].

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**	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 sustainability 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 achieving sustainable urban development leading to end-to-end resiliency. A federated approach to smart city services can integrate different critical systems 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&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 uses 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 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 evaluating 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)
		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 smart city services 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) • Time: time constraints & windows (when known and where applicable) for Federation of specific assets (per asset/asset group)	Globally applicable, nationally and across country boarders. 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)** *NOTE – Need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification,*	APIs for the testbeds federation would need to be developed and implemented internally.

		interfaces, etc.) *ToBeCompleted/Elaborated*	
	4.c	**Reference Points**	The relevant reference points that would need to be implemented should be: testbed manger, shared testbed current status, FCTaaS
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	The diagrams presented below shows the steps required to establish the federation of any smart services CPS into single shared status to enable data exchanged and experimentation in real-time [b-AICCSA-6] [b-AICCSA-7]:  **Figure 1 –The general architecture for the federation connecting different user to dispersed CPSs** This enables users access and establishment of federated connection among heterogeneous testbeds.

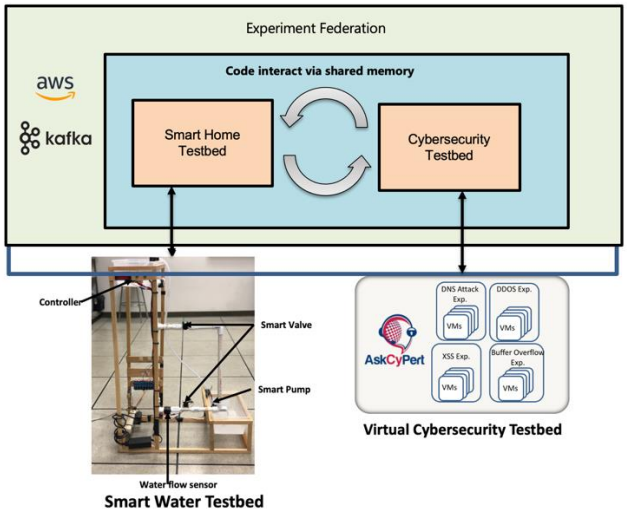


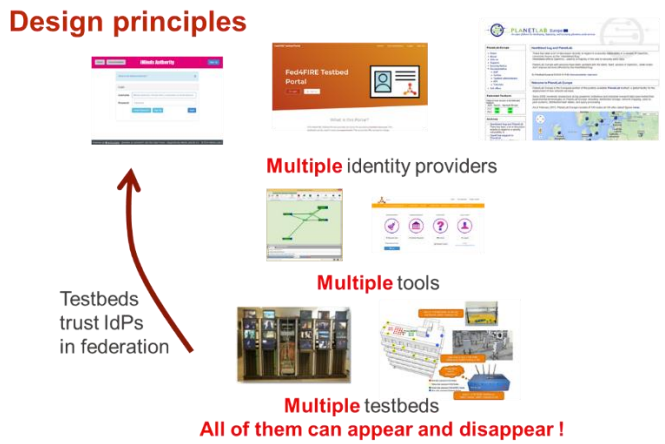
Figure 2

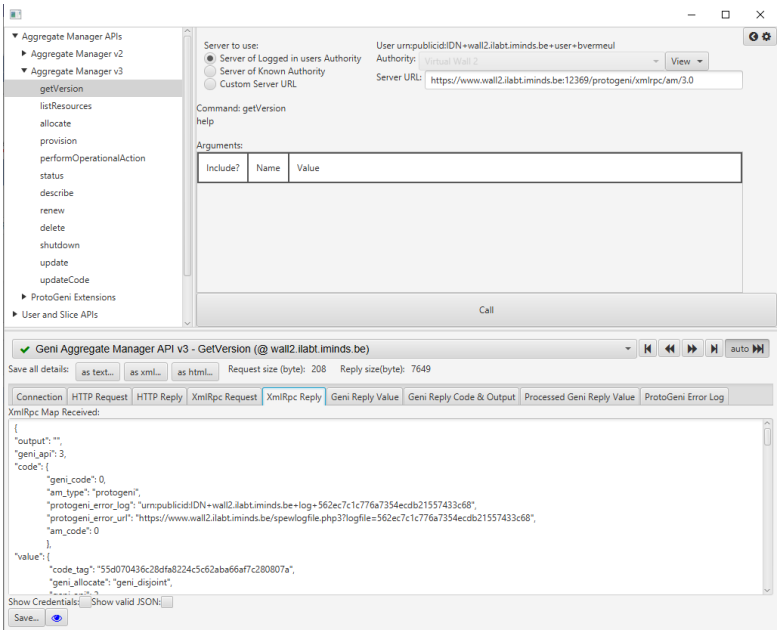
After the establishment of the experiment, data are shared in real-time through the federation. Current sensors and actuators data are exchanged through Shared Current Status implemented in the FCTaaS [b-AICCSA-6] [b-AICCSA-7] [b-AICCSA-9]. The federation allows both entities to communicate to enhance the performance according to customers' needs and facilitate further enhancement to urban cities infrastructure. Further, it allows deeper understanding of the systems 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**	The experimental validation of wired network research (ATM with connected servers) and wireless network research (wifi based) started in 1998. Each researcher had his own 'testbed' of 5-10 nodes which made it very expensive and very limited in scale. From 2005 onwards all hardware were combined in 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, so that was a problem, and they tried to (ab)use one testbed for a use case which was more typical for the other testbed. It evolved also that people wanted to use both testbeds at the same time (e.g., core wired network with wireless clients). At that moment the Fed4FIRE (Federation for Future Internet Research and Experimentation) project [b-Fed4FIRE] was started for federation of similar testbeds through Europe. With a single tool and account the researchers could now easily use multiple testbeds and even interconnect them with layer 2 connections.

	2.b	**Gaps&Problems solved via the Use Case**	It was made easy for experimenters to use or combine multiple testbeds: • Single account • Single tool Multiple testbeds are useful to: • 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 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.
	2.c	**Rationale and Objective/Purpose of the Use Case**	Make it easier to use multiple testbeds and to make specific experiments possible that would need otherwise a lot of manual interventions (e.g., to set up interconnectivity or to repeat the same experiment with other 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, …)	Not applicable
		iii) Logistical Scope • Location: (countries, states, locations, sites) • Time: time constraints & windows (when known and where applicable) for Federation of specific assets (per asset/asset group)	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, GPU testbeds
	4.b	**APIs requirements for Testbed Federations (if known)** *Note: need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs*	The current APIs for federation that are used are the GENI Aggregate Manager and Federation APIs [b-GENI]

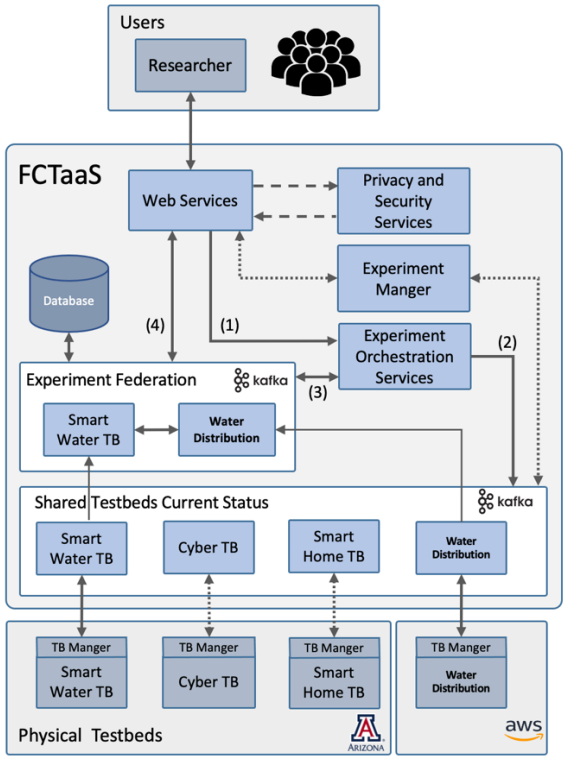
		(internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated	
	4.c	**Reference Points**	 [b-IoT-week-2021]
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	See figure of reference points. The technology used is XML-RPC with client-based authentication. The testbeds do implement the 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 exists out of testbeds which trust one or more identity providers. The resource specification (RSpec) is used to describe resources. (https://fed4fire-testbeds.ilabt.iminds.be/asciidoc/rspec.html). A light federation model is to federate through OAuth which only shares the account, no APIs. (https://doc.fed4fire.eu/testbed_owner/oauth.html). 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.

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 sustainability of cyber-attacks and reduces the resiliency 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 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&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 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

			uses 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 evaluating 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)
		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 smart water treatment 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) • Time: time constraints & windows (when known and where applicable) for Federation of specific assets (per asset/asset group)	Worldwide, nationally and across country boarders. 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)** *Note: need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have*	APIs for the testbeds federation would need to be developed and implemented internally.

		different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated	
	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**	The diagrams presented below shows the steps required to establish the federation of smart water treatment with distribution network that contains multiple disrupted sensors [b-AICCSA-6]:  **Figure 1 – The general architecture for the federation connecting different user to dispersed CPSs**

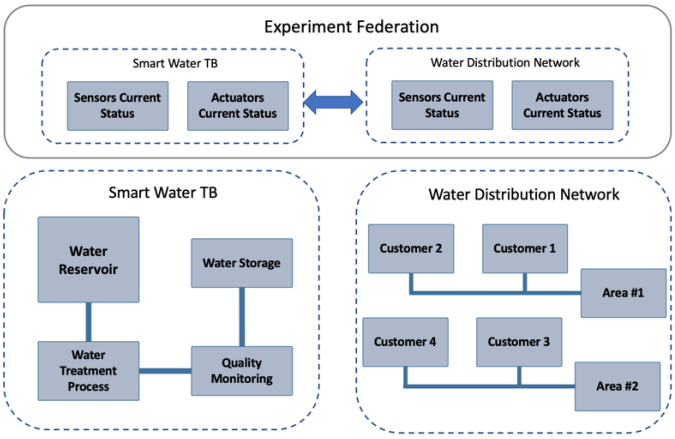


Figure 2: After the establishment of the experiment, data are shared in real-time the federation. Current sensors and actuators data are exchanged through Shared Current Status implemented in the FCTaaS [b-AICCSA-6]. The federation allows both entities to communicate to enhance the performance according to customers' needs and facilitate further enhancement to urban cities infrastructure.

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&Problems solved via the Use Case**	
	2.c	**Rationale and Objective/Purpose of the Use Case**	End-to-end features like UE registration, 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 the Annex 3.
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 & windows (when known and where applicable) for 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)** *Note: need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	
	4.c	**Reference Points**	
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	Multiple domains and parts are involved specifically, RAN+ UE emulator and 5GC. Dependency on the RAN and UE side changes at the RAN+UE emulator for end-to-end integration testing. Inter NF dependency: Multiple NFs are involved like AMF, which depends on AuSF to complete the UE registration. Relevant design and implementation have to be done on all the dependent NFs. The figure in Appendix A.1 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. The following figure depicts the design of AMF with various layers in the implementation of the protocol stack on N1-N2 interfaces, SBI interfaces, and the respective modules. Similar designs and implementations are incorporated at other NFs such as AuSF, UDM, UDR, SMF, NRF, etc.

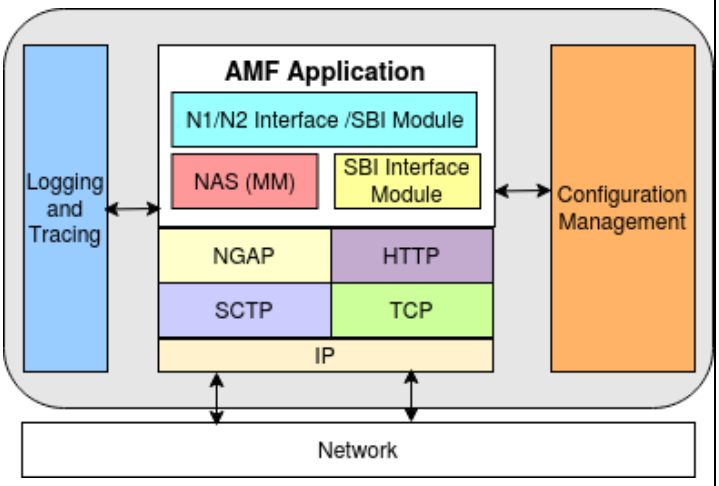


Figure 2 – High-level view of AMF design

Logging and tracing features - Helpful for large-scale testing. This is enabled or disabled based on the severity of the specific feature tested.

Error handling code to be present - not everything we assume works smoothly. For example, to check if the memory allocation is successful for a certain to be decoded or to be encoded. If not release any memory previously allocated so far in that function.

Security requirements should not be ignored (like marking them as FFS) but should be incorporated for every feature added to the 5GC design. This is applicable to all the NFs as appropriate.

Code coverage testing - Test cases shall be developed with a static code analysis tool if a block of code is needed or simply placed as a dead code.

UC13: Continues Integration/Continues 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**	Whenever new features are added it is important to test existing features through the respective test cases.
	2.b	**Gaps&Problems solved via the Use Case**	Function integrity
	2.c	**Rationale and Objective/Purpose of the Use Case**	Preserving existing functionality. For example, end-to-end basic functionality like UE registration and PDU session establishment should work fine even though new features like support for network slicing are added. End-to-end Network Slicing for IMT-2020 is highlighted in Annex 4.

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 & windows (when known and where applicable) for 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)** *Note: need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	
	4.c	**Reference Points**	
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	CI/CD must be built from the beginning. Adding new features in the testbed demanded changes in the CI/CD. Developing new features may be across NFs of the 5GC. For example, supporting end-to-end network slicing needed changes on AMF, UDM, SMF, and UPF. The end-to-end sequence diagram of network slicing is shown in Appendices A.2 and A.3.

			1 Changes at the AMF AMF should decode the "Requested NSSAI" 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. Thereby 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. 2 Changes at the RAN+UE Emulator a) Here, the UE should send the Requested NSSAI IE in the NAS registration message. So, 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 NGAP message and NAS Registration Accept message. c) Correct Slice Service Type (SST) value has to be placed in the MM-NAS Transport for the corresponding PDU session establishment message. d) New run-time configuration field to indicate the value for Requested NSSAI IE. 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 has to happen with existing testbed code. Hence, adding new features consists of two parts: 1) product CI/CD and 2) scripting and automation. 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 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&Problems solved via the Use Case**	1) Parameters Configuration • PLMN • Slicing support • Applications specific configurations

			2) 3GPP Release version mismatch • E.g.: Separate Registration Accept message than inside the Initial Context Setup Request msg from AMF to RAN • Mismatch in the IEs of the NGAP messages between AMF and RAN, GTP messages between UPF and RAN. Simultaneous multi-version handling of 3GPP TS, vendor-specific extensions, handled with run-time configuration control and build-time control macros.
	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.** 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 & windows (when known and where applicable) for 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)** *Note: need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and*	

		design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated	
	4.c	**Reference Points**	
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	No changes in the overall framework. But code changes are done at RAN+UE emulator and 5GC whenever there is a mismatch in the corresponding UE procedure testing regarding message (NGAP, NAS) contents. Some changes are also done in the run-time configuration as appropriate.

UC15: Large scale UE testing

1	**Use Case Name/Title**		Large scale UE testing
2	**Use Case Short Description**		
	2.a	**Current Practice in Testbeds, Federation, and Testbeds Federations**	
	2.b	**Gaps&Problems solved via the Use Case**	Scalability with load balancing
	2.c	**Rationale and Objective/Purpose of the Use Case**	Supporting a variety and a huge set of users connecting to 5G. Evaluating the challenges faced in the process.
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 & windows (when known and where applicable) for	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)** *Note: need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	
	4.c	**Reference Points**	
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	For large-scale UE testing UERANSIM [b-UERANSIM] instantiates a new docker container for each UE. It is not friendly to test thousands of UEs in a single host. So, changes to the RAN+UE Emulator are needed. There are following takeaways: • Some open-source code-bases can be useful for end-to-end functional testing but not for non-functional testing (e.g., load, stress testing as described above). • Moreover, an open-source code-base 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&Problems solved via the Use Case**	Leveraging open-source software. Open Source MANO (OSM) [b-OSM] Release is upgraded regularly. So, dependency on the previous version, using which testbed was previously deployed, becomes a challenge to resolve any related issues on the OSM. 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 leveraging it further for analytics and building cognitive autonomous networks. Open-Source MANO – 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 & windows (when known and where applicable) for 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)** *Note: need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	
	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 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], are 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 & 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: • Separate Registration Accept message than inside the Initial Context Setup Request message from AMF to RAN • Mismatch in the IEs of the NGAP messages between AMF and RAN, GTP messages between UPF and RAN.
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 • Location: (countries, states, locations, sites) • Time: time constraints & windows (when known and where applicable) for	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)** *Note: need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	
	4.c	**Reference Points**	For further study.
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	No changes in the overall framework. But code changes are done at RAN+UE emulator and 5GC whenever there is a mismatch in the corresponding UE procedure testing regarding message (NGAP, NAS) contents. Some changes are also done in the run-time configuration as appropriate. E.g., adding run-time configuration parameters to enable/disable GTP Extension Header support at the Core & RAN Sides, enable/disable separate Registration Accept message than 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 & Problems solved via the Use Case**	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: • 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 with Zero Trust Architecture.

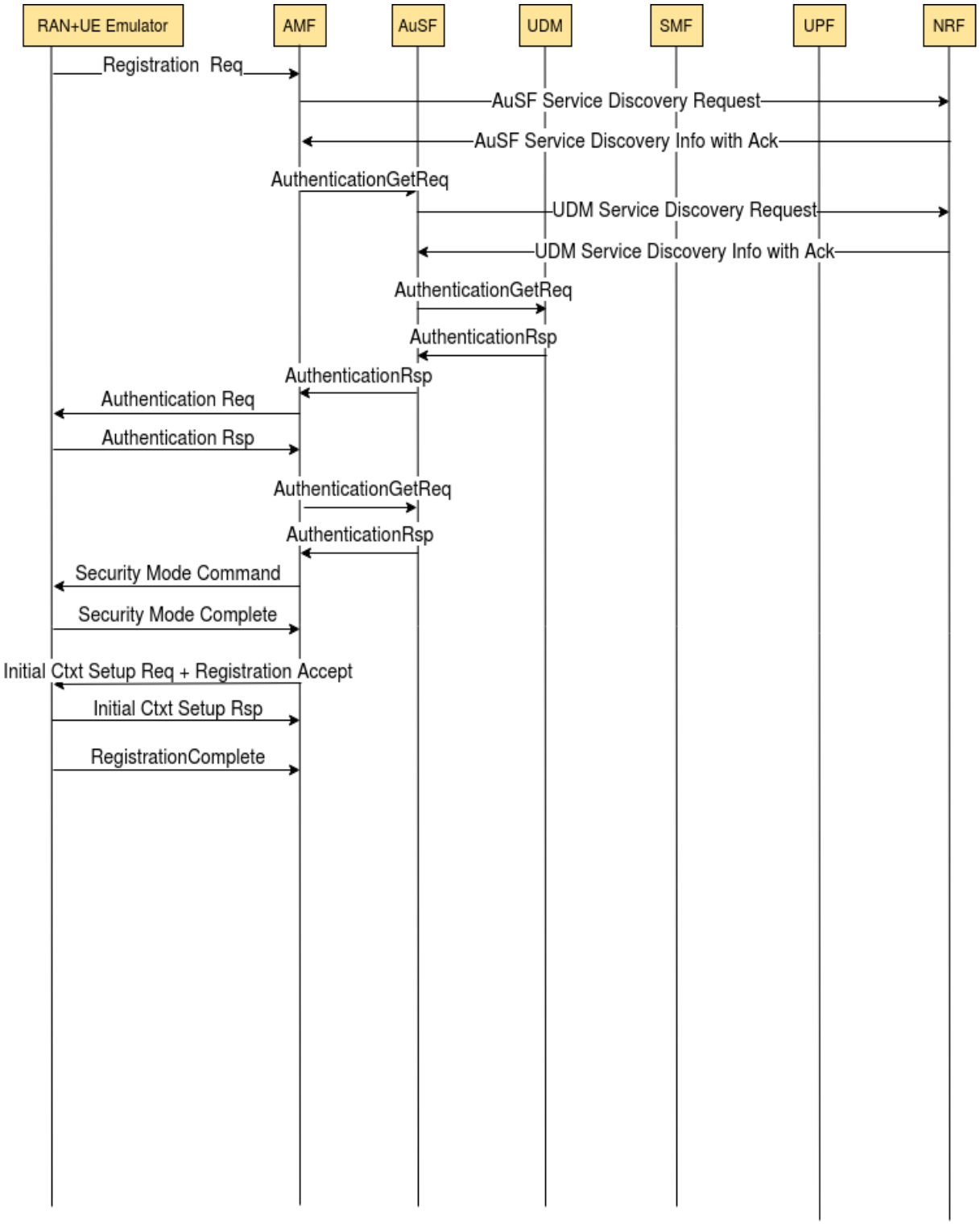
3	**Use Case High-Level Technical Specification**		
	3.a	**Type of Use Case**	
	3.b	**Types of Stakeholders, their Roles, Demarcations, Interactions.** i) Types of Roles for actors within each stakeholder	
	3.c	**Scope:**	
		i) Domain: inter or intra stakeholder span [e.g., for a CSP stakeholder, within 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 • Location: (countries, states, locations, sites) • Time: time constraints & windows (when known and where applicable) for 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)** *Note: need to differentiate between internal vs. 3rd party (within same eco-system or value chain) APIs (internal vs external APIs have different implementation and design requirements regarding security, rights, certification, interfaces, etc.) ToBeCompleted/Elaborated*	
	4.c	**Reference Points**	
5	**Use Case Detailed Technical Specifications**		
	5.a	**Architecture/Architectural Framework**	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. These changes need to be made at the testbeds participating in the federated setup to make it secure against unauthorised access to protect the testbed resources. 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 data flooding attack towards the RAN/UPF Instance initiated from either of the sides. There was a scenario suggested by the following reference [b-IEEE-netsoft-2023]. The preventive measures considered in this scenario can be incorporated within the testbeds involved. Additionally, following operations can be incorporated within the federated testbed framework using the principles of ZTA: • 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. NOTE – Remote Attestation is a method by which a host (client) authenticates its hardware and software configuration to a remote host (server).

Annex 3

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

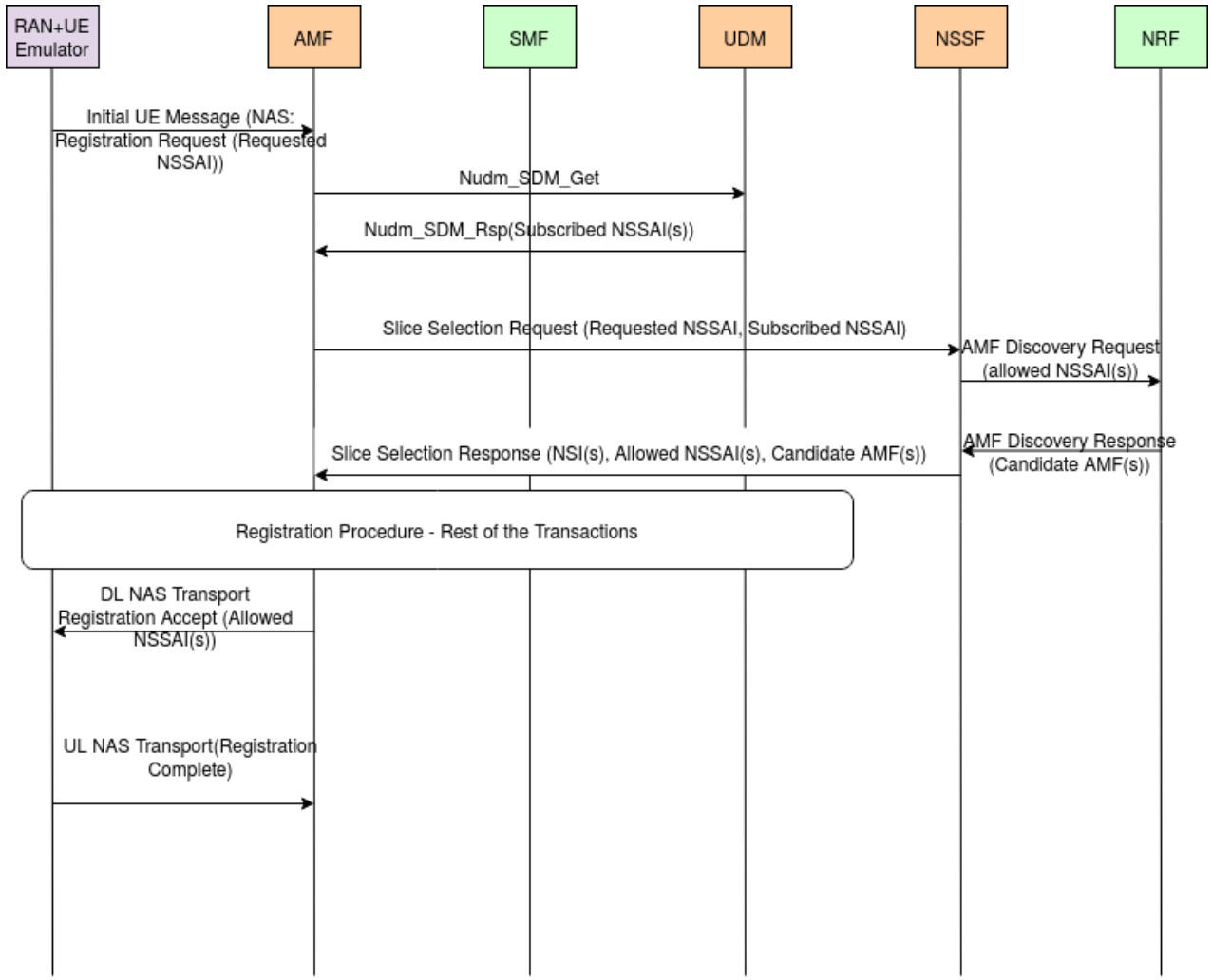
The following figure depicts the end-to-end call flow of the UE registration (as given in 3GPP TS 23.502) implemented in IMT-2020 Testbed.



Annex 4

End-to-end Network Slicing for IMT-2020

The following figure 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).



Bibliography

[b-AICCSA-1] H. A. Kholidy, A. Berrouachedi, E. Benkhelifa and R. Jaziri, "Enhancing Security in 5G Networks: A Hybrid Machine Learning Approach for Attack Classification," 2023 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, "A New Hybrid Cipher based on Prime Numbers Generation Complexity: Application in Securing 5G Networks," 2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Giza, Egypt, 2023, pp. 1-8, doi: 10.1109/AICCSA59173.2023.10479316.

[b-AICCSA-3] H. A. Kholidy, "A Smart Network Slicing Provisioning Framework for 5G-based IoT Networks," 2023 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), San Antonio, TX, USA, 2023, pp. 104-110, doi: 10.1109/IOTSMS59855.2023.10325712.

[b-AICCSA-4] H. A. Kholidy et al., "Secure the 5G and Beyond Networks with Zero Trust and Access Control Systems for Cloud Native Architectures," 2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Giza, Egypt, 2023, pp. 1-8, doi: 10.1109/AICCSA59173.2023.10479308.

[b-AICCSA-5] A. A. Abushgra, H. A. Kholidy, A. Berrouachedi and R. Jaziri, "Innovative Routing Solutions: Centralized Hypercube Routing Among Multiple Clusters in 5G Networks," 2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Giza, Egypt, 2023, pp. 1-7, doi: 10.1109/AICCSA59173.2023.10479277.

[b-AICCSA-6] I. Almazyad, S. Shao, S. Hariri and H. A. Kholidy, "Anomaly Behavior Analysis of Smart Water Treatment Facility Service: Design, Analysis, and Evaluation," 2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Giza, Egypt, 2023, pp. 1-7, doi: 10.1109/AICCSA59173.2023.10479312.

[b-AICCSA-7] H. A. Kholidy, "A Smart Network Slicing Provisioning Framework for 5G-based IoT Networks," 2023 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), San Antonio, TX, USA, 2023, pp. 104-110, doi: 10.1109/IOTSMS59855.2023.10325712.

[b-AICCSA-8] Elmadani, S., Hariri, S., & Shao, S. (2022, December). 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) (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

[b-Fed4FIRE] https://www.fed4fire.eu/

[b-GENI] https://github.com/open-multinet/federation-am-api and https://groups.geni.net/geni/wiki/CommonFederationAPIv2

[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, "Preventing Cross Network Slice Disruptions in a Zero-Trust and Multi-Tenant Future 5G Networks," 2023 IEEE 9th International Conference on Network Softwarization (NetSoft), Madrid, Spain, 2023, pp. 227-231.

[b-IITH] Indian Institute of Technology, Hyderabad, https://newslab.iith.ac.in/5gtest-bed.html

[b-Imec] Imec iLab.t testbeds (Virtual Wall, w-iLab.t and GPULab), https://doc.ilabt.imec.be/

[b-IoT-week-2021] IoT week 2021, Aug 30-Sep 3, online, Brecht Vermeulen, "Federated testbeds in Fed4FIRE", https://www.fed4fire.eu/wp-content/uploads/sites/10/2021/09/brecht-vermeulen_20210903_iotweek_fed4fire.pdf

[b-kafka] https://kafka.apache.org/

[b-NIST-ZTA] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[b-OSM] https://osm.etsi.org/

[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

[b-UERANSIM] https://github.com/aligungr/UERANSIM

[b-WSHP-ITU-ETSI-IEEE] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20210316/Documents/Anwer%20Al%20Dulaimi_Future%20Networks%20Industry%20Consortium_ITU_Workshop.pdf