Security MoU Zero trust approach commitment

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 Zero Trust Architecture.

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.

The MoU group recognizes the paramount significance of Zero Trust Architecture (ZTA) as the foundation for open and disaggregated networks. We acknowledge the pivotal role of ZTA in fortifying network security and align with the National Institute of Standards and Technology's (NIST) comprehensive definition of the seven Zero Trust tenets established in 2020 [1].

Furthermore, the MoU group draws inspiration from the 3rd Generation Partnership Project (3GPP) Release 18, specifically TR 33.894 [2]. The Rel-18 FS_ZTS study assessed the disparity between current security mechanisms and Zero Trust (ZT) security principles in the context of 5G Core (5GC). Further research is needed to provide recommendations for supporting ZT principles in 5GC security architecture, particularly regarding Tenets 4, 5, 6, and 7 in [1].

As we prioritize security, it is crucial to extend the evaluation of ZT principles to the Radio Access Network (RAN). Following 3GPP's comprehensive approach for assessing ZTA in the core, the O-RAN ALLIANCE should explore all ZT principles within the context of the RAN, using them as a foundational framework. By adopting a Zero Trust mindset throughout the network architecture, the O-RAN ALLIANCE contributes to advancing secure, open, and interoperable networks [3].

However, it is important to evaluate the impact of ZT principles and comprehend the impact of a ZTA based RAN especially on site dimensioning for different topologies.

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

[2] https://www.3gpp.org/ftp/Specs/archive/33_series/33.894/33894-i00.zip

[3] https://access.atis.org/apps/group_public/download.php/72390/ATIS-I-0000095.pdf