The NetApps Certification Environment for 5G and beyond Vertical Ecosystems: The EVOLVED-5G Approach

Foteini Setaki, Ioanna Mesogiti, Eleni Theodoropoulou, George Lyberopoulos
COSMOTE S.A, Athens, Greece
(fsetaki, imesogiti, etheodorop, glimperop)@cosmote.gr

David Artunedo Guillen, Javier Garcia Rodrigo
Telefonica, Madrid, Spain
(david.artunedoguillen, javier.garciarodrigo)@telefonica.com

Yiannis Karadimas
Maggioli SPA, Athens, Greece
john.karadimas@maggioli.gr

Harilaos Koumaras
NCSRD Demokritos, Athens, Greece
koumaras@iit.demokritos.gr

George Avdikos, Ioannis Margaritis, Emmanouil Kafetzakis
8BELLS, Nicosia, Cyprus
(george.avdikos, ioannis.margaritis, mkafetz)@8bellsresearch.com

Dimitrios Tsolkas
FOGUS Innovations & Services, Athens, Greece
dtsolkas@fogus.gr

***Abstract*— Certification is the means to promote excellence through adherence to best practices, and ensure the appropriate security and transparency, in alignment to regulations set by the market and (various levels of) administrations. In the mobile telecommunications domain, certification for the radio equipment and user terminals has been a fundamental practice. With the 3GPP 5G specifications, a novel core network (5GC) model comes to promote dynamic, open 5G services and enable network programmability through standard APIs unlocking the network intelligence to the vertical application needs. A consequence of this "openness" is the mandate for supplements in the established practices of the mobile network operators (MNOs) to include beyond device also software conformance and quality assessment certification. This study describes the work carried out by EU Horizon 2020 EVOLVED-5G project, to define the relevant certification framework for the NetApps, a novel concept introduced as an enabler for the 5G adoption from the vertical industries. The paper goes beyond the definition of the key constructs for the appropriate certification creation process, and explores the technical characteristics of the execution environment to support the certification auditing in an effective, automated and repeatable manner.**

Keywords—5G, NetApps, Certification, Stakeholders, Verticals

I. INTRODUCTION

The NetApp concept has emerged as an enabling service layer for vertical stakeholders in the 5G ecosystem. The EU-funded Horizon 2020 project EVOLVED-5G has introduced NetApp to be a separate middleware interacting with 5GC NEF (5G Core Network Exposure Function) with the purpose of masking the complexity of the network APIs and simplifying the implementation and deployment of vertical applications by providing the necessary adaptations. In this definition, the NetApp is a software typically implemented by business-native Third Parties to bridge the application logic with the network operation. In current practice, the components of the 5G technology that relate to equipment (either end-user devices or network products) have a firm background on interoperability and compliance, through mature certification standards and regulations. With the advent of NetApps, and the virtualization/softwarisation openness of the 5G network, there is an evident gap; the established certification practice in the mobile network business needs to extend beyond the current practice and include supplementary software specification conformance and quality assessments for the NetApps. The purpose of the EVOLVED-5G certification study is to bridge this gap by building upon the existing status quo in the telecommunications and ICT domains and increment the certification process with the capabilities seen necessary for the incorporation and interoperability of the NetApps in a 5G Standalone (SA) network. The study extends beyond the recommended methodology towards the technical characteristics of the execution environment and tools-chain in order to support the certification auditing in an effective, automated and repeatable manner.

This paper provides an overarching view of the relevant work starting by clarifying the NetApp advent and briefing on the state-of-the-art in mobile telecommunications certification. Subsequently, it introduces the proposed NetApps certification process, including the key stakeholders involved and explaining the relevant certification lifecycle before delving into the certification criteria and associated technical assessment. Finally, it presents the target architecture for the

certification execution environment and discusses the set of tools that can implement the audit systemically.

II. NetApps and State-of-the-Art Certification Frameworks

A. NetApps in the 5G Ecosystem

The 3GPP 5G specifications introduce a novel core network (5GC) model that promotes dynamic, open 5G services through virtualized core network functions, targeting improvements in terms of flexibility, performance, and time to market. Network programmability through standard APIs, so that higher-level service orchestrators can handle configurations for a variety of services and slices, becomes a key enabler for a dynamic environment with innovative technology and marketing potentials. The Network Exposure Function (NEF) provides a set of northbound APIs for exposing network data and receiving management commands. External third parties with permission, such as industries, platform developers, and designers, may use these standard APIs for building network-aware (5G-enabled) applications that establish a bi-directional communication with the 5GC, retrieving network statistics, but also triggering specific policies and commands to the network. Moreover, 3GPP has also established the foundations for the appropriate interconnection of 5GC network capabilities with the vertical applications. The key concepts that have emerged are the Common API Framework (CAPIF) [1] and the Service Enabler Architecture Layer (SEAL) [2].

In this ecosystem, the NetApp concept [3] has emerged as an enabling service layer for verticals. EVOLVED-5G has introduced NetApp to be a separate middleware interacting with 5GC NEF and, in alignment with the 3GPP SA6 Vertical Application Enablers (VAE) [4] simplify the implementation and deployment of vertical applications by providing the necessary adaptations. The NetApps are primarily expected to be implemented by business native Third Parties, to be either instantiated in a non-standalone mode, exposing simple friendly APIs to be consumed by the relevant vertical applications (vApps), or in a standalone mode, in the form of Software Development Kit (SDK) linked with the vertical application executable. In both cases, the NetApp stands as a third-party layer to be incorporated within the network domain, bringing closer the application logic to the network operation.

B. Certification in the Mobile Telecommunications Domain

Certification is the means to promote excellence through adherence to the identified best practices per case, as well as, to ensure the appropriate security and transparency in alignment to regulations set by the market and governmental administrations. A broad set of certification schemes exist for products, systems, solutions, services and organizations. For the equipment industry, apart from the vendors' internal conformance testing practices, specific regulations apply per target market. In Europe, with DECISION No 768/2008/EC of the European Parliament [5] and the aspiration for the 'EU single market for goods', the European Commission's main goal is to ensure the free movement of goods within the market, and to set high safety standards for consumers and the protection of the environment. To achieve this, the Blue Guide [6] sets the framework focusing on non-food and non-agricultural products, referred to as industrial products or products whether for use by consumers or professionals, and serves as a guide for the Member States on harmonizing obligations of product manufacturers, distributors, importers and authorized representatives. Especially in Sections 4, 5 of the Blue Guide, the product requirements and conformity assessment are set, with special care on the CE Conformitè Europëenne sign, mandatory for the products in the EU market.

In the mobile telecommunications domain, certification for the radio equipment and user terminals has been a fundamental practice driven not only by the practical interoperability and compliance mandates of the operators, but also by strict regulation obligations with main concern on the public health and environmental protection. The European RE Directive 2014/53/EU (RED) [7] establishes a regulatory framework for placing radio equipment (including airborne, marine and other radio applications) on the market by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum, including technical features for the protection of privacy, personal data and against fraud. Furthermore, additional aspects cover interoperability, access to emergency services, and compliance regarding the combination of radio equipment and software. The conformity assessment procedures are defined in RED Annexes III and IV of the and typically involve an accredited third-party test laboratory and third-party certification body, such as Telefication [8]. Furthermore, PTCRB [9] is a certification program established in 1997 by leading wireless operators to define test specifications and processes to ensure device interoperability on global wireless networks. Especially for the mobile User Equipment (UE), the appropriate conformance testing is specified by 3GPP WG RAN5 [10] and the certification process is performed by the Global Certification Forum (GCF) [11].

In the Information Communication Technologies (ICT) domain, conformity with international standards such as ITU Recommendations is one of the core principles underlying the global interoperability of ICT networks, devices and services. ITU has taken action to achieve the interoperability of ICTs globally (according to international ISO/IEC standards) through the Conformity and Interoperability (C&I) Programme [12] that organizes in four pillars the basic concepts, practices and relevant standards and incorporates the ITU Product Conformity Database.

III. The EVOLVED-5G NetApps Certification Process

It becomes evident, that the components of the 5G technology that relate to equipment (either end-user or network products) have a firm background on the proper compliance with mature standards and regulations as referenced above. Nonetheless, as the technology evolution moves network functions to the software layer, and through virtualization allows open and dynamic composition of network services extending capabilities to the business through the NetApps concept, the established certification practice in the mobile network business needs to extend beyond the current practice and include supplementary software specification conformance

and quality assessments. NetApps, as primarily third-party software interworking with the network, shall need certification in accordance to the equipment paradigm.

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 concept in the network operators' domain. To this end, EVOLVED-5G has explored the best practices for the certification process in order to devise the recommended approach. As NetApps certification is corresponding to software product quality, SQuaRE (System and Software Quality Requirements and Evaluation) that is part of the ISO/IEC 25000 series [14] with the goal of creating a framework for the evaluation of software product quality, is considered as the suitable methodology to follow. As a result, the project has applied the SQuaRE methodology to design the proposed certification process as documented below.

A. Key Stakeholders

SQuaRE involves a stakeholder ecosystem equivalent to the current equipment-oriented certification framework, facilitating the adaptation of SQuaRE in telecoms. As a result, the following actor types are identified for the NetApps SQuaRE certification:

- **Organization interested in the evaluation**, intending improvement and certification of its software product. It can be the NetApp's developer or a company interested in acquiring the NetApp.
- **Certification/Audit/Accreditation Body**, awarding certificates for software product quality. The Accreditation Body has an established internal regulation for software product certification, so that by reviewing an evaluation report issued by an accredited laboratory and auditing the company that develops the product at their premises, to be in the position to issue a certificate specifying the quality level of the product. Accreditation bodies operate in accordance with ISO/IEC 17011 [16] that specifies the general requirements for the assessment and accreditation of conformity assessment bodies and for the peer assessment of accreditation bodies for mutual recognition arrangements.
- **Accredited software product quality evaluation laboratory**, an external entity capable of providing an independent evaluation: The independent laboratory provides the Certification Body with the evaluation reports made, as an input to the certification process. The technical competence of the laboratory must be confirmed through relevant accreditation (according to ISO/IEC 17025) so that to guarantee the reliability of the evaluation results. ISO/IEC 17025 [15] is useful for any organization that performs testing, sampling or calibration including all types of laboratories, either owned and operated by government, industry or, in fact, any other organization.
- **Expert consultant** in software quality, either internal or external, employed by the organization interested, to assure the quality of a software product before the execution of the certification process.
- **Tool developer** for software product measurement. Measurement tools are an important mechanism for the expert consultant and the accredited laboratory to evaluate, improve and certify the quality of software products. The company developing such tools must follow the specifications and be in alignment with the measurements and thresholds set by the evaluation laboratory and the certification body.

B. NetApps Certification Lifecycle

The Certification Life Cycle starts by setting the certification scope, and relevant auditing artefacts, namely the "Certification Creation" process that formalizes the "Certification Execution" process to be followed every time a NetApp needs to be certified. As typical to most certification schemes, a "Certification Revocation" process will ensure that a compromised NetApp will be stripped from the provided certification. In this work we shall focus on the primary processes that set the basic certification frame.

As part of the **certification creation process**, graphically depicted in Fig. 1, the fundamental aspects are to:

- Deliver a concrete audit checklist so that to support interested partners to ensure that the objectives set for the NetApps certification are met. During this process, the certification objectives must become more specific and the technical evaluation criteria must be specified.
- Propose the appropriate testing methodology, framing the certification execution environment for field testing where necessary.
- Design and implement tools to execute the defined testing methodology in a transparent and repeatable manner.

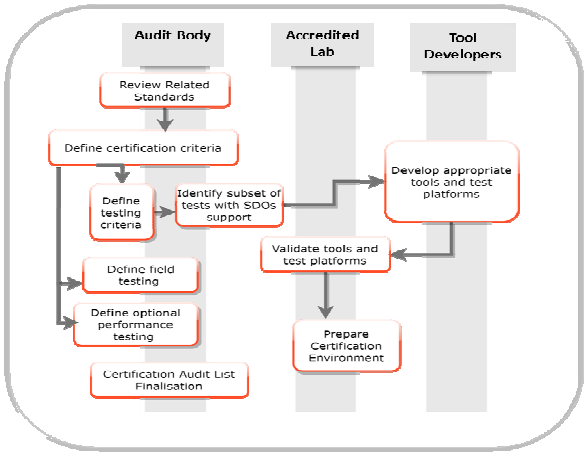

Fig. 1: NetApps Certification Creation Process

The **certification execution process** (Fig. 2) based on the above constructs and the availability of the execution environment, is basically focusing on execution of the certification audit for each requested NetApp. The execution process, apart from setting the initial contractual agreements to formalise the responsibilities per party, and the submission of supporting material, primarily refers to the audit list evaluation, performed as an automated testing process. In this process, it is possible that several testing iterations shall be necessary to achieve conformance, and findings of the certification process can trigger the software development process, providing concrete feedback on missing capabilities and issues to be treated.

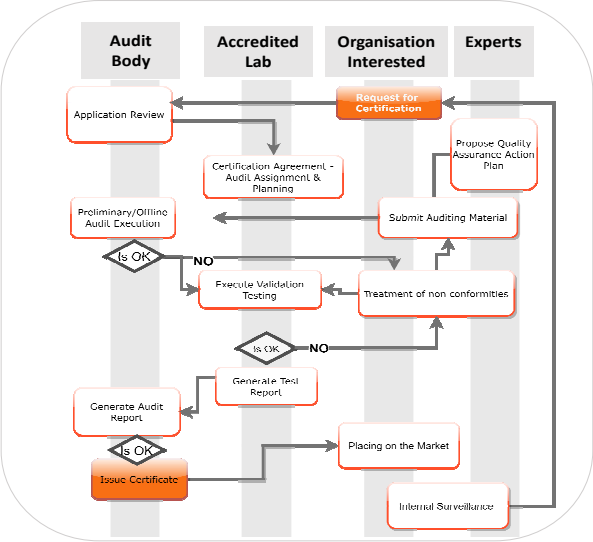

Fig. 2: NetApps Certification Execution Process

IV. EVOLVED-5G NETAPPS CERTIFICATION CRITERIA

Reflecting on the certification objectives as set for the device and ICT interoperability, as well as the EU Directives regulating market and security considerations, the criteria that are relevant for the NetApps certification can be classified around the following pillars:

- Software product quality (functional suitability)
- Security, with primary focus on fraud protection and data privacy
- Conformance to market mandates.

Decomposing these pillars, we can identify the technical validation criteria and the means to evaluate them transparently. An initial approach is presented in the next sections, with focus on the NetApps concept, while an exhaustive list is expected to incorporate specific mandates coming from the market and the target network operator domain as most appropriate.

A. Software Product Quality

The certification objectives around software quality primarily relate to the NetApps conformance with 3GPPP standards that would allow tight integration and effortless interworking with the 5G SA mobile core networks. TABLE I analyses the core criteria, key technical validation criteria and means for verification.

TABLE I: SOFTWARE QUALITY CRITERIA & VALIDATION

Criterion	Validation	Means
CAPIF Compliance	• NetApp API Invoker Mgmt. • NetApp Security Context setup • API Discover Service • NetApp Event Subscription • NetApp Event Notifications	Automatic (Tool-based)
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)	Automatic (Tool-based)
Documentation Quality	• Design & Specification Document • Installation & Configuration Manual • Operational Manual	Manual

B. Security

The certification objectives around security focus in detecting vulnerabilities in the coding and the deployment of the NetApps, preventing, data bridges and fraud as well as ensuring data privacy, considering that the NetApps are hosted, and therefore foreign to the execution environment, software components. In this respect code auditing and application security analysis play a pivotal role as part of the security application development lifecycle, ensuring the security and the privacy of data exchanges through NetApps interfacing with the NEF core function and accessing sensitive user data (such as location and user identification). Security application analysis is realized with both static and dynamic application security testing (SAST and DAST) [18]. The former involves white-box testing of the underlying framework, design and implementation of the application, aiming to audit the source code and identify vulnerabilities, unique defects and errors without the need to execute the application. The latter, involves black-box security testing of the NetApp, detecting the vulnerabilities and their exposed attack surface during runtime. Incorporating in the certification criteria the Security Considerations in the System Development Life Cycle as described in [19] a list of indicative criteria considered for the certification of security is listed in TABLE II.

TABLE II: SECURITY CRITERIA AND VALIDATION

Criterion	Validation	Means
Application Security	• Static Application (code) Security testing • Dynamic Application (binary) Security testing	Manual and/or Automatic (Tool based)
Fraud	• Test data streams to and from NetApp	Automatic

Protection	• Detailed Logging • Fraud detection • Continuous Monitoring • False Positive management	(Tool-based)
GDPR	• End User License Agreement, Accountability • Ensure data remains private • Inquire about data collection	Manual and/or Automatic (Tool-based)
Connection	• Ensure Privacy of Connection	Automatic (Tool-based)

C. *Marketplace*

The Marketplace is the final stage of commercialization for the NetApps, and includes 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 III.

TABLE III: MARKETPLACE CRITERIA AND VALIDATION

Criterion	Validation	Means
Policy/Terms	• End-user Use Policy • Terms of Service	Manual
Open Source Scan Report	• Catalogue all third-party software components, associated licenses	Automatic (Tool-based)
Valid Binary	• Binary Container file validation • Endpoints validation	Automatic (Tool-based)

V. THE NETAPPS CERTIFICATION ENVIRONMENT

Having set the basic concepts around the certification process, EVOLVED-5G has examined the functional specification of the Certification environment that need to be implemented and incorporated in the Accredited Labs that will undertake the technical evaluation. This work is incorporated in the overall EVOLVED-5G framework that is addressing the NetApps design/develop/verify/certify/publish methodology and tools.

A. *Reference Architecture*

A fundamental mandate for the certification execution environment is the need to be open to incorporate validation criteria that can come up as the technology and market evolve. Continuous Integration, Continuous Development (CI/CD) is thus, a core concept to build upon.

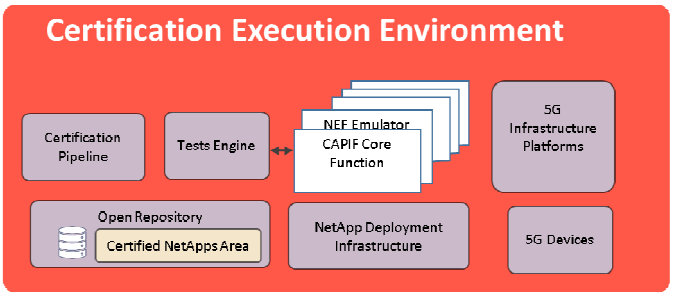

Fig. 3: NetApps Certification Execution Environment

Certification environment, displayed in Fig. 3 includes the following elements:

- **Certification Pipeline**: The pipeline orchestrates the whole certification phase and automates all steps towards the completion of the certification tests exploiting CI/CD capabilities. Technically the pipeline refers to the:
  - Infrastructure Deployment Automation
  - Automatic Software Installation and Configuration
  - Image Builder.
- **Open Repository**: The repository serves two purposes; as input, the open repository is the source of candidate NetApps that can go through the certification process. As output, once the Certification is complete, the Certification Pipeline will upload the certified NetApp to the certified area of the open repository.
- **Test Engine**: Certification phase as detailed above comprises a set of technical tests to be performed over the NetApp. These tests shall be triggered by the Certification Pipeline and will use a test engine that will execute the tests and report the results.
- **NetApp Deployment Infrastructure**: The EVOLVED-5G framework considers that a NetApp will be deployed and instantiated in container infrastructure. This infrastructure will be connected to the elements that are offering the 5G network capabilities.
- **5G Devices**: Devices connected using 5G are required to interact with the NetApp as required by the use case and the vertical applications.

All test reports, generated by the Test Engine, will be consolidated and reported as part of the Certification phase and upon successful completion, the NetApp shall be uploaded to the Certified area of the Open Repository.

B. *Certification Tools*

The tools involved in Certification aim to implement the technical evaluation tests reported in previous sections in a systemic and automated manner, and include the following:

- **NEF Services**: The EVOLVED-5G NEF Emulator is incorporated to certify the proper interaction of the NetApps with the (yet emulated) NEF services.
- **CAPIF Services**: To enable compliant use of CAPIF APIs by NetApps. EVOLVED-5G develops CAPIF Services Endpoint to implement the set of 3GPP APIs and subsequently verify that NetApps consume these APIs properly. CAPIF Services will audit the proper usage of CAPIF APIs and provide audited information of APIs, methods, headers, information elements, and error codes used between the interaction of the NetApp and CAPIF.
- **Security Tools**: Include tools for pre-certification security evaluation of NetApps (white-box and black-box testing tools) in order to determine whether such an application can be classified as malware, or vulnerable to application and data bridge attacks and classify them as secure and privacy preserving, or not according to the guidelines of the OWASP Top 10 [20]. An indicative list of relevant tools includes:
  - Veracode [21] is a tool capable of performing continuous static and dynamic application

security analysis thus decreasing the time software vulnerabilities such as cross-site scripting (XSS) and SQL injection can be accurately identified by many orders of magnitude.
  - Metasploit [22] is a tool that provides information about systematic vulnerabilities on networks and servers. It includes modules that can perform scanning, fuzzing, sniffing, etc.
  - Nessus [23] is a remote scanning tool, that raises alert if discovers any vulnerabilities, such as those that could allow unauthorized access, misconfigurations, default or common passwords, denial of service vulnerabilities, etc.
- **License Compliance Tool:** To automate the license compliance processes, various COTS alternatives can be considered. The Debricked tool [24] is a recommended candidate as it handles efficiently the open-source management and can be integrated in the CI/CD process of the development to export a license report to be shared with relevant stakeholders and keep track of the compliance progress over time.
- **Container Image Validator**: Chef InSpec 0 is an open-source testing framework for infrastructure with a human-readable language for specifying compliance, security and other policy requirements. While InSpec is used primarily to test security configurations, it is well suited for acceptance testing as well.
- **Container endpoint Health check**: A tool to validate the health status of the Docker container is developed by the EVOLVED-5G project, using custom command scripts on the Dockerfile.

VI. CONCLUSIONS

The NetApp concept has emerged as an enabling service layer for vertical stakeholders in the 5G ecosystem to promote dynamic, open 5G services and enable network programmability through standard APIs unlocking the network intelligence to the verticals. Consequently, the established terminals and equipment certification procedure in the mobile network business needs to extend to include supplementary software specification conformance and quality assessments for the NetApps. This study has presented the analysis performed by the EU-funded Horizon 2020 EVOLVED-5G project to incorporate the appropriate NetApps certification process in the current practice as well as the technical characteristics of an execution environment to implement the certification auditing in an effective, automated and repeatable manner. As a next step, the process shall be implemented and tested on selective Industry 4.0 use cases, and the relevant feedback will be used to further enhance the presented methodology execution and environment. Future work shall include lessons-learnt from the application of the methodology in experimental and industrial environments as part of the EVOLVED-5G deployments.

ACKNOWLEDGMENT

This work is supported by the EVOLVED-5G European Union's Horizon 2020 project, under the Grant Agreement No 101016608.

REFERENCES

[1] 3GPP TS 23.222, "Common API Framework for 3GPP Northbound APIs", Release 17, V17.4.0, April 2021

[2] 3GPP TS 23.434, "Service Enabler Architecture Layer for Verticals (SEAL)", Release 17, V17.1.0, April 2021

[3] 5GPP Architecture Working Group, "View on 5G Architecture", 5g-ppp.eu/wp-content/uploads/2021/11/Architecture-WP-V4.0-final.pdf

[4] "3GPP SA6 initiatives to enable new applications" https://www.3gpp.org/ftp/Information/presentations/presentations_2019/2019_09_SA6_vertical_apps.pdf

[5] DECISION No 768/2008/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0082:0128:EN:PDF

[6] Blue Guide, https://ec.europa.eu/growth/content/%E2%80%98blue-guide%E2%80%99-implementation-eu-product-rules_en

[7] The radio equipment directive 2014/53/EU (RED), https://ec.europa.eu/growth/sectors/electrical-engineering/red-directive_en

[8] https://www.telefication.com/wp-content/uploads/2017/12/RD_061_05-Conformity-assessment-procedures-for-the-RED-Scheme.pdf

[9] The PTCRB certification program, https://www.ptcrb.com/

[10] RAN5 - Mobile terminal conformance testing https://www.3gpp.org/Specifications-groups/ran-plenary/49-ran5-mobile-terminal-conformance

[11] Global Certification Forum (GCF), https://www.globalcertificationforum.org/

[12] ITUConformity and Interoperability (C&I) Programme, https://www.itu.int/en/ITU-D/Technology/Pages/ConformanceandInteroperability.aspx

[13] ISO25000, Software Product Evaluation and Certification Process, https://iso25000.com/index.php/en/product-evaluation/process

[14] ISO25000, Software Product Evaluation Ecosystem, https://iso25000.com/index.php/en/product-evaluation/ecosystem

[15] ISO/IEC 17025 Testing and Calibration Labatories, https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html

[16] ISO/IEC 17011 Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies, https://www.iso.org/standard/67198.html

[17] EVOLVED-5G, Deliverable 2.1 "Overall Framework Design and Industry 4.0 Requirements"

[18] Muñoz A, Farao A, Correia JRC, Xenakis C. P2ISE: Preserving Project Integrity in CI/CD Based on Secure Elements. Information. 2021; 12(9):357.

[19] Ross, Ronald S., Michael McEvilley, and Janet C. Oren. "Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems [including updates as of 1-03-2018]." (2018).

[20] OWASP Top 10: https://owasp.org/Top10/

[21] https://www.veracode.com/platform

[22] Metasploit tool: www.metasploit.com/

[23] Nessus tool: https://www.tenable.com/products/nessus/nessus-professional

[24] Debricked tool: https://sourceforge.net/software/product/Debricked/

Chef InSpec: https://www.chef.io/products/chef-inspec