GCOT Open RAN Certification Principles

1. Introduction

1.1. Background

The mobile cellular Radio Access Network (RAN) is a highly complex operation. The RAN has incredibly high-performance requirements to ensure that customer demands are met and that the network maintains a high "uptime." The RAN often covers a large geographic area with the expectations of a seamless experience for users regardless of location or whether they are mobile. This has historically led to suppliers delivering single-vendor solutions for the RAN which in turn has created industry concentration.

Open RAN (Open Radio Access Network) represents a development in the telecommunications industry that offers an alternative approach. Emerging in the early 2010s alongside technologies like Software-Defined Networking (SDN) and Network Functions Virtualization (NFV), Open RAN aimed to decouple hardware and software components. 3GPP Release 15, the first phase of the 5G standard, significantly influenced Open RAN by establishing a foundational framework for 5G networks that emphasized flexibility and modularity. Release 15 introduced key functions and interfaces, such as the Centralized Unit (CU), Distributed Unit (DU), and Radio Unit (RU), enabling the disaggregation of the RAN. The O-RAN ALLIANCE further expanded this flexibility by specifying a fronthaul interface between the DU and RU, allowing operators to integrate solutions from multiple vendors. Additionally, the O-RAN ALLIANCE standardized the RAN Intelligent Controller (RIC) with non-Real Time and Real Time components, and other element interfaces, enabling the customization of the RAN for specific use cases that require additional capabilities or functionality beyond what was defined by 3GPP.

As a result of the combined efforts of 3GPP and the O-RAN ALLIANCE, mobile operators now have multiple options for architecting their RAN, selecting vendors, and customizing radio functions. This newfound flexibility also introduces complexity and potential interoperability issues when integrating multi-vendor solutions.

1.2. Need for Certification in Open RAN

For commercial deployments, Open RAN solutions need to be interoperable, highly conformant, performant, and secure. Given the complexity of the RAN, ensuring that Open RAN solutions meet these criteria is challenging. Mobile Network Operators (MNOs) may lack the resources to independently test each integrated Open RAN solution, and Open RAN suppliers may be unable individually to demonstrate interoperability, conformance, performance, and security to every potential customer, especially if the expectation is that the supplier will bear the demonstration costs.

There is therefore a clear need for certification in the Open RAN market to provide confidence that customers will receive a sufficiently mature product that is conformant, interoperable, and performant. This is particularly crucial for the emerging private wireless market, where specific industry verticals, such as agriculture, manufacturing or mining, may deploy Open RAN networks to support operations differently than traditional MNOs. However, while certification can help address some of these challenges, it alone may not solve all the complexities and

resource demands of Open RAN deployments. The Open RAN ecosystem will need to continue to innovate and iterate in addition to any certification program that is established.

Existing certification programmes, for example those being developed by the Telecom Infra Project (TIP) and the O-RAN ALLIANCE, are making an important first step towards addressing these challenges. The principles outlined in this document seek to build on existing testing and certification work to provide a framework to maximise the potency of such regimes going forward.

1.3. Purpose of this Document

This document proposes, on behalf of GCOT partners, a voluntary framework for the Open RAN ecosystem stakeholders to develop a robust, comprehensive certification program for Open RAN equipment. It provides in our view the steps necessary to accomplish this goal in order to facilitate a discussion with industry about how to bring this about as a next step. However, this document does not serve as a certification program itself nor does it offer an exhaustive list of instructions on how to create an Open RAN certification program.

1.4. Target Audience

The intended audience comprises Open RAN ecosystem stakeholders, such as MNOs, Open RAN hardware and software suppliers, infrastructure providers, system integrators, and any other entity that may be involved in the development and operation of an Open RAN certification program.

2. Certification Governance and Integrity

2.1. Roles and Responsibilities

Clearly defining roles and responsibilities for all stakeholders is a crucial element in facilitating Open RAN adoption.

- *MNOs* select certified Open RAN solutions that align with their specific network requirements and performance goals. Where possible they publish these requirements to support product development and useful performance testing.
- *Hardware/Software Providers* innovate and develop Open RAN compliant equipment that adheres to established certification standards. They should seek for these not only to be interoperable on paper, but also demonstrably so in practice.
- *Passive Infrastructure Providers* can offer physical and virtual resources necessary for the operation and management of representative Open RAN networks used in testing. This includes elements such as fiber, tower sites, data centers and cloud services.
- *System Integrators* ensure seamless integration of certified Open RAN components from different vendors within the network architecture. Integrators should not create so-called ‘islands of interoperability’, where only approved partner vendors can be used within their systems, but genuinely open systems that can be implemented neutrally.
- *Certification Bodies* establish and manage the entire Open RAN certification process. This includes defining certification requirements, reviewing test results, and granting certifications.
- *Testing Laboratories* conduct rigorous testing on Open RAN equipment against established standards, Key Performance Indicators (KPIs), and security levels.

- *Government* should not lead in developing or operating certification programs nor testing regimes – it should be an industry led process. In some cases though, governments, or other public bodies, may wish to participate in the development process (e.g., cybersecurity entities), or fund bodies that issue certifications (e.g., publicly-funded labs), in order to ensure robustness, representation of public interest, and that uptake is maximised. Some governments may also require certified products for public sector and military adoption of Open RAN, but this should be determined by each government individually.

2.2. Source(s) of Certifications

A certification program should work with existing standards and specification organizations, such as 3GPP and the O-RAN ALLIANCE, to develop the requisite certification tests. These should be developed in such a way that they are standard across testing labs and, where possible, do not require any specific, idiosyncratic, or self-developed test in addition (e.g., for a given region). Both 3GPP and the O-RAN ALLIANCE have produced test specifications for the disaggregated RAN. For example, 3GPP's TS 38.141 defines conformance tests for the NR Base Station. The O-RAN ALLIANCE's WG4, WG5, and WG6 specifications focus on conformance, integration, and security testing for Open RAN components. Such products could be leveraged to create an Open RAN certification program.

2.3. Types of Testing

Certification testing should focus on the primary areas of conformance, interoperability, and performance. Each of these has its own critical role in ensuring the viability of an Open RAN solution.

- **Conformance:** Conformance testing is defined as the adherence of interfaces, subsystems, and end-to-end systems to specifications produced by the appropriate standards and specification bodies. This includes conformance testing of Radio Units (RUs), Distributed Units (DUs), and Central Units (CUs) to verify adherence to standards for RF processing, baseband processing, and control/user plane functions. It also involves validating interfaces such as the fronthaul (e.g., lower layer split, higher layer split), midhaul (e.g., F1), backhaul (e.g., E1), and others like the management plane (e.g.,O1) and service management interfaces (e.g.,A1, E2).
- **Interoperability** testing involves verifying that components from different vendors can seamlessly work together within the Open RAN ecosystem. This testing ensures that RUs, DUs, CUs, and other network elements conform to defined standards and protocols, enabling them to communicate and operate effectively without compatibility issues. It also includes validating interfaces like fronthaul, midhaul, and backhaul, ensuring that they support interoperability across various configurations and deployments.
- **Performance** testing should focus on customer (e.g., MNO) defined requirements, KPIs, and features. These should be sufficiently tailored to specific use cases, architectures, and deployment environments in order to be meaningful, whilst avoiding being overly specific.
- **Security** testing should adhere to local legal and regulatory security requirements and encompass various aspects of conformance testing. Additional security testing can be

tailored to specific use cases. This testing should capture best practices, such as those outlined in the O-RAN ALLIANCE's WG11 Security Working Group and 3GPP Security Assurance Specification (SCAS) tests, as well as security frameworks from organizations like NIST, IEC, and ETSI. In general, an informative approach to assessment, rather than a pass/fail-style certification, ensures a comprehensive evaluation of security measures. However, there will still be certain aspects that require a minimum baseline to pass as part of that holistic assessment.

2.4. Oversight

Development, governance, and oversight of an Open RAN certification program should be reflective of the diverse marketplace it is supporting and not be biased in favor of one market segment or region. Existing industry bodies involved in certification programs are well-equipped to undertake this level of oversight but should remain alert to the potential for bias in their work due to over- or under-representation of a given group of stakeholders, whether that be geographical or a particular industry segment.

2.5. Transparency

Industry groups developing a certification program should adopt an open and rigorous approach, allowing fair access for new participants and external scrutiny, including by public bodies. Access to certification processes by public authorities is necessary to ensure that these embed cybersecurity best practices, in line with the 2021 Prague Proposals on Telecommunications Supplier Diversity,[1] and to ensure that overall security is enhanced by open practices despite the opening of additional interfaces. The onus and responsibility to lead certification is with industry, but external scrutiny can support and ensure favorable outcomes.

2.6. Conformity Assessment Bodies Accreditation

Conformity assessment bodies (CABs) are organizations such as laboratories and certification bodies that evaluate and certify whether products, services, or systems meet specific standards and regulations. Certifications issued should be independently verifiable and repeatable by other qualified labs, ensuring consistency and minimizing the risk of errors specific to a particular testing environment. This should be ensured through consistent and standard testing protocols, without regard to geography, as per Section 2.2. Furthermore, labs should be accredited in accordance with industry best practices and standards, such as ISO/IEC 17025 and ISO/IEC 17065. This approach should also avoid duplication of efforts, (e.g., a certificate issued by an American CAB should hold equivalent credence in a European market to the same certificate issued locally).

Before labs can be accredited, evaluation criteria should be defined. Organizations like 3GPP, O-RAN ALLIANCE, TIP, and GSMA could help define and publish such criteria, which does not currently exist.

2.7. Continuous Improvement

The certification program should not consider any previously granted certifications as static. The certification program should adopt a dynamic certification process to keep pace with innovations in 5G/xG and as Open RAN specifications and standards develop, the

[1] https://nukib.gov.cz/download/Prague_Proposals_on_Telecommunications_Supplier_Diversity.pdf

certifications should be updated to reflect those changes. Beyond this, certifications should be designed to ensure secure backward compatibility between Open RAN standards and specifications, and the interfaces used in existing networks. In addition, test protocols should be updated as testing equipment capability improves in order to ensure robustness.

3. Cost-Effective Implementation

3.1. Accessibility

Open RAN certification should be accessible to companies of all sizes. Barriers to implementation should be minimized.

The cost structure for network equipment certification is complex, with manufacturers bearing primary responsibility and often passing costs to end users. Certification bodies and test labs also play crucial roles, earning revenue through service fees.

Governments can optimize these costs by supporting the harmonization of standards internationally and providing financial support through subsidies and grants. Establishing government-funded testing facilities, promoting public-private partnerships, and encouraging innovation in testing methods can further reduce costs. These strategies can create a more efficient and affordable certification process, benefiting both the industry and consumers.

3.2. Automation

Open RAN certification should leverage automation when testing to the maximum extent possible, in order to reduce the cost of certification and the risk of error.

3.3. Leverage Existing Resources

An Open RAN certification program should consider how to leverage existing resources such as professional certification laboratory services, rather than requiring the development of new infrastructure.

3.4. Structure of Certification

Development of a certification program should consider the impacts of a tiered approach to certification. All tiers should be meaningful and spur customer demand, rather than solely amounting to gating criteria for the next step of certification.

When considering different tiers of Open RAN certification, it is important to account for the varied needs and scales of different deployments. The requirements for a large MNO differ significantly from those for a small-scale private deployment. For instance, large-scale Open RAN deployments may focus on network efficiency and vendor diversity, while private networks (e.g., in the mining or agriculture sectors) emphasize reliability and real-time monitoring. Neutral host networks, rural deployments in remote communities, or public safety applications further demonstrate the versatility of Open RAN in supporting diverse use cases. One suggested structure for potential (and non-exhaustive) tiers of Open RAN certification could be as follows:

1. Private Network Tier
   - **Scope:** Small-scale deployments such as those for smaller enterprises, remote facilities, or localized private networks. While typically focused on simplicity and cost-effectiveness,

this tier can also address niche cases where heightened security is required despite the limited scale such as an outpatient clinic.

- **Technical Requirements:**
  - Basic functionality testing to ensure core operational standards and reliable connectivity;
  - Interoperability with common Open RAN components and interfaces, enabling seamless integration of equipment from multiple vendors;
  - Baseline security compliance to protect against common vulnerabilities for standard use cases, while allowing for the inclusion of tailored, robust security measures (e.g., end-to-end encryption and advanced threat detection) in scenarios where the deployment involves sensitive operations even with limited deployment size; and
  - Simplified deployment and management capabilities.

2. Enterprise Network Tier

- **Scope:** Medium-scale deployments such as those for regional service providers, bespoke verticals and larger enterprises
- **Technical Requirements:**
  - Enhanced functionality testing across broader operational capabilities;
  - Advanced interoperability with diverse Open RAN components and systems;
  - Heightened security measures with advanced threat detection and mitigation capabilities;
  - Performance metrics to ensure reliable operation under typical workloads; and
  - Moderate scalability to accommodate an intermediate-level number of users and devices.

3. Carrier Network Tier

- **Scope:** Large-scale deployments for MNOs and global service providers, covering different deployment cases (e.g. rural macro, urban neutral host, and mMIMO).
- **Technical Requirements:**
  - Comprehensive functionality testing covering all operational aspects, including edge cases;
  - Full interoperability across extensive Open RAN ecosystems and legacy systems;
  - Advanced security protocols meeting stringent standards and best practices;
  - Rigorous performance and reliability testing under diverse and heavy operational conditions;
  - High scalability to support large numbers of users and devices with flexible deployment options; and
  - Regulatory compliance with all relevant standards and requirements.

This structure would benefit both suppliers and MNOs. Smaller suppliers could enter the marketplace more easily by satisfying basic requirements first, then gradually pursue advanced modules based on their strengths and commercial priorities. Small scale deployments which are simpler to test and certify will be lower cost compared to large scale deployments which require extensive technical testing leading to higher cost. This approach would also help MNOs by providing detailed insights into supplier capabilities, enabling them to select vendors with

products and solutions that meet the specific requirements that are most aligned with their network needs. The program could also scale by adding new modules as Open RAN technology evolves.

3.5. Scope of Certification

In tandem with the structure of certification, the scope of any such regime should be calibrated to promote relevance to the broadest segment of the marketplace while still being meaningful. Certification should not become so specialized that in practice there is little demand for it, clearly diminishing value.

Further, the scope of Open RAN certification should ensure that the interface (e.g., fronthaul and midhaul) or function (RU/CU/DU combinations) being evaluated is standards compliant, functions seamlessly, and integrates smoothly with other network elements as defined by the use case for the certification. This adaptable scope ensures robust performance, security, and interoperability across different deployment scales.

3.6. Recertification

Open RAN systems can be very complex. Recertification of software, computational hardware, or firmware updates may be necessary, particularly with regard to major updates. Industry should take necessary steps to ensure that such recertification is expeditious, meaningful, and cost effective. Relevant recertification should be determined based on criteria such as standards evolution, specific use cases, regulatory compliance, industry best practices, risk assessment, stakeholder feedback, historical data, and the technical and operational context of the deployment. This approach ensures critical aspects are tested without unnecessary redundancy, over-testing, or over-certification

4. Facilitating Adoption

4.1. Customer Demand

An Open RAN certification program can only be successful if MNOs and other network builders and users, such as wireless Internet service providers and private network customers, require this certification in their procurement processes. The certification program should consider highlighting key sources of value to customers, including:

- Noting that the certification provides a means to stimulate a robust and competitive market which can in turn drive more innovation and generate operational efficiencies;
- Showcasing how certification can minimize deployment risks by ensuring Open RAN components meet interoperability, conformance, and performance requirements. Minimizing compatibility issues should lead to smoother deployments and reduced network downtime, a key benefit for operators;
- Emphasizing how the certification program allows for flexibility to align with evolving Open RAN technology and standards, enabling operators to build future-proof networks; and
- Creating opportunities for operators to showcase successful deployments of certified Open RAN solutions where case studies and testimonials can serve as valuable proof points and encourage others to follow suit.

4.2. Industry Support

A certification program needs to build support amongst suppliers in the Open RAN marketplace and avoid fragmentation across jurisdictions, since this can make market entry difficult for small players.

The program should be designed to attract and retain a broad range of suppliers, including by fostering a supportive environment for industry participants. Key aspects of this should include:

- **Fostering Consistency**: Develop a publicly accessible platform for certification standards, processes, and guidance, ensuring transparency and reducing fragmentation across different regions. Leverage established global standards to create a consistent certification framework that fosters trust and aligns with international best practices.
- **Optimizing Certification Processes**: Adopt cost-effective and flexible certification strategies, such as modular or tiered frameworks, to cater to deployments of different sizes and capabilities.
- **Encouraging Collaboration and Knowledge Exchange:** Organize industry events and conferences to showcase technology trends, innovations, and best practices, enabling knowledge exchange while maintaining intellectual property and competitive integrity.
- **Establishing a Certification Registry:** Create and maintain a publicly accessible certification database that recognizes all certified suppliers and their capabilities, ensuring a transparent and level playing field for participants.
- **Delivering Detailed Certification Insights**: Transform certification programs by moving beyond simple pass/fail-style results to include comprehensive reports that highlight a product's strengths and provide insights into KPIs.

4.3. Government Support

Governments can play a key role in accelerating the adoption of an Open RAN certification program. To support this, governments could consider exploring multiple approaches, taking into consideration their unique national circumstances and priorities. Steps could include:

- Considering within appropriate frameworks whether relevant products should be certified in order to qualify for public sector procurement (however, governments should avoid developing or operating their own Open RAN certification programs);
- Providing tax incentives, grants, or other funding programs for Open RAN certification initiatives, including those aimed at supporting the participation of smaller MNOs and suppliers;
- Coordinate with international partners to share experiences such as R&D breakthroughs, pilot programs, best practices, capacity building, and regulatory measures to advance the adoption of Open RAN; and
- In tandem with industry, collaborate with international partners to support capacity building, general education, and workforce development initiatives around the world to ensure access to the necessary talent to test, develop, and integrate Open RAN solutions globally.

5. Conclusion

To drive robust Open RAN adoption, stakeholders should establish and maintain a comprehensive certification framework that ensures interoperability, conformance, performance, and security. The growing complexity of RAN systems, resource constraints among MNOs, and difficulties

faced by suppliers in demonstrating their products' capabilities underscore the value of developing such a framework. Certification is key to overcoming such obstacles, providing customers with confidence in product maturity and facilitating broader adoption. While existing initiatives in this vein are promising, they remain at early stages and must evolve to address these challenges effectively.

Collaboration among relevant stakeholders, including MNOs, vendors, research institutions, and policymakers, is crucial for shaping responsive certification frameworks. Regional testing labs can also play a pivotal role in enabling transparent validation processes, reducing the burden on suppliers. While industry should lead the development of a certification program, policymakers can consider whether to encourage adoption through incentives such as subsidies, tax breaks, and expedited regulatory approvals. The potential application of a certification program to public procurement could also accelerate adoption. Finally, policymakers can help to foster local industry ecosystems and innovators, address trade barriers, and support workforce development initiatives.

The GCOT partners believe that governments have a role to play in supporting the development of such approaches as well as their durability and usefulness in the long term. The GCOT partners have and will continue to support the principles through the establishment of neutral labs, like the UK's SmartRAN Open Network Interoperability Center (SONIC Labs) and the U.S. Communications Research and Innovation Network (CRAIN), as well as government investment in the Open RAN ecosystem through Research & Development funds, such as the Public Wireless Supply Chain Innovation Fund, and competitions, like the Open Network Ecosystem Competition. The GCOT partners welcome additional government support and engagement. The GCOT partners will continue to support the industry-led shift towards Open RAN approaches and engage constructively with interested stakeholders in developing a certification framework as a key step in this direction.