EXPERIMENTATION AND VALIDATION OPENNESS FOR LONGTERM EVOLUTION OF VERTICAL INDUSTRIES IN 5G ERA AND BEYOND

[H2020 - Grant Agreement No.101016608]

Deliverable D2.3

Overall framework for NetApp development and evaluation

Editor	Angela Dimitriou (INTRA)
Contributors	(TID), (NCRSD), (MAG), (ATOS), (INTRA), (COS), (LNV), (UMA), (GMI), (ININ), (CAF), (IQB), (FOGUS), (INF), (8BELLS), (PAL), (QUCOM), (IMM), (UML), (UPV)
Version	1.0
Date	October 31st, 2022
Distribution	PUBLIC (PU)

DISCLAIMER

This document contains information, which is proprietary to the EVOLVED-5G ("Experimentation and Validation Openness for Longterm evolution of VErtical inDustries in 5G era and beyond) Consortium that is subject to the rights and obligations and to the terms and conditions applicable to the Grant Agreement number: 101016608. The action of the EVOLVED-5G Consortium is funded by the European Commission.

Neither this document nor the information contained herein shall be used, copied, duplicated, reproduced, modified, or communicated by any means to any third party, in whole or in parts, except with prior written consent of the EVOLVED-5G Consortium. In such case, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced. In the event of infringement, the consortium reserves the right to take any legal action it deems appropriate.

This document reflects only the authors' view and does not necessarily reflect the view of the European Commission. Neither the EVOLVED-5G Consortium as a whole, nor a certain party of the EVOLVED-5G Consortium warrant that the information contained in this document is suitable for use, nor that the use of the information is accurate or free from risk, and accepts no liability for loss or damage suffered by any person using this information.

The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

REVISION HISTORY

Revision	***Date***	***Responsible***	***Comment***
0.1	*22/8/2022*	*Angela Dimitriou*	*ToC creation*
0.2	*14/9/2022*	*Angela Dimitriou*	*1st draft*
0.3	*4/10/2022*	*Angela Dimitriou*	*2nd draft*
0.4	*21/10/2022*	*Angela Dimitriou*	*Final version ready for internal review*
1.0	*28/10/2022*	*Angela Dimitriou*	*Final version*

LIST OF AUTHORS

Partner ACRONYM	*Partner FULL NAME*	*Name & Surname*
TID	*TELEFONICA INVESTIGACION Y DESARROLLO SA*	*Javier Garcia* *David Artuñedo* *Alejandro Molina*
NCSRD	*NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS"*	*Harilaos Koumaras, George Makropoulos, Anastasios Gogos Dimitrios Fragkos*
MAG	*MAGGIOLI SPA*	*Yannis Karadimas*
ATOS	*ATOS IT SOLUTIONS AND SERVICES IBERIA SL*	*Ricardo Marco* Alaez *Paula Encinar Sanz*
INTRA	*NETCOMPANY INTRASOFT*	*Angela Dimitriou*
COS	*COSMOTE KINITES TILEPIKOINONIES AE*	*Fofy Setaki* *Elina Theodoropoulou*
LNV	*LENOVO DEUTSCHLAND GMBH*	*Apostolis Salkintzis* *Dimitrios Dimopoulos*
UMA	*UNIVERSIDAD DE MALAGA*	*Bruno Garcia*
GMI	*GMI AERO*	*George Kanderakis*
ININ	*INTERNET INSTITUTE, COMMUNICATIONS SOLUTIONS AND CONSULTING LTD*	*Janez Sterle*
CAF	*CAFA TECH OU*	*Tanel Jarvet*
IQB	*INQBIT INNOVATIONS SRL*	*Ioannis Stylianou*
FOGUS	*FOGUS INNOVATIONS & SERVICES P.C.*	*Dimitrios Tsolkas* *Anastasios-Stavros Charismiadis* *Katerina Giannopoulou*
INF	*INFOLYSIS P.C.*	*Christos Sakkas* *Theoni Dounia* *George Theodoropoulos*
8BELLS	*EIGHT BELLS LTD*	*George Chatzikonstantis*
PAL	*PAL ROBOTICS SL*	*Alessandro DiFava* *Thomas Peyrucain*
QCOM	*QUCOMM IDIOTIKI KEFALAIOUXIKI ETAIREIA*	*George Xylouris*
IMM	*IMMERSION*	*Charles Bailly*
UML	*UNMANNED SYSTEMS LIMITED*	*Pradyumna Vyshnav*
UPV	*UNIVERSITAT POLITECNICA DE VALENCIA*	*Regel G. Usach*

GLOSSARY

Acronym	***Description***
3GPP	*3rd Generation Partnership Project*
5GS	*5G system*
5G SA	*5G Stand Alone*
5GC	*5G core*
ADB	*Android Debug Bridge*
AEF	*API ExposureFunction*
APF	*API Publishing Function*
API	*Application Programming Interface*
CAPIF	*Common API Framework*
CCF	*CAPIF Core Function*
CI/CD	*Continuous Integration/Continuous Development*
CLI	*Command Line Interface*
DAST	*Dynamic Application Security Testing*
ELCM	*Experiment Lifecycle Manager*
FoF	*Factory of the Future*
GBR	*Guaranteed Bit Rate*
GUID	*Globally Unique Identifier*
HTTPS	*Hypertext Transfer Protocol Secure*
ICT	*Information and Communication Technology*
ID	*Identifier*
IoT	*Internet of Things*
KPI	*Key Performance Indicator*
NEF	*Network Exposure Function*
NetApps	*Network Application*
NPN	*Non-Public networks*
OAuth	*Open Authorization*
PKI	*Public Key Infrastructure*
PSK	*Pre-Shared Key*
REST	*Representational State Transfer*
SaaP	*Service as a Product*
SAST	*Static Application Security Testing*
SCPI	*Standard Commands for Programmable Instruments*
SDK	*Software Development Kit*
SME	*Small Medium Companies*
SSH	*Secure Shell*
TLS	*Transport Layer Security*
UE	*User Equipment*
vAPP	*Vertical Application*
VIM	*Virtual Infrastructure Management*

VNF	*Virtual Network Function*
VPN	*Virtual Private Network*

EXECUTIVE SUMMARY

This document concludes with the requirements, design and architecture of the EVOLVED-5G facility. At the centre of the design of the framework lies the concept of the NetApp. The NetApp takes advantage of the CAPIF and NEF APIs exposed by the 5G network to introduce an intermediate layer of intelligence between the 5G network and a multitude of applications brought by various vertical industries. Focusing on the concept of the NetApp, the EVOLVED-5G facility enables the creation of NetApps, implementing the tools that support the NetApp's lifecycle, i.e. development, verification, validation, certification and distribution through the EVOLVED-5G Marketplace.

The overall architecture of the framework comprises five environments, i.e., the Workspace, the Validation Environment, the Certification Environment, the Marketplace, the 5G NPN and some additional shared resources, i.e., a CI/CD platform and an Open Repository of various artifacts. These system modules formulate the facility that supports the creation of the NetApp throughout its lifecycle. Each environment consists of various functional blocks, each one of which fulfils a certain functionality. A multitude of communication channels, employing appropriate security mechanisms, when necessary, interconnect the environments with each other enabling the exchange of various assets (data, code, containerized images, certificates, reports). As a result, these components are efficiently integrated, and at the same time they provide seamless access to the actors who use the system in all the NetApp lifecycle stages.

The stakeholders related with the EVOLVED-5G facility include SMEs, 5G HW/SW providers, 5G network providers, virtualization platform providers, academia and telecom certification authorities. All these stakeholders are identified as potential actors in the EVOLVED-5G ecosystem. They may take on various roles, namely NetApp developer, vApp developer, verifier, validator, certificate issuer, Marketplace manager or infrastructure provider, which are related with the NetApp lifecycle and grant them access to the necessary EVOLVED-5G platform components.

The Workspace environment provides mainly an SDK that the NetApp developers may use to start creating NetApps out of the box. With the provision of appropriate libraries, NetApp templates and a rich CLI tool, the process of creating a NetApp, capable of communicating with a 5G network becomes a single step process. The interconnection of the Workspace with the CI/CD infrastructure through relevant APIs enables, in addition, the building and deployment of the NetApp. Finally, the Workspace provides to the developer through the CLI the mechanisms for verifying the NetApp as a software component in various levels.

The Validation Environment offers the opportunity to the developer to go one step further, by validating the NetApp in conjunction with real 5G network infrastructure. Various experiments may be defined to evaluate the performance of the NetApp in a controlled environment. At the same time the validation process checks the integration of the NetApp with selected vApps.

The exploitation of the Certification Environment follows, by executing a variety of tests that have been defined adopting the SQUARE (System and Software Quality Requirements and Evaluation) [1] methodology. This methodology enables a certification authority to issue a certificate in an automatic and repeatable manner for any NetApp that meets product quality criteria and that satisfies the requirements imposed by the EVOLVED-5G Marketplace policies.

Finally, the certified NetApp ends up in the Marketplace environment along with its certificate and relevant metadata. The developer of the certified NetApp sets its price, and interested users may purchase the NetApp by downloading it in a containerized form through the Marketplace.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

1.1 Purpose of the document

This document follows the submission of the deliverables D2.1 “Overall Framework Design and Industry 4.0 requirements” (submitted in September 2021) [2] and D2.2 “Design of the NetApps development and evaluation environments” (submitted in October 2021) [3]. It concludes the work of WP2, which sets up the foundation for implementing the EVOLVED-5G framework.

In the previous deliverables, the stakeholders and roles of the EVOLVED-5G ecosystem were identified, business and user requirements of the framework were analysed, the initial architectural design was introduced and the pilot use cases were described. This document proceeds with the elicitation of the system requirements specifically for each architecture environment and it presents the finalization of the architectural design both at a high level and in detail for each platform environment.

This deliverable focuses on the integration design of the architecture, explaining the process flows, communication channels and APIs used to realize this integration in all levels of analysis of the architecture. Although considered finalized, in the eventuality of the architecture being changed in the rest of the duration of the project, these modifications will be reflected in the deliverables of WP3 and WP5. Refinements in terms of the use cases will, on the other hand, be included in the deliverables of WP4.

An indicative list of the changes documented in this report in comparison to the deliverables D2.1 [2] and D2.2 [3] follows:

- The details of the integration design of the architecture are presented in a complete and analytical fashion, including the supported process flows by the architectural components, the communication channels between components, the shared resources, the APIs used and the security mechanisms employed.
- The overall architecture of the EVOLVED-5G facility has been restructured affecting its integration design, especially in relation with the CI/CD services and the Open Repository of artifacts, which are now identified as central components of the EVOLVED-5G framework.
- The list of stakeholders and roles involved in the EVOLVED-5G ecosystem has been refined.
- The requirements elicitation process resulted in the extraction of the functional and non-functional system requirements of the EVOLVED-5G framework, which are reported in this document, following the business and user requirements analysis presented in the deliverable D2.1 [2].
- The criteria for the Certification Environment have been refined, resulting in an automated testing process that certifies NetApps.

1.2 Structure of the document

The document is structured in 9 chapters. The current chapter includes introductory content about the deliverable. Chapter 2 presents the finalized version of the overall architecture. Chapter 3 follows with the report of the functional and non-functional requirements elicited in the final stages of WP2, as well as the refinement of the stakeholders and roles related with the EVOLVED-5G framework. The next five chapters, i.e., Chapters 4-8, present the finalized architecture of each one of the environment components, that is, the Workspace, the Validation Environment, the Certification Environment, the Marketplace and 5G NPN framework. The structure of each one of these chapters, as well as of Chapter 2, contains (i) an introductory section describing the role of each component, (ii) an indicative usage scenario of the corresponding component that reveals the integration of its internal functional blocks, and finally (iii) the integration design of the component. For the integration design, the shared resources exchanged among components are identified, the APIs employed for the communication among its functional blocks and the security mechanisms adopted to ensure secure data exchange whenever necessary. Finally, Chapter 9 presents the conclusions of this report.

1.3 Target Audience

The release of the deliverable is public, intending to expose the overall EVOLVED-5G framework design and key Industry 4.0 requirements to a wide variety of research individuals and communities.

From specific to broader, different target audiences for D2.3 are identified as detailed below:

- **Project Consortium**: To validate that all objectives and proposed technological advancements have been analysed and to ensure that, through the identified requirements and the proposed architecture, further work can be concretely derived. Furthermore, the deliverable sets to establish a common understanding among the consortium with regards to:
    - The NetApp Ecosystem in the context of latest 5G technology advancements and main groups of technical requirements that are fundamental for the realization of this ecosystem.
    - The blueprint architecture to be set for future reference and evolution, including tools and technologies to be utilized.
    - Industry 4.0-related use cases that will show the added value of the NetApp ecosystem in real industry 4.0 scenarios.
- **Industry 4.0 and FoF (factories of the future) vertical groups:** To crystallize a common understanding of standards, technologies, and design principles that underline the architectural design of EVOLVED-5G, and to understand main technical requirements that should be considered beforehand and essential for later implementations of the EVOLVED-5G facility. A non-exhaustive list of Industry 4.0-related groups is as follows:
    - Manufacturing industries (including both large and SMEs) and IIoT technology providers.
    - European, national and regional manufacturing initiatives, including funding programs, 5G-related research projects, public bodies and policy makers.
    - Technology transfer organizations and market-uptake experts, researchers and individuals.
    - Standardisation bodies and open source communities.
    - Industry 4.0 professionals and researchers with technical knowledge and expertise, who have an industrial professional background and work on industry 4.0-related areas.

  - Industry 4.0-focused RTOs and institutes, marketers of exploitable results, potential users of exploitable results
  - Industry 4.0 Investors and business angels.
- **Other vertical industries and groups**: This deliverable seeks impact on other 5G-enabled vertical industries and groups in the long run. Indeed, all the architectural components of the facility are designed to secure interoperability beyond vendor specific implementation and across multiple domains. The same categorization as the above but beyond Industry 4.0 can be of application.

The general public: including citizens students, and non-governmental organizations (NGOs) to get a better understanding of the underlying components and design approach behind the EVOLVED-5G facility.

2 EVOLVED-5G Ecosystem Architecture

The EVOLVED-5G Architecture was last described as part of Deliverable D3.1 “Implementations and integrations towards EVOLVED-5G framework realization (intermediate)” (submitted in December 2021) [4], in section 3.3. At the time, all the major components were in place, as well as the separation in different levels, starting with the EVOLVED-5G environments, that is, the Workspace, the Validation Environment, the Certification Environment, the Marketplace and the 5G NPN. However, as a result of the work performed since the finalization of this deliverable, a new architectural diagram has been created, that better reflects the interconnection between the environments and the interfaces used for their communication. The following main differences can be identified:

- All environments revolve around a set of shared components that interconnect them, namely the **CI/CD services** and the **Open Repository**.
- The **CI/CD Services** were initially included as internal components of some of the EVOLVED-5G facility environments, but are now considered a central part of the architecture and presented as such, along with the **Community**, which has been included in this revision.
- The **Marketplace** has been decoupled from the **Certification Environment**, and now communicates directly with the **Open Repository**.
- The description of each of the environments has been refined, in order to clarify the exposed functionalities of each component.
- The integration among the architectural components has changed, as a result of the implementation activities in the technical work packages of the project.

The architecture described in this deliverable presents the latest version created by the EVOLVED-5G consortium and can be considered final or near-final. In case some modifications emerge, coming from potential improvements performed during the second period of the EVOLVED-5G project, they will be presented as part of future deliverables in the scope of WP3.

2.1 EVOLVED-5G facility Architectural components

The EVOLVED-5G facility is based on an architecture that is composed by five separate environments, which are interconnected through a unified CI/CD framework and a shared artifact repository. The architecture, shown in Figure 1, presents the refinements and improvements identified during the first reporting period of the project, and will be more thoroughly described in the following paragraphs and sections.

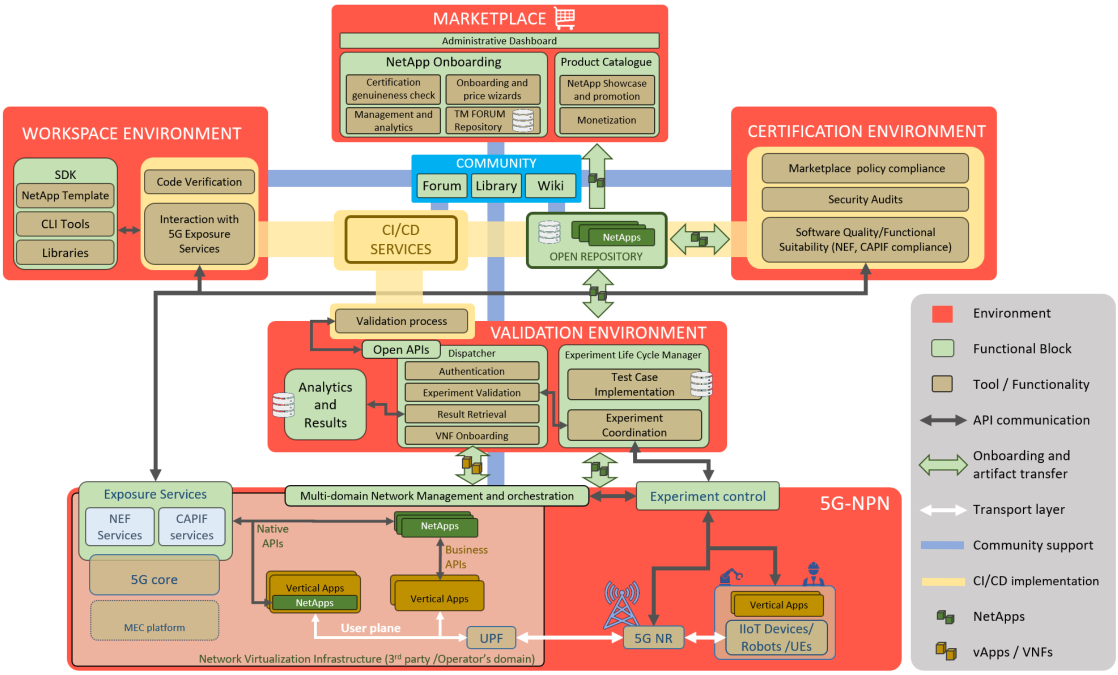

Figure 1 EVOLVED-5G system architecture

In order to describe the rationale behind the finalized architecture it is important to explain the main design principles that have been followed during its creation:

- The EVOLVED-5G facility components are organized in groups, called environments, that are associated with the phases of the lifecycle of the NetApp: development and verification (Workspace), validation (Validation Environment), certification (Certification environment), and release to the Marketplace. The 5G NPN, in addition, is needed to support both the validation and certification phases of the NetApplifecycle.
- System components are grouped in different levels of abstraction according to the compositional and structural logic of the EVOLVED-5G architecture. From the most abstract to the most concrete, they are as follows:
  - **Tier1 - Environments:** They are derived from and give support to the different phases of the lifecycle of the NetApp, or act as the foundation of other environments.
  - **Tier 2 - Functional blocks:** They encapsulate related functionalities and define the main building blocks that compose each *environment*.
  - **Tier 3 - Tools and functionalities:** Inside each *environment* and *functional block*, several components support the implementation of the different capabilities. In Figure 1, these are identified either by the name of the component or (in order to improve clarity) by stating the functionality offered.

Following these principles, the system architecture results in being composed by five environments that are interconnected by the usage of (i) **CI/CD services**, (ii) a centralized repository (the **Open Repository**), which encapsulates a source code repository and an artifacts repository, and (iii) an additional block that contains all the services that support the creation of a **Community** around the EVOLVED-5G ecosystem. In Figure 1, the tiered structural composition of the architecture is reflected by distinctively styled boxes (tier 1: red, tier 2: green, tier 3: brown). In terms of the different components' integration, different arrows are used to refer to available APIs usage, and exchange of artifacts and data.

2.2 INDICATIVE USAGE SCENARIO AND RELEVANT PROCESS FLOWS

This section provides a general view of the usage and rationale behind each of the different environments in the architecture, passing through all the phases that may be part of the lifecycle of a NetApp in their expected order. The relation between the architectural components and the different phases of the NetApp lifecycle is illustrated in Figure 2.

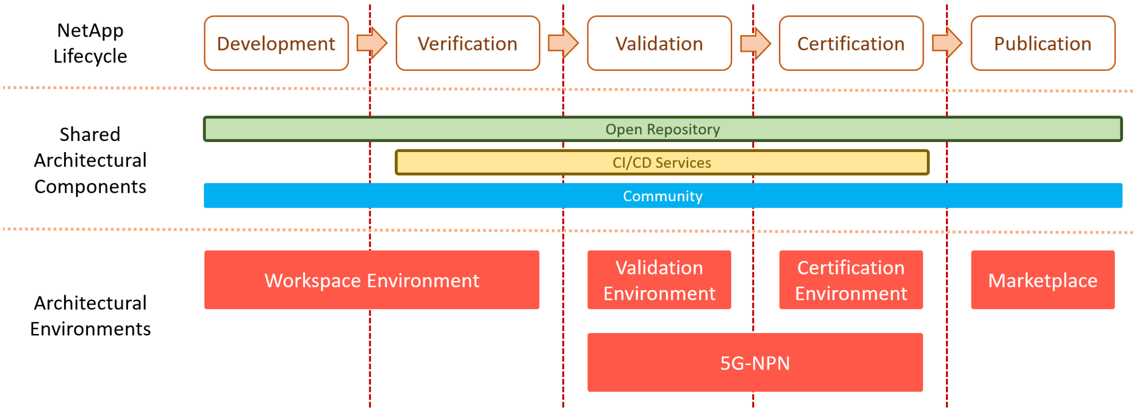

Figure 2 NetApp lifecycle phases and relation with architectural components

The **Workspace Environment** supports the development and verification of the NetApp. These two phases refer to:

- The implementation of the NetApp, including the basic functionality and compatibility with the exposure services of the 5G network. For this, the Workspace provides an SDK (Software Development Kit) to Developers, which includes documentation, libraries, pre-defined templates and a CLI (Command Line Interface) tool that ease the creation of NetApps.
- The verification of the NetApp corresponds to the assessment of the correctness of the NetApp in terms of basic functionality and compatibility with the 5G exposure services. This is implemented as a set of tests, available to NetApp developers in the form of a verification pipeline in the CI/CD services.

NetApp developers can make use of the SDK in their local premises and can have access to the CI/CD services at any time, which allows them to work independently and without any time constraints. Once developers are confident in the functionality of their NetApp, they can proceed to the next phase in the lifecycle of the NetApp: the validation.

The **Validation Environment** aims at providing the means for testing the suitability of the NetApp for working under real network conditions, and the successful integration of the NetApp with a vertical application (vApp). For this reason, the validation is performed within the premises of the validation platforms, which have access to experimental 5G deployments, and as such they can provide a realistic but controlled environment, where KPIs (Key Performance Indicators) can be measured under different network conditions.

For the validation of a specific NetApp, developers, platform owners and vApp providers agree on a set of tests designed for computing any KPI that is of interest to the involved parties. These customized tests are closely related to the nature of the selected NetApp + vApp pair, and aim at measuring the fitness of the NetApp in supporting their specific use case. These tests are complemented by a set of pre-defined trials (similar to the ones provided as part of the verification process) that assess the correctness of the NetApp in terms of basic functionality, quality of the code and integration with the 5G exposure services.

Not directly related to the NetApp, but of importance in order to guarantee the repeatability and validity of the results, the validation also includes an initial set of platform assessment tests, which verify the performance of the 5G NPN infrastructure before testing the NetApp.

Validated NetApps can be considered for the next phase of the NetApp lifecycle, that is the certification phase. In the **Certification Environment** the NetApp becomes a subject of an extensive quality assessment and conformance testing, performed in an automatic way by making use of a dedicated pipeline in the EVOLVED-5G CI/CD services. A certified NetApp is guaranteed to be interoperable with commercial 5G networks and can be released to the market.

The release to the **Marketplace** is the last stage of the NetApp lifecycle. In the Marketplace, a successfully certified NetApp can be made available to end users, who can have access to the artifacts required for the correct deployment of the NetApp in their public or private 5G networks.

The fifth environment of the EVOLVED-5G architecture, the **5G NPN**, supports the validation and certification of the NetApps by providing the required 5G APIs (5G exposure services), as well as a 5G network where the NetApp can be tested. For this testing to be possible, the 5G NPN integrates the software (such as the Open5Genesis Suite) and hardware (computational resources, storage, measurement equipment, etc.) components, which are necessary for the coordination and execution of the actions described in the corresponding test cases.

Apart from the five environments, two components of critical importance act as the connecting glue of the architecture, and thus, underpin all the stages of the NetApp lifecycle. These are the CI/CD Services and the Open Repository.

The **CI/CD Services** perform an important role to all of the intermediate stages of the NetApp lifecycle (i.e., all stages except for development and the publication to the Marketplace) by implementing most of the logic required for the automated actions that constitute the verification, validation and certification processes.

The CI/CD Services implement a set of pipelines which are exposed to the NetApp developers via appropriate commands of the CLI tool of the Workspace. Each of these pipelines automatically execute a set of actions while registering the results (such as logs, measurements or any other information) for the generation of a complete report that is made available to the developer.

The **Open Repository** acts as a central storage component that is accessible to all the other environments in the architecture. In this storage, all artifacts that are related to a NetApp, such as its source code, its binary images, relevant documentation or reports generated during verification, validation and certification, are saved and made available for retrieval. The role of the Open Repository is served by two different tools: Github [1] acts as a code repository, given its ubiquity and familiarity among developers, while Artifactor [2] is used for the storage of heterogeneous artifacts.

[1] https://github.com/

[2] https://jfrog.com/artifactory/

Finally, the **Community** plays an important role in the EVOLVED-5G ecosystem, centralizing the support provided to any external entities in exploiting the EVOLVED-5G framework. The Community comprises the Forum [3], the Accelerator Library [4] and the Wiki of the platform (not yet online), which are open for registration and freely available.

2.3 INTEGRATION DESIGN

2.3.1 Shared resources

The integration of the different environments of the EVOLVED-5G framework is realized via the Open Repository, which is used for the storage of all the necessary artifacts, either created as the output or needed as input for any of the processes in the NetApp lifecycle. In more detail, the Open Repository comprises two different entities:

- A code repository with version control (EVOLVED-5G Github group [5]), is used for storing the source code of all the available NetApps.
- An artifact repository, based on the Artifactory software, hosts heterogeneous resources such as binary images that can be used for the instantiation of the NetApps, or reports generated during the execution of the verification, validation or certification processes.

Since all the environments in the architecture have access to the Open Repository, the latter facilitates the exchange of all shared resources in the framework. Each environment retrieves the necessary resources from the Open Repository when, for instance, the source code of the NetApp is needed to build its image, or its certification report and its binary images are retrieved for publication in the Marketplace.

In terms of the implementation of the verification, validation and certification processes, the CI/CD Services implement a set of pipelines that are shared for all NetApps and communicate with the Environments involved in each one of these processes.

2.3.2 Exposed APIs

The first step a developer needs to make to start creating a NetApp using the EVOLVED-5G framework is to download the SDK [6] from the Open Repository. The SDK enables the NetApp developer to create a new repository, based on the NetApp templates provided. In the repository, the developer can independently work on the implementation and verification of her NetApp. As a result, the EVOLVED-5G SDK acts as the main interface for NetApp developers during most of the stages of the NetApp lifecycle:

- For the development, the SDK provides the means for creating new NetApp repositories and includes the necessary libraries for interfacing with CAPIF and the NEF emulator, along with documentation.
- For the verification, validation and certification of the NetApp, the Workspace provides commands for initiating the execution of each process, providing a unified user interface.

[3] https://forum.evolved-5g.eu
[4] https://forum.evolved-5g.eu/c/library/7
[5] https://github.com/evolved-5g
[6] https://github.com/EVOLVED-5G/SDK-CLI

The Marketplace, on the other hand, offers a fine-tuned web interface dedicated to the publication of NetApps, as well as for the management of such NetApps at a later stage.

Details about the interfaces offered by the different framework components are presented in the relevant chapters that follow.

2.3.3 Security

All components within the architecture are secured with standard user authentication and TLS support. Only certain parts of the architecture are accessible to external users through the usage of the SDK, however, in order to make use of such functionality, access to the EVOLVED-5G Github repository must be explicitly requested and accepted by the consortium.

The Marketplace and Community are the exception to this rule: since these elements are geared towards the creation of a NetApp ecosystem, access to them is immediately granted once a user account is created through registration.

More details about the security features of specific environments can be seen in their respective chapters of this document.

3 SYSTEM REQUIREMENTS

3.1 INTRODUCTION

The initial work of the project falling into the scope of WP2 aimed at the analysis of the context of the EVOLVED-5G framework and at positioning the framework in that context. Relying on literature, standards and best practices collected, the consortium identified the main stakeholders expected to interact and affect the system, and extracted the business and user requirements associated with EVOLVED-5G. This document reports the analysis, at the level of system requirements, which followed, and which has led to the final architectural and implementation decisions adopted by the consortium.

3.2 STAKEHOLDERS AND PLATFORM ROLES

In the deliverable D2.1 [2], the initial identification of the stakeholders related with the EVOLVED-5G framework was presented, inspired by the analysis of the background of the 5G ecosystem, in general. These stakeholders were also associated with their potential role in the EVOLVED-5G realm. The process of progressively developing the EVOLVED-5G facility since then clarified the landscape of stakeholders and roles in the system and led to the refinement of their standpoint in relation to the framework.

The refinement process resulted in the following changes in the initial stakeholders' and roles' analysis:

- The "Developers/Industry 4.0 NetApp developer" stakeholder was removed from the list of stakeholders, as not identifying a single entity but rather as defining a role in the system
- The "Technology providers/5G Equipment Vendor and Device Manufacturer" stakeholder was renamed as "5G HW/SW provider" to denote any entity that provides hardware or software components that support the operation of the EVOLVED-5G ecosystem
- The "Connectivity providers/5G network Provider" and the "5G testbed operator" stakeholders were unified to designate any entity that provides 5G connectivity to the devices involved in the EVOLVED-5G operations, regardless of the type of service through which they offer the connectivity
- The "Platform provider" stakeholder was renamed to "Virtualization platform provider" to more specifically describe any entity that provides infrastructure as a service for the deployment of the EVOLVED-5G facility components
- The "Open source community/research institutes/universities" was renamed to "Academia" to more generically encapsulate entities that bear any kind of research interest in using the EVOLVED-5G platform
- The "Policy makers/telecom certification organizations" is simply referred as "Telecom certification organizations" to follow the naming convention applied to all stakeholders in their refined version
- The "Development" role yielded two distinct roles, namely the NetApp developer and the vApp developer with distinct permissions and functionalities offered by the system

- The “Testing” role was mapped to the new “Verifier” to reflect specifically the testing process executed in the verification phase of the NetApp
- The “vApp+NetApp integration” role is now covered by the new “vApp developer” role, since the integration of a vApp with one or more NetApps acquired through the EVOLVED-5G Marketplace is of interest and a responsibility of the vApp developer
- The “Integration testing (quality assurance)” and “5G experimentation” where unified to the “Validator” role, which is assigned to anyone running the validation phase of the lifecycle of the NetApp
- The “Connectivity provisioning” and the “Testing service provisioning” were removed from the roles of the system, as they more accurately represent stakeholders in the ecosystem (i.e., “5G network provider” and “Virtualization platform provider”) rather than specific roles mapped to a particular phase of the lifecycle of the NetApp
- The “NetApp certification / Marketplace management” role was replaced by two distinct roles, that is, the “Certificate issuer” role, assigned to whoever executes the certification phase of the NetApp lifecycle, and the “Marketplace manager” role to refer to the entity with administrative permissions in the EVOLVED-5G Marketplace

The detailed description of the refined set of stakeholders and roles of the EVOLVED-5G ecosystem follows in the subsequent sections.

3.2.1 Stakeholders of the EVOLVED-5G ecosystem

The set of stakeholders related with the EVOLVED-5G framework comprises the entities that exist independently to the existence of the EVOLVED-5G ecosystem but which are identified as candidates for assuming a role in the EVOLVED-5G ecosystem. That is, they are actors pursuing a goal that can be fulfilled by the EVOLVED-5G framework or providing a service that affects the design of the EVOLVED-5G framework. These stakeholders were taken into account for collecting the business and user requirements of the Evolced-5G platform. The set of stakeholders is not exclusive but can potentially be augmented by additional entities of the 5G ecosystem, which might develop interest for NetApps and their development process in the future.

The updated list of stakeholders identified as important for the EVOLVED-5G realm follows:

- **(Industry 4.0) SMEs:** They are vertical providers and businesses that are interested in exploiting and bringing new functionalities provided by the 5G infrastructure. Their aim is to improve existing applications or introduce new ones (vertical applications or vApps) in an easy, modular and extensible fashion. Although the main target of the project is i4.0 SMEs, EVOLVED-5G also seeks impact on other 5G-enabled vertical industries. This broader vision makes the project also consider SMEs from other verticals that could potentially benefit from the ecosystem.
- **5G HW/SW providers**: They may provide the software and hardware required for the establishment of a 5G infrastructure, as well as the services be consumed by end users.
- **5G network providers**: Traditionally, this stakeholder refers to the MNOs (Mobile Network Operator) that have control over the network infrastructure and radio spectrum allocation required in order to provide wireless communication services to end users. Nevertheless, as the Industry 4.0 business case has a strong footprint on Non Public networks (NPN), a company or research organization that has the license and expertise to operate a campus network may also act as a 5G network provider in the EVOLVED-5G ecosystem. For a research organization, the 5G infrastructure can be

deployed inside a laboratory (making use of network emulators and other equipment) or include a real network infrastructure that can be used with commercial devices in a limited area, but which is not commercialized to end users. The European Digital Innovation Hubs (EDIHs) or the 5G-PPP ICT-17 platforms, such as 5GENESIS, constitute such examples.

- **Virtualization platform providers:** It is a core stakeholder and addresses the software and hardware systems' hosting and operation of the NetApps and the EVOLVED-5G facility components. EVOLVED-5G is considering a clear separation between the 5G network provider and the virtualization platform provider stakeholder, for reasons of versatility as this separation allows more dynamic setups, including public or hybrid cloud infrastructures and revealing the potentials of more business models.
- **Academia**: Higher education institutions that demonstrate research and education (training events, hackathons, workshops) activity around the 5G technology.
- **Telecom certification authorities:** These are independent organizations whose purpose is to ensure reliable and secure communication deployments according to international standards and criteria. Telecom certification authorities (like the Global Certification Forum) may act as main guarantors of interoperability in communications certifying NetApps created in the EVOLVED-5G ecosystem.

3.2.2 EVOLVED-5G Ecosystem Roles

The roles that stakeholders can assume in the EVOLVED-5G framework are dictated by the environments of the ecosystem and the functionalities offered by them to support the NetApp lifecycle. In principle, each role corresponds to a set of permissions, various stakeholders may be granted with, to execute certain actions in the EVOLVED-5G ecosystem. The finalized list of EVOLVED-5G roles follows:

- **NetApp developer**: The NetApp developers make use of the EVOLVED-5G SDK provided by the framework's Workspace environment, in order to create NetApps. They have a moderate understanding of the functionalities provided by the 5G APIs and their general usage procedure, albeit not necessarily an in-depth knowledge of the underlying network architecture. Developers may be interested in creating NetApps that are specifically tailored to certain vertical Apps, in which case they have a deep understanding of the requirements of that particular vApp. On the other hand, a NetApp developer may focus on the creation of generic NetApps that enhance 5G offered capabilities with an additional layer of intelligence that could serve a broader set of use cases.
- **vApp developer:** The vApp developer can be anybody interested in a NetApp published in the EVOLVED-5G Marketplace. A vApp developer has a deep understanding of the operation of the envisioned vertical App, as well as the benefits that the vApp under consideration can enjoy, by exploiting 5G technology. With these two aspects in mind, the vApp developer selects the most appropriate NetApp(s) from the EVOLVED-5G Marketplace to serve the desired goals of the application. The developer is the one with the responsibility of developing the envisioned vApp, as well as of integrating the vApp with the NetApp(s) required. In addition, the vApp developer may use the Validation Environment to validate the vApp-NetApp integration.
- **Verifier**: Verifiers perform the verification of the NetApp. The verification task is supported by the SDK component of the EVOLVED-5G Workspace and makes also use of the CI/CD component. In most cases, the verifier coincides with the NetApp

developer, but for clarity in mapping roles with distinct processes that in principle can be executed by different stakeholders in the EVOLVED-5G facility, the roles are kept distinguished.

- **Validator:** Validators take advantage of the Validation Environment of the EVOLVED-5G facility to implement the validation of a NetApp, in order to ensure the correct functionality of an integrated pair of a vApp and a NetApp in a given 5G environment. A validator might also be interested in analysing the performance of vertical Apps in conjunction with appropriate NetApps, by measuring and comparing KPIs in different experiment setups.
- **Certification issuer:** Stakeholders with this role coordinate the certification and quality assurance of the NetApp, in order to guarantee that they meet the required criteria for being published in the EVOLVED-5G Marketplace. As expected, they are granted access to the Certification Environment to fulfil their goal.
- **Marketplace manager:** This role manages the publication of NetApps along with their metadata and certificates in the Marketplace of the EVOLVED-5G facility. A Marketplace manager provides also support to end users that publish or download NetApps from the Marketplace.
- **Infrastructure provider:** This role is not related directly with the lifecycle of the NetApp but is assumed by stakeholders that cater for the hardware and software infrastructure that underpins the EVOLVED-5G facility environments. The stakeholders providing the infrastructure manage and provide support to the rest of the stakeholders that take on all the rest of the roles of the ecosystem.

3.2.3 Mapping of roles to stakeholders

Table 1 lists the roles of the EVOLVED-5G framework and associates them with the environment of the EVOLVED-5G facility they are granted access to, as well as with the stakeholders that are normally expected to assume the specific role. The facility environment corresponding to each role also reveals directly the relevance of that role with a specific phase of the NetApp lifecycle, with the exception of the infrastructure provider role, which is not involved in the NetApp development, integration and testing.

Table 1 Role - stakeholder mappings

Role	Access granted to	Stakeholders
NetApp developer	Workspace Validation Environment Marketplace 5G NPN	SME 5G HW/SW provider 5G network provider Academia
vApp developer	Marketplace Validation Environment	SME 5G HW/SW provider 5G network provider Academia
Verifier	Workspace	SME 5G HW/SW provider 5G network provider Academia
Validator	Validation Environment	SME 5G HW/SW provider 5G network provider

		Academia
Certificate issuer	Certification Environment	Telecom certification authority
Marketplace manager	Marketplace Certification environment	5G network provider
Infrastructure provider	Validation Environment Certification Environment Marketplace 5G NPN	5G HW/SW provider 5G network provider Virtualization platform provider

SMEs aim at developing new vertical applications or enhance existing ones with new features. As a result, they mainly act as vApp developers. However, in case they are creating their own NetApps, to support their own vApps, they may equally become NetApp developers, too. Naturally, they can also be the verifiers, as well as the validators of their NetApps and of their integration with the developed vApps. In the process of integrating their vApps with the 5G network, they may take advantage of NetApps offered by the EVOLVED-5G Marketplace, or even create their own NetApps and publish them in the Marketplace. Finally, throughout the development, verification and validation processes, they are necessarily given access to the 5G NPN, for letting their applications interact with the 5G underlying network.

5G HW/SW providers and 5G network providers are of course expected to act as infrastructure providers. Both types of stakeholders, though, may also act in a similar way to an SME. That is, they may be interested in making use of or creating NetApps for the implementation of the control software of the equipment they provide or for giving added value to the services offered to their end users. In addition, a 5G network provider is the stakeholder expected to act as the EVOLVED-5G Marketplace provider to distribute and promote NetApps to the users of their network.

Members of the academia focusing on the 5G technology are supported by the EVOLVED-5G framework to conduct their research by creating NetApps, vApps and by testing 5G network capabilities. Similarly to the previous stakeholders, since members of academia may develop their own NetApps and vApps, they are also responsible for verifying and validating their software.

Finally, the role of the certificate issuer is one-to-one mapped to the certification authority as expected. The same holds for the virtualization platform provider that can only act as an infrastructure provider.

3.3 System requirements

In the deliverable D2.1 [2], business and user requirements of the EVOLVED-5G framework were extracted and related to the identified stakeholders connected with the EVOLVED-5G ecosystem. These requirements have been in depth analysed by the consortium to yield the detailed system requirements that have guided the development process. In this document, these requirements are presented and are classified in two categories: functional and non-functional.

Functional requirements correspond to the functionalities offered by the various components and non-functional reflect the quality properties that these software components need to demonstrate. Starting from the requirements of the deliverable D2.1 [2] and with the overall architecture of the system into consideration, a set of system requirements was defined for each one of the core environments and components of the EVOLVED-5G facility.

During the implementation phase of the EVOLVED-5G framework, a monitoring compliance process was followed in iterations, verifying whether the extracted system requirements are fulfilled by the respective framework components' implementation. At this stage of the project, the first release of the system has become available, and only the relevant results are presented. The final report on the compliance of the second release of the EVOLVED-5G facility with the system requirements will be reported in the final deliverables of WP3 and WP5.

The functional and non-functional requirements are presented in the next sections. For each system requirement, the following attributes are given:

- An identifier of the requirement (formed as REQ-{F/NF for functional/non-functional}-{initial letter of the component}-{numeric identifier})
- The title of the requirement
- Its priority (mandatory - M, desirable - D)
- The relevant requirements from D2.1
- The compliance of the relevant component's first release with the requirement

Table 2 lists the set of functional system requirements. Most of the requirements are mapped to business and user requirements identified in the deliverable D2.1 [2]. However, in the course of the development process of the project additional requirements presented themselves as mandatory or desirable for achieving an effective system design. At the same time, part of the requirements initially identified have been deemed invalid or substituted by others.

Table 2 EVOLVED-5G functional requirements

ID	title	priority	D2.1 requirement	Release I
WORKSPACE				
REQ-F-W-1	The Workspace must provide a software development kit (SDK)	D	REQ-DEV-S-FUNC-4	YES
REQ-F-W-2	The Workspace must provide a command line interface (CLI)	D	REQ-DEV-S-USE-3	YES
REQ-F-W-3	The CLI must provide a command for creating a NetApp repository in the Open Repository	D		YES
REQ-F-W-4	A user of the EVOLVED-5G SDK must be able to generate a new NetApp repository via a configuration file	D	REQ-DEV-S-FUNC-4	YES
REQ-F-W-5	The EVOLVED-5G SDK must expose the different endpoints for CAPIF APIs	D		NO
REQ-F-W-6	The CLI must provide a command for building a NetApp into a Docker container	D		YES
REQ-F-W-7	The CLI must provide a command for deploying a NetApp as a container to a given virtualized environment	D		YES
REQ-F-W-8	The CLI must provide a command for removing (destroying) the NetApp container instance from a given virtualized environment	D		YES
REQ-F-W-9	The CLI must provide a command for checking the building status of a NetApp in the CI/CD platform	D		YES
REQ-F-W-10	The CLI must provide a command for checking the deployment status of a NetApp in the CI/CD platform	D		YES

REQ-F-W-11	The CLI must provide a command for checking the status of a NetApp containers removal in a virtualized environment	D		YES
REQ-F-W-12	The EVOLVED-5G CLI must provide a command to retrieve the NetApps deployed in a given virtualized environment.	D		NO
REQ-F-W-13	The CLI must provide a command for running verification tests for a given NetApp	D		YES
REQ-F-W-14	The CLI must provide a command for running validation tests for a given NetApp	D		NO
REQ-F-W-15	The verification environment must provide tests for checking that the NetApp can invoke the NEF API properly.	M	REQ-I4-M-FUNC-1	NO
REQ-F-W-16	The verification environment must provide tests for checking that the NetApp can invoke the CAPIF API properly.	M	REQ-I4-M-FUNC-10, REQ-I4-M-FUNC-11, REQ-I4-M-FUNC-12, REQ-I4-M-FUNC-13, REQ-I4-M-FUNC-14	NO
REQ-F-W-17	The verification environment must provide tests for checking that the NetApp can handle NEF callback requests.	M	REQ-I4-M-FUNC-1	NO
REQ-F-W-18	The verification environment must provide tests for checking that the NetApp can handle CAPIF callback requests.	M	REQ-I4-M-FUNC-15	NO
REQ-F-W-19	The verification environment must provide vulnerability scanning tests for NetApps	D	REQ-I4-S-REL-9	NO
REQ-F-W-20	The verification environment must provide tests for verifying that the source code of the NetApp does not disclose sensitive information	D		NO
REQ-F-W-21	The verification environment must provide tests for checking the integrity of the containerized image of the NetApp	M	REQ-PI-M-FUNC-6	NO
REQ-F-W-22	The verification environment must provide tests for verifying the code quality of the NetApp	D		NO
REQ-F-W-23	The verification environment must provide tests for checking that the containerized image of the NetApp can be successfully deployed in a given virtualized environment	M		NO
REQ-F-W-24	The verification environment must provide tests for checking that the NetApp is actually using the ports declared in its containerized image	M		NO
	CI/CD PLATFORM			
REQ-F-CC-1	The CI/CD environment must provide a user authentication mechanism	M	REQ-I4-S-SEC-5	YES
REQ-F-CC-2	An administrator must be able to define pipelines in the CI/CD platform	M	REQ-DEV-M-PORT-6	YES
REQ-F-CC-3	The CI/CD environment must provide APIs to let external entities launch pipelines	M	REQ-I4MARKET-M-MAIN-4	YES
REQ-F-CC-4	The CI/CD environment must provide feedback (logs) on Pipeline execution results	M		YES
REQ-F-CC-5	Reports produced by a pipeline executed in the CI/CD environment must be automatically uploaded to the Open Repository	M		YES
REQ-F-CC-6	Containerized images produced by a pipeline executed in the CI/CD environment must be automatically uploaded to the Open Repository	M	REQ-I4MARKET-M-FUNC-11	NO
	OPEN REPOSITORY			
REQ-F-OR-1	A user must be able to register to the Open Repository			

REQ-F-OR-2	Access to the Open Repository must be granted through an authentication mechanism	M	REQ-DEV-S-FUNC-4	YES
REQ-F-OR-3	Different level access resources of the Open Repository must be controlled through an authorization mechanism	M	REQ-DEV-S-FUNC-4	YES
REQ-F-OR-4	The Open Repository must provide an API for new source code project creation	M	REQ-DEV-S-FUNC-4	YES
REQ-F-OR-5	The Open Repository must provide source code branching functionality	M	REQ-DEV-S-FUNC-4	YES
REQ-F-OR-6	The Open Repository must provide source code versioning functionality	M	REQ-DEV-S-FUNC-4	YES
REQ-F-OR-7	The Open Repository must provide NetApp source code synchronization functionalities	M	REQ-DEV-S-FUNC-4	YES
REQ-F-OR-8	The Open Repository should provide creation and cloning of repositories functionality.	M	REQ-DEV-S-FUNC-4	YES
REQ-F-OR-9	The Open Repository should offer an issue tracking system	M	REQ-DEV-S-FUNC-4	YES
VALIDATION ENVIRONMENT				
REQ-F-V-1	The EVOLVED-5G CI/CD shall be able to invoke validation tests of a given NetApp in the Validation Environment	M	REQ-DEV-M-USE-12	YES
REQ-F-V-2	The Validation Environment must provide means for storing logs, raw results and data generated during a NetApp validation	M	REQ-DEV-M-FUNC-17	YES
REQ-F-V-3	A user must be able to extract validation reports generated during a NetApp validation from the Validation Environment	M	REQ-DEV-M-FUNC-17	NO
REQ-F-V-4	The Validation Environment must allow the definition of customized test cases for different NetApp validations	M	REQ-DEV-M-FUNC-16	YES
REQ-F-V-5	The Validation Environment must provide tests for verifying the code quality of the NetApp	M	REQ-I4-S-SEC-5	NO
REQ-F-V-6	The Validation Environment must provide tests for verifying that the source code of the NetApp does not disclose sensitive information	M		NO
REQ-F-V-7	The Validation Environment must provide tests for checking the quality of the containerized image of the NetApp	M	REQ-PI-M-FUNC-6	NO
REQ-F-V-8	The Validation Environment must provide tests for checking that the containerized image of the NetApp can be successfully deployed in a given virtualized environment	M		NO
REQ-F-V-9	The Validation Environment must provide tests for checking that the NetApp can invoke the NEF API properly.	M		NO
REQ-F-V-10	The Validation Environment must provide tests for checking that the NetApp can invoke the CAPIF API properly.	M	REQ-I4-M-FUNC-10, REQ-I4-M-FUNC-11, REQ-I4-M-FUNC-12, REQ-I4-M-FUNC-13, REQ-I4-M-FUNC-14	NO
REQ-F-V-11	The Validation Environment must provide tests for checking that the NetApp can handle NEF callback requests from a network component.	M		NO
REQ-F-V-12	The Validation Environment must provide tests for checking that the NetApp can handle CAPIF callback requests from a network component.	M	REQ-I4-M-FUNC-15	NO
REQ-F-V-13	The Validation Environment must be able to perform open source license scanning	D		NO
REQ-F-V-14	The Validation Environment may provide vulnerability scanning tests for NetApps	D	REQ-I4-S-REL-9	NO
REQ-F-V-15	The Validation Environment must provide tests for verifying the code quality of the NetApp	D		YES

REQ-F-V-16	The Validation Environment must provide tests for checking that the NetApp is actually using the ports declared in its containerized image	D		NO
REQ-F-V-17	The Validation Environment must be able to test the effective integration of a NetApp with a given vApp	D	REQ-I4-M-FUNC-3	YES
CERTIFICATION ENVIRONMENT				
REQ-F-CE-1	The Certification Environment must execute a performance Assessment of the 5G infrastructure before the NetApp certification tests	M		NO
REQ-F-CE-2	The Certification Environment must be able to deploy NetApp artifacts in a defined virtualized environment	M	REQ-PI-M-FUNC-2, REQ-PI-M-FUNC-3, REQ-PI-M-FUNC-6	NO
REQ-F-CE-3	The Certification Environment must expose NEF services for NetApps to interact with, during test execution	M	REQ-PI-M-FUNC-4, REQ-PI-M-FUNC-3, REQ-PI-M-FUNC-6	NO
REQ-F-CE-4	The Certification Environment must test the provision of NEF services before testing the NetApps	M		NO
REQ-F-CE-5	The Certification Environment must expose CAPIF services for NetApps to interact with, during test execution	M	REQ-I4-M-FUNC-10, REQ-I4-M-FUNC-11, REQ-I4-M-FUNC-12, REQ-I4-M-FUNC-13, REQ-I4-M-FUNC-14, REQ-I4-M-FUNC-15, REQ-5G-S-SEC-15, REQ-5G-S-SEC-16, REQ-5G-S-SEC-17, REQ-5G-S-SEC-18, REQ-5G-M-FUNC-3, REQ-5G-M-FUNC-21, REQ-5G-M-FUNC-22, REQ-5G-M-FUNC-23, REQ-5G-M-FUNC-24	NO
REQ-F-CE-6	The Certification Environment must test the provision of CAPIF services before testing the NetApps	M		NO
REQ-F-CE-7	The Certification Environment must test and certify that NetApps successfully onboard to CAPIF	M		NO
REQ-F-CE-8	The Certification Environment must test and certify that NetApps do Discover APIs using CAPIF	M		NO
REQ-F-CE-9	The Certification Environment must test and certify that NetApps do receive events from CAPIF	M		NO
REQ-F-CE-10	The Certification Environment must test and certify that NetApps successfully offboard from CAPIF	M		NO
REQ-F-CE-11	The Certification Environment must provide tests for checking that the NetApp can handle CAPIF callback requests from a network component.	M		NO
REQ-F-CE-12	The Certification Environment must test is the NetApp can successfully invoke the NEF AsSessionWithQoS API	M	REQ-I4-M-FUNC-1	NO
REQ-F-CE-13	The Certification Environment must test is the NetApp can successfully invoke the NEF MonitoringEvent API	N	REQ-I4-M-FUNC-1	NO
REQ-F-CE-14	The Certification Environment must provide tests for checking that the NetApp can handle NEF callback requests from a network component.	M	REQ-I4-M-FUNC-15	NO
REQ-F-CE-15	The Certification Environment must execute static code analysis on NetApps	M	REQ-DEV-S-USE-3	NO
REQ-F-CE-16	The Certification Environment must execute vulnerability analysis on NetApps	M	REQ-DEV-S-USE-3, REQ-DEV-S-FUNC-4	NO
REQ-F-CE-17	The Certification Environment must execute secret leakage scanning analysis on NetApps	M	REQ-DEV-S-USE-3, REQ-DEV-S-FUNC-4	NO
REQ-F-CE-18	The Certification Environment must execute licensing checks on NetApps	M	REQ-I4MARKET-W-DATA-6	NO
REQ-F-CE-19	The Certification Environment must execute open source scan analysis on NetApps	M	REQ-I4MARKET-W-DATA-6	NO
REQ-F-CE-20	The Certification Environment must execute container image integrity analysis on NetApps	M	REQ-DEV-S-USE-3, REQ-DEV-S-FUNC-4	NO
REQ-F-CE-21	The Certification Environment must test NetApp connectivity to validate NetApp deployment	M	REQ-DEV-M-FUNC-1	NO
REQ-F-CE-22	The Certification Environment must execute scalability test to NetApps	M	REQ-PI-S-PERF-7	NO

REQ-F-CE-23	The Certification Environment must provide tests for checking that the NetApp is actually using the ports declared in its containerized image	D		NO
REQ-F-CE-24	The Certification Environment must check if a NetApp blueprint that describes how the NetApp is built, deployed and communicates is provided together with the NetApp.	M	REQ-DEV-M-FUNC-1	NO
REQ-F-CE-25	The certification process must produce a certification report describing the certification results	M	REQ-I4MARKET-M-USE-1, REQ-I4MARKET-M-FUNC-2, REQ-I4MARKET-M-REL-3, REQ-I4MARKET-M-FUNC-5	NO
REQ-F-CE-26	The Certification Environment must upload the containerized image of a certified NetApp to a specified repository	D		NO
MARKETPLACE				
REQ-F-M-1	The marketplace must provide a responsive web interface	M	REQ-I4MARKET-M-FUNC-17	YES
REQ-F-M-2	A user must be able to register to the marketplace	M	REQ-I4MARKET-M-FUNC-12	YES
REQ-F-M-3	The Marketplace administrator must be provided with a page for monitoring KPIs of the platform	M		YES
REQ-F-M-4	A company must be able to register to the marketplace	M	REQ-I4MARKET-M-FUNC-12	YES
REQ-F-M-5	An authenticated user must be able to upload a NetApp to the marketplace via a wizard	M	REQ-I4MARKET-M-FUNC-18	YES
REQ-F-M-6	An owner of a NetApp must be able to upload the certificate of a NetApp	M		YES
REQ-F-M-7	An owner of a NetApp must be able to upload metadata for their NetApp	D	REQ-I4MARKET-C-FUNC-16	YES
REQ-F-M-8	An owner of NetApp must be able to set a price configuration for their NetApp using a wizard	M	REQ-I4MARKET-S-FUNC-14, REQ-I4MARKET-M-FUNC-18, REQ-I4MARKET-M-FUNC-19	YES
REQ-F-M-9	An owner of the NetApp must be able to upload to the Marketplace different versions of a NetApp	M		YES
REQ-F-M-10	An end user must be able to purchase a NetApp	M	REQ-I4MARKET-M-FUNC-13	YES
REQ-F-M-11	An end user must be able to download from the Marketplace a container image of a purchased NetApp	M	REQ-I4MARKET-M-FUNC-13	YES
REQ-F-M-12	A NetApp owner must be able to provide a certification URL during the process of uploading a NetApp to the Marketplace	M	REQ-I4MARKET-M-FUNC-8	YES
REQ-F-M-13	A user must be able to view the documentation of the NetApps at the product catalogue	M	REQ-I4MARKET-M-FUNC-9	YES
REQ-F-M-14	The Marketplace should request from NetApp owners to provide technical details for the usage of the NetApp	M	REQ-DEV-M-FUNC-1	YES
REQ-F-M-15	A user must be able to search for a NetApp by name and category	M	REQ-I4MARKET-M-FUNC-11	YES
REQ-F-M-16	The Marketplace must present one webpage for each NetApp containing its description and metadata	M	REQ-I4MARKET-M-FUNC-11	YES
REQ-F-M-17	The Marketplace shall provide a dashboard for NetApp publishers for monitoring their revenue/balance	D	REQ-I4MARKET-M-FUNC-20	YES
REQ-F-M-18	The Marketplace shall provide a dashboard for NetApp buyers for monitoring the number and price of their purchased NetApps	D	REQ-I4MARKET-M-FUNC-20	YES

REQ-F-M-19	The Marketplace shall provide wizard interfaces for onboarding of NetApps.	M	REQ-I4MARKET-M-FUNC-18	YES
REQ-F-M-20	The Marketplace shall provide wizard interfaces for order Management of NetApps.	M	REQ-I4MARKET-M-FUNC-18	YES
REQ-F-M-21	The Marketplace should store digital signatures of NetApp purchases to the Ethereum network, via a smart contract	M	REQ-I4MARKET-W-FUNC-22	YES
REQ-F-M-22	The Marketplace should host Q&A section	D		YES
REQ-F-M-23	The Marketplace should allow a user to initiate a topic for discussion	D		YES
REQ-F-M-24	The Marketplace should provide the ability to search for topics	D		YES
REQ-F-M-25	The Marketplace should provide the ability to respond to topics	D		YES
5G NPN				
REQ-F-5G-1	The NEF emulator must provide request/response and subscribe/notify communication as defined in 3GPP TS 29.501	M	REQ-DEV-M-COMP-8	YES
REQ-F-5G-2	The NEF emulator of the 5G Northbound APIs should provide a graphical user interface for defining network and UE parameters	D	REQ-DEV-M-USE-7	YES
REQ-F-5G-3	The NEF Memulator must offer the MonitoringEvent API through N33 interface to external applications (i.e., NetApps)	M	REQ-5G-M-FUNC-1, REQ-5G-M-FUNC-2	YES
REQ-F-5G-4	The NEF emulator must offer the AsSessionWithQoS API through N33 interface to external applications (i.e., NetApps)	M	REQ-5G-M-FUNC-1, REQ-5G-M-FUNC-2	YES
REQ-F-5G-5	The NEF emulator must provide an authentIcation mechanism for NetApps [3GPP TS 33501-h10]	M	REQ-5G-M-SEC-17	YES
REQ-F-5G-6	TLS shall be used by the NEF emulator to provide integrity protection [3GPP TS 33501-h10]	D	REQ-5G-M-SEC-16	YES
REQ-F-5G-7	TLS shall be used the NEF emulator to provide relay protection [3GPP TS 33501-h10]	D	REQ-5G-M-SEC-16	YES
REQ-F-5G-8	TLS shall be used to provide confidentiality protection [3GPP TS 33501-h10]	D	REQ-5G-M-SEC-16	YES
REQ-F-5G-9	NEF shall support OAuth-based authorization mechanism [3GPP TS 33501-h10]	M	REQ-5G-M-SEC-17	YES
REQ-F-5G-10	The CAPIF tool must choose the apropriate security method for mutual authentication and protection between NEF and NetApps [3GPP TS 33501-h10]	M		NO
REQ-F-5G-11	The CAPIF tool must provide the CAPIF_Discover_Service_API	M	REQ-5G-M-FUNC-22	NO
REQ-F-5G-12	The CAPIF tool must provide the CAPIF_Security_API	M	REQ-5G-M-FUNC-23	NO
REQ-F-5G-13	The CAPIF tool must provide the CAPIF_Events_API	M	REQ-5G-M-FUNC-24	NO

3.3.1 Non-functional system requirements

Table 3 lists the non-functional requirements of the EVOLVED-5G framework. As expected, most of the non-functional requirements refer to the infrastructure supporting the EVOLVED-5G facility, that is the 5G NPN, the CI/CD platform and Open Repository. Some constraints and prerequisites for the processes implemented by the rest of the environments are also defined.

Table 3 EVOLVED-5G non-functional requirements

ID	title	priority	D2.1 requirement	Release I
WORKSPACE				
REQ-NF-W-1	The EVOLVED-5G SDK must provide a NetApp template (repository file structure) for generating the NetApp repository	D	REQ-DEV-S-FUNC-4	YES

REQ-NF-W-2	The EVOLVED-5G SDK must provide a NetApp example (dummy NetApp)	D		YES
REQ-NF-W-3	The EVOLVED-5G SDK must contain libraries for NEF APIs	D		YES
REQ-NF-W-4	The EVOLVED-5G SDK must contain libraries for CAPIF APIs	D		NO
CI/CD PLATFORM				
REQ-NF-CC-1	The CI/CD environment must be connected to Athens 5G Platform	M	REQ-PI-M-FUNC-4	YES
REQ-NF-CC-2	The CI/CD environment must be connected to Málaga 5G Platform	M	REQ-PI-M-FUNC-4	YES
REQ-NF-CC-3	Pipelines that require deployment of artifact containers must be supported by appropriate virtualized environment	M	REQ-DEV-M-PORT-6	YES
REQ-NF-CC-4	The CI/CD environment must provide a virtualized platform for local deployment of NetApps	M	REQ-PI-M-FUNC-2, REQ-PI-M-FUNC-3	YES
REQ-NF-CC-5	A NetApp deployment pipeline must be available in the CI/CD platform	M	REQ-I4MARKET-M-MAIN-4	YES
REQ-NF-CC-6	A pipeline for removing a NetApp instance from the environment must be available	M	REQ-I4MARKET-M-MAIN-4	YES
REQ-NF-CC-7	A NetApp validation pipeline must be available in the CI/CD	M	REQ-I4MARKET-M-MAIN-4	YES
REQ-NF-CC-8	A NetApp certification pipeline must be available in the CI/CD	M	REQ-I4MARKET-M-MAIN-4	NO
OPEN REPOSITORY				
REQ-NF-OR-1	The Open repository must support the storage of NetApp source code	D	REQ-DEV-S-MAINT-2	
REQ-NF-OR-2	The Open Repository must support the storage of containerized images of software	D		
REQ-NF-OR-3	Only registered users to the EVOLVED-5G GitHub organization shall be able to upload NetApps to the Open Repository	M		YES
REQ-NF-OR-4	A resource hosted by the Open Repository must be accessible through the web via a dedicated URL	M	REQ-I4MARKET-M-FUNC-11	YES
VALIDATION ENVIRONMENT				
REQ-NF-V-1	Experimentation test cases and data must be private to a specific experiment	M	REQ-I4-S-SEC-5	YES
REQ-NF-V-2	Validation tools developed in the context of EVOLVED-5G should be open-source, unless specific IP or contractual obligations forbid this for certain circumstances	D	REQ-DEV-S-MAIN-13	YES
REQ-NF-V-3	The Validation Environment must provide mechanisms for isolating the execution of different validations, so that the results are not affected by unrelated experiments	M	REQ-DEV-M-USE-11	YES
MARKETPLACE				
REQ-NF-M-1	Only certified NetApps must be published in the marketplace	M	REQ-I4MARKET-M-FUNC-8	YES
REQ-NF-M-2	Only NetApps with defined pricing information can be available in the marketplace	M	REQ-I4MARKET-S-FUNC-14	YES
REQ-NF-M-3	The Marketplace should rely on the TMF620 (Product Catalog Management open API to store NetApp metadata	M	REQ-I4MARKET-S-MAIN-21	YES
5G NPN				
REQ-NF-5G-1	Relay protection shall be supported for the communication between NEF and NetApps [3GPP TS 33501-h10]	M	REQ-5G-M-SEC-16	YES
REQ-NF-5G-2	SUPI shall not be sent outside the 3GPP operator domain by NEF [3GPP TS 33501-h10]	M		YES
REQ-NF-5G-3	Confidentiality protection shall be supported for the communication between NEF and NetApps [3GPP TS 33501-h10]	M	REQ-5G-M-SEC-16	YES

REQ-NF-5G-4	Integrity protection shall be supported for the communication between NEF and NetApps [3GPP TS 33501-h10]	M	REQ-5G-M-SEC-16	YES
REQ-NF-5G-5	Athens platform shall support Kubernetes for deploying NetApps	M	REQ-5G-M-FUNC-3	YES
REQ-NF-5G-6	Malaga platform shall support Kubernetes for deploying NetApps	M	REQ-5G-M-FUNC-3	YES
REQ-NF-5G-7	Compliance with 5G SA in n78 band supporting 5G connectivity	D	REQ-5G-S-USE-5, REQ-5G-M-MAIN-7	YES
REQ-NF-5G-8	5G equipment should provide the means to connect to 5G RAN through 802.11 a/b/g/n/ac/ax technology, for vApps that require devices (e.g., robots, VR headsets) incapable of connecting to 5G network	D	REQ-5G-S-USE-5, REQ-5G-M-MAIN-7	YES
REQ-NF-5G-9	The 5G system shall support standalone mode of 5G operation in n78 band	M	REQ-5G-M-COMP-4	YES
REQ-NF-5G-10	Mutual authentication based on client and server certificates shall be performed between the NEF and NetApps using TLS [3GPP TS 33501-h10]	M		YES

3.4 NetApp requirements and testing plan

The business and user requirements elicited in the first period of the project and documented in D2.1 [2] suggested a list of requirements referring to the NetApps. Some of these requirements are requirements specific for certain NetApps, which are developed by SMEs in the project (e.g., REQ-IEM-M-PERF-3: "*The NetApp must provide a file server to enable the vApp to share multimedia files (images, videos)*"). These requirements have been disregarded in the elicitation process of the system requirements, since they do not affect the design of the EVOLVED-5G facility. Actions regarding pilot-specific design and implementation decisions of NetApps and relevant vApps will be reported in the final deliverables of WP4.

Another set of requirements referring to NetApps, impose certain constraints on the development of the NetApp itself. For instance, REQ-PI-M-FUNC-5 dictates that *NetApps shall support being instantiated in a "public infrastructure provider" to be defined*. In principle, the NetApp developer is the consumer of the EVOLVED-5G facility services. Therefore, no requirements can be enforced on the product of the work of the NetApp developer. The NetApp design depends only on the goals of the developer. However, the system may or may not certify and further publish a NetApp that does not comply with the adopted design principles and marketplace policies.

The toolset for ensuring NetApp compliance with the EVOLVED-5G concept and framework is the three-level testing procedure realized at the core of the system by the Workspace (via the verification process), the Validation Environment and the Certification Environment. As a result, requirements of this kind, i.e., initially referring to NetApps, have been transformed to requirements imposed on at least one of the environments of the framework commissioned with one of the testing tasks.

In fact, these system requirements have shaped the testing plan adopted in each testing phase of the NetApp lifecycle. This is reflected in Table 4, which lists the steps of the testing plan, i.e., individual tests, executed for each NetApp that enters the EVOLVED-5G realm. Each test may be performed by one or more testing processes of the lifecycle of the NetApp (i.e., verification, validation and certification). Each entry of the table represents a mapping between a test and the system requirement it addresses.

Table 4 Mapping of NetApps' requirements to testing process

Test	Verification	Validation	Certification
Build NetApp	REQ-F-W-9	REQ-F-V-7	NA
Grab the NetApp from Artifactory	NA	NA	REQ-F-CE-2
Upload NetApp to Docker Registry	NA	NA	REQ-F-CE-26
Deploy NetApp	REQ-F-W-10	REQ-F-V-8	REQ-F-CE-2
Destroy NetApp	REQ-F-W-11	REQ-F-V-8	NA
Onboarding NetApp in CAPIF (API Invoker)	REQ-F-W-16	REQ-F-V-10	REQ-F-CE-7
Publish Netapp API in CAPIF	REQ-F-W-16	REQ-F-V-10	REQ-F-CE-7
Discover APIs using CAPIF	REQ-F-W-16	REQ-F-V-10	REQ-F-CE-8
Offboarding a Netapp (CAPIF)	REQ-F-W-16	REQ-F-V-10	REQ-F-CE-10
CAPIF Security API	REQ-F-W-16	REQ-F-V-10	REQ-F-CE-7
CAPIF Events API	REQ-F-W-16	REQ-F-V-10	REQ-F-CE-7
NetApp callback CAPIF	REQ-F-W-18	REQ-F-V-12	REQ-F-CE-11
NEF AsSessionWithQoS API	REQ-F-W-15	REQ-F-V-9	REQ-F-CE-12
NEF MonitoringEvent API	REQ-F-W-15	REQ-F-V-9	REQ-F-CE-13
NetApp callback NEF	REQ-F-W-17	REQ-F-V-11	REQ-F-CE-14
Syntax analysis NetApp source code	REQ-F-W-22	REQ-F-V-15	REQ-F-CE-15
Scale out ReplicaSet NetApps	NA	NA	REQ-F-CE-16
Shrink ReplicaSet NetApps	NA	NA	REQ-F-CE-16
NetApp open ports scan	REQ-F-W-24	REQ-F-V-16	REQ-F-CE-23
Vulnerability scan	REQ-F-W-19	REQ-F-V-14	REQ-F-CE-16
Open Source License Scanning	NA	REQ-F-V-13	REQ-F-CE-18
Certification environment performance assessment	NA	NA	REQ-F-CE-1
Container integrity check	REQ-F-W-21	REQ-F-V-7	REQ-F-CE-16
NetApp - vAPP integration	NA	REQ-F-V-17	
CAPIF services	NA	NA	REQ-F-CE-6
NEF services	NA	NA	REQ-F-CE-4

More details regarding the testing plan adopted by each one of the Workspace, Validation and Certification Environments are provided in the respective chapters of this report.

4 WORKSPACE AND NETAPP DEVELOPMENT PROCESS

4.1 INTRODUCTION

The Workspace is the entry point or where the developer will make the first steps of the NetApp lifecycle, that is the NetApp's development phase and the NetApps' verification phase. The Workspace offers the software tools, as well as detailed instructions to guide developers on how to use those tools and to demonstrate what it can be achieved by making use of them.

The Workspace environment has been properly described in D2.2 [3] and D3.1 [4]. Nevertheless, as the project has demonstrated significant progress, certain adjustments have been performed, which are listed below:

- CI/CD services are not part of the Workspace anymore, but constitute a separate component accessible by all framework environments throughout the NetApp lifecycle.
- CAPIF and NEF interaction, necessary for the verification of a NetApp under development, is now ensured through the integration of the relevant emulators as components of the Workspace.
- A new Community block is now linked to the Workspace, to guide them during the whole development process on how to make optimum use of the Workspace environment.
- A NetApp template has been added to the SDK, to cater for an out of the box initiation of the NetApp development process.

4.2 FUNCTIONAL BLOCKS

The Workspace is composed by two main blocks, that is the Software Development Kit (SDK) and the Code Verification block, as depicted in Figure 3. At the same time, it is tightly integrated with external blocks, namely the CI/CD Services, the Open Repository and the Community, which are also connected with the rest of the environments of the architecture.

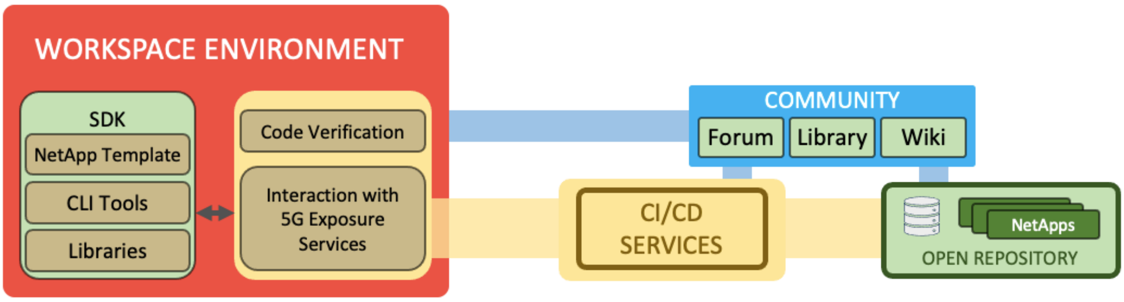

Figure 3 Main functional blocks of the Workspace

The Workspace supports the first two phases of the lifecycle of the NetApp, that is, the development with the SDK component and the verification with the Code Verification component in conjunction with the 5G Exposure Services. The Workspace is interacting with the CI/CD Services platform, but the initial vision has changed and the CI/CD does not constitute a part of the Workspace in the final architectural design, as it was considered in D2.2 [3]. The CI/CD acts as the orchestrator during the whole lifecycle of a NetApp, and, in the case of the Workspace, it is the component that executes the NetApp verification testing plan.

Within the development phase, different components of the SDK functional block offer various functionalities:

- A **CLI tool**, which provides the ability to create a NetApp based on the NetApp template, to upload it to the Open Repository, as well as, to launch the verification and validation phase.
- A **NetApp template**, which is a NetApp source code example to be used by developers as a reference for developing the NetApp and which aligns all the NetApp repositories created under the EVOLVED-5G umbrella.
- Several **SDK libraries** that let the NetApp under development communicate with the 5G system (5GS). They relieve them from the tedious work of understanding and creating from scratch the interaction with a 5GS.

The verification phase involves the rest of the Workspace components and interacts with external functional blocks for the execution of the verification of the NetApp. The whole process is initiated and monitored by the developer through the CLI Tool which communicates with the CI/CD Services component. The **CI/CD Services** component hosts and controls (via an orchestrator) the basic verification tests, which a developer should run to verify the functionalities of a NetApp, in the form of proper execution pipelines. At the same time, it hosts (via a virtualized environment) the running instances of the necessary artifacts that support the process. In particular, the **CI/CD Services** component:

- Manages the basic verification tests that a developer should run to verify the basic functionalities of a NetApp. These are the build, deploy and destroy pipelines that create, instantiate and destroy the container of the NetApp, respectively. For building the NetApp, the orchestrator retrieves the source code of the NetApp from the Open Repository.
- Executes static code analysis and vulnerability scans of the container of the NetApp.
- Performs connectivity tests with the NEF and CAPIF services with the support of the **Interaction with 5G Exposure Service** component. These tests verify the connectivity of the NetApp to the 5G network, relying on a generic scenario common for all NetApps.
- Checks the ports, to which the NetApp is expected to listen, for communicating with a vertical Application (vApp) or other service.

The **Open Repository** is the functional block where source code and binary artifacts are stored. For EVOLVED-5G, GitHub is selected to act as the Code Repository for all NetApps and other software implementations related to EVOLVED-5G, such as NEF and CAPIF, among others. Finally, a **Community** block is related to the Workspace. In the **Community** component, developers can find all the necessary software code, documentation, guides and instructions for using the EVOLVED-5G software hosted in GitHub and related to the Workspace like, for instance, instructions on how to use the SDK libraries.

4.3 NetApp development Process flow

The main process flow supported by the Workspace and showcasing the integration of the components explained in the previous section is the development and the verification of the NetApp, which can be iteratively executed until the developer reaches the desired result. The NetApp development and verification is a process in which the NetApp developer leverages the

SDK tools provided in EVOLVED-5G towards the creation of a NetApp. As illustrated in Figure 4, this process consists of a series of steps which are explained below:

- **Step 1**: The developer downloads from the Open Repository and installs the EVOLVED-5G software with all the necessary dependencies according to the operating system used, following the instructions provided in the SDK and in the Community.
- **Step 2**: Once the SDK package is installed, a new NetApp repository is created from the commands provided by the CLI Tool.
- **Step 3**: The newly created NetApp repository is automatically uploaded to GitHub, creating a new remote repository.
- **Steps 4 – 6**: The developer develops the NetApp, starting from the NetApp template, adding the necessary functionalities, taking advantage of the SDK libraries to provide the NetApp with 5G connectivity capabilities, and testing it locally. The source code ends up stored in the NetApp repository on GitHub.
- **Steps 7 – 9**: The developer, assuming the role of verifier, leverages the CLI Tool to initiate the verification pipeline in the CI/CD Services component.
- **Steps 10 – 18**: A multitude of verification tests (including code correctness, containerization success, 5G connectivity and vulnerability scans, as described in Section 3.4) are executed by the CI/CD Services component. To enable the process, the CI/CD component builds and deploys the NetApp, as well as the NEF emulator and the CAPIF tool.
- **Steps 19 – 21**: When the verification is complete, the result report is generated by CI/CD Services component and is returned and displayed through the CLI to the developer.

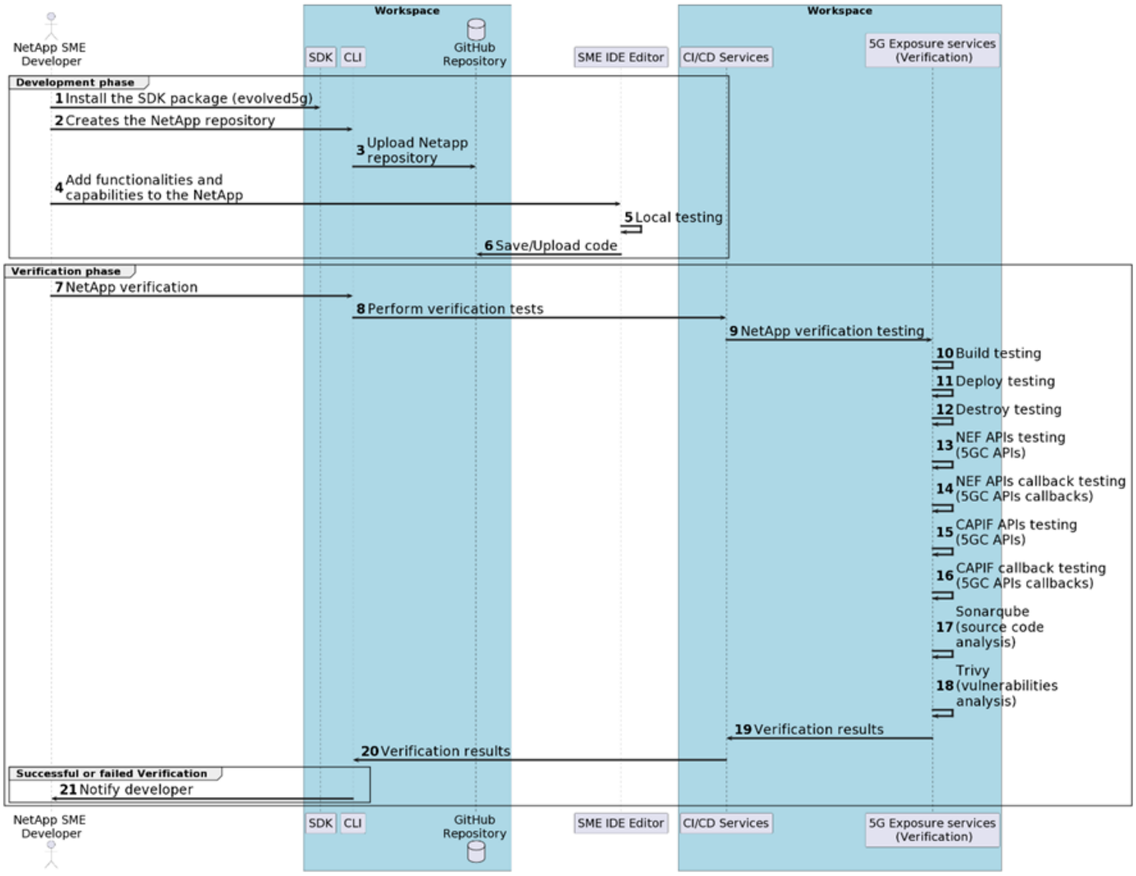
Workspace
Workspace
NetApp SME Developer
SDK
CLI
GitHub Repository
SME IDE Editor
CI/CD Services
5G Exposure services (Verification)
Development phase
1 Install the SDK package (evolved5g)
2 Creates the NetApp repository
3 Upload Netapp repository
4 Add functionalities and capabilities to the NetApp
5 Local testing
6 Save/Upload code
Verification phase
7 NetApp verification
8 Perform verification tests
9 NetApp verification testing
10 Build testing
11 Deploy testing
12 Destroy testing
13 NEF APIs testing (5GC APIs)
14 NEF APIs callback testing (5GC APIs callbacks)
15 CAPIF APIs testing (5GC APIs)
16 CAPIF callback testing (5GC APIs callbacks)
17 Sonarqube (source code analysis)
18 Trivy (vulnerabilities analysis)
19 Verification results
20 Verification results
Successful or failed Verification
21 Notify developer
NetApp SME Developer
SDK
CLI
GitHub Repository
SME IDE Editor
CI/CD Services
5G Exposure services (Verification)

Figure 4 NetApp development process

4.4 Integration Design

4.4.1 Shared resources

The Workspace environment is fully integrated in the EVOLVED-5G architecture as presented in Chapter 0. During the development phase, the Workspace is interacting with the Open Repository (GitHub), which hosts the source code of the NetApps.

During the verification phase, the source code of the NetApps, the NEF emulator and the CAPIF tool are retrieved by the CI/CD Services component and are built to produce the necessary images (artifacts). These images, in turn, are deployed in the CI/CD Services and are used for the verification process. The latter produces the result reports that are sent back to the Workspace.

4.4.2 Exposed APIs

The central point of interaction of the user with the Workspace is the CLI Tool. The CLI Tool is the frontend of the SDK that allows the developer interact with the SDK and the CI/CD Services component.

The CLI Tool is communicating with the CI/CD Services component for the initiation, control and monitoring of the verification phase. As explained in Section 3.4, the verification process encompasses a subset of tests of the validation and the certification process. Thus, the APIs exposed by the CI/CD Services for the verification process are covered in detail in Section 6.4.2, where the complete list of the CI/CD services APIs, which are relevant to the certification process, are documented.

Finally, for the verification process the NEF emulator and CAPIF Tool are deployed. These interact with the NetApp under verification through the exposure of the NEF and CAPIF APIs. These APIs are analysed in the APIs section of the 5G NPN environment, i.e., Section 8.3.1.

4.4.3 Security

A central role of crucial importance for the Workspace environment is played by Github. This is where everyone – internal and external to the project – may have access to the source code for several components of the project, as well as all the source code of all NetApps. In order to preserve security, a set of methodologies are employed to protect these resources from any type of risk.

The consortium of EVOLVED-5G has created a GitHub organization[7], access to which is granted only by an administrator of the organization as a result of a relevant request by the aspired NetApp developer. The developer will receive an invitation that must be accepted in order to obtain the necessary permissions for contributing to the EVOLVED-5G repository. Different level of permissions is granted to the developer depending on the role of the developer in the system.

In case the developer wants to store her NetApp in a GitHub repository, besides having access to the organization, the developer needs to be given specific authorization for creating a NetApp repository remotely. A developer creates an appropriate token with the necessary permissions and an SSH key corresponding to the computer where the NetApp will be developed and from where it will be uploaded to GitHub.

[7] https://github.com/EVOLVED-5G/

For contributing to repositories relevant with the source code of the EVOLVED-5G framework itself, besides having access to the organization, one needs to be member of the contributors of that particular repository. But even in this case, specific access control policies prevent certain contributors from being able to update code branches that are connected through the CI/CD platform with the production environment.

In addition to these access control mechanisms regarding the code of the EVOLVED-5G and the NetApps, security mechanisms are employed by the NEF and CAPIF components for their communication with the NetApps. These aspects are analysed in the relevant section of the 5G NPN environment, i.e., Section 8.3.2.

5 VALIDATION ENVIRONMENT

5.1 INTRODUCTION

The validation process is composed by a number of testing steps and can be seen as a superset of the verification process, as it includes all the tests of the verification process. This approach serves three purposes: (i) the developer gets a complete assessment of the NetApp already from the verification phase, which can iteratively be followed by more development-verification cycles before going to the validation phase, (ii) the tests performed during the validation phase are executed in a real environment giving a different perspective to the validation results in comparison to the verification results, (iii) during validation, the results can be audited by the platform operators, which is important as it can possibly detect issues in the NetApp that could be fixed before reaching the certification phase, and (iv) the validation phase also ensures that the NetApp is able to operate under real or near-real network conditions with, at least, one vertical application (vApp). This vApp may be chosen by the NetApp developer (either coming from the same entity or as a collaboration) or agreed during the consultation stage with the platform owners.

5.2 FUNCTIONAL BLOCKS

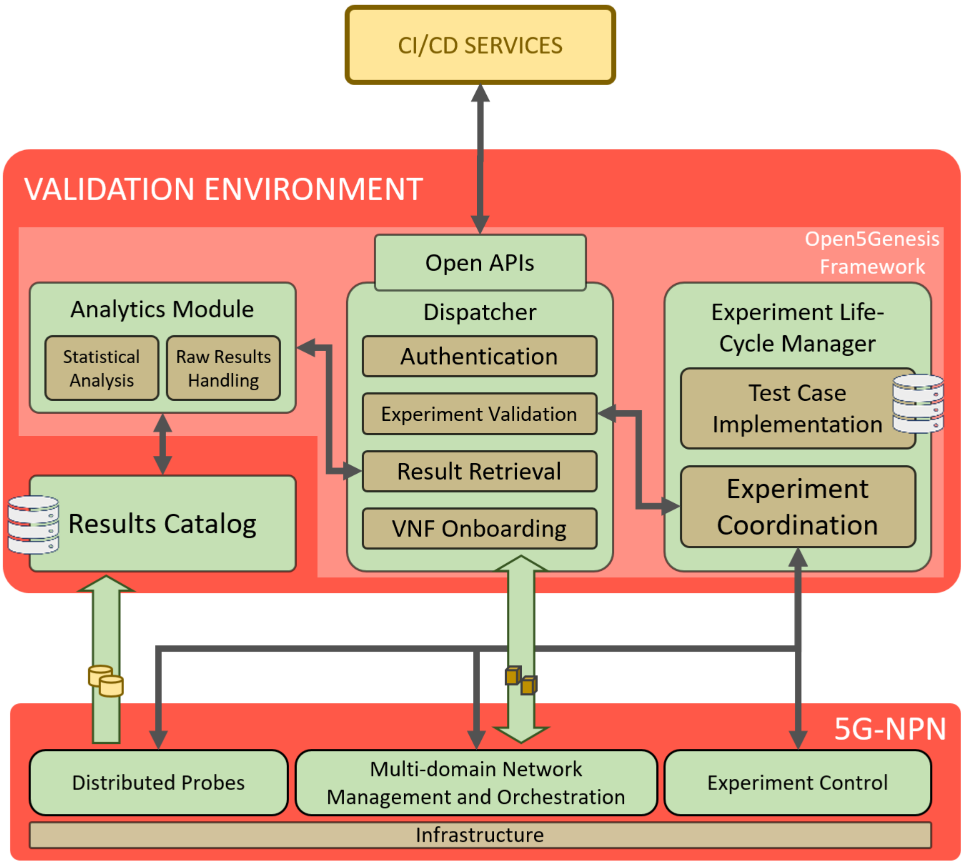

Figure 5: Validation Environment architecture

The Validation Environment is based on the Open5Genesis Suite, which includes components for authentication and distribution, experiment coordination, long term storage, retrieval and analysis of results, and VIM (Virtual Infrastructure Management). These components are depicted in Figure 5 and are described next:

- The frontend of the Validation Environment is the Dispatcher. This component implements the Open API that provides endpoints for authentication, experiment execution and results retrieval, among others. Through the Dispatcher, the Validation Environment exposes a single point of entry that can handle all authentication and user management, before transparently redirecting each request to the corresponding component in the backend. During the NetApp's validation, the CI/CD Services request the execution of the corresponding NetApp test case from the Dispatcher.
- The Experiment Life-Cycle Manager (ELCM) is the entity that coordinates the execution of experiments in any validation platform, which in this case corresponds to the Validation Environment of the EVOLVED-5G facility. It provides capabilities for defining test case implementations, which are files that specify a set of tasks and the relevant flow of actions that must be performed during the execution of an experiment. A task can make use of available interfaces for controlling heterogeneous software or hardware components in the platform. Otherwise, control can be offloaded to other automation tools (e.g., OpenTAP[8], Robot Framework[9]) during the execution of a test case.
- Measurements generated during an experiment execution are stored in the Results Catalogue, which is in principle a time-series database. The storage of raw results is complemented by the Analytics Module, which is a web interface providing access to a set of statistical analysis tools that can be applied to experimental results. The Analytics Module also provides a REST API that can be used to retrieve raw or statistical results, and it is also exposed by the Dispatcher as part of the Open APIs.

The **Slice Manager** is also part of the Open5Genesis Suite and is able to orchestrate the deployment of network services. In the context of EVOLVED-5G, it is considered part of the multi-domain network management and orchestration functional block of the 5G NPN (please, refer to Chapter 8), and remains as an optional component that can be used for the handling of VNFs

5.3 Validation process

The validation aims at testing NetApps both in terms of their functionality and in terms of their performance. The validation process is executed in real network conditions and it also involves tests of the NetApp-vApp integration. In particular, during the validation process, the following properties of the NetApp are examined:

- It is ensured that the NetApp is able to complete successfully all the tests that are part of the verification phase.
- The NetApp is tested in a real infrastructure and under real or near-real network conditions in a 5G NPN.
- The NetApp functionality is tested to check if it is suitable for integration with a vApp. In case of NetApps tailored for a particular vApp, the vApp is known a priori. For NetApps

[8] https://opentap.io/
[9] https://robotframework.org/

that provide generic functionality and which can serve multiple vApps, any available vApp option can be selected, depending on the functionality offered by the NetApp.

- The NetApp's performance is examined as designated by KPIs that are agreed between the NetApp developers, platform owners and, possibly, vApp providers.

5.3.1 NetApp performance assessment

At the core of the validation process lies the performance assessment of the NetApp that is based on the Open5Genesis experimentation methodology (please, refer to Section 6.4 of the deliverable D2.2 [3]). The following steps lead to a successful NetApp validation:

1. The NetApp developer contacts any of the available validation platforms. Communication between the selected validation platform, the NetApp developer and, possibly, the vApp provider starts. This is known as the **consultation phase**, and is used to discuss the scope and details of the NetApp validation, including, but not limited to:
   - Details about the use case, which includes the functionality provided by the NetApp, as well as the expected results or improvements that may derive from its usage.
   - Details about the selected vertical application, if known, or criteria that may be used for the selection of a third-party vertical application, for use as part of the validation.
   - The set of Key Performance Indicators (KPIs) that are of interest to all parties, along with information on how to obtain raw measurements and calculation methods to be used.
   - Details about the deployment of additional equipment or devices in the validation platform, about the deployment of the vApp, or about access to any additional resources needed for the validation process.
   - Details about any control or measurement interfaces that may be used during the coordination of the validation process.
   - The sequence of steps that are performed by the validation process, along with possible radio conditions that shall be applied, or details about the set of resources to be reserved for the validation task. This information will be used during the definition of the **test-case scenario(s)**, and the **network slice** for the validation.
   - Any other business, security or regulation details.
2. Once the details of the NetApp validation are agreed between all parties, the implementation of the test case takes place. During this phase, known as the **non-automated testing**:
   - Any necessary equipment or devices are deployed within the validation platform, along with the NetApp and the required vertical application components.
   - Any additional functionality required for the validation is implemented and tested.
   - In an iterative process, all steps that are part of the test case are tested, at first manually and then automated as much as possible. Actions or configurations, which are impossible to perform in an automatic way, may be added to the set of pre-conditions of the experiment.
   - Once the NetApp is deployed within the validation platform, an early execution of the verification tests can be performed, in order to detect any possible issue at an early stage.

3. When all of the functionality required is confirmed to work, the **automated testing** takes place. For this stage, a fully implemented test case is made available in the validation platform, which is then executed as part of the validation pipeline of the EVOLVED-5G CI/CD environment. In particular:
    - On the timeframe agreed between all parties, the platform operators configure the environment according to the requirements of the NetApp validation.
    - Using the CI/CD environment, the NetApp developer initiates the validation process.
    - As part of the validation pipeline, the CI/CD environment executes the tests that are common to all NetApps:
        - An initial platform assessment, in which the basic functionality and performance of the platform is tested. This is to ensure that all equipment is working within the expected values and no interferences are affecting the execution of the validation.
        - All tests that are also part of the NetApp verification are executed, ensuring that the basic functionality of the NetApp is performing as expected.
    - The CI/CD environment, then, requests the execution of the validation test case implemented in the platform. This includes all the tests that are specific to the NetApp-vApp pair under test, and that were agreed during the consultation phase.
    - The CI/CD environment prepares the final validation report, which includes information generated during all the previous steps along with the KPIs generated by the validation platform. This report is made available to the NetApp developer.

If no errors are detected during the validation, and all measured KPIs are within the range agreed by the NetApp developer and the vApp provider, then the NetApp is considered validated and may become eligible for the certification process. These steps, along with their inputs and expected outputs can be seen in Figure 6.

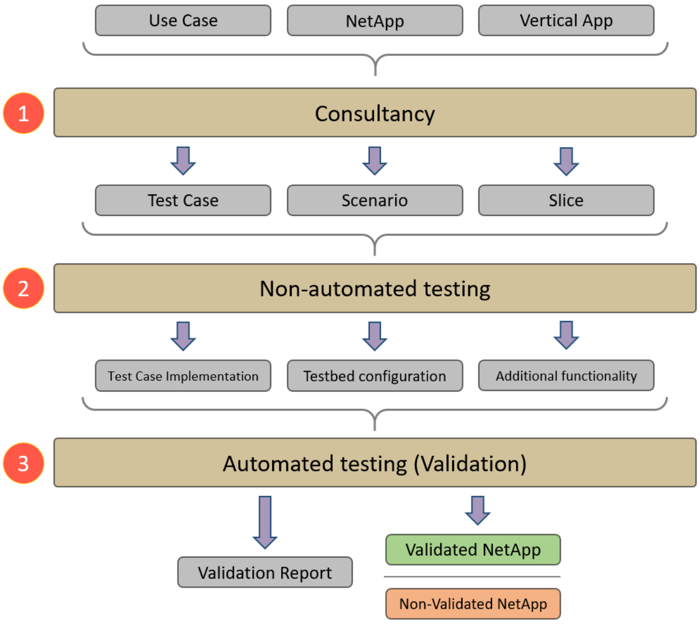

Figure 6: Validation process description

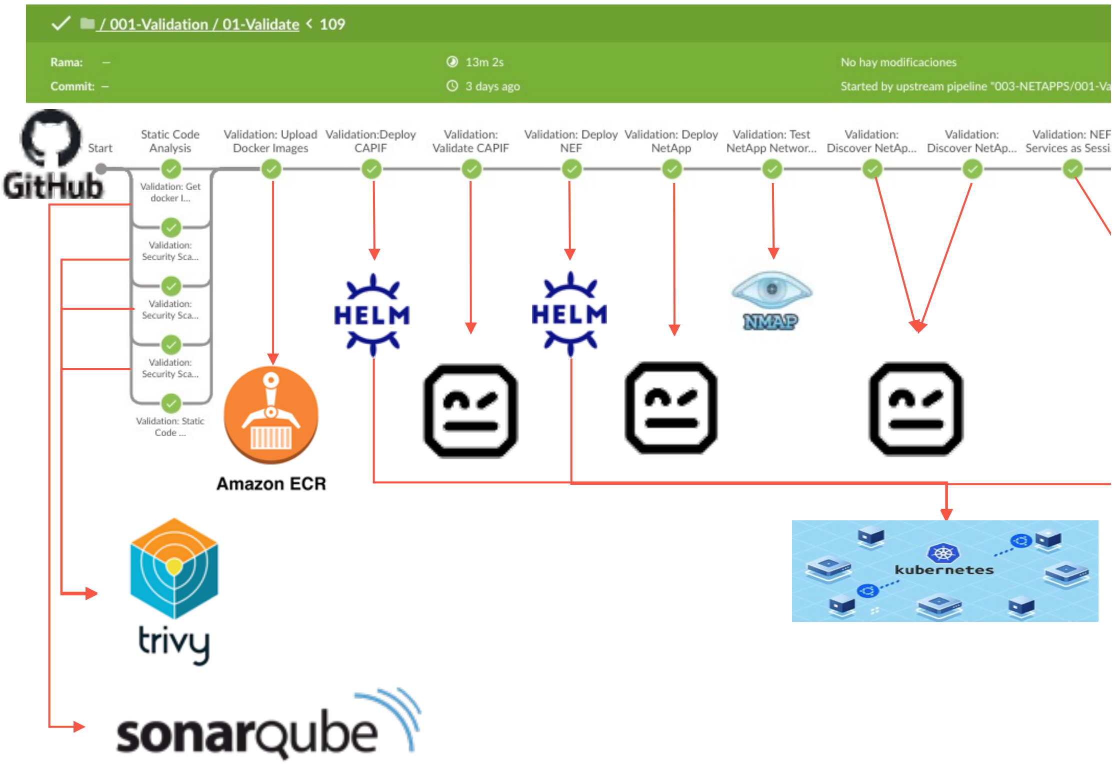
✓ / 001-Validation / 01-Validate < 109
Rama: –
Commit: –
13m 2s
3 days ago
No hay modificaciones
Started by upstream pipeline "003-NETAPPS/001-Va
GitHub
Start
Static Code Analysis
Validation: Get docker I...
Validation: Security Sca...
Validation: Security Sca...
Validation: Security Sca...
Validation: Static Code ...
Validation: Upload Docker Images
Validation:Deploy CAPIF
Validation: Validate CAPIF
Validation: Deploy NEF
Validation: Deploy NetApp
Validation: Test NetApp Networ...
Validation: Discover NetAp...
Validation: Discover NetAp...
Validation: NEF Services as Sessi
HELM
HELM
NMAP
Amazon ECR
kubernetes
trivy
sonarqube

Figure 7 Validation pipeline (part 1)

5.3.2 Functional validation of NetApp

The functional testing of the NetApp is realized by a validation pipeline built in the CI/CD platform of the EVOLVED-5G facility, which for clarity is depicted in two parts in Figure 7 and Figure 8. This pipeline comprises a sequence of steps, each one of which interacts with different platform components.

The entry point of the pipeline is the Github repository of the NetApp. The source code of the NetApp is scanned for vulnerabilities with proper tools (e.g., SonarQube, Trivy). Once the software is scanned, the NetApp container image is uploaded to a virtualized platform (e.g., Docker Registry in AWS) for the deployment of the NetApp.

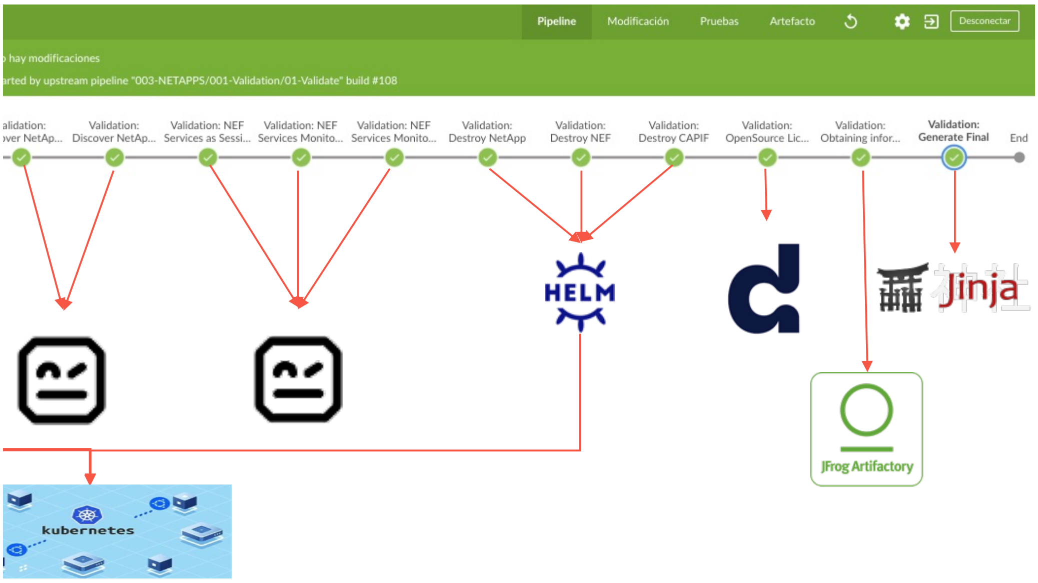
Pipeline
Modificación
Pruebas
Artefacto
Desconectar
hay modificaciones
rted by upstream pipeline "003-NETAPPS/001-Validation/01-Validate" build #108
alidation: ver NetAp...
Validation: Discover NetAp...
Validation: NEF Services as Sessi...
Validation: NEF Services Monito...
Validation: NEF Services Monito...
Validation: Destroy NetApp
Validation: Destroy NEF
Validation: Destroy CAPIF
Validation: OpenSource Lic...
Validation: Obtaining infor...
Validation: Generate Final
End
HELM
Jinja
JFrog Artifactory
kubernetes

Figure 8 Validation pipeline (part 2)

The next step involves the preparation of the environment, deploying and testing the functionalities of the CAPIF and NEF tools (e.g., using HELM, Robot Framework testing engines). Once the environment is ready, the NetApp can be deployed.

The NetApp is deployed in a virtualized platform (e.g., Kubernetes), and its connectivity with the network is put into test. Once the NetApp is validated to be deployed properly, automated tests to validate CAPIF and NEF integration of the NetApp are performed. After completing these tests, which results in a successful functional validation of the NetApp, the environment can be cleaned destroying the NetApp, CAPIF and NEF containers from the virtualized platform.

Finally, license assessment tools (e.g., Debricked) check the licenses required by the NetApp.

The results of each validation step are recorded and are stored in the Open Repository (artifactory) of the platform. The final step is to produce a complete validation report consolidating the results of the individual validation steps.

5.3.3 Integrated validation process flow

As already explained, the validation process contains three steps that make use of the infrastructure and resources of the validation platform and associated 5G NPN. These steps correspond (i) to the functional NetApp validation, (ii) to the initial platform assessment, which ensures that all the equipment of the platforms is functional and above certain performance thresholds, and (iii) to the custom validation test case that is able to extract the KPIs of interest for the NetApp developer and for the selected vertical application case.

These steps result in two experiment executions that take place within the Validation Environment. The experiments are preceded by a functional validation of the NetApp similar to the verification process (see Figure 4), which is not analysed here again. The actions performed and the recorded measurements are different between the platform assessment experiment and the customized experimentation for each NetApp. However, they follow an integrated execution flow that is presented in Figure 9.

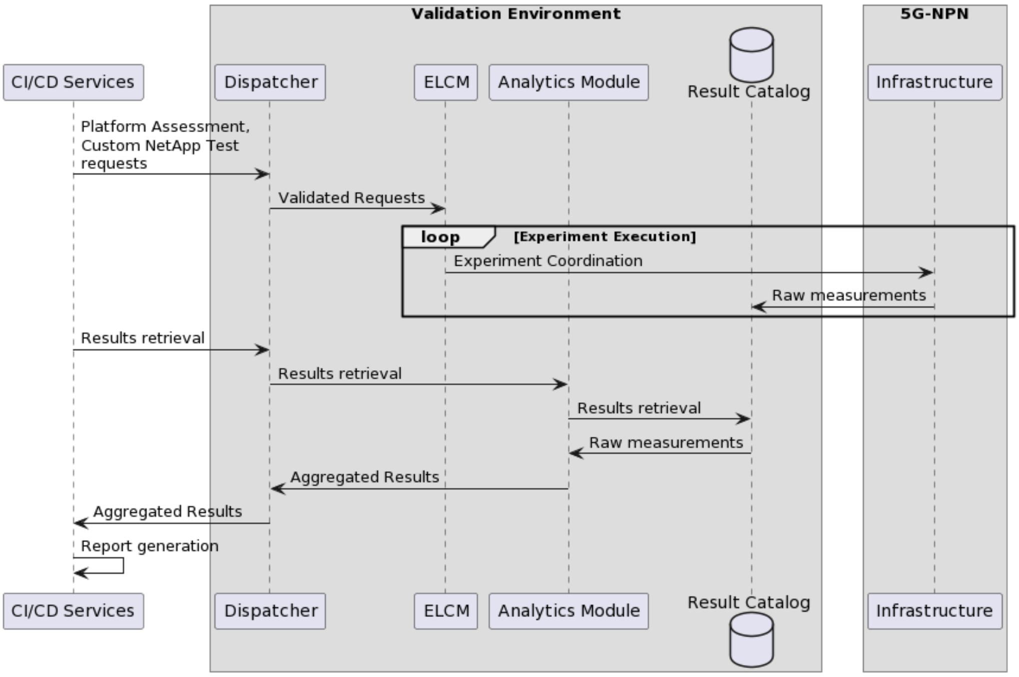

Figure 9 Validation process sequence diagram

The request is generated by the CI/CD services, as part of the validation pipeline, and is sent to the Open API implemented by the Dispatcher. The Dispatcher, after ensuring that the request is well formed and comes from a trusted source, forwards the request to the ELCM, which then coordinates the experiment.

The ELCM makes use of the interfaces exposed by the different elements in the infrastructure (**Experiment Control** in Figure 5), orchestrating the different actions required for the experiment. A set of distributed probes and monitoring tools extract various measurements from the infrastructure, which are tagged and sent to the results catalogue.

Once the experiment finishes, the CI/CD Services component retrieves the generated results, which are also requested via the Open APIs. The Dispatcher makes contact with the Analytics Module, which in turn retrieves the necessary raw results from the Results Catalogue and computes the aggregated KPIs required.

The CI/CD Services then include the generated results in the validation report that will be later made available to the NetApp developer.

5.4 INTEGRATION DESIGN

5.4.1 Shared resources

A variety of messages and resources are exchanged among the Validation Environment components, as well as between the Validation Environment and external components, like the CI/CD services. Throughout the validation process, source code, artifacts, measurements and experiment results are sent from one component to the other to realize the integration of the various functional blocks of the Validation Environment.

Communication between the different components inside the Validation Environment, and through the frontend, is based on REST APIs, with each component exposing a different set of endpoints. As usual for REST APIs, the data exchange is formatted in JSON [5]. Some examples of these can be seen in Section 5.4.2. The experiments executed by the Validation Environment are defined via experiment descriptors, the schema of which follows:

```
{
  "Application": <str, may be null>,
  "Automated": <bool>,
  "ExclusiveExecution": <bool>,
  "ExperimentType": <str>,
  "Extra": <Object[str, str], may be empty>,
  "NSs": <Array[Array[str]], (nsd id, vim location) pairs. May be empty>,
  "Parameters": <Object[str, str], may be empty>,
  "Remote": <str, may be null>,
  "RemoteDescriptor": <Same format, without “RemoteDescriptor” May be null>,
  "ReservationTime": <int, may be null>,
  "Scenario": <str, may be null>,
  "Slice": <str, may be null>,
  "TestCases": <Array[str]>,
  "UEs": <Array[str], may be empty>,
  "Version": <str>
}
```

The Result Catalogue is a time-series database (e.g., InfluxDb[10]).

[10] https://www.influxdata.com/products/influxdb-overview/

During the validation process, the CI/CD Services are in charge of the instantiation of the NetApp in the platforms. This includes the retrieval of the source code from the Open Repository, as well as the storage of the generated binary images and reports.

5.4.2 Exposed APIs

The Validation Environment exposes its functionalities through a north-bound API. This API is divided, according to the components that process each request in the backend, in two collections of endpoints. For EVOLVED-5G, the two collections of endpoints serve the tasks of experiment management (listed in Table 5) and result retrieval (listed in Table 6).

Table 5 Open APIs experiment management endpoints

API prefix: /elcm		
Endpoint	Method	Description
/experiment/run	POST	Creates and queues a new experiment execution, based on the contents of the received experiment descriptor. Replies with the following response JSON: `{“ExecutionId”: <id>}` Where <id> is a unique execution identification that can be used as input in other endpoints.

/execution/<id>/status	GET	Returns a JSON that contains general information about the status of the selected execution id, with the following schema:
		{
		“Coarse”: *Global status or current stage of execution,*
		“Status”: *Global status or status within the current stage,*
		“PerCent”: *Percentage of completion of current stage,*
		“Messages”: *List of global messages generated by the execution,*
		“Verdict”: *Current or final verdict of the execution*
		}

/execution/<id>/logs	GET	Returns a JSON that contains all the log messages generated by the execution, separated by stage:
		{
		“Status”: *Either “Success” or “Not Found”,*
		“PreRun”: *Messages generated during Pre-Run stage,*
		“Executor”: *Messages generated during the Run stage,*
		“PostRun”: *Messages generated during Post-Run stage*
		}

/execution/<id>/results	GET	Returns a compressed file that includes the logs and all files generated by the experiment execution.

/execution/<id>	DELETE	Marks the selected execution for cancellation. The execution will be cancelled after finalization of the current task.

Table 6 Open APIs result retrieval endpoints

API prefix: /result_catalog		
Endpoint	Method	Description
/statistical_analysis/<datasource>	GET	Returns a JSON structure that contains the statistical analysis of the selected KPIs, where <datasource> is the internal database to query. Accepts the following URL parameters: **experimentid**: Execution ID of the experiment, the same as returned by the experiment management endpoints. **measurement**: Measurement to obtain (table) **kpi**: KPI to obtain (column)
/get_data/<datasource>/<id>	GET	Returns a JSON structure that contains the raw measurements of the selected KPIs. Accepts the following URL parameters: **measurement**: Measurement to obtain (table). Returns all measurements by default **remove_outliers**: ‘none’, ‘zscore’ or ‘mad’. Defaults to none **match_series**: Synchronize data from multiple measurements (default: false) **max_lag***:* Time threshold for synchronization (default: 1s) **limit***:* Maximum number of rows to return (default: none) **offset***:* Number of rows to skip on the returned results (default: none) **additional_clause***:* Custom InfluxDb clause (default: none) **chunked***:* Whether to retrieve the results from the server in chunks (default: false) **chunk_size***:* Number of records per chunk (default: 10000, if *chunked* is enabled)

On the south-bound interface, the Validation Platform communicates with the different elements of the platform’s infrastructure. Given that the 5G NPN is composed by a large amount of heterogeneous equipment, there is no standard interface for the communication. The validation platform (in particular, the ELCM) is prepared to make use of any script, helper or additional orchestrator (such as OpenTAP) that is required for controlling the elements in the infrastructure. Examples of interfaces that have been successfully integrated for experiment execution include REST APIs, SCPI and Android devices (through ADB), among others.

5.4.3 Security

Security in terms of user authentication within the Validation Environment is provided by the Dispatcher, which is a single access point to the offered functionalities. This approach enables the user management and authorization for the whole validation platform to be controlled in a single component in the frontend. The Dispatcher becomes, as a result, the responsible entity for redirecting specific requests to the appropriate component in the backend that is expected to perform the necessary actions.

The communication with the Dispatcher is secured by TLS, and every request received through its endpoints must be complemented with additional authorization headers (either in the form of time limited access tokens or as encoded username and password pairs). The Dispatcher exposes endpoints for self-registration of new users. However, these users must be activated by a platform operator with administrative access to the Dispatcher, in order to gain access to any functionality (the Dispatcher will reject any request from an inactive user, returning the appropriate REST status codes for such situations).

6 CERTIFICATION ENVIRONMENT

6.1 INTRODUCTION

As presented in D2.2 [3], the NetApp concept stands as a new service/middleware layer towards vertical stakeholders promoting dynamic, open 5G services and becomes a new integration point for the mobile networks. The telecommunication business addresses interoperability and conformance through certification adopting a variety of best practices [6] to achieve this. However, the established practices refer to terminals and equipment certification, and consequently the procedure needs to be enhanced to include supplementary software and quality assessments for the NetApps.

The identified necessity has been the subject of extensive analysis as part of the EVOLVED-5G Experimentation Framework blueprint, considered as being a decisive factor for the practical adoption of the NetApps software artifacts in the network operators' domain. SQuaRE (System and Software Quality Requirements and Evaluation) [1, 7, 8] that is part of the ISO/IEC 25000 series with the goal of creating a framework for the evaluation of software product quality, was identified as the suitable methodology to follow, primarily due to its conceptual proximity with the already established telecom certification practices. As a result, in the project the SQuaRE methodology has been applied to design the adopted certification process.

The core stakeholders in the certification process, apart from the organization interested in the evaluation, are the Certification/Audit/Accreditation Authority/Body, awarding certificates by specifying the audit objectives and reviewing their evaluation, and the accredited laboratory in charge of executing well-specified and pre-agreed certification audit tests in the relevant technical environment. Both the certification authority and the accredited labs, need to be themselves appropriately certified through ISO/IEC 17011 [7] and ISO/IEC 17025 [8] respectively.

The NetApp certification lifecycle mainly includes the **certification creation process** that is designed by the certification authority to identify the appropriate SQuaRE criteria for the effective certification, and **the certification execution process** that must ensure that the certification process is untampered, by providing the technical means in an automated, transparent and repeatable manner, typically performed by the accredited labs.

The state-of-art for the NetApp certification, the key stakeholders envisaged and the certification criteria considered are already documented in D2.2 [3] together with the initial architecture of the target Certification Environment. The following section provides a high-level overview of the overall approach for reasons of completeness, and delves into updates performed in the project's second reporting period, which are as follows:

- Revisit the certification criteria that should be in scope, especially considering the cyber-security requirements
- Conclude on the criteria that can be systemically evaluated, and analyse the existing capabilities and tools offered either in the open community or as widely accepted enterprise solutions. Confirm the missing support for NEF and CAPIF evaluation, that is designed to be incorporated as an EVOLVED-5G prototype.
- Design the execution process flow for the automated certification (see Section 6.3)

- Specify the integration design, including details for the shared resources and the APIs to be exposed (see 6.4)

6.2 Functional Blocks

The Certification Environment is assisting the execution of the Certification Phase. This phase is managed by the Certification Authority, through an accredited Certification lab, and is initiated by the organization interested in certifying (most likely the NetApp developers) already validated NetApps through a formal application process.

The Certification Environment has the responsibility to execute the certification audit list on the target NetApp binary, in a transparent, repeatable and automated manner and gather the results in the form of a certification report that will guide the final verdict, including recommended remedies if need be. Consequently, the functional blocks of the Certification Environment, illustrated in Figure 10, support the automation and execution functionalities, and at the same time comprise the necessary repositories and toolchains to evaluate the audit list. Building upon the background on certification objectives already set in the telecommunications and ICT domains, as well as the EU Directives regulating market and security aspects, the proposed certification criteria to be incorporated in the audit list are classified in the following pillars:

1. <u>Software Product Quality</u>

The certification objectives around software quality primarily relate to the NetApps conformance with 3GPPP standards (Functional Suitability) that allow tight integration and effortless interworking with the 5G Standalone (5G SA) mobile core networks. Table 7 lists the core criteria for software quality, the respective test cases for each criterion and the methodology to perform the relevant tests.

Table 7: Software quality/functional suitability criteria & validation

Criterion	Evaluation Test Case	Methodology
CAPIF Compliance	• NetApp API Invoker Mgmt. • NetApp Security Context setup • API Discover Service • NetApp Event Subscription • NetApp Event Notifications	Automated
5G Integration (NEF API Exposure)	• MonitoringEvent API (TS 29.522 - TS 29.122) • MoLcsNotify API (TS 29.522) • AsSessionWithQoS API (TS 29.522 - TS 29.122) • AnalyticsExposure API (TS 29.522) • 5GLANParameterProvision API (TS 29.522) • ServiceParameter API (TS 29.522) • LpiParameterProvision API • AKMA API (TS 29.522)	Automated
Documentation Quality	• Design & Specification Document • Installation & Configuration Manual • Operational Manual	Manual

2. <u>Security</u>

The certification objectives, in term of security, focus on detecting vulnerabilities in the source code of and the deployed artifacts of the NetApps. Vulnerabilities' detection prevents data bridges or fraud and ensures data privacy and isolation from the execution environment. In this respect, code auditing and application security analysis play a pivotal role, ensuring security and privacy of data exchange between NetApps and the NEF core function and preventing access to sensitive user data (e.g., user location, user identification). Security analysis of NetApps is realized both with static and dynamic application security testing (SAST and DAST) [6]. The former involves white-box testing of the underlying framework and of the design and implementation of the application, aiming at auditing the source code and identifying vulnerabilities, unique defects and errors without the need of executing the application itself. The latter, involves black-box security testing of the NetApp, detecting the vulnerabilities and their exposed attack surface during runtime. Taking into account these security considerations in the System Development Life Cycle, as described in [6], additional certification criteria are defined, as shown in Table 8.

Table 8: Security criteria and validation

Criterion	Evaluation Test Case	Methodology/Tools
Application Security	• Static Application (code) Security testing • Dynamic Application (binary) Security testing	White-box/black-box testing tools like Veracode [11]
Fraud Protection	• Test data streams to and from NetApp • Detailed Logging • Fraud detection • Continuous Monitoring • False Positive management	Metasploit [12] Nessus [13]
GDPR	• End User License Agreement, Accountability • Ensure data remains private • Inquire about data collection	Debricked [14] Pseudo-anonymisation
Connection	• Ensure Privacy of Connection	HTTPS, SSL, VPN protocols for communication

3. Marketplace

The Marketplace is the final stage of commercialization of the NetApps and constitutes the repository where certified NetApps shall be published. Following the paradigm of public cloud providers, these Marketplaces impose policies that need to be satisfied before final publishing, as shown in Table 9.

Table 9: Marketplace criteria and validation

Criterion	Evaluation Test Case	Means/Tools
Policy/Terms	• End-user Use Policy • Terms of Service	Manual, proposed Marketplace Privacy policy file
Open Source Scan Report	• Catalogue all third-party software components, associated licenses	Debricked [14]
Valid Binary	• Binary Container file validation • Endpoints validation	Trivy [15] Chef In Spec [16]

[11] https://www.veracode.com/platform
[12] https://www.metasploit.com/
[13] https://www.tenable.com/products/nessus/nessus-professional
[14] https://sourceforge.net/software/product/Debricked/
[15] https://aquasecurity.github.io/trivy/v0.32/
[16] https://www.chef.io/products/chef-inspec

The analysis of the certification criteria and the relevant methodologies and tools that need to be employed by the Certification Environment shapes the architecture of the Certification Environment.

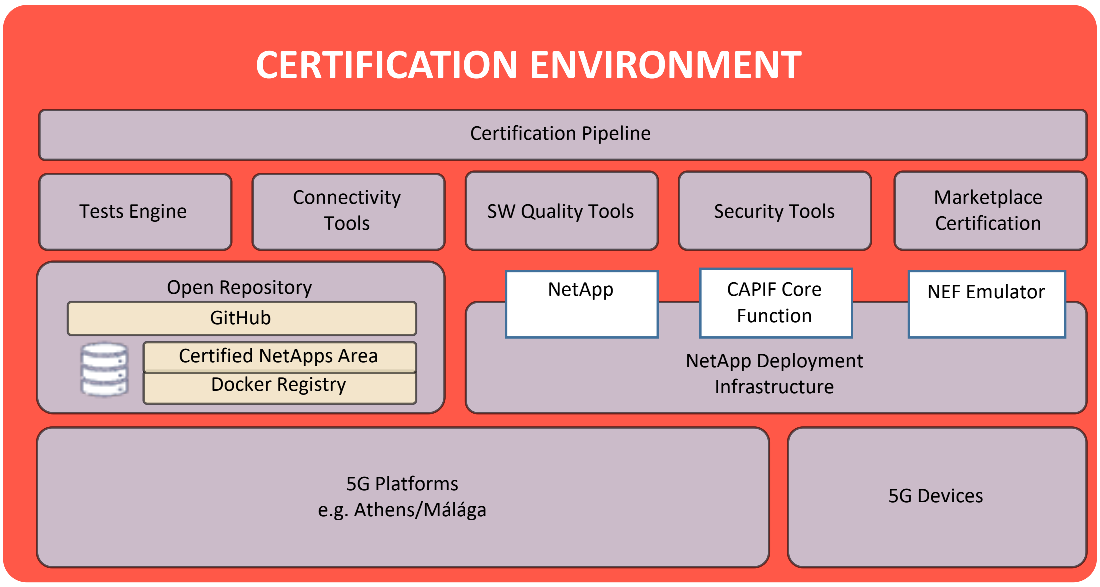

Figure 10: Certification Environment Architecture

As a result, the Certification Environment, depicted in Figure 10, includes the following elements:

- **Certification Pipeline:** It constitutes a sequence of automated tests (Table 7 - Table 9) and orchestrates the certification process resulting in a certification report. Relevant implementation details will be presented in the deliverables of WP5.
- **Open Repository**: This repository hosts the NetApp binaries and has been described in the deliverable D3.2 “NetApp Certification Tools and Marketplace development” (submitted in June 2022) [9]. It also contains the Docker registry that is used for deploying the NetApp containers during the certification phase.
- **Test Engine**: It executes the set of identified tests over the target NetApp and reports the results (please, refer to the deliverable D3.2 [9] for more details).
- **NetApp Deployment Infrastructure**: During the certification process, the NetApp is deployed and instantiated in virtualized infrastructure (please, refer to the deliverable D3.2 [9] for more details).
- **CAPIF and NEF**: These tools emulate the services offered by the 5G core and are provided by the EVOLVED-5G facility. They are deployed as independent containers during the certification phase of the NetApp lifecycle.
- **Connectivity tools**: Tools to test connectivity of the NetApps with the 5G network.
- **Software quality tools**: Tools to assess the quality of the NetApp software. These tools include among others static code analysis and secret leakage detection.
- **Security tools**: These tools perform security scans of NetApp images to detect vulnerabilities in the relevant containers (both for the operating system and the NetApp application).
- **Marketplace certification:** Tools to certify that the NetApp meets Marketplace criteria.
- **5G infrastructure:** 5G Network infrastructure that will support connectivity of the 5G devices to the NetApps.

- **5G devices**: Devices connected using 5G will be required so as to interact with the NetApp depending on the use case, the vAPP and the overall functionality of the NetApp.

All test reports are consolidated and reported as part of the certification phase of the NetApp lifecycle. If a NetApp successfully completes this phase, it gets uploaded to the certified area of the Open Repository.

It must be noted that EVOLVED-5G is targeting the implementation of a prototype of the specified Certification Environment based on the existing 5GENESIS infrastructure and capabilities. This environment cannot stand as a full-fledged Certification Environment, given that the necessary accreditations are not available in the 5GENESIS platforms. However, the certification's environment configuration and setup, together with the tools developed by the project for the certification tests, can be provided by the EVOLVED-5G project partners to the accredited labs that wish to instantiate a relevant environment.

The certification execution environment for EVOLVED-5G prototype is treated as an isolated environment from the EVOLVED-5G Validation Environment, that can be nevertheless share infrastructure and utilities, if need be, but under different configuration and provisioning setups. The main reason is that while the validation process is a rigorous process that follows each minor NetApp software update, the certification process shall need to be executed rarely incurring cost and upon very specific recommendations and mandates (for example periodically so that to be re-enforced, or upon major software releases as documented during the certification execution process). Potentially loose integration between the validation and Certification Environments and optimizations through the utilization of same automation tools (like a CI/CD framework) can be considered, as long as the lifecycle of each process is not intervening with the other.

6.3 Certification Process Flow

The certification process is automated through a CI/CD pipeline of tests. This pipeline comprises a sequence of steps, each one of which may involve several interactions of the CI/CD with different components. Figure 11 and Figure 12 depict an indicative certification process, consisting of a sequence of tests as those described in the previous section.

1. The entry point of the pipeline is the Github repository of the NetApp.
   - The security criteria (see Table 8), including source code analysis, where the NetApp must be first scanned for vulnerabilities (e.g., using SonarQube[17] and Trivy tools) are the first to be evaluated. Once the software is scanned, the NetApp container images can be uploaded to the target infrastructure (e.g., a Docker[18] Registry in AWS [19] for NetApp deployment).
2. The appropriate deployment and testing environment (e.g., running CAPIF and NEF tools) is set up. In the EVOLVED-5G practice the target environment is in Kubernetes infrastructure and is prepared using HELM[20] and the Robot Framework testing engine while connectivity is tested using the NMAP tool [21].

[17] https://www.sonarqube.org/
[18] https://www.docker.com/
[19] https://aws.amazon.com/
[20] https://helm.sh/
[21] https://nmap.org

- Once the NetApp is deployed properly, automated tests for **functional suitability** (see Table 7) including CAPIF and NEF integration, are executed. For this purpose, the images of NEF and CAPIF are also instantiated in the CI/CD platform.
- The next tests focus on **Marketplace compliance** (see Table 9) and certify that the NetApp is cloud native, e.g., by scaling out and shrinking the pods of the NetApp deployed in Kubernetes. Following this test, the availability of the required licenses (e.g., using Debricked tool) is assessed.

3. After completing the cloud native tests, the deployment environment can be cleaned, destroying the NetApp, CAPIF and NEF image instances in the virtualized platform.
4. The final step is the generation of a certification report of the NetApp in JSON and PDF. The certification report is fingerprinted with a unique identifier, which is mandatory for the publication of the NetApp to the Marketplace to verify that the certificate refers to the specific NetApp.

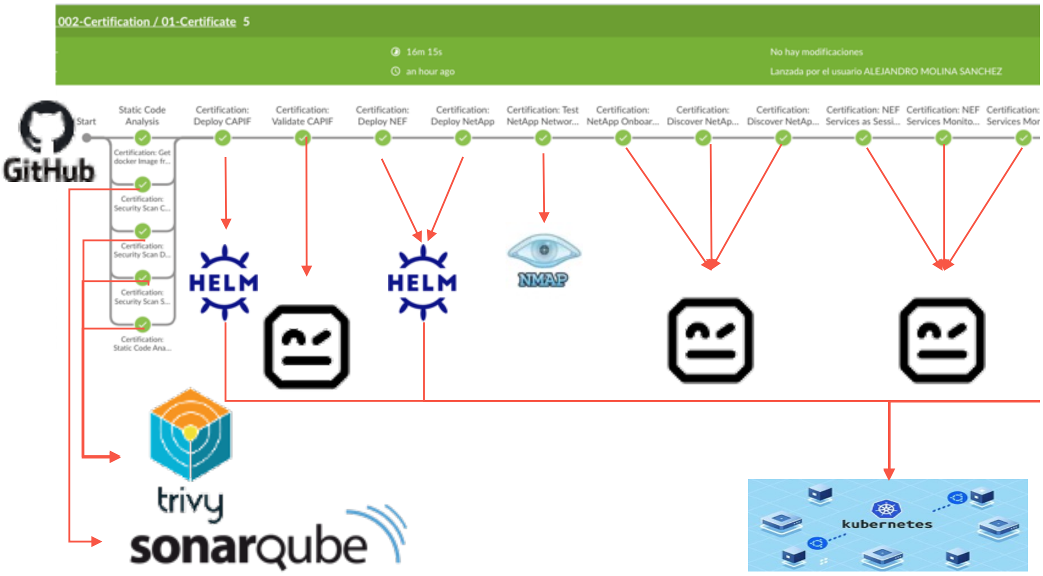
002-Certification / 01-Certificate 5
16m 15s
an hour ago
No hay modificaciones
Lanzada por el usuario ALEJANDRO MOLINA SANCHEZ
GitHub
Start
Static Code Analysis
Certification: Get docker Image fr...
Certification: Security Scan C...
Certification: Security Scan D...
Certification: Security Scan S...
Certification: Static Code Ana...
Certification: Deploy CAPIF
Certification: Validate CAPIF
Certification: Deploy NEF
Certification: Deploy NetApp
Certification: Test NetApp Networ...
Certification: NetApp Onboar...
Certification: Discover NetAp...
Certification: Discover NetAp...
Certification: NEF Services as Sessi...
Certification: NEF Services Monito...
Certification: Services Mor
HELM
HELM
NMAP
trivy
sonarqube
kubernetes

Figure 11: Certification process flow (part 1)

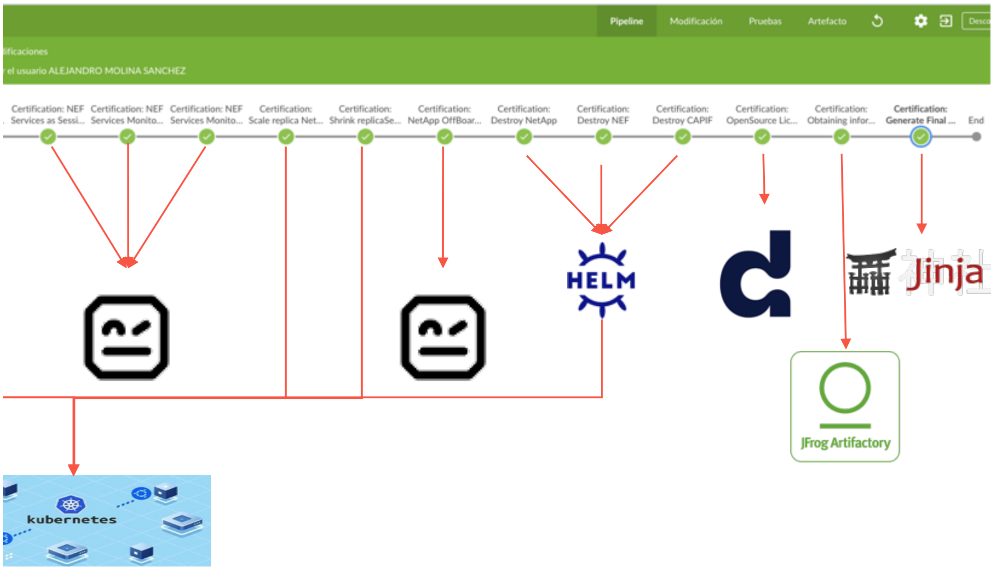
Pipeline
Modificación
Pruebas
Artefacto
Desco
lificaciones
r el usuario ALEJANDRO MOLINA SANCHEZ
Certification: NEF Services as Sessi...
Certification: NEF Services Monito...
Certification: NEF Services Monito...
Certification: Scale replica Net...
Certification: Shrink replicaSe...
Certification: NetApp OffBoar...
Certification: Destroy NetApp
Certification: Destroy NEF
Certification: Destroy CAPIF
Certification: OpenSource Lic...
Certification: Obtaining infor...
Certification: Generate Final ...
End
HELM
Jinja
JFrog Artifactory
kubernetes

Figure 12: Certification process flow (part 2)

6.4 INTEGRATION DESIGN

6.4.1 Shared resources

The Certification Environment of the EVOLVED-5G facility is treated as an isolated environment. However, in the scope of the project's prototype development, it can share infrastructure and utilities with the Validation Environment of the EVOLVED-5G ecosystem, but under different configuration and provisioning setups. In practice, the Certification Environment needs to share resources, hosted by the Open Repository, with the Validation Environment and with the Marketplace for the NetApp release.

From the Open Repository, the Certification Environment gets the NetApp images that are validated during the validation phase of the NetApp lifecycle. These images are stored in the validated area of the Open Repository.

For the publication of the NetApp in the Marketplace, the certification process concludes with uploading certified images of the NetApp to the certification area of the Open Repository, from where NetApps are released to the EVOLVED-5G Marketplace. The certification process also generates a fingerprint file with a unique GUID (globally unique identifier) to facilitate the onboarding of the NetApp in the Marketplace. This GUID is sent via email to the NetApp developer to proceed with onboarding the NetApp in the EVOLVED-5G Marketplace.

Finally, a certification report is produced as a result of a successful certification process, which is also shared with the NetApp owner via email, to be uploaded together with the NetApp in the Marketplace.

6.4.2 Exposed APIs

Due to the extensive use of tools in the EVOLVED-5G project, different APIs enable the Certification Environment to expose a rich set of functionalities, useful for the integration of the rest of the EVOLVED-5G facility components with the Certification Environment. There are a few tools that expose their APIs to the user directly, and other tools that are accessible via the pipelines defined in the CI/CD platform. Table 10 lists all APIs used for the integration of the components of the Certification Environment according to the implementation decisions of the consortium.

Table 10: Validation and certification endpoints

Endpoint	Method	Description
/api/executions	POST	Jenkins APIs to launch Certification Pipeline
/api/executions/<id>	GET	Jenkins APIs to check the status of the Certification Pipeline
/sonar-scanner/<netapp_path>	GET	SonarQube APIs
/v1/scan-image?<artifactory_path>	POST	Trivy APIs
/k8s/cluster/projects/<openshift>	GET	Openshift URL

/artifactory/docker/evolved-5g/validation/<netapp_name>	POST	Upload certification docker images to Artifactory
/artifactory/docker/evolved-5g/validation/<netapp_name>	GET	Download certification docker images from Artifactory
/ecr/repositories/private/<aws_id>/evolved5g?region=<aws_region>	GET/POST	Upload/Download in Amazon ECR
<kubernetes_cluster_ip>/	POST	Kubernetes APIs for Scaling Out and Shrinking Pods (HELM)

6.4.3 Security

The Certification Environment is designed to be managed by a certification authority independently from any other resource and environment used previously in the verification and the validation phases of the NetApp. Therefore, all components that are part of the certification process need to be deployed as part of the Certification Environment in a secure fashion. Table 11 lists the different components integrated in the Certification Environment and the security mechanisms they provide for a secure deployment.

Table 11: Certification components and security mechanisms

Component	Method	Security Technologies
Open Repository Code (Github)		Github supports authentication using username and password, Two-factor authentication and SAML single sign on as described in [32]
Open Repository Images (Artifactory)		Artifactory supports authentication using username and password. Artifactory instance is allocated in a private subnet of Telefonica.
Docker Registry (AWS ECR)		User authenticates using a username and password to retrieve an authentication token. After, this authentication token is used to access the Amazon ECR registry.

Static Code Analysis tools (SonarQube)		Sonarqube supports authentication using username and password.
Vulnerability Scan Tools (Trivy)		Trivy is running in one of the CICD slaves. TOKEN authentication has been enabled in order to secure the calls to the Trivy APIs. Trivy instance is running in a private subnet of Telefonica.
CAPIF Tool		CAPIF Tool implements the following reference points a s specified by TS 29.222: CAPIF-1/1e, CAPIF-2/2e, CAPIF-3, CAPIF-4 and CAPIF-5. All these interfaces DO support TLS with mutual authentication as specified in TS 33.122.
NEF Emulator		NEF Emulator supports authentication using username and password.
License Scan Tool (Debricked)		Debricked supports authentication using Username and Password.
CICD Pipeline orchestrator (Jenkins)		Jenkins supports authentication using Username and Password. Jenkins instance is allocated in a private subnet of Telefonica.

7 EVOLVED-5G Marketplace

7.1 Introduction

The EVOLVED-5G Marketplace[22] is the main interaction point between NetApp creators and NetApp consumers. It targets three different user profiles: (i) NetApp creators, i.e., developers publishing their NetApps to a public catalogue, (ii) NetApp consumers, i.e., people purchasing and using NetApps, and (iii) Marketplace administrators, i.e., a group of people that have elevated access to manage the platform and monitor a set of defined KPIs.

Compared to D2.1 [2] and D2.2 [3], certain adaptations have been made to the design of the Marketplace:

- The environment's functional blocks have been organized to be aligned with the user scenarios that have been implemented in the user interface. For instance, the certification of NetApps and the configuration of billing plans (presented at D2.2 [3]) are now part of NetApp onboarding.
- The certification process has been simplified, interacting only with the Open Repository environment.
- The TM Forum Open API has been introduced.
- The Evolved 5G Forum component has been introduced.

The updated architecture overview of the Marketplace can be seen in the following diagram and the related functional blocks are explained in the upcoming sections.

7.2 Functional Blocks

The EVOLVED-5G Marketplace is the main interface of the framework in production. It publishes the developed and certified NetApps, and allows for vApp developers to search, read information and download binaries and possibly source code of NetApps. Pricing plans are defined by NetApp developers and interested end users may purchase them allowing their transaction to be tracked by an external blockchain component. Finally, appropriate dashboards give an overview of Marketplace KPIs to platform administrators, of their revenue from their NetApp purchases to developers and of their downloaded NetApps to the end users.

[22] https://Marketplace.evolved-5g.eu

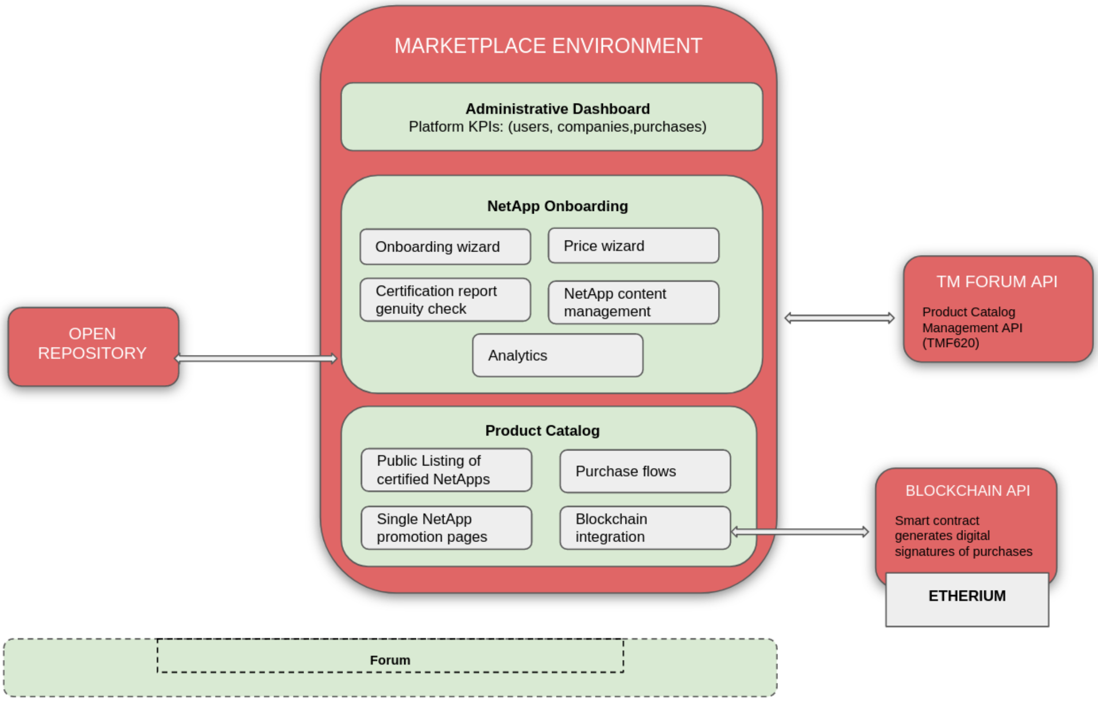
MARKETPLACE ENVIRONMENT
Administrative Dashboard
Platform KPIs: (users, companies,purchases)
NetApp Onboarding
Onboarding wizard
Price wizard
Certification report genuity check
NetApp content management
Analytics
Product Catalog
Public Listing of certified NetApps
Purchase flows
Single NetApp promotion pages
Blockchain integration
OPEN REPOSITORY
TM FORUM API
Product Catalog Management API (TMF620)
BLOCKCHAIN API
Smart contract generates digital signatures of purchases
ETHERIUM
Forum

Figure 13 Marketplace architecture

Figure 13 illustrates the architecture of the Marketplace, revealing the different functional blocks that serve all kinds of functionalities.

7.2.1 Administrative Dashboard

The **Administrative Dashboard** contains a user interface where platform administrators (user accounts with elevated access) have the ability to view high level platform indicators. The number of users that have registered to the platform, the number of companies, the number of NetApps that have been uploaded and the number of purchases that have been completed.

7.2.2 Onboarding wizard

NetApp onboarding allows a NetApp creator to publish their NetApp to the Marketplace. It consists of the following functional blocks:

- **Onboarding wizard:** It defines a series of steps where the user has to upload NetApp metadata (version, basic information, logos, categories etc.)
- **Price wizard:** It allows the user to define a price configuration that showcases how a NetApp can charge the end-user depending on the usage.
- **NetApp content management:** It allows the user to describe the usage of the NetApp (for example by uploading a technical tutorial).
- **Certification report genuineness check:** It interacts with the Open Repository in order to validate that the NetApp is certified and ready to be consumed.
- **Analytics:** It allows the NetApp creator to view a high-level report of how many NetApps have been purchased.

During the NetApp onboarding, the **Onboarding Wizard** interacts with the TM Forum API environment which is described next.

7.2.3 TM Forum API

The **TM Forum API,** and more specifically the TMF620 (Product Catalog Management[23]), provides a repository that is exposed via an Open API in order to store NetApps information. The EVOLVED-5G Marketplace utilizes this API (i) to store NetApps information as part of the onboarding process, (ii) to store the list of product catalog categories that are available for selection while onboarding a NetApp.

TM Forum has already defined a Telco Data Space architectural blueprint implemented in the open API server we choose to use. This is also built upon GAIAX[24] and IDSA[25] standards.

GAIA-X is a European beacon project that will both connect existing cloud services and spark innovative new modes of connectivity to create a federated digital infrastructure for Europe. A critical success factor is to ensure data sovereignty and interoperability — a shared goal of GAIA-X and IDSA, which is why IDSA concepts are an integral element of the GAIA-X architecture.

The IDSA — a cross-industry, transnational coalition of more than 120 leading companies and research organizations — has been working together on the concept and design principles for data spaces since 2016. As a leader in this field, IDSA is contributing its knowledge to GAIA-X. IDSA has been very active in GAIA-X from day one and is a founding member of the GAIA-X AISBL, the initiative’s not-for-profit association.

7.2.4 Product Catalog

The Product Catalog allows a visitor of the Marketplace to search for NetApps, understand their value propositions and purchase them, in order to use them. It consists of the following functional blocks:

- **Public listing of certified NetApps:** It consists of a public web page, where users can search for NetApps.
- **Single NetApp promotion pages:** It allows a user to view specific information about a NetApp and understand what kind of problem it solves and how it can be used.
- **Purchase flows:** It allows a user to purchase a NetApp and get access to the related containerized image along with details on how to use it.
- **Blockchain integration:** It allows the Marketplace to send digital signatures to the Ethereum network. During the purchase of a NetApp a digital signature (hash string) of the transaction combining information of the NetApp and its buyer is generated. This signature becomes publicly available to Ethereum Network via the Blockchain API, as described next.

7.2.5 Blockchain API

The Blockchain API retrieves a digital signature from the Marketplace and initiates a blockchain transaction. The transaction is posted on the Ethereum blockchain network and is publicly visible, containing the digital signature.

[23] TMF620 Product Catalog Management API User Guide v4.1.0 | TM Forum
[24] https://internationaldataspaces.org/we/gaia-x/
[25] https://internationaldataspaces.org/

7.2.6 Forum

The Marketplace Forum acts as a reference point for any help needed for the NetApps. Marketplace users have the opportunity to create topics for discussion with the community and participate in Q&A sections also provided.

7.3 MARKETPLACE PROCESS FLOWS

7.3.1 Publishing a NetApp

The onboarding process consists of a series of steps that result with the NetApp being published to the Marketplace, as shown in Figure 14.

When a NetApp creator starts the onboarding process, the Marketplace environment requires some NetApp metadata (e.g., title, description, logo, version, technical tutorial, etc.), as well as the pricing scheme of the NetApp. This process is facilitated by the Onboarding Wizard, the Price Wizard and the NetApp content management functional block. During the onboarding, the Marketplace performs a request to the Open Repository, in order to retrieve information about the specified NetApp. The NetApp fingerprint, i.e., a unique code associated with the NetApp is retrieved from the Open Repository. Assuming that the validation of the fingerprint is successful, the Marketplace proceeds with storing NetApp metadata to the TM Forum API and returning a response back to the client, informing the user creator that the onboarding process is complete, and that the NetApp is now published and publicly available to the Marketplace's Product Catalog.

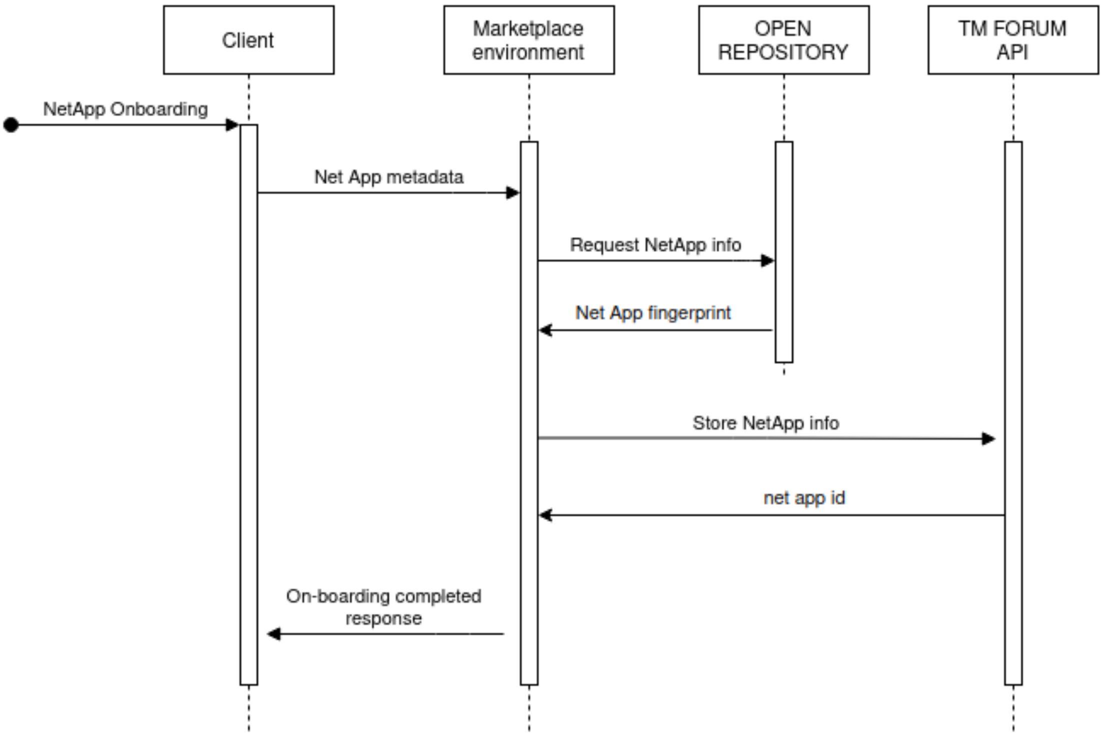

Figure 14 NetApp on-boarding process

7.3.2 Purchasing a NetApp

When a NetApp consumer visits the product catalogue, the collection of NetApps available in the marketplace is displayed. Search and filtering functionalities are offered. Upon selection of a NetApp an informative web page is presented to the user with the NetApp metadata and the relevant links for purchasing and downloading the NetApp. If a request for purchasing a NetApp is sent to the Marketplace environment, the digital signature of the transaction is created and submitted to the Blockchain API via a service that initiates a blockchain transaction and stores this digital signature to the ETH Network. If the transaction is successful, a response is returned back to the NetApp buyer, who now has access to all the information needed to download and use the NetApp.

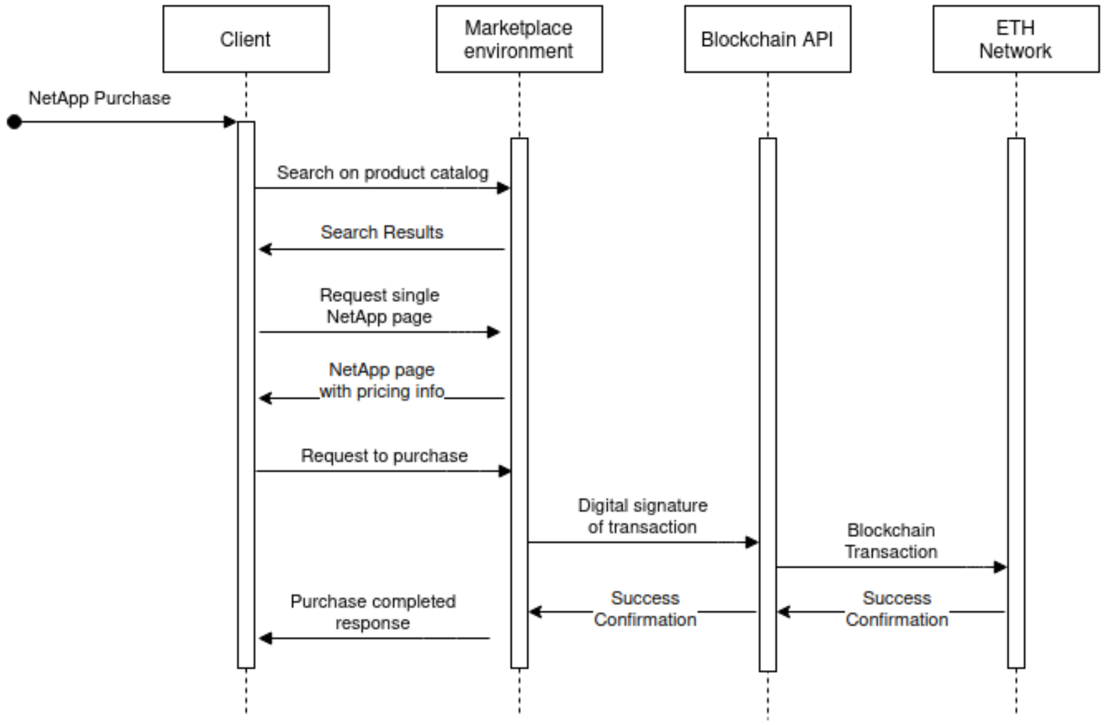

Figure 15 Purchasing a NetApp process

7.4 INTEGRATION DESIGN

In this chapter the integration design of the Marketplace is described. The analysis focuses on each one of the Marketplace components explaining the information and resources exchanged, the APIs used and the secure communication channels employed, when necessary.

7.4.1 Marketplace - Open Repository

During the onboarding process, the Marketplace interacts with the Open Repository in order to validate that the NetApp is certified and ready to be published. To that end, the Open Repository exposes an HTTP endpoint that expects a certification fingerprint, which is associated with the specific NetApp. The NetApp creator may find the code in the respective certification report of the NetApp. This code needs to be provided to the Marketplace via the user interface and sent back to the Open Repository. The communication between the two environments is established through a secure transport layer (SSL). If the certification fingerprint provided by the user matches the one found in the Open Repository, the NetApp creator can successfully publish the NetApp. If it is not, the NetApp owner is prevented from proceeding further and gets appropriately notified.

7.4.2 Marketplace - TM FORUM

The TM620 Product Catalog Management is a containerized component that exposes a set of Open API endpoints accessible via HTTP. The Marketplace uses a subset of the TM620 Forum APIs related with storing generic categories, which are used as filters in the Product Catalog's user interface[26]. These categories group NetApps based on their respective metadata like name, description and price. The communication between the Marketplace and the TM620 API is established via HTTP and only inside a private network they share, to ensure security constraints.

7.4.3 Marketplace - Blockchain API

During the purchasing process, the Marketplace interacts with a Blockchain API in order to store the digital signature of the payment in the ETH network. The Blockchain API is based on Infura.io[27] blockchain development platform that offers a REST API for executing blockchain transactions. The Marketplace generates a hashed unique identifier of the NetApp, for the specific transaction executed by the specific buyer, and publishes this hash to a smart contract in a Infura.io service that initiates a blockchain transaction. This transaction is publicly available and contains the digital signature. Communication between the Marketplace and the Blockchain API is established over secure transport layer (SSL) and is supported by public key authentication.

[26] https://Marketplace.evolved-5g.eu/product-catalogue
[27] https://infura.io/product/ethereum

8 5G NPN INFRASTRUCTURE

8.1 INTRODUCTION

EVOLVED-5G facility includes the 5G NPN environment that is composed by two platforms, namely the Malaga and Athens platforms, which provide a dynamic and controllable infrastructure for experimentation. Different components of the ecosystem can be deployed in these platforms, such as NetApps, vApps and the exposure services of the 5G core (5GC), using the CI/CD framework of the EVOLVED-5G facility. The 5G NPN environment offers, as a service, a complete 5G system that can be used to offer 5G connectivity. Despite the fact that both platforms comply with the same architectural paradigm, depicted in Figure 16, they offer different 5G capabilities that can be utilized by a diverse range of use cases. For example, the Malaga platform provides capabilities for TSN (Time-Sensitive Networking). On the other hand, the Athens platform supports multi-domain deployments with a common 5G core, spanning over two distinct sites, namely NCDR "Demokritos" and COSMOTE. More details about the 5G NPN platforms can be found in D2.2 [3]. On top of that, platforms contain all the hardware and software components that are essential to execute the various functional and performance tests in the scope of the validation phase of the NetApp lifecycle. Therefore, the 5G NPN environment lays the foundation for the validation and certification of the NetApps. All the components of the 5G NPN environment are presented in Figure 16.

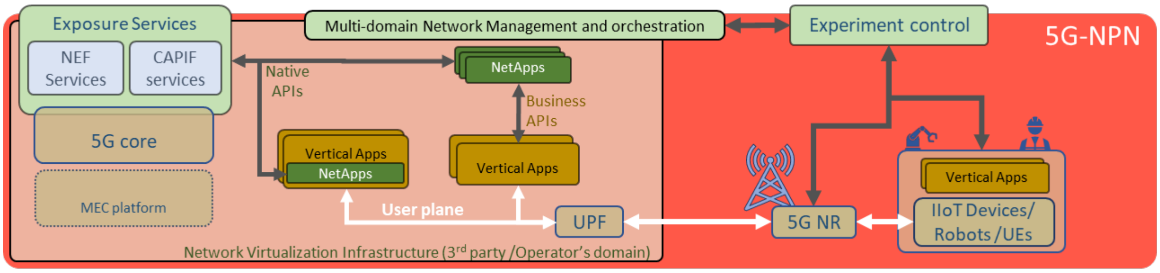

Figure 16 5G NPN architecture

The 5G NPN infrastructure has preserved the design initially defined in the deliverable D2.2 [3]. No significant architectural changes have been applied since then.

8.2 FUNCTIONAL BLOCKS

In the 5G NPN infrastructure several components serve different functional purposes and are integrated to expose the necessary services to the EVOLVED-5G facility.

The **Multi-domain Network Management and Orchestration** module supports the management of virtualized resources. As part of the Open5Genesis Suite, the Slice Manager is the tool responsible for orchestration and deployment of the resources. This functional block is logically connected with the Validation Environment through the Dispatcher, which is the entry point of the system. The Dispatcher offers functionalities to experimenters for the onboarding of virtual machines, that can be instantiated in the virtualization infrastructure.

The **Experiment Control** module represents the different interfaces used by the components of the 5G NPN, that are involved in the experimentation phase, such as NetApps, vApps and the

NEF Emulator. Mainly, it is an abstraction of the ELCM's logical interfaces. More details for the ELCM and the overall validation process are presented in Chapter 5.

The **5G Core** (5GC) network, handles a wide variety of essential functions in the mobile network, such as connectivity and mobility management, authentication and authorization, subscriber data management and policy management, among others. 5G New Radio (NR) together with the user equipment (UE), e.g., IoT devices, robots, mobile phones etc., comprise the Radio Access Network (RAN) of the 5G NPN. 5GC architecture inherits a cloud-native design approach, based on what is called a Service-Based Architecture (SBA), where each network function offers its services through APIs.

The 5GC network exposes the required services in a trusted and standardized way through the Common API Framework (CAPIF). Due to the unavailability of such **Exposure Services** in the platform's current 5GC solutions, the exposure of NEF services through CAPIF by the 5G NPN infrastructure is realized by the NEF Emulator (please, refer to D3.1 [4]). CAPIF and NEF services are thoroughly described and analysed in the deliverables D3.2 [9] and D4.1 "5G Exposure Capabilities for Vertical Applications (Intermediate)" (submitted in February 2022) [10], respectively.

Multi-access Edge Computing (MEC) technology offers additional computational resources, when required. It is located near the end user, in order to support critical use cases (e.g., delay sensitive applications). MEC functionality is optional in the EVOLVED-5G ecosystem (reason why it is presented in dotted line in Figure 16), although MEC capabilities can be interconnected effortlessly with the 5G NPN. NetApps and vApps although depicted in the figure for a complete presentation, they are not bound to the 5G NPN infrastructure. They are only deployed in the 5G NPN infrastructure during the validation and certification phases. On top of that, NetApps interact with the 5GC network to consume the 5GC capabilities through the relevant northbound APIs (i.e., CAPIF Core Function and NEF Emulator).

8.3 INTEGRATION DESIGN

8.3.1 Exposed APIs

8.3.1.1 NEF Services

As already mentioned above, the exposure of the NEF services by the 5G NPN infrastructure has been realized by the NEF emulator tool. The NEF emulator is a software component, which at this stage of the project, implements two commonly identified APIs, as both defined in TS29.522 [11] in order to support all the use cases, namely the AsSessionWithQoS and the MonitoringEvent API. The implementation details of the NEF emulator can be found in D3.1 [4].

The main NEF services provided by the emulator are implemented as RESTful APIs, and are described below:

- **Monitoring Event API**: This API allows a NetApp to access several events that may occur in the 5GC. The MonitoringEvent API supports location reporting events. Specifically, when a UE handover takes place to a neighbour cell, NEF informs the NetApp for this event, letting the NetApp know the new cell ID of the cell where the UE moved to. As part of the location reporting events, the aforementioned API supports the LOSS_OF_CONNECTIVITY, where the network detects that the UE is no longer reachable for either signalling or user plane communication, and UE_REACHABILITY that indicates when the UE becomes reachable (for sending downlink data to the UE), respectively.

- **AsSessionWithQoS API**: The AsSessionWithQoS API allows a NetApp to choose a predefined QoS profile from a list retrieved from the 5GC. Moreover, a NetApp can indicate the desired level of QoS (e.g., jitter, latency, and priority) for a given IP traffic flow. If the UE requests a guaranteed bit rate (GBR) flow and enters a cell with no available resources (for instance, other UEs are connected to the same cell), the NEF emulator notifies the NetApp that the QoS cannot be guaranteed. An additional functionality on top of the AsSessionWithQoS API is the provision of periodic reports for which the NetApp indicates the reporting period in seconds.

8.3.1.2 CAPIF Services

CAPIF services are provided by the CAPIF tool in the EVOLVED-5G framework, a software component that implements the 3GPP CAPIF APIs [12] and is thoroughly described in D3.2 [9]. The CAPIF tool provides APIs, that enable various functionalities for both CAPIF API invokers and CAPIF API provider entities:

For the API Invokers (i.e., NetApps) the following services, as defined in TS29.222 [13], are offered as RESTful APIs by the CAPIF tool:

- **CAPIF_API_Invoker_Management**: it allows the NetApps to register as API invokers to the CCF.
- **CAPIF_Security_API**: it enables the NetApps to define the security preferences when interacting with CAPIF API endpoints.
- **CAPIF_Discover_Service_API**: it lets NetApps discover what APIs are exposed by the NEF Emulator.
- **CAPIF_Events_API**: it allows the NetApps to receive notifications from CCFs.

For the API provider (i.e., the NEF emulator) the following services, as defined in TS29.222 [13], are offered as RESTful APIs by the CAPIF tool:

- **CAPIF_API_Provider_Management_API**: it enables NEF, which represents an API provider’s domain entity to register in the CCF.
- **CAPIF_Publish_Service_API**: it is used by exposers, that adopt the functionalities of the APF/AEF from the API provider’s domain, to expose the available APIs into the CCF.

8.3.2 Security

Since the exposure of the APIs refers to a 3rd party’s application domain, NEF needs to securely expose the services to NetApps. Therefore, the communication between NEF and NetApps relies on the following security aspects; authentication, authorization and interface protection as defined in the 3GPP TS 33501 [14]. For authentication, mutual authentication based on client and server certificates is performed. After the successful authorization of a NetApp, an OAuth token is generated, which authorizes the NetApp to consume the exposed APIs. Every communication step between NEF and NetApps should be performed applying the TLS protocol that fulfils integrity, replay and confidentiality protection. On the other hand, whenever NEF exposes the APIs through CAPIF, then the CAPIF Core Function is in charge of the authentication method that is applied between NEF and NetApps. According to 3GPP TS 33501 [14], the supported methods are TLS-PSK, TLS-PKI and TLS with OAuth. However, on the onboarding procedures for both NEF and NetApps into CCF, TLS sessions based on certificate based mutual authentication should be supported.

9 SUMMARY AND CONCLUSIONS

The EVOLVED-5G facility presents a quite complex architecture that is composed by several components, which collectively cater for a rich development framework for NetApps. Three levels of abstraction analyse the architecture in environments, functional blocks and individual components. Despite the multitude and complexity of components, the latest architectural decisions achieve a certain level of simplification of integration, which enables an easy replication of the EVOLVED-5G paradigm without necessarily adopting the exact implementation decisions of the consortium of the project.

Putting at the centre of the architecture the CI/CD Services component, the Open Repository and in some cases the 5G NPN, as expected, a snowflake schema is created, in practice. This arrangement routes the communication among the different environments, but also at a second level the communication among functional blocks, through these central components. As a result, these entities are the ones which mainly bear the burden of exposing APIs, exchanging resources and be responsible for executing these tasks in a secure manner.

Source code, containerized images, a variety of control and monitoring messages and various reports (experimental results, certificates etc.) are the resources that are exchanged among the building blocks of the architecture. The exchange is facilitated by a rich set of APIs that are exposed by the orchestrator of the CI/CD Services component and the Open Repository. These APIs get appropriately exploited by all EVOLVED-5G environments in the whole NetApp lifecycle. At the same time, the APIs exposed by the 5G NPN and, in particular, by the NEF and CAPIF emulators, which are developed and integrated in the Workspace environment by the consortium, ensure the provision of 5G network connectivity at all stages of the NetApp development.

NetApps are being tested in three stages of their lifecycle, namely verification, validation and certification. This in-depth testing process facilitates the ease of development, even from the beginning. The compliance of the NetApps with the design decisions and policies that have been defined through the analysis of the system requirements of the framework is ensured by the final stage of testing, that is, the certification process. Most of the requirements have already been addressed, as revealed by the compliance monitoring methodology followed during the development phase of the project. Mandatory requirements not addressed, yet, will be met by the final release of the platform and will be covered in the deliverables of WP3, WP4 and WP5 that will follow.

Finally, the open design of the Marketplace of the framework enables the interaction with the community interested in 5G technology, even outside the consortium. NetApps can be onboarded, checked for proper certification and licenses used, and finally be purchased and tracked through blockchain technology. The analytics dashboards enable the monitoring of the process for the different roles of the end users. The community tools (forum, wiki, accelerator library) incorporated in the environment offer useful information and facilitate the communication among the members of the community.

In summary, in this document, it is demonstrated that the EVOLVED-5G architecture fosters the development of NetApps in an easy, productive way by providing the necessary toolset to serve a range of users that span from individual developers to certification organizations. The architecture is modular and may very well rely on open source software, in conjunction with the software developed in the project, to provide a multitude of functionalities. Refinements of the architecture that may arise as a result of the work of the rest of the duration of the project, will be reflected in the deliverables to come until the finalization of the work of the consortium.

10 References

[1] International Organization for Standardization, “ISO/IEC 25000:2014 "Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE",” 2020. [Online]. Available: https://www.iso.org/standard/64764.html.

[2] EVOLVED-5G, “D2.1: Overall Framework Design and Industry 4.0 Requirements,” September 2021. [Online]. Available: https://evolved-5g.eu/wp-content/uploads/2021/11/EVOLVED-5G-D2.1_v1.4.pdf.

[3] EVOLVED-5G, “D2.2: Design of the NetApps development and evaluation environments,” October 2021. [Online]. Available: https://evolved-5g.eu/wp-content/uploads/2021/11/EVOLVED-5G-D2.2-v1.0_final.pdf.

[4] EVOLVED-5G, “D3.1: Implementations and integrations towards EVOLVED-5G framework realisation (intermediate),” December 2021. [Online]. Available: https://evolved-5g.eu/wp-content/uploads/2022/01/EVOLVED-5G-D3.1-v1.0.pdf.

[5] ECMA International , “The JSON data interchange syntax,” December 2017. [Online]. Available: https://www.ecma-international.org/wp-content/uploads/ECMA-404_2nd_edition_december_2017.pdf.

[6] M. M. J. C. O. Ronald S. Ross, “Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [including updates as of 1-03-2018],” *Special Publication (NIST SP),* 3 January 2018.

[7] International Organization for Standardization, “ISO/IEC 17011 Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies,” [Online]. Available: https://www.iso.org/standard/67198.html.

[8] International Organization for Standardization, “ISO/IEC 17025 Testing and Calibration Labatories,” [Online]. Available: https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html.

[9] EVOLVED-5G, “D3.2: NetApp Certification Tools and Marketplace,” June 2022. [Online]. Available: https://evolved-5g.eu/wp-content/uploads/2022/09/EVOLVED-5G-D3.2_FINAL.pdf.

[10] EVOLVED-5G, “D4.1: 5G Exposure Capabilities for Vertical Applications (Intermediate),” February 2022. [Online]. Available: https://evolved-5g.eu/wp-content/uploads/2022/03/EVOLVED-5G-D4.1_v2.0-final.pdf.

[11] 3. T. 29.522, “Network Exposure Function Northbound APIs, Release 17,” September 2021. [Online].

[12] 3. T. 23.222, “Common API Framework for 3GPP Northbound APIs, Release 17, V17.4.0,” April 2021. [Online].

[13] 3. T. 29.222, “Common API Framework for 3GPP Northbound APIs, Release 17, V17.6.0,” September 2022. [Online].

[14] 3. T. 33.501, “Security architecture and procedures for 5G system, Release 17, v17.2.1,” June 2021. [Online].