Ortiz, Jordi; Sanchez-Iborra, Ramon; Bernabe, Jorge Bernal; Skarmeta, Antonio; Benzaid, Chafika; Taleb, Tarik; Alemany, Pol; Muñoz, Raul; Vilalta, Ricard; Gaber, Chrystel; Wary, Jean Philippe; Ayed, Dhouha; Bisson, Pascal; Christopoulou, Maria; Xilouris, George; De Oca, Edgardo Montes; Gür, Gürkan; Santinelli, Gianni; Lefebvre, Vincent; Pastor, Antonio; Lopez, Diego

INSPIRE-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks

Published in:
Proceedings of the 15th International Conference on Availability, Reliability and Security, ARES 2020

DOI:
10.1145/3407023.3409219

Published: 25/08/2020

Document Version
Publisher's PDF, also known as Version of record

INSPIRE-5Gplus: Intelligent Security and Pervasive Trust for 5G and Beyond Networks

Jordi Ortiz, Ramon Sanchez-Iborra, Jorge Bernal Bernabe, Antonio Skarmeta
University of Murcia
{jordi.ortiz,ramonsanchez, jorgebernal,skarmeta}@um.es

Chafika Benzaid, Tarik Taleb
Aalto University
{chafika.benzaid,tarik.taleb}@aalto.fi

Pol Alemany, Raul Muñoz, Ricard Vilalta
Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA)
{pol.alemany,raul.munoz,ricard.vilalta}@cttc.es

Chrystel Gaber, Jean-Philippe Wary
Orange
{chrystel.gaber,jeanphilippe.wary}@orange.com

Dhouha Ayed, Pascal Bisson
Thales
{dhouha.ayed,pascal.bisson}@thalesgroup.com

Maria Christopoulou, George Xilouris
NCSR Demokritos
{maria.christopoulou,xilouris}@iit.demokritos.gr

Edgardo Montes de Oca
Montimage
edgardo.montesdeoca@montimage.com

Gürkan Gür
Zurich University of Applied Sciences
gueu@zhaw.ch

Gianni Santinelli, Vincent Lefebvre
Solidshield
gianni,vincent@solidshield.com

Antonio Pastor, Diego Lopez
Telefonica R&D
{antonio.pastorperales,diego.r.lopez}@telefonica.com

ABSTRACT

The promise of disparate features envisioned by the 3GPP for 5G, such as offering enhanced Mobile Broadband connectivity while providing massive Machine Type Communications likely with very low data rates and maintaining Ultra Reliable Low Latency Communications requirements, create a very challenging environment for protecting the 5G networks themselves and associated assets. To overcome such complexity, future 5G networks must employ a very high degree of network and service management automation, which is a security challenge by itself as well as an opportunity for smarter and more efficient security functions. In this paper, we present the smart, trustworthy and liable 5G security platform being designed and developed in the INSPIRE-5Gplus[1] project. This platform takes advantage of new techniques such as Machine Learning (ML), Artificial Intelligence (AI), Distributed Ledger Technologies (DLT), network softwarization and Trusted Execution Environment (TEE) for closed-loop and end-to-end security management following a zero-touch model in 5G and Beyond 5G networks. To this end, we specifically elaborate on two key aspects of our platform, namely security management with Security Service Level Agreements (SSLAs) and liability management, in addition to the description of the overall architecture.

CCS CONCEPTS

• **Networks** → **Network architectures**; • **Security and privacy** → **Distributed systems security**; *Trusted computing*; *Virtualization and security*; **Mobile and wireless security**;

KEYWORDS

5G, Security, ZSM, Cognitive security, liability

[1]https://www.inspire-5gplus.eu

ARES 2020, August 25–28, 2020, Virtual Event, Ireland

ACM ISBN 978-1-4503-8833-7/20/08.
https://doi.org/10.1145/3407023.3409219

ACM Reference Format:
Jordi Ortiz, Ramon Sanchez-Iborra, Jorge Bernal Bernabe, Antonio Skarmeta, Chafika Benzaid, Tarik Taleb, Pol Alemany, Raul Muñoz, Ricard Vilalta, Chrystel Gaber, Jean-Philippe Wary, Dhouha Ayed, Pascal Bisson, Maria Christopoulou, George Xilouris, Edgardo Montes de Oca, Gürkan Gür, Gianni Santinelli, Vincent Lefebvre, and Antonio Pastor, Diego Lopez. 2020. INSPIRE-5Gplus: Intelligent Security and Pervasive Trust for 5G and Beyond Networks. In *The 15th International Conference on Availability, Reliability and Security (ARES 2020), August 25–28, 2020, Virtual Event, Ireland.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3407023.3409219

1 INTRODUCTION

5G networks will play a fundamental role in the implementation of pervasive and digital services with anytime-anywhere connectivity. They will enable a wide range of applications ranging from ubiquitous broadband connectivity to autonomous vehicles. Apparently, the utility and importance of communication systems and connected services have been corroborated in the current COVID-19 pandemic era. This role is expected to become more crucial for realization of future digital society with Beyond 5G systems, providing novel services such as holographic communications, Virtual Reality (VR), and fully-autonomous transportation infrastructures.

For secure and trustworthy 5G networks, there is a need to deliver more efficient and smarter end-to-end security while exploiting the emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), Distributed Ledger Technologies (DLT) and hardware-supported liability mechanisms [2]. This end-to-end paradigm needs to expand also over multiple verticals, markets and across multiple administrative domains. Furthermore, the security challenges are expected to be exacerbated in Beyond 5G networks with more automated and diverse service environments and infrastructure. Actually, full automation, while desirable as a way to enhancing capabilities and services, may introduce new vectors of attack by replicating small security issues, and thus magnifying their impact [6].

To address the security challenges and realize a well-founded security vision in 5G and Beyond networks, there are important technological aspects to be considered. The promising AI-driven Software-Defined Security (SD-SEC) is still in its infancy and there is a need to build smart SD-SEC solutions that cover the whole cybersecurity spectrum [7]. The smart, autonomic and closed-loop architecture should be seamlessly integrated into security management [14]. Unfortunately, zero-risk security can not be achieved even with these advances. Therefore, defining liability and responsibilities when the security breaches happen is also imperative to support confidence between parties. Policy management based on Security Service Level Agreements (SSLAs) in an important instrument to define and manage the commitments and security provisioning agreed between 5G entities. Additionally, liability management should be supported with manifest formalizations and hardware-based enablers such as Trusted Execution Environment (TEE) for trustworthy monitoring, execution and attestation. In fact, TEE is envisioned as a game-changer to provide integrity and confidentiality in virtualized environments even in the presence of malicious operators or even a malicious and vulnerable kernel [15].

This paper presents the work carried out by the INSPIRE-5Gplus project to realize this 5G and Beyond security vision as a smart, trustworthy and liable security platform. We describe our platform's overall architecture, highlighting the core components and functions. We also specifically elaborate on two key aspects of our system, namely security management with SSLAs and liability management. The remainder of this work is structured as follows. Section 2 presents an overview of the INSPIRE-5Gplus project. Section 3 explains the technical approach to realize the envisaged security platform, followed by the description of policy management via SSLAs and liability management in 4. Section 5 provides the rationale behind the integration of INSPIRE-5Gplus architecture into Zero-touch and Service Management (ZSM) architecture proposed by ETSI. Section 6 addresses liability in the context of liable and trustworthy future networks including 5G. Finally, conclusions are presented with a discussion on future work in Section 7.

2 INSPIRE-5GPLUS OVERVIEW

The INSPIRE-5Gplus approach proposes an step ahead in the 5G and beyond security vision by progressing 5G security and by devising a smart, trustworthy and liability-aware 5G security platform for future connected system (Figure 1). The developed system will contribute to the advancement of 5G security through the adoption of a set of emerging trends and technologies, such as ZSM, SD-SEC models, AI-based techniques and TEEs. In this line, INSPIRE-5Gplus platform enables that the provided security level is in conformance to legislations', verticals' and standards' security requirements. Besides, trust and liability is fostered through the integration of novel mechanisms supporting confidence between parties and compliance with regulation.

To achieve the aforementioned security vision, the INSPIRE-5Gplus platform relies on key emerging trends and technologies, including:

- A conceptual architecture for supporting zero-touch end-to-end smart network and service security management in 5G and beyond networks. This architecture leverages on flexibility of softwarization technologies (e.g., Software Defined Networks (SDN)/Network Function Virtualization (NFV)) and AI/ML techniques.
- SD-SEC orchestration and management that enforce and control security policies in real-time and adapt to dynamic changes in threats landscape and security requirements in 5G and beyond networks.
- Novel AI-driven security models, including AI-empowered Moving Target Defense (MTD) mechanisms, Root Cause Analysis (RCA) and Cyber Threat Intelligence (CTI) to empower smart security management with proactive defensive posture.
- Advanced mechanisms to foster trustworthiness of smart SD-SEC solutions in a multi-tenant/multi-domain setting by empowering trust in software components (e.g., VNFs) and AI/ML techniques. Trust in software components will be based on TEEs, new Digital Rights Management (DRM) approaches, novel AI-powered validation tools, and a new labelling scheme.
- New mechanisms to enforce liability of involved parties when security breaches occur and/or system fail, including smart contracts and potentially VNF package Manifest to define Trust Level Agreement (TLA), mechanisms to enable AI-based liability and RCA techniques.

Therefore, INSPIRE-5Gplus platform contributes to enforce security, trust and liability features, in smart and autonomous way, for 5G and beyond services. The security management in INSPIRE-5Gplus leverages on advanced and emerging enablers as detailed in the following sections.

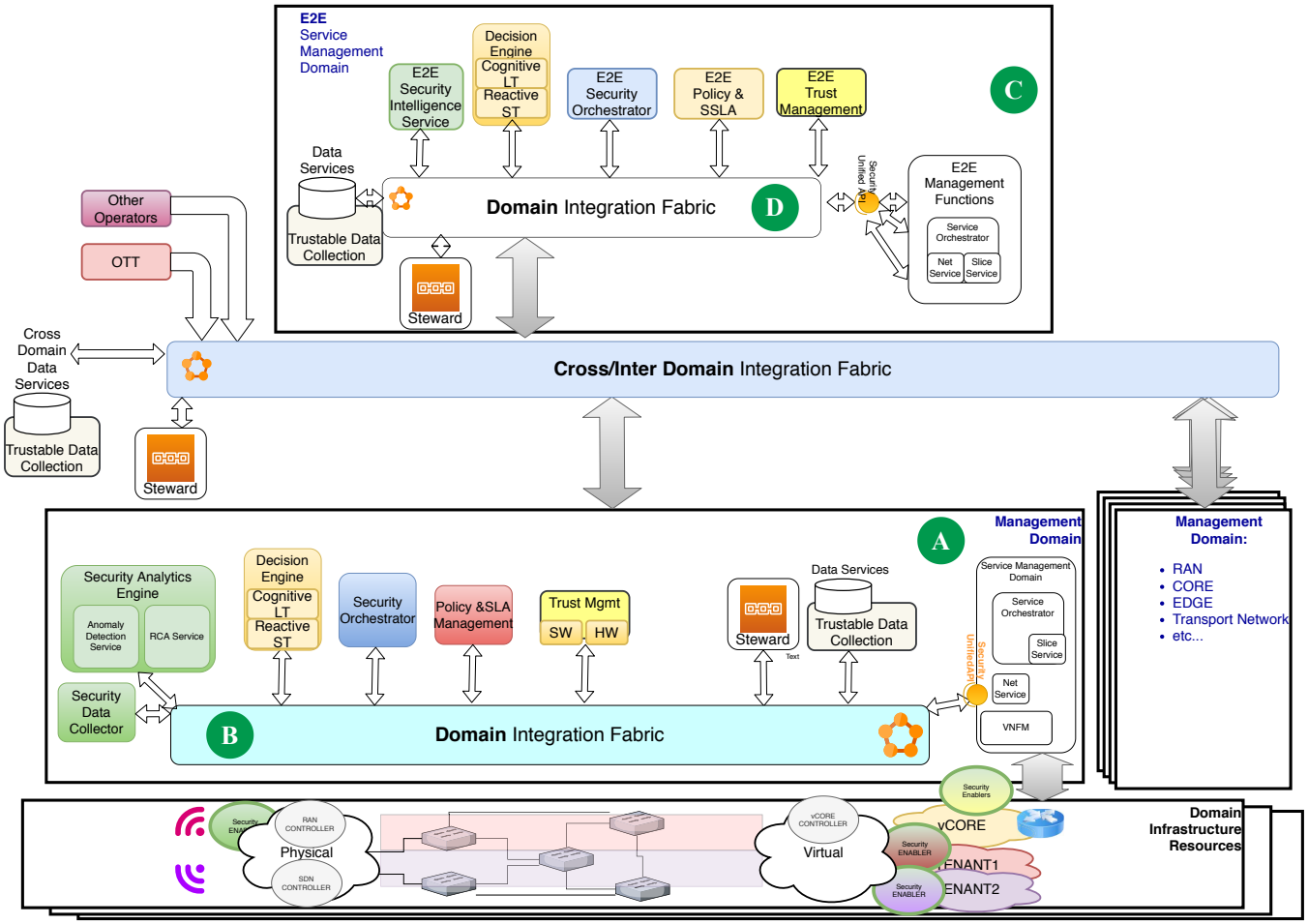

Figure 1: INSPIRE-5Gplus security oriented architecture.

3 TECHNICAL APPROACH

5G is being designed to address the diverse requirements of a multitude of use cases, including enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC) and massive Machine Type Communications (mMTC), by providing a unified and interoperable ecosystem of different and complementary technologies. The pervasive utility and importance of 5G networks necessitates a secure and trustworthy system to meet the stringent requirements that envisages use cases and services. As such, INSPIRE-5Gplus aspires to deliver an innovative platform for 5G security management by adopting advanced technology enablers, including Zero-touch end-to-end security management, Smart security management leveraging ML, as well as SD-SEC and trust.

As shown in Figure 1, INSPIRE-5Gplus has an End-To-End (E2E) security management architecture supporting the separation of security management concerns. In fact, the decoupling of the E2E security management domain from the other domains allows escaping from monolithic systems, reducing the overall system's complexity, and enabling the independent evolution of security management at both domain and cross-domain levels. Each security management domain, including the E2E domain, comprises a set of functional modules (e.g. security intelligence engine, security orchestrator, trust manager) that operate in an intelligent closed-loop way to provide SD-SEC orchestration and management, such as the one defined by Marin et al. [17] in the context of IETFs I2NSF working group to distribute keying material for IPSec tunneling from a central entity (I2NSF controller) in a coordinated way, that enforces and controls security policies of network resources and services in real-time. Each functional module provides a set of security management services that can be exposed inside the same domain or cross-domain using the domain integration fabric or the cross-domain integration fabric, respectively.

3.1 The Key Attributes of INSPIRE-5Gplus Approach

INSPIRE-5Gplus considers an E2E view for the network services as well as for the security architecture it brings forth. This is reflected in the multi-resolution nature of the design of the INSPIRE-5Gplus

security architecture: the security elements go beyond the micro-scale of domain-specific security and cover multi-domains (e.g. RAN, core, and transport) as shown in Figure 1. This is crucial since a robust and efficient security architecture should guarantee secure delivery of data and service in an E2E manner.

To enable a holistic security approach, the INSPIRE-5Gplus architecture also considers the technological factors since emerging technologies, such as NFV, SDN, Edge Computing and Network Slicing, introduce challenges and additional complexities on the way networks and services are deployed, managed and orchestrated. Software-driven and programmable networks lead to the creation of new business models and use cases with diverse and stringent requirements in terms of capacity, latency, reliability and availability. Conventional network operations require excessive human intervention when introducing new services or coping with operational errors. They introduce the need for trade-offs between reliability, scalability and efficiency. As a result, the shift towards full Automation of Network and Service Management and Operation (ANSMO) has become imperative for both Network Operators and Digital Service Providers [9]. To this end, ETSI established the Zero-touch and Service Management (ZSM) Industry Specification Group (ISG) in 2017, whose main objective is the definition of technical specifications on network and service automation [14]. "Zero-touch" refers to minimizing or eliminating human intervention when managing the lifecycle of networks and services across the Radio Access, Transport, Core, and Cloud domains [5]. The main target is not removing completely humans from operations or reducing costs, but to introduce agility in adhering to Service Level Agreements (SLAs), while meeting the requirements of new services [4] by supporting human decisions.

The smart and flexible security architecture is realized via the integration of novel and emerging enabler technologies, including AI/ML, TEE and DLT. AI, supported by ML and Big Data analytic techniques, plays a pivotal role in empowering autonomic cyber-capabilities (e.g. self-protection, self-healing). Indeed, AI has the power of unveiling hidden patterns from a large-scale and time-varying data, while providing faster and accurate decisions. INSPIRE-5Gplus leverages on emerging AI/ML techniques to empower key security functions, such as intelligent security enforcement, efficient prediction of security anomalies and efficient decisions on mitigation mechanisms to deploy. Furthermore, for trusted data sharing, it utilizes blockchains as part of data collection functions. TEEs are hardware-based solutions providing data and code integrity and confidentiality even in high adversary conditions. INSPIRE-5Gplus takes advantage of TEE to offer a trusted environment to execute critical software components in a multi-tenant/multi-domain setting, allowing to address introspection issue and foster both VNF's security and trust.

In addition to a multi-domain design, the INSPIRE-5Gplus security architecture is essentially extensible to multi-operator and OTT environments by considering their security threats and requirements. Although it is developed with a focus on single operator environment needs, the inter-domain fabric provides an inherent capability for security management among disparate networks, as shown in Figure 1. In the following subsections, we detail the INSPIRE-5Gplus architecture at the intra-domain and then inter-domain level with concise descriptions of key modules and functions.

3.2 Intra-domain Architectural Approach

In INSPIRE-5Gplus, the nomenclature "domain" refers to network constituents such as radio access network, Mobile Edge Computing (MEC) environment and core network, i.e. the decked representation on the right side of the Figure 1. Each management domain includes the closed-loop security functions in the architecture (A in Figure 1). The domain integration fabric is the communication substrate for messaging based on extensible interfaces defined according to security requirements and scenarios adopted in the project (B in Figure 1).

Security data collector uses telemetry and probing to collect security related data from a domain.

Trustable data collection uses permissioned blockchains for trusted multiparty data collection. This function provides data service to other security related functions via the integration fabric. The use of stewards is envisioned, these nodes are capable of participation in the validation process and help maintaining the DLT.

3.2.1 Smart security enablers. INSPIRE-5Gplus relies on smart security enablers to implement the ZSM based security architecture. Therefore, the domain specific implementation includes:

The Security Analytics Engine (SAE): The main function of SAE is to derive insights and predictions on the domain's conditions based on data collected in the specific domain or even other domains. As shown in Figure 1, in the context of INSPIRE-5Gplus, SAE provides the Anomaly Detection and RCA services, although the set of offered services can be extended in case the need arises. The Anomaly Detection service identifies patterns in data or behaviour not conforming to the ones expected, which are usually designated as outliers or anomalies. The service detects anomalous conditions which may correspond to security incidents or malfunctions and utilizes data aggregated from the managed entities of the domain with regards to their performance, usage, configuration and status. The RCA service identifies the cause of the observed incidents by analyzing and correlating data collected by the Anomaly Detection service or other services. One of the ambitions of INSPIRE-5Gplus is to develop RCA techniques based on network traffic analytics, ML techniques, remote attestation, path proof mechanisms and model-based root cause algorithms for identifying the cause and determining responsibilities when security breaches occur.

Security Intelligence Engine (SIE): SIE is responsible for decision making and action planning as part of the intelligent closed-loop automation formed inside a security management domain, as defined in [14]. SIE services include assessment and management of deployed AI models and their training data in order to ensure the operational and up-to-date state, despite changes in incoming data and domain network conditions. These evolving models allow more adaptive and exploratory security functions than conventional reactionary models. Decision making takes place based on data collected by SAE and the Security Data Collector or other domain specific services deemed necessary. SIE also provides services pertaining to action planning, including the management of lifecycle of services of the specific domain through automated

work-flows and configuring of domain managed entities and services. The cognitive aspect of this engine provides more extensible security provisioning beyond pre-defined action portfolios.

These functions rely on the **Security Data Collector** for obtaining the data that is needed for the analysis and training/inference functions.

3.2.2 Security orchestration. The architecture is endowed with a policy-based security orchestrator in charge of driving the security management in 5G and beyond networks, by interacting, through the integration fabric, with the different SDN Controllers, NFV controllers and management security services. The orchestrator will enforce proactively or reactively the security policies through the allocation, chaining and configuration of dedicated virtual network security functions (VSF) such as vFirewall, vChannelProtection, virtual Intrussion Detection System (vIDS), virtual Authentication, Authorization and Accounting (vAAA) and vProxy. The security orchestration will be fed by the evolving system model, the trust and reputations indicators coming from the Trust Management component, as well as the conclusions and evolved plans inferred by the Security Intelligence engine. This cognitive behaviour will provide self-healing and self-protection capabilities to the entire managed system, allowing the orchestrator to react automatically according to the actual context, and trigger the countermeasures to mitigate ongoing attacks or threats in the 5G network. This reactions encompass, among other, applying security policies which will control the traffic (e.g. by dropping or diverting it) through the SDN controllers; and deploying, decommissioning, re-configuring or migrating the VSFs.

3.2.3 Policy and SSLA management. SSLAs represent the security policies in terms of commitments and requirements, and thus enable their management in a multi-party environment for maintaining a certain Level of Security (LoS). The Policy and SSLA management function in INSPIRE-5Gplus architecture provides specification and monitoring capabilities to define SSLAs based on policies and assess them in real-time in cooperation with other INSPIRE-5Gplus functions. Network slicing oriented security policies and SSLA is a specific use-case addressed in the architecture. The policy and SSLA management are presented in more detail in Section 4.

3.2.4 Trust management (HW, SW). INSPIRE-5Gplus uses software and hardware enablers for trust management for domain elements. It provides risk analysis framework that enables to supervise risks in complex and distributed systems in relation trust. This function uses risk analysis techniques, specifically Risk Assessment Graphs (RAGs) as a graph-based model for risk, which is adaptable to the system evolution or temporal dynamicity. It models mathematical propagation of impacts and risk analysis between components and allows dynamic representation and re-evaluation of security exposure of the network and service infrastructure. Moreover, a Trust and Reputation Management System (TRM) subfunction assigns reputation values to management entities in the 5G softwarised networks based on the impact of their actions on the network. This impact is measured with anomaly detection algorithms able to detect network state deviations impacting the resilience level.

3.3 Inter-domain Architectural Approach

E2E service management domain entails security functions providing this management across the different domains (C in Figure 1). For achieving this, INSPIRE-5Gplus builds on an inter-domain integration fabric (D in Figure 1). This lightweight communication bus defines message exchange interfaces, as well as message flows, at a higher level compared to the domain integration fabric. There are also architectural elements which reside in cross-domain space, namely data repositories which can serve different domains. This inter-domain fabric also provides an integration interface with other operators and over-the-top (OTT) providers.

The functions in this domain act as counterparts of the corresponding ones in the domain scope. The data from a given management domain, that needs to be shared with the cross-domain fabric, will be collected and distributed by a special distribution function using trustable data collection based on blockchain technology. This function will interact with the domain-resident functions to provide security orchestration at E2E level.

4 INSPIRE-5GPLUS POLICY MANAGEMENT BASED ON SSLAS

SSLAs provide the means to specify the security requirements or policies and assessing or enforcing their fulfillment to obtain the desired Quality of Service (QoS) from a Security point of view. They can be selected and applied specifying the required security properties of the network slices that will be deployed or they can be used for assessing the 5G services during operation.

4.1 Real-time SSLAs monitoring and enforcement

SSLA monitoring relies on the specification of rules that can represent what should happen (security properties) or what should not happen (attacks anomalies, vulnerabilities) as well as the definition of reaction mechanisms when threats are detected and how they should be activated (e.g. manually by the operator or automatically by interacting with the orchestrators and controllers). Instead of the traditional SLAs dealing with network performance parameters (i.e. bandwidth consumed or the latency offered by a service), SSLAs consider security parameters such as the correct functioning of the security services (e.g. the frequency of a security analysis such as vulnerability scanning, delay in applying patches, time it takes to switch instances), the integrity of the information (e.g. an unauthorized actor modifies a certain content), and the detection and mitigation of unwanted network traffic situations (e.g. Distributed Denial of Service attacks, resilience to an attack meaning that the service continues with a certain quality).

4.2 SSLAs for Network Slicing

Each slice provided by the INSPIRE-5Gplus Framework has to be defined with respect to the SSLAs that specifies the security properties and guarantees that are needed.

INSPIRE-5Gplus framework manages the whole SSLA lifecycle in a slice: a) it collects security requirements from verticals/end-users; b) deploys the security controls that are needed to enforce the agreed SSLAs by enriching the services of SPs or configuring

them; c) monitors in real-time the fulfillment of SSLAs; d) detects violations in the security provisioning level based on an analytics engine and notifies both end-users and Service Providers; and, e) reacts in real-time to adapt the provided level of security or to apply proper countermeasures.

In order to automate the SSLA life cycle in a slice, a machine readable format for SSLAs is adopted based on the SPECS SSLA model that has been extended to support slicing. This model is based on a WS-Agreement XML schema extended with security-related information allowing to specify the following sections in a slice term description:

- Slice resource providers that describes the available infrastructure of the resource providers (e.g. appliances, networks);
- Security capabilities required in a slice. A capability is defined as a set of security controls. In our case, the NIST's Control Framework is used to specify these security controls;
- Security Metrics referenced in the slice service properties and used to define Security Service Level Objectives (SLOs) in the guarantee terms section. A metric specification includes information about it and also information to process the SLOs, such as the metric name and definition, its scale of measurement, and the expressions used to compute its value.

4.3 Network Slicing SSLAs management

One of the enablers under discussion in the INSPIRE-5Gplus context is a SSLA Manager for Network Slices. Using the previously presented SSLA model -i.e. Slice resource providers, Slice required security capabilities and security metrics-, the enabler must ensure that the SSLAs associated to the slice are accomplished and if they are not, to apply the correct solution.

This enabler will control the complete SSLAs lifecycle as long as the slices are running, so its responsibilities are:

- Based on the vertical's request, to associate the SSLA(s) selected with the chosen slice when the last one is requested to be deployed.
- Once the slice is instantiated, the deployment of all the Security Functions (SFs) -i.e. probes and security controls- to have the proper context elements that will gather the data from the slice and its components (slice-subnets) for the monitoring action.
- Slice monitoring in order to determine whether the QoS from a security point of view is fulfilled by the slice as a unit and by each slice internal component.
- While the slice is running and being monitored, it must try to apply the best of the available policies to resolve to each possible SSLA violation that may occur.

5 BUILDING SECURITY ON TOP OF ETSI'S ZSM

INSPIRE-5Gplus defines its zero-touch security approach to network and service automation based on ETSI's ZSM framework [14]. The ZSM framework's reference architecture is designed to empower full automated network and service management in multi-domain environments that include operations across legal operational boundaries [6]. As illustrated in Figure 2, the ZSM architecture comprises multiple management domains (MDs) including E2E service MD, intra- and cross-domain integration fabrics, and cross-domain data services. Each MD is responsible for intelligent automation of management and orchestration of resources and services within its scope. The E2E service MD is a special MD that manages E2E, customer-facing services across multiple administrative domains. It is worth mentioning that the decoupling of MDs from the service MD reduces the overall system's complexity and allows independent evolution of domains and E2E management operations. Each MD, including the E2E service MD, encompasses several management functions grouped into logical groups (e.g., domain collection services, domain analytics services, domain intelligence services, domain control services, and domain orchestration services) and supplies a set of management services via service interfaces. The services are provided and consumed through either the intra-domain integration fabric (for services local to a domain) or the cross-domain integration fabric (for services that can be exposed cross-domain). The Cross-domain Data Services facilitate access to data and its cross-domain exposure. The data can be used by intelligence services to enable AI-based closed-loop automation at domain-level and cross-domain.

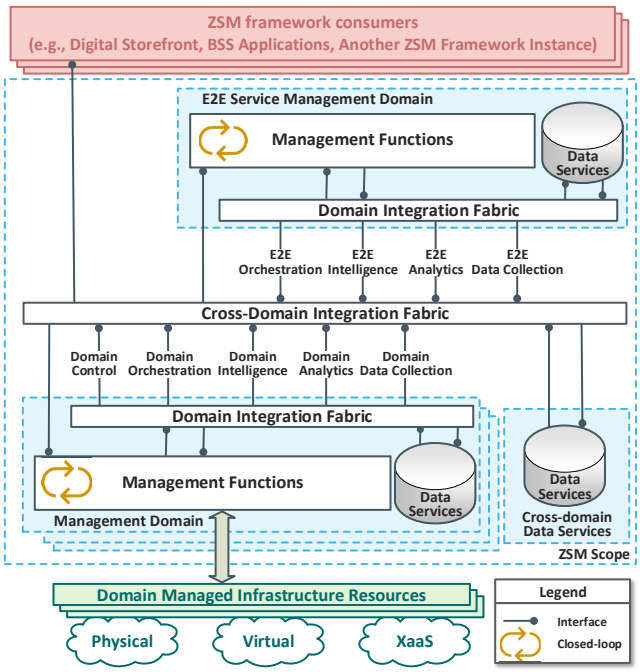

Figure 2: The ZSM Reference Architecture [6].

In INSPIRE-5Gplus, the ZSM framework architecture is extended by adding security modules that integrate the End-to-End service management domain level and each service management domain level so that the ZSM concept can span over multiple domains in parallel.

Working beyond 5G to provide liable end-to-end 5G services means considering an inter-operator and cross-domain environment. ZSM architecture can be extended by integrating and relying on closed-loop automation. The INSPIRE-5Gplus approach adopts

existing closed-loops concepts to allow the definition of specific security oriented closed-loops.

End-to-End operations can also involve several operators where each of them can be seen as a management domain. This greatly simplifies the technical actions and allows to smoothly map the ZSM concept into 5G. Nonetheless, multi-operator environments depend on political issues that complicate the straightforward mapping between architectures. As such, considering ZSM end-to-end management domain as a single operator brings the desired independence of how the ZSM architecture is finally implemented by an operator. To maintain the capability of providing multi-operator end-to-end secure 5G services requires defining the interfaces that allow the interaction between the operators or even other OTT providers and third parties. From INSPIRE-5Gplus' point of view, these interactions, interfaces and service producer and consumers need to be attached to the cross-domain integration fabric (as shown in Figure 1. This interaction is foreseen to be defined and provided through SSLAs, giving the operators the freedom on how to finally implement the enforcement of the requested SSLAs.

Distributed liability is highly tied to the concept of Distributed Ledger Technology (DLT) and how audition of chain modifications can be enforced. These DLTs may be operated by Stewards[13], which are nodes capable of participating in the validation process and maintaining the DLT providing stability aligned to the operator interests. Some security functions may need a higher degree of liability on the data being consumed by the Data Services at any level (domain, cross-domain or end-to-end) from the ZSM architecture. Therefore, INSPIRE-5Gplus defines the Trustable Data Collection as the Data produced and processed or analysed by the security architecture.

The criticity and vectors of attack on ZSM are introduced and exposed in section 6.2.1 to provide the relation of Liability and ZSM.

6 LIABILITY

As zero-risk security cannot be achieved, defining liability and responsibilities when security breaches occur is of paramount importance to support confidence between parties and compliance with regulation.

Following the example of the "Y2k Act" [20] in the US, one can assume that legal and financial responsibility in 5G contexts will have to be distributed proportionately among any liable companies and claimants will need solutions to gather proofs of any malfunction or wrongdoing. However, with 5G worldwide deployment, multiple stakeholders with different requirements and security levels will interact, and complex interconnections of hardware, software, plane levels (e.g. data or control planes) will defy the appreciation of the stakeholder's liabilities.

INSPIRE-5Gplus aims at defining new mechanisms to allow liable end-to-end delivery of 5G services, defining and enforcing liabilities as well as detecting the cases of security breaches. This section details how INSPIRE-5Gplus plans to leverage manifests and TEEs as cornerstones of these mechanisms.

6.1 Liabilities formalization with manifests

Opening up infrastructure to third parties, such as IoT devices or VNF providers, outside of direct and bilateral contractual relationships raises questions regarding the responsibilities of the infrastructure operator. Indeed, while it has no prior trust relationship with these third parties and no control or guarantees over the third-party components that will be loaded into its infrastructure, the operator always bears the cost, impact and image of the risks towards his customers and users.

This problem, already encountered for mobile devices [10] and web services [11], can be solved by formalizing mutual obligations and benefits through a manifest[12].

The INSPIRE-5Gplus manifest shall generalize the notion of 5G components to include VNFs, IoT or physical equipment, with or without hosting capacities, and leverage existing descriptions such as MUD profiles[16], SUIT manifests [18] or NFV manifests[1].

As depicted in figure 3, the INSPIRE-5Gplus manifest shall define and assign different levels of responsibilities. It shall be modular and follow the 5G infrastructure component throughout its lifecycle:

- **Manufacturing**. The manufacturer builds the component by using building blocks provided by software editors, hardware manufacturers or Service Providers. The manufacturer provides a first version of the manifest based on the description of features and preliminary usage recommendations,
- **Testing**. The validator tests the component, evaluates risks and compliance to applicable requirements. Based on his observations, the validator can add properties or describe controls or requirements, called usage constraints, that need to be enforced by the infrastructure operator to guarantee normal functioning or avoid exploitation of a known vulnerability,
- **Listing**. The infrastructure operator lists the component in its Catalog and may perform additional tests. It identifies operation constraints, similar to usage constraints, except that they express conditions to comply with specific infrastructure requirements, company policy or local regulation and are not available to other stakeholders,
- **Deploying**. The infrastructure operator uses the manifest to decide whether to use the Component in a particular subset of its infrastructure and under which conditions,
- **Exploiting**. The infrastructure operator uses the Manifest to decide whether and how to observe and manage the Component. It can also be used as a baseline to define expected behavior for monitoring.

Thus, each stakeholder is able to express its commitments and expectations from other parties. In turn, this will help 5G infrastructure operators to formalize its risks and take decisions in order to manage the level of risk of its infrastructure. A perspective of this work is to propose organizational and technical mechanisms that allow infrastructure operators to publish their extensions to manifests and experts or risk managers from authorized stakeholders to share information.

6.2 Secured slicing main threats and security assets

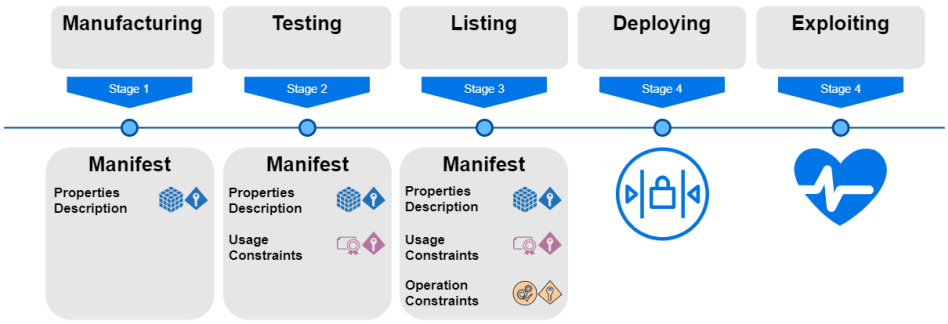

Figure 3: Lifecycle of a 5G component and its manifest

6.2.1 Threats on slices and ZSM criticity. Security threats on a slice are listed below (generic, basic and non exhaustive theats):

- User or service impersonation.
- DoS or degradation of quality of service.
- Data integrity and confidentiality.
- Slice isolation loss (cross-slice data transfer-inference)
- Non repudiation and attribution

Regarding the attack modus operandi, they are either mounted from a payload (Container or Virtual Machine (VM) embedded application) or from a poor security parameter configuration, typically exposing the processing memory to malicious eyes (on the cloud-based machine). Attacks can exploit a vulnerability from one of the executed applications (VNF or CNF) or exploit system configuration vulnerabilities introduced by weak policy enforcement. ETSI ZSM is designed with a motivation of delivering secured slices (end-to-end single domain or cross domain slice). To reach that goal, ZSM orchestrates all resources and security functions where they must be implemented.As stated by ETSI ZSM working group, automatic management function must feature the highest trustworthiness as its decisions impact the security of all slices in any of the key threats given above.

There are three main core security assets for secure slicing: TEE, Trusted Processing Modules and kernel-level virtualization techniques. These solutions bring different security guaranties and main operational features and can be used either independently or in combination. We will specifically focus on how TEE can be used to bring more security above the other two.

6.2.2 TEE and secure slicing. TEE concept is to deliver isolation to a process (application and its data) against any other process including the operating system or any other kernel modules. In fact, the original goal of processor manufacturers with TEE is to deliver full trustfulness to cloud processing to swallow the legitimate security concerns when transferring critical processing and data to an external party. TEE creates fully isolated silos that no one can violate, including high privilege supervisors. TEE could be viewed as a key asset of slice isolation, as it delivers isolation to the slice process. In fact, various practical reasons (TEE market fragmentation, workflow and performance) and even a security motivation coincide to refrain using TEE for sheltering complete slices. Conversely, it shall be smartly used on a restricted safe code perimeter, typically dealing with slice security instead. Slice VSFs are good targets for being processed in part ideally in TEE. To the best of our knowledge and as of today, the ideal balance and efficient modus operandi to leverage TEE in SDN networking is still be defined today (as in other domains).

6.2.3 Remote attestation by TPM. Remote attestation is a technique that has gain momentum in Telco NFV environment because it generates trust and liability for the NFVI and VNFs. Indeed, this technology has been standardized by ETSI NFV-SEC group as a clear statement of intentions to be adopted. Remote attestation is another strong asset for secure slicing as it makes certain that deployment software (including kernel) are as expected. It is in fact imperative step to take for secure slicing. Remote attestation leverages Trusted Processing Modules (TPM) separate chipsets, dedicated for checking software integrity and capable to create a chain of trust of any software modules, successively loaded then executed.TPM-based Remote Attestation is an essential pillar to construct software trust in ZSM.TPM integrity however does not handle memory footprint of the process (but only cold storage file). Introspection attacks subverting in-memory process integrity during run time are possible.
This security threat is where TEE brings an extra security edge.

6.2.4 Kernel level Isolation by virtualization. The future of cloud infrastructure will leverage either the lightweight hardware-level virtualization (aka, lightweight virtual machine which embarks one single bare minimal guest kernel) or operating system-level virtualization (aka, containers). Both technologies are backed by intense researches and industrial deployments by I.T leaders (Intel, IBM, Amazon, Google among others) resulting from internal developments and first running deployments. The relative strengths on the two techniques are accepted as follows: Virtual machines bring higher process isolation and deployment flexibility but at higher memory costs (i.e., replication of different feature-rich guest operating systems in each VM) and are slower to start. However, none of these techniques protect against a malicious operator with root access credentials. This is where TEE could bring an extra security but with their own difficulties and limitations as stated below. A co-lateral area of research is to protect the system calls (container to host) or hyper-calls (virtual machine to hypervisor) filtering policy enforcement module. Enforcing the policy management inside a TEE is the ultimate security scheme.

6.2.5 Workflow difficulties in using TEE. TEE are undeniably strong security enablers but the obstacles to use them are several and serious. They relate to the performance overhead, effort to setup, compilation requirement and source level code change requirement (for the emblematic Intel SGX at least). More importantly, they are not cross compatible. Typically, the TEE-protected VNF cloud deployment becomes troublesome as the VNF will run only on a special type of processor. Abstraction layer frameworks break this fragmentation with a unique API based setup. In the meantime, easier setup frameworks targeting specifically Intel SGX have emerged. Simplification and abstraction come with higher performance impact and lower security as distorting architectural vendor designs. At INSPIRE-5Gplus, we will work on the workflow aspect as we consider that this is a crucial aspect for adoption. We do this without distorting Intel's small size Trusted Computing Basis (i.e., the size of code and data inserted in the TEE) concept and which radically diverts from AMD complete V.M insertion (i.e., extra large TCB).

6.2.6 Liability shortcomings by use of TEE. An important aspect to keep in mind with TEE is that it does not cope with vulnerabilities. A vulnerable code inside a TEE is still 1:1 vulnerable inside or outside the TEE. TEE is the best place to be for exploits as they will not reveal with binary scanners. This backside can only be minimized by inserting there safe code only. No formal proof (if it would bring a trust guaranty) has been delivered to any system code dealing with TEE. However, this system code had obviously been carefully specified and crafted by processor vendor security architect. As TEE contain any selected application code, the best practice is to limit the code size. Hence, low TCB (i.e., code size) scheme as developed with Intel SGX is interesting. Conversely, one should look carefully new easier TEE setup frameworks which tend to expand the TCB dramatically.

6.2.7 Non repudiation and attribution. Slice creation and definition requires secure interactions between multiple actors from (potentially) multiple administrative domains (e.g., RAN, 5G core or Edge) to provide vertical oriented activities over public and non-public networks. Those interactions and the actions derivated from them need to be performed by a verifiable and trustable orchestration and control stack that oversees request-response messages between actors and components. In order to have some liability of the slice implementation, non-repudiation and attribution mechanisms need to be defined and integrated into the platform for those messages. The non-repudiation principle is the ability of demonstrating that the message has been originated by its trustworthy sender, therefore creating a consistent temporal line when relating them to previous messages of the same conversation. That ability provides with the means for external verification that in turn leads to system auditability and liability. One promising technique is using permissioned DLTs to provide a trusted store for the trusted message interaction history.

6.2.8 Path proofs. If we think in terms of dynamicity of 5G resources allocation, multiples slices per user or per service and multiple distributed locations, then it will be necessary to provide trust on implementation of the service function chain (SFC) that connect multiple intermediate nodes (some of them out of the control of the operator). Proof of the traffic paths can be defined as a complementary to the TEE based isolation technology, securing that the routing paths in the data plane cross critical nodes within the SFC (e.g. a firewall). To mitigate this problem a new standard definition, proof-of-transit technique [8], is being developed as part of the IETF to verify that a packet is traversing the list of nodes predefined. The steps described in the IETF's PoT working group can be sumarized as follows. A centralize entity (i.e. INSPIRE-5Gplus security orchestrator) create a secret and use the Shamir Secret Sharing (SSS) cryptographic method to create and a set of shares of the secret. The property of this mechanism is that the original secret can only be reconstructed only if all the shared are combined together. The orchestrator prepares a set of metadata based on previous algorithm and distribute to all nodes involved in the data path. The first node designated in the path, when receive a packet, add a header based on the metadata received, before delivering the packet. Each node in the data path make verifications of incoming packets, alter the metadata to increment the shared information and forward the packet. The last node in the path, make the final verification and deliver the packet without metadata. This mechanism can be enhanced to verify the order of the nodes being traversed with additional techniques[3].

6.3 INSPIRE-5Gplus TEE special focus

For the avoidance of confusion, TEE do not remove software vulnerabilities which are still exploitable, even if the code is within the TEE. Other points that need to be stressed about TEE follow:

- Remote code attestation is the baseline security for ZSM, bringing a guarantee that at least, the loaded code (i.e., CNF, VNF) corresponds to what it is supposed to be. It is not enough however to ensure that running code has not been tampered (locally, through code introspection) once duly loaded, after attestation verification check and through process memory access and violation. At INSPIRE-5Gplus, we will consider bringing a zero-touch integrity solution that checks any application during run time. For that, we are considering the interesting work of [19] that leverages Intel SGX and a distant remote attestation server. Our approach will be focused on a stand alone (local) layout as a loss of transmission link to the remote verification server could become an attack path.
- Virtualization technique domain is plenty of competing emerging technologies for hardening containers and virtual machines, solving the equation of isolation versus overhead. System calls between the payload and the host is where maximum control shall be placed. Security policy monitor can possibly be tampered or abused. At INSPIRE-5Gplus, we will devise (syscalls/hypercalls) security policy monitor under the shielding of Trusted Execution.
- ZSM centralized management functions highly expose new security risks. These functions whether based on ML or traditional empirical status analysis decision taking, must be protected against all types of attacks, including introspection by a high adversary malicious maintenance operator with root access on the machine. The probability of suffering that

kind of attack worsens with VM and container escape derived from kernel-land vulneravilities among others. Against all of these introspection attacks (either directly triggered from the host or from a malicious payload), TEE are efficient barriers. Guarding ZSM function inside a TEE is a question of design, by a security architect which shall identify what part deserve more security and at which acceptable performance impact. This work can be done with or without ML-based orchestration. Hardening ML is a concern of many and addressed at ETSI Secure AI working group. This matter will be duly considered in INSPIRE-5Gplus.

7 CONCLUSIONS

The architecture presented is focused in introducing zero-touch secure operations into 5G leveraging on novel techniques such as AI and, TEE or DLT. The ANSMO like management of such an automated architecture justifies the integration of security functions and components inside ZSM and the use of SSLAs to extend the traditional concept securing and hardening the QoS provisioning promised by 5G. There is no bullet-proof solution, therefore liability is mandatory to enforce obligations and pursue outlawers.

INSPIRE-5Gplus is now on the verge of starting the integration of the different enablers described in previous sections and will continue evolving the architecture and deepening into the solutions aforementioned and yet to come.

ACKNOWLEDGMENTS

The research leading to these results received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 871808 (5G PPP project INSPIRE-5Gplus). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

REFERENCES

[1] [n. d.]. ETSI GS NFV-SOL007 Network Service Descriptor File Structure Specification. ([n. d.]). https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/007/02.06.01_60/gs_NFV-SOL007v020601p.pdf

[2] 5G PPP Security Work Group. 2017. *5G PPP Phase 1 Security Landscape.* Technical Report. 5G PPP Security WG. 1–68 pages. https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdfhttps://5g-ppp.eu/new-security-group-5g-ppp-white-paper-phase-1-security-landscape/

[3] A. Aguado, D. R. Lopez, A. Pastor, V. Lopez, J. P. Brito, M. Peev, A. Poppe, and V. Martin. 2020. Quantum cryptography networks in support of path verification in service function chains. *IEEE/OSA Journal of Optical Communications and Networking* 12, 4 (2020), B9–B19.

[4] Silvia Lins Allan Vidal, Pedro Henrique Gomes. 2018. Next stop: Zero-touch automation standardization. https://www.ericsson.com/en/blog/2018/11/next-stop-zero-touch-automation-standardization. (2018). [Online; accessed 04-June-2020].

[5] Chafika Benzaid and Tarik Taleb. 2020. AI-driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions. *IEEE Network* 34, 2 (2020), 186–194.

[6] C. Benzaid and T. Taleb. 2020. ZSM Security: Threat Surface and Best Practices. *IEEE Network Magazine* 34, 3 (May/June 2020), 124 – 133.

[7] Gregory Blanc, Nizar Kheir, Dhouha Ayed, Vincent Lefebvre, Edgardo Montes de Oca, and Pascal Bisson. 2018. Towards a 5G Security Architecture. (2018), 1–8. https://doi.org/10.1145/3230833.3233251

[8] Frank Brockners, Shwetha Bhandari, Tal Mizrahi, Sashank Dara, and Stephen Youell. 2020. *Proof of Transit.* Internet-Draft draft-ietf-sfc-proof-of-transit-05. Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/draft-ietf-sfc-proof-of-transit-05 Work in Progress.

[9] China Unicom, Deutsche Telekom, DOCOMO, NTT, Sprint, Telefonica). 2017. Zero-touch Network and Service Management - Introductory White Paper . ZSM Operator white paper. (2017). https://portal.etsi.org/Portals/0/TBpages/ZSM/Docs/ZSM%20Operator%20white%20paper.pdf?ver=2017-12-07-142037-453 Accessed on 25.05.2020.

[10] G. Costa, N. Dragoni, A. Lazouski, F. Martinelli, F. Massacci, and I. Matteucci. 2010. Extending Security-by-Contract with Quantitative Trust on Mobile Devices. In *2010 International Conference on Complex, Intelligent and Software Intensive Systems.* 872–877.

[11] Nicola Dragoni and Fabio Massacci. 2007. Security-by-contract for web services. *SWS* (2007).

[12] N. Dragoni, F. Massacci, C. Schaefer, T. Walter, and E. Vetillard. 2007. A Security-by-Contract Architecture for Pervasive Services. In *Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2007).* 49–54.

[13] P. Dunphy and F. A. P. Petitcolas. 2018. A First Look at Identity Management Schemes on the Blockchain. *IEEE Security Privacy* 16, 4 (2018), 20–29.

[14] ETSI INDUSTRY SPECIFICATION GROUP (ISG) ZERO TOUCH NETWORK AND SERVICE MANAGEMENT (ZSM). 2019. Zero-touch network and Service Management (ZSM); Reference Architecture . ETSI GS ZSM 002 V1.1.1. (2019). https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf Accessed on 24.05.2020.

[15] European Telecommunications Standards Institute. 2013. Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV. 1, GS~NFV~003~–~V1.1.1 (2013), 1–13. https://doi.org/DGS/NFV-0011

[16] Eliot Lear, Ralph Droms, and Dan Romascanu. 2019. RFC 8520 - Manufacturer Usage Description Specification. https://tools.ietf.org/html/rfc8520, last visited on 31 07 2019. (March 2019). https://tools.ietf.org/html/rfc8520#page-5

[17] Rafael Lopez, Gabriel Lopez-Millan, and Fernando Pereniguez-Garcia. 2020. *Software-Defined Networking (SDN)-based IPsec Flow Protection.* Internet-Draft draft-ietf-i2nsf-sdn-ipsec-flow-protection-08. IETF Secretariat. http://www.ietf.org/internet-drafts/draft-ietf-i2nsf-sdn-ipsec-flow-protection-08.txt http://www.ietf.org/internet-drafts/draft-ietf-i2nsf-sdn-ipsec-flow-protection-08.txt.

[18] B. Moran, H. Tschofenig, and H. Birkholz. 2019. SUIT CBOR manifest serialisation format (draft). (July 2019). https://www.ietf.org/archive/id/draft-moran-suit-manifest-05.txt

[19] M. Morbitzer. 2019. Scanclave: Verifying Application Runtime Integrity in Untrusted Environments. *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (2019).

[20] Dylan Mulvin. 2020. The legal and political battles of Y2K. *IEEE Annals of the History of Computing* (2020).