Security and Trust in Open and Disaggregated 6G networks

P.Alemany*, R.Muñoz*, R.Vilalta*, Ll.Gifre*, R.Martínez *, R.Casellas* M.Castro†, P.Ferreira†, D.Moreira†, J.García†, J.Cunha†, I.Núñez†, G.Gómez‡, S.Castro‡, A.Pastor§, D.López§
* Centre Tecnològic de Telecomunicacions de Catalunya (CTTC-CERCA), Spain
† Optare Solutions, Spain
‡ EVIDEN, Spain
§ Telefónica Innovación Digital, Spain

ABSTRACT Telecommunication networks are undergoing a significant shift from closed and proprietary systems towards open and interoperable networks. This transition allows for greater flexibility and reduced dependence on single providers. However, this openness also raises substantial security and trust issues, necessitating new approaches like the use of an intelligent and autonomous 6G network slicing security manager to manage security in multi-provider environments. Additionally, trust management is becoming increasingly crucial, with technologies such as Blockchain proposed to ensure the reliability and integrity of operations across this new, decentralized landscape. This model supports a dynamic marketplace where providers can freely negotiate and manage resources, thereby enhancing service delivery and network management.

Keywords 6G networks, multi-provider, network slices, security management, trust management, blockchain.

1. Introduction

Traditionally, network equipment has relied on closed software and hardware systems, integrated and patented by a few providers, creating well-known provider islands in telecom networks. In the last years, there has been a trend toward replacing these closed systems across various network segments (RAN, aggregation, transport, and core) with open and interoperable multi-vendor systems [1]. Industry-led initiatives like the O-RAN Alliance (ORAN) and the Telecom Infra Project (TIP) are promoting this change, which enhances competition, fosters innovation, and supports a more cost-effective and competitive deployment of technologies such as 6G. However, open telecom networks pose significant questions regarding security and trust in this complex multi-provider environment.

Network operators relies on proprietary solutions from closed system providers for network security. However, the emergence of open and disaggregated 6G networks provides a unique opportunity for operators to manage their network security more directly and flexibly using open technologies. The introduction of a 6G network slicing security manager (NSSM) is key for managing security requirements across multi-provider networks [2]. This manager will enable the definition of service level agreements (SLAs) with specific security requirements, ensuring that network slices not only meet technical and quality of service needs but also adhere to stringent security standards. The NSSM will use a range of security policies and tools, including monitoring probes and closed-control loops, to maintain security compliance and reactively address potential security threats.

Trust management is becoming increasingly critical in the transition to open and disaggregated 6G networks, where traditional, reputation-based methods are insufficient. In such networks, the complexity of multi-provider scenarios requires a robust system for measuring and evaluating trust, with Blockchain technology identified as a key solution [3]. Blockchain's attributes—decentralization, immutability, transparency, and verifiability—make it ideal for establishing a new foundation of trust. By verifying the actions and responsibilities of various providers, Blockchain allows for a more dynamic and transparent approach to network management. It replaces the conventional centralized model with a distributed framework where infrastructure and network services can be negotiated and managed in real time, enhancing the overall integrity and efficiency of 6G networks. The trust manager is the key element to compute a set of reputation and trust parameters (based on a set of per domain metrics) and distribute them transparently across the whole system and keeping an immutable history of how trustworthy each provider is to fulfil an operator's request.

2. Network Slicing Security Manager overview

The NSSM is designed with several key components to ensure robust security management across network slices. These include:

- Security SLA & Policies (SSLA&P): This component is responsible for designing and managing the data objects that encapsulate the security service level agreements (SSLA) and associated policies. These policies govern how services are configured initially or adjusted in response to threats. SSLA&P operates at both the end-to-end (E2E) and domain-specific levels.
- Security Closed-loop (CL) Automation: This component processes monitoring data to evaluate security threats by comparing observed events against predefined SSLA thresholds. If a violation is detected, it triggers policies designed to mitigate the threat.

979-8-3503-7732-3/24/$31.00

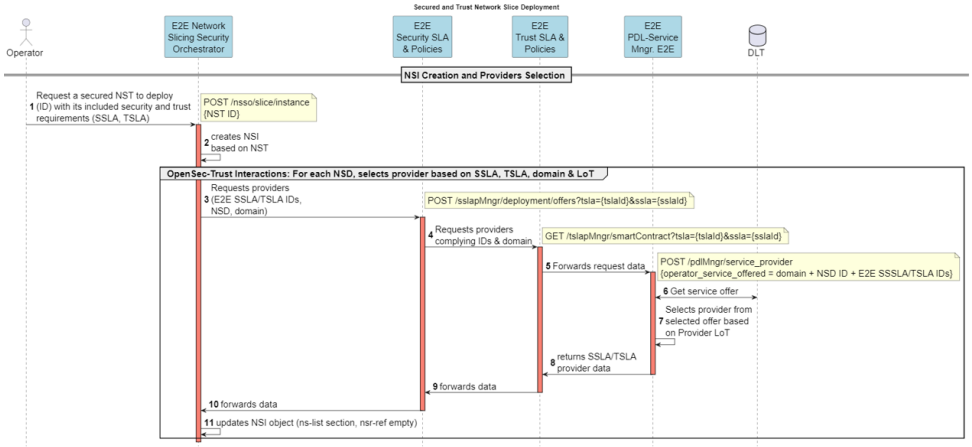

Figure 1. NSI Creation and Providers Selection

- Security CL Governance: While the full development of this component is beyond the scope of the current project, it is crucial for coordinating and governing all created closed-loops.
- Network Slicing Security Orchestrator (NSSO): Tasked with managing and orchestrating both the network slices and their security configurations. If an SSLA is violated, the NSSO applies the necessary measures in accordance with the established SSLAs and policies. The NSSO also exists in two versions, one for E2E operations and another at the domain level.

3. Trust Manager overview

The Trust Manager in a network setting is structured around several components aimed at managing and ensuring trust across network services:

- Trust SLA & Policies (TSLA&P): This component is responsible for creating and managing Trust Service Level Agreements (TSLA) and the associated policies. These agreements and policies set the framework for how services are configured to meet the expected Level of Trust (LoT), both initially and in response to changes. TSLA&P operates at both the end-to-end (E2E) and domain-specific levels.
- Trust Controller: This component manages the metrics used to compute the trust parameters for each provider, focusing on their reliability in fulfilling user-defined requirements. These parameters help in selecting providers for new service requests based on their ability to meet predefined trust criteria.
- PDL-Service Manager (PSM): Responsible for integrating with Blockchain technology to store and distribute trust parameters securely and transparently. The PSM utilizes smart contracts (SC) within the Blockchain to handle and disseminate trust-related data and event requests across all network nodes. This component is also developed for both E2E and domain-specific applications.

4. Workflows

This section presents a set of workflows to illustrate and describe the deployment of a secured network slice and how the most trusted providers are selected to deploy the security resources. The deployment workflow is divided into four phases: the Network Slice Instance (NSI) Creation and Providers Selection, the Service and Security Deployment, the Trust Deployment & Activation and, finally, the Closed-Loop Configuration.

As illustrated in Fig. 1, the deployment process begins when the operator requests to the E2E NSSO a specific Network Slice Template (NST) which contains the services to deploy and the E2E SSLA and TSLA identifiers defining the expected security and trust requirements (step 1). Then the E2E NSSO creates the NSI based on the NST (step 2) and triggers the process to select the security and trust providers based on the capabilities required and the capabilities offered. To do so, the E2E NSSO requests the providers capable to fulfil the E2E SSLA and TSLA to the E2E SSLA&P (step 3) component, which forward this request to the E2E TSLA&P (step 4), and it to the E2E PSM (step 5). Then the E2E PSM obtains the providers registered as capable of fulfilling the E2E SSLA/TSLA (step 6) and based on their Level of Trust (LoT) selects the most trusted ones for each domain involved (step 7). Then, the selected data is sent back to the E2E NSSO (steps 8-10), which uses it to update the created NSI (step 11).

Fig.2 presents the phase where the service and security elements (i.e., Network Security Functions (NSF) and security probes) are deployed (step 12). It is possible to identify four main groups of actions: 1) the service deployment composing the NSI (steps 14 – 15); 2) the identification of NSFs and security probes by requesting an SSLA to domain policies translation (steps 16 – 20); 3) the identified NSFs deployment (steps 21 - 23) and finally; 4) the security probes (steps 24,25). Once all these actions are confirmed (step 26), the NSI is updated

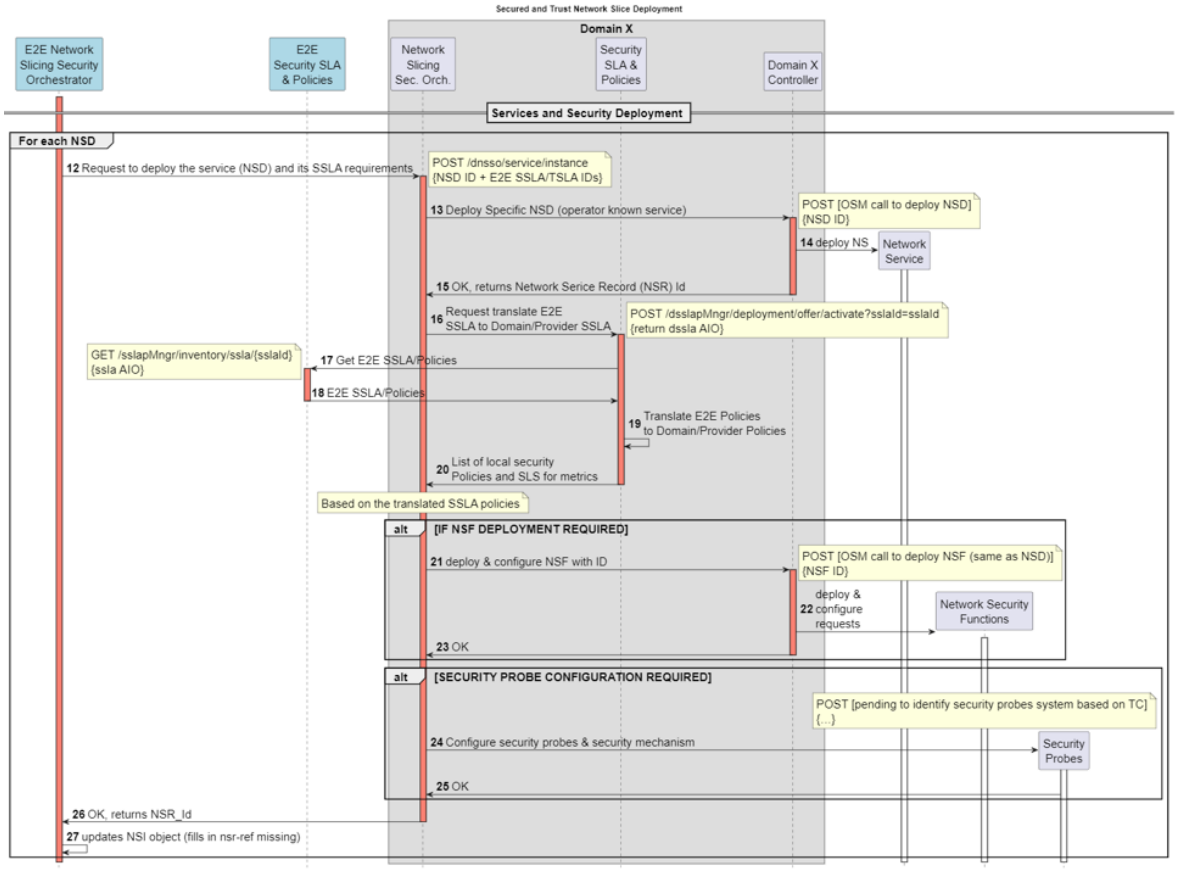

Figure 2. Services and Security Deployment

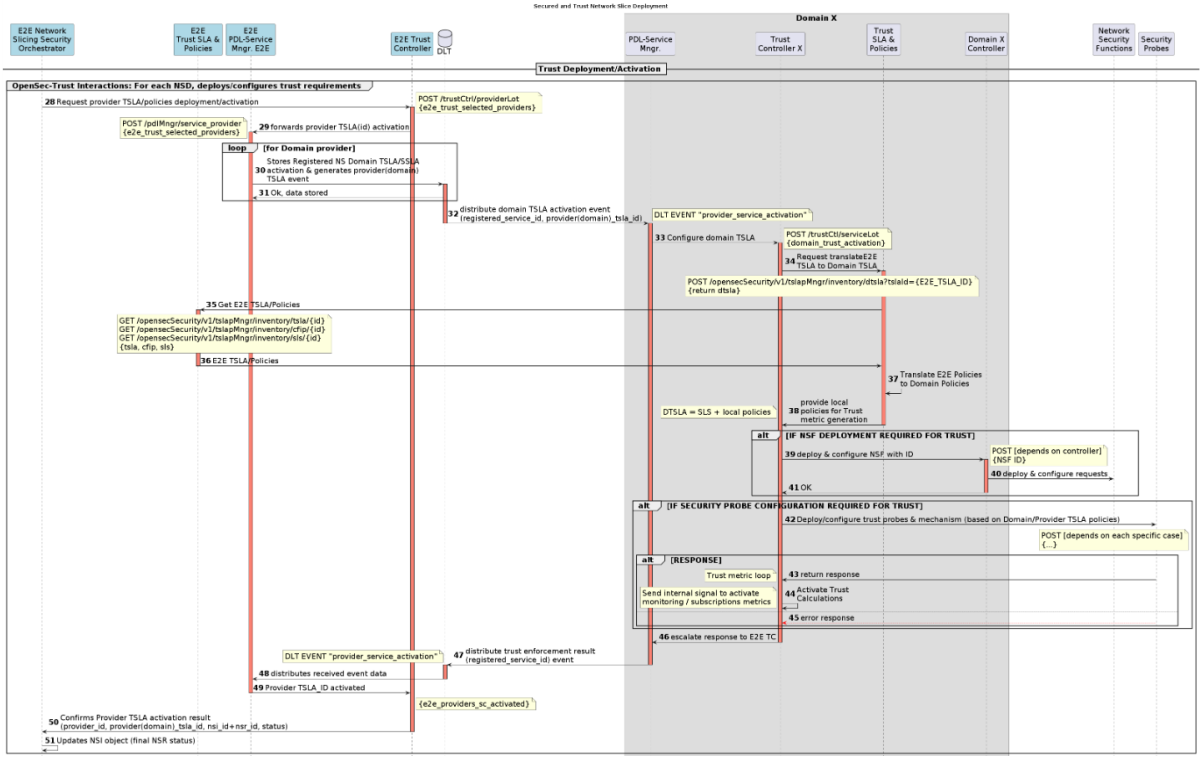

Figure 3. Trust Deployment & Activation

(step 27) and the E2E NSSO continues with the next service within the NSI (repeating this process) or with the trust deployment & activation phase.

As illustrated in Fig.3, the next phase in the deployment workflow is the Trust Deployment & Activation. At this stage of the workflow, there is a NSI with the basic service and NSFs already deployed and configured in

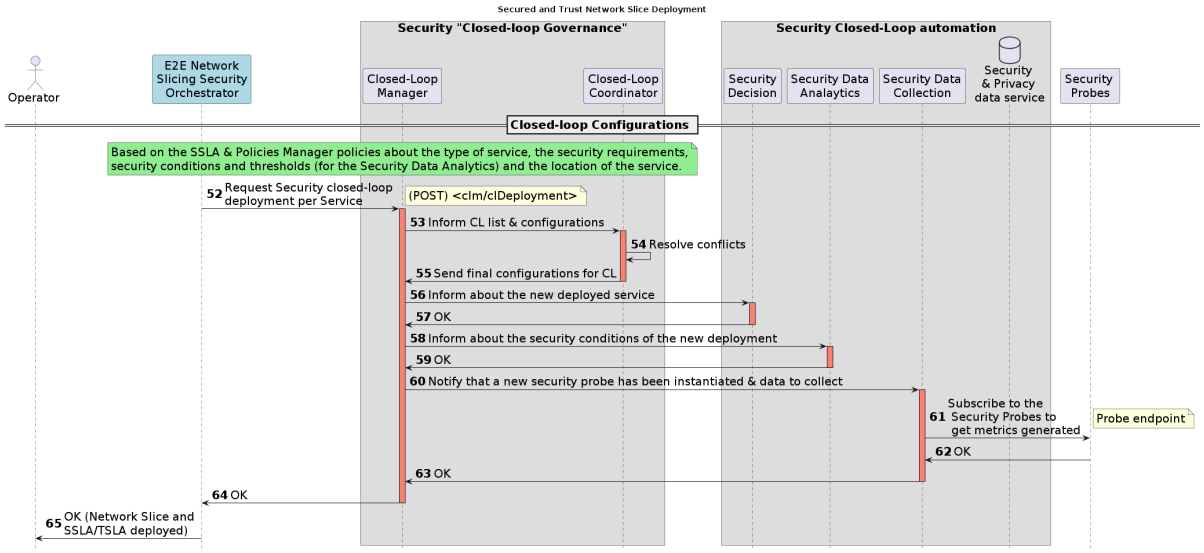

Figure 4. Closed-Loop Configuration.

terms of security. Now, the idea is to follow a similar procedure but looking to achieve the trust requirements defined in the selected E2E TSLA. To do so, the E2E NSSO requests the activation of the E2E TSLA (step 28) to the E2E Trust Controller (TC), which forwards this information to the E2E PSM (step 29) so this one may generate the event for the right domain and provider type (steps 30 – 32). After the right domain PSM receives the event, it requests the TSLA configuration to the TC (step 33), which in turn needs to get the translation of the E2E TSLA into policies using the E2E and domain TSLA&P components (steps 34 – 38). At this moment, and depending on the policies, the TC may deploy and configure new required NSFs focused on trust or simply configure those already deployed elements from the previous phase (steps 39 – 41). The same applies for the security probes illustrated in steps 42 to 45. In both cases, once these steps are done, the resulting outcomes are forwarded back to the E2E PSM through the domain PSM and DLT (steps 46-48), leaving the TSLA and the selected provider registered as active. Finally, this information is also sent back to the E2E NSSO through the E2E TC to update the NSI (steps 49 – 51).

The next phase is the configuration of the CL associated to the NSI, which is illustrated in Fig.4. Based on the policies identified from the selected E2E SSLA/TSLA, the E2E NSSO will trigger this process by requesting to the CL Manager (CLM) to deploy a CL (step 52) (data objects presented in section 5.2.4). At this moment, the CL Manager takes care of the following actions: first, to validate with the CL Coordinator (CLC) if there are conflicts with other existing CLs (steps 53 – 55); secondly, to inform the Security Decision (SD) about the deployed NSF (steps 56,57); third, to inform to the Security Data Analytics (SDA) about the security conditions of the new deployed NSF (steps 58,59); and finally, to notify to the Security Data Collection (SDC) to subscribe to the security probes (steps 60 – 63). Once all these four actions are done, the CLM reports back to the E2E NSSO (step 64), which notifies the operator about the full deployment and configuration of the requested Secured network slice (step 65).

5. Conclusion

This paper has presented a security and trust management architecture for open and disaggregated 6G networks in multi-provider environments composed of RAN, transport and core network segments.

Acknowledgment

Work supported by the Ministerio de Asuntos Económicos y Transformación Digital and the European Union-Next GenerationEU in the frameworks of the Plan de Recuperación, Transformación y Resiliencia and of the Mecanismo de Recuperación y Resiliencia through UNICO-5G I+D 6G-OPENSEC project under references TSI-063000-2021-58, TSI-063000-2021-60, TSI-063000-2021-61; MCIN/AEI/10.13039/501100011033/ FEDER/UE by ERDF A way of making Europe through the Spanish RELAMPAGO (PID2021-127916OB-I00) project; Horizon Europe ACROSS Project (grant agreement No. 101097122).

References

[1] P. Alemany *et al.*, "Multi-stakeholder intent-based service management automation for 6g networks," in *Proc. of European Conference on Networks and Communications (EUCNC)*, Antwerp, Belgium, 2024.

[2] ——, "Management and enforcement of secured e2e network slices across transport domains," *Optical Fiber Technology*, vol. 73, p. 103010, 2022.

[3] ——, "Peer-to-peer blockchain-based nfv service platform for end-to-end network slice orchestration across multiple nfvi domains," in *IEEE 5G World Forum*, 2020.