MoU Security certification for security requirements

UNDER THE OPEN RAN MOU

by Deutsche Telekom, Orange, Telefónica, TIM and Vodafone

This document provides a high-level description of the MoU signatories' technical requirements on Security Certification.

For the avoidance of doubt, the technical requirements set out in this document are those that the signatories of the Open RAN MoU consider priorities for Open RAN solutions. They serve as guidance to the RAN supplier industry on where to focus to accelerate market deployments in Europe.

1. **Improvement of the coverage of security requirements by security test specifications in order to reach 60% by the end of the year.**

   In current situation the level of coverage of security requirements by test specifications is around 34% and there is a problem to have a Security Certification in place when you don't have a majority of security requirements covered by related security tests.

2. **Security Certification process to be put in place by the end of 2024.**

   The Open RAN MoU recommendation and priority is to have O-RAN ALLIANCE SCAS documentation included in GSMA NESAS to be able to have the security certification possible using NESAS scheme and be aligned also with ENISA EU5G Certification Scheme assuring also worldwide recognition.

   OTIC laboratories could provide also their ORAN Security Certification but there is a risk that this certification is not recognized by the National Authorities of those Countries where MNOs want to deploy the Open RAN solutions. While GSMA NESAS and its adapted versions for Europe or other Countries are or will be recognized as security certification.

3. **E2E Security Certification should not be mandatory for vendors.**

   Since the system is in responsibility of the MNO, certification of E2E should be done only when it is required in the Country/ region where the system is deployed.

   E2E Security tests must be included in the documentation to be used when needed by the MNOs but should not be included in the Certification for the vendors.

4. **Shift the object of certification from products and interfaces towards Network Functions**

   Both interfaces and components should be certified and be a subject to security testing. In NESAS setup a network function includes interfaces.

5. **The priority for having a good level of maturity in Security Certification should be around O-RU (O-FH) as the most exposed component.**

6. **Coordination with 3GPP SA3 SCAS is required.**

   Some areas of Open RAN are already covered by 3GPP SA3 SCAS and overlapping should be avoided. Reutilization should be encouraged.

7. **Security tests to be organized similar with SCAS in order to integrated in both GSMA NESAS and EU 5G Cybersecurity Scheme since they are following also NESAS**

   O-RAN ALLIANCE should assure compatibility when building SCASs with GSMA and ETSI in order to make possible the inclusion in EU 5G Cybersecurity Certification Scheme.