European Commission

5G PPP

5G PPP Phase1 Security Landscape

Produced by the 5G PPP Security WG

Table of Contents

Glossary

3P	3rd party
3rd Generation Mobile System	3rd Generation Mobile System
AAA	Authentication, Authorization and Accounting
AN	Access Network
APDoS	Advanced Persistent Denial of Service
API	Application Programming Interface
BGP-LS	Border Gateway Protocol-Link State
C&C	Command & Control
CA	Certification Authority
CAL	Converged Aggregation Levels
CN	Core Network
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DevOps	Software DEVelopment and information technology OPerationS
DPI	Deep Packet Inspection
E2E	End to End
ECA	Event, Condition and Action
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GSMA	GSM Association
GUI	Graphical User Interface
HN	Home Network
HW	Hardware
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IM	Identity Module
IMSI	International Mobile Subscriber Identity
InP	Infrastructure Provider
IP	Internet Protocol
IPS	Intrusion Prevention System
IoT	Internet of Things
ITU	International Telecommunication Union
KPI	Key Performance Indicator
LI	Lawful Interception
M2M	Machine-to-machine
MANO	Management and Orchestration
ME	Mobile Equipment
MEC	Mobile Edge Computing
MME	Mobile Management Entity
MNO	Mobile Network Operator

MOCN	Multi-operator Core Network
MTC	Machine-type Communication
NFV	Network Function Virtualization
NGMN	Next Generation Mobile Networks
NSSA	Network Security Situational Awareness
NTD	Network Topology Database
ONF	Open Networking Foundation
OSS/BSS	Operations Support System/Business Support System
PCE	Path Computation Element
PDN	Packet Data Network
PGW	Packet Data Network Gateway
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PNF	Physical Network Function
PulSAR	Proactive security analysis and remediation
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
SA	Situational Awareness
SCADA	Supervisory Control And Data Acquisition
SDN	Software Defined Networking
SFC	Service Function Chaining
SGW	Serving Gateway
SLA	Service Level Agreement
SON	Self-Organizing Network
TC	Technical Committee
TRL	Technology Readiness Level
UE	User Equipment
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
vFW	Virtualized FireWall
vIDS	Virtualized Intrusion Detection System
VIP	Virtualized Infrastructure Provider
VM	Virtual Machine
VMNO	Virtual Mobile Network Operator
VNF	Virtual Network Function
VNO	Virtual Network Operator
VPN	Virtual Private Network
VSF	Virtual Security Function
VTN	Virtual Tenant Network

Introduction

1 Introduction

This is the first white paper of the 5G PPP Security Working Group. Launched in early April 2016 and led by 5G-ENSURE, this WG encompasses all Phase 1 projects either active and/or interested in 5G security. The largest contributions are from the two projects most active in security (5G-ENSURE and CHARISMA), but most of the 5G PPP Phase 1 Projects have joined the 5G PPP Security WG and provided inputs to this white paper (namely SELFNET, VirtuWind, COGNET, 5G-NORMA, Speed-5G, 5GEx, SONATA).

This white paper describes the 5G PPP Security Landscape of Phase 1 projects, covering the scope in 5G PPP Phase 1 Projects with specific reference to 5G Security.

The objective of this white paper is thus twofold: first get the reader acquainted with 5G Security the way it has been addressed through Phase 1 in terms of the "What" and "Why" but also, and probably most importantly, pave the way for Phase 2 Projects so they can leverage the achievements resulting from this first phase.

While this white paper has been produced in the context of the 5G PPP Phase 1, it is hoped that it can serve as a reference document in other contexts.

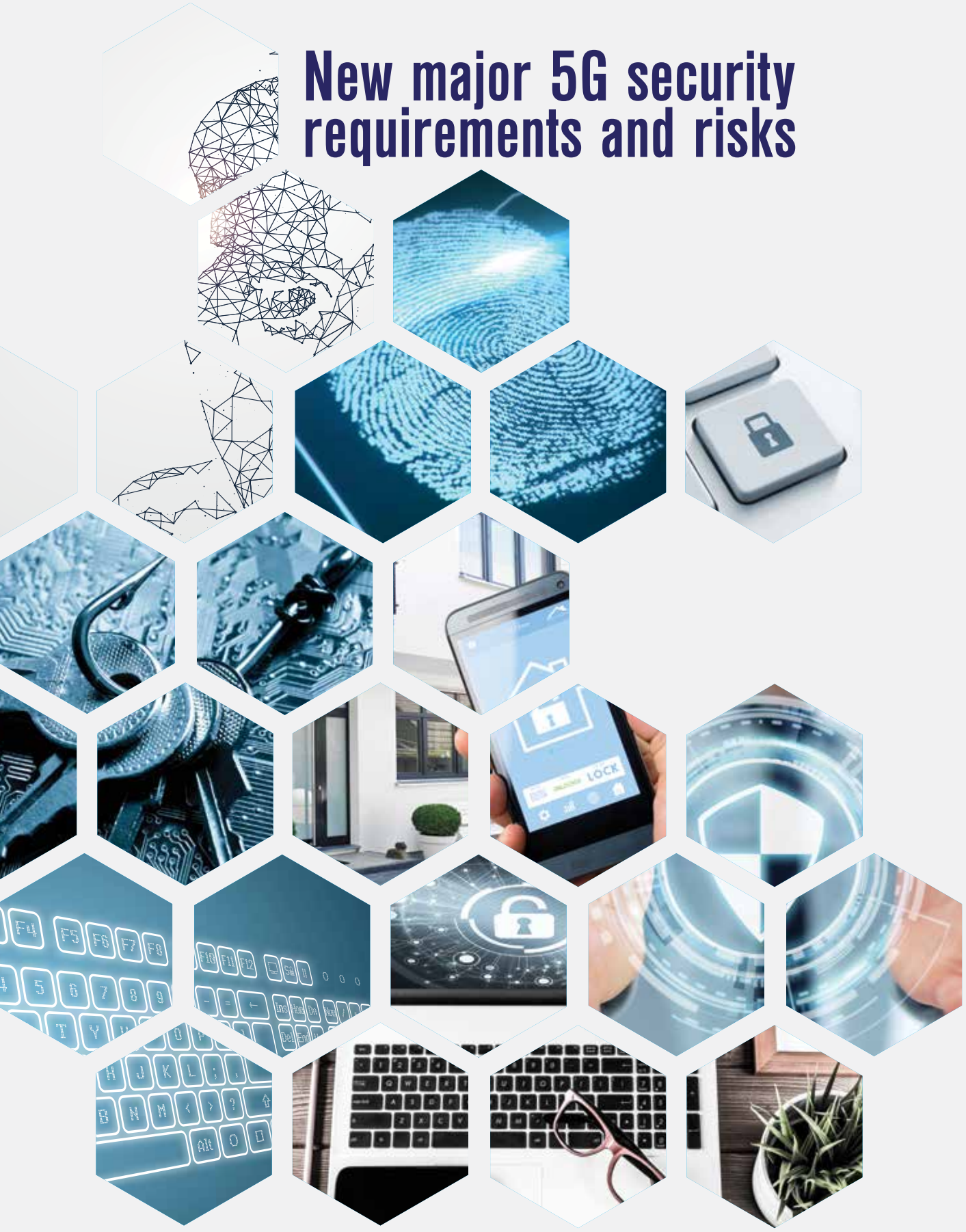
The rest of this document is organized as follows:

- Section 2 is devoted to raising awareness of new, major 5G security requirements and risks.
- Section 3 introduces 5G security architecture the way it should be.
- Section 4 is dedicated to Access control in 5G.
- Section 5 focuses on Privacy in 5G.
- Section 6 deals with Trust in 5G.
- Section 7 is concerned with Security monitoring and management in 5G.
- Section 8 looks at Slicing.
- Section 9 centres on standardization in 5G Security.

Each of the sections has been authored by one of the projects with inputs from the others. As such, the process has been balanced across the projects as encouraged by the chairs/editors.

In each of the sections (3 to 9) the projects active in the topic in question are mentioned along with the targeted results, providing a pool of projects active in the field as well as clarity on their respective contributions.

New major 5G security requirements and risks



2 New major 5G security requirements and risks

The challenging traits of 5G networks to support novel and diverse business requirements of vertical sectors have rendered current network security approaches inadequate. For example, multi-tenancy in 5G networks, i.e. infrastructure sharing by multiple virtual network operators will require strict isolation at multiple levels to ensure absolute security. In 5G networks, reliability does not only refer to availability or up-time of the network infrastructure but also to ensuring high connectivity, infinite capacity and coverage (and other promised 5G features) anytime and anywhere. This implies a security makeover of how confidentiality, integrity, and availability will be maintained and managed in 5G networks. Furthermore, the already high complexity of securing a network and its services has scaled up another notch with the introduction of SDN and NFV in 5G networks, i.e., due to "softwarization" and "virtualization" of networks and network functions. These are just a few examples of security challenges out of the many that are anticipated in 5G networks. In addition, service specific security requirements must also be considered as the 5G ecosystem is anticipated to be service-oriented. For example, remote healthcare requires resilient and robust security while IoT demands lightweight security. Security requirements can therefore vary substantially.

This chapter lists major 5G security risks and requirements as foreseen by the 5G PPP Phase 1 projects. This list is the result of a joint effort across the various projects, but it is not claimed to be exhaustive given that 5G technology is still continuously evolving. Furthermore, requirements and risk analysis has not been performed in detail by some of the 5G PPP Phase 1 projects. Therefore, the list presented here is preliminary and does not reflect the final view of all projects. Nevertheless, the security risks and requirements presented in this section highlight some of the main security aspects that must be considered in 5G.

2.1 5G Security Risks

2.1.1 Unauthorized access or usage of assets

» The heterogeneous nature of the 5G infrastructure requires multi-level access along with seamless usage and continuity of services between them, which may result in unauthorized and opportunistic access or usage of assets. In Chapter 4 we investigate potential AAA evolutions, which may induce potential heterogeneity of access control security levels to 5G. In a multi-tenant 5G infrastructure, composed of many diverse types of domains or slices i.e. RAN slice, Vertical slice, Core slice, the Access controls performed at each of those sub-parties may be heterogeneous and not easily interoperable with the other sub-parties of the 5G infrastructure (access control to: the RAN slice, the slices interconnection between the RAN/Core level and the slice interconnection between the Core Level and the Verticals services itself).

This risk may include, for example:

» 5G Identity thefts or cloning (to gain for instance unauthorized access to network or sensitive slices, or charge access to other customers).

» Opportunistic and fraudulent usages of shared resources, unauthorized access and/or modification of 5G connected devices critical data such as subscriber credentials (software based security technology may allow modification or duplication/cloning of credentials).

» Exposure of the security level of 5G network access technologies to new threats due to their seamless interworking as requested for 5G (i.e., mobile, fixed as well as satellite).

» Massive IoT 5G security protocols introduced (with low security level) may negatively impact security of non IoT services.

2.1.2 Weak slices isolation and connectivity

In the context of 5G infrastructure slicing, a weak slice isolation and connection may compromise the entire 5G security, e.g. sensitive data, managed inside a slice, could be exposed to applications running in other slices services, through side channel attacks. This risk is even higher since isolation is distributed over each of the security domains of the underlying 5G security architecture.

An additional complexity comes from the fact that monitoring and management of such a chain of connections among each of the security domains might not be properly handled.

2.1.3 Traffic embezzlement due to recursive/additive virtualization

The double level of virtualization delivered by the combination of SDN/NFV in 5G infrastructures may allow traffic capture and rerouting. That is, inconsistency between Orchestrator abstraction, SDN control abstraction and the physical and network resources may allow third parties to capture /embezzle/alter control plane and user plane, without any knowledge nor detection by the operator of the whole infrastructure.

This point is particularly sensitive for local regulation constraints (eHealth or Lawful Interception flows for instance), which may take precedence over National or EU contextualization of sensitive services (e.g. NIS Directive).

2.1.4 Insufficient technology level readiness

Although, 5G PPP Phase 3 projects will target the highest possible technology readiness level (TRLs) for their potential outcomes, in the first steps of 5G deployments (2020), new and non-mature technologies may be put into production. This may allow new attack vectors, e.g. violation of network integrity, seamless based fraud (opportunistic), data leakage/privacy and side channel between slices, resources sharing, etc. As Security by Design (THINK / BUILD) will not be fully accessible by 2020, we may prioritize Security by Operation (RUN) for the first steps of 5G deployments to manage and adapt the delivered security level to 5G customers and Vertical services providers.

2.1.5 Difficulties to manage vertical SLA and regulation compliance

This risk refers to the difficulties to address, manage and deliver, from an E2E perspective, the Verticals' SLA and to comply with actual present regulations and known evolutions of the regulatory framework.

This risk if foreseen due to multiple factors including:

1. customer's assets could be delivered to a third party without a clear and formalized acceptance of the customer (for instance API for geo-localization of a car through an API at Orchestrator level);
2. the Orchestrator may allow direct access or command from third party to operator's infrastructure or assets;
3. there is no available scheme of Liability describing who is responsible for what, at which time and in which location (liability and responsibility chain regarding potential services chaining at VNF level);
4. VNF lifecycle is outside of Operator control, there is no scheme to establish evidence of VNF-Backdoor/Trojan proof;
5. regulation may require use or force usage of VNF in some geographical area.

5G systems must comply with LI regulations, in which third party shouldn't be aware of those activities (issues with Slice concepts spanning multiple domains and regulations, also potentially ciphered outside Operator's control).

2.1.6 Slicing VS Neutrality

The slicing concept seems not to be fully compatible, as of today's understanding, with Neutrality concepts. Indeed, neither network neutrality nor network slicing is defined by EU legislation. Both concepts, however, are regulated by the EU Regulation laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Telecom Single Market Regulation 2015/2120 - TSM). The second relevant document is the BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules (BoR (16) 127). BEREC in its guidelines mentions that "Network-slicing in 5G networks may be used to deliver specialized services", which are defined in the art. 3(5) of TSM as "services other than internet access services which are optimized for specific content, applications or services, or a combination thereof, where the optimization is necessary to meet requirements of the content, applications or services for a specific level of quality". Therefore, it is assumed

that slicing will always deliver services that need optimization and that the services delivered need to be in line with the regulation.

As rules for application level slicing or sub-slicing are unknown, the risk is clearly to deliver 5G technologies not compliant with applicable legislation/regulation.

2.1.7 Trust Management Complexity

Trusts concepts, as understood now, are insufficient to manage complex 5G infrastructures.

Trust may also include liability, i.e., new concept of liabilities between parties should emerge, and particularly regarding the delivery of Verticals services that may oblige delegation to third party some regulation constraints.

2.1.8 Provisions to facilitate change of service provider Domain Lock-in

5G network slices are expected to span multiple administrative domains. The tenant/owner of a given network slice will have its virtual service infrastructure distributed across different domains, each one having its own security services and SLAs. The lack of common security standards and guarantees across multiple domains could lead to provider lock-ins, a slice owner being unable to easily and flexibly migrate all or parts of its virtual service infrastructure from one provider to the other, without affecting or degrading the security requirements and the expected levels of security SLAs. This could lead to adverse effects, since the tenants of virtual 5G slices will be unable to leverage the full potential of 5G, including the flexibility in managing and seamlessly operating their virtual service infrastructures over multiple physical / administrative domains.

2.2 5G Security Requirements

2.2.1 Security Level

5G must provide a security and privacy level higher or at least equal to the security and privacy level in 4G. That is, 5G must be able to deliver and maintain SLA to verticals in terms of: availability, security, resilience, latency, bandwidth, access control from an end to end perspective. Furthermore, 5G systems and components must provide strong mutual authentication and authorization and should not be negatively affected by the security of legacy systems with which it interworks.

2.2.2 Security Automation

5G infrastructures' heterogeneity and complexity require security to be dealt at multiple levels and across domains. Therefore, automation of 5G security is vital to successful functioning and adaptation of 5G technologies. This is also in favour of 5G security to be composed and dynamically adapted upon context at hands, as a service (5G Security As A Service: SecaaS).

2.2.3 Security Monitoring

5G systems must support security monitoring capable of detecting advanced cyber security threats and support coordinated monitoring between different domains and systems (e.g. mobile and satellite). New innovative approaches to predict, detect and counter these challenges may need to be considered. For example we may think of relying on analytics for enhanced security operations (based, for instance, on Machine Learning or Artificial Intelligence approaches) to develop intelligence-driven security capabilities able to gain a more accurate understanding of the risks and exposures of SDN infrastructures.

One of future solution could be to collect and analyse in real time events and logs within each slice (from RAN to vertical services) and among slices (this approach is identified as FAST Data technologies, due to its reactivity time and the very short storage duration to achieve massive collect of information).

2.2.4 Security Management

End to End security management and orchestration should be put in place taking into account correlation and coherence / consistency between data exchanged/shared at Security Architecture Inter-domain interfaces (see Section 3).

For example, an appropriate use of Big Data technologies may allow consistency evaluation between RAT to Verticals in term of customer 5G security context (i.e. notification of country localization during service delivery).

Customers, slice owners and vertical services should be aware of their technical 5G contextualization,

particularly to asses and address their security needs. For example, security KPI and proofs should be available and collected at 5G infrastructure. 5G systems and components must provide functionality to mutually assess the trustworthiness before, and during interactions. Furthermore, if required by local regulation, 5G infrastructure operator must have means to demonstrate their provided level of security.

2.2.5 Security liability Schemes

New responsibility schemes should be proposed, in coherence with existing Regulation, regarding the distribution and allocation of responsibilities and obligations in a multi-tenant softwarized telecom infrastructure, and in particular for potential delegation of regulation obligation to non-regulated third parties (today Licence obligations are intuitae personae and may not be subdelegated).

2.2.6 Inter-tenant/Slice Isolation

Infrastructure sharing by multiple network operators will require strict isolation at multiple levels to ensure the expected security level. Various aspects of control-plane, data-plane and resource isolation must be guaranteed to ensure zero correlation among different slices/tenant operations. Tenant/slice isolation is important to ensure a reliable and warranted service assurance, together with data and communication integrity and confidentiality. Therefore, inter-tenant/slice isolation security of sensitive data, should at least be equal that of physically separated networks. Moreover, this strong slice/tenant isolation should be demonstrable and evidence should be collected and computed over the entire infrastructure.

2.2.7 5G Liability

The chain of Trust and liability of multi-tenants should be managed and auditable for each service, component supplier, operator and customer.

5G Liability schemes will have to be defined and applied, particularly to address breach of Trust/Security (backdoor, Quality impact, regulation impacts, data leakage etc.) between parties.

5G Liability could be reinforced by VNF certification or labelization, SDN Controller or Orchestrator evaluation, or proper orchestration of virtualized security functions.

For instance, it is important to address the security of the VNF itself as an element, e.g., VNF hardening, VNF verification/certification/attestation and corresponding industrial processes, VNF code robustness, etc.

2.2.8 Enabling Value Added Services with end to end encryption

Enabling value-added security services in the context of encrypted traffic. In order to comply with privacy regulations and protection of user data, traffic encryption is expected to be generalized across 5G networks. End-to-end encryption may hamper the use of multiple value-added security services such as attack detection, QoS monitoring, fine-grained access control, among others. In this respect, high-level privacy guarantees may have the adverse effect of lowering security guarantees. Therefore, the development and wide adoption of 5G should happen alongside new technologies and capabilities that enable value-added security services in the context of encrypted traffic, thus conciliating between security requirements and privacy guarantees.

2.2.9 5G regulation conformity

5G technology should be developed in compliance with legislation/regulation that apply or could anticipate be anticipated (for instance LI and Data Retention Regulations appeared as difficult to comply with and mist be taken into account in the case of Slicing implementation).

5G Security Architecture

3 5G Security Architecture

3.1 The need for a 5G security architecture

The current 3G/4G networks already have security architectures defined in [1] [2]. Why is a new security architecture for 5G needed?

First, there is no explicit and complete *trust model* documented for 3G and 4G networks. This produces an issue in 5G context where we have new actors entering the value chain, new types of services and devices, etc. Also, the trust model applied in the inter-operator networks (designed for a small number of large national operators) is already now problematic, causing concerns of e.g. impersonation on signalling interchange networks. Second, *virtualization and management* is largely left outside the scope of [3], which is not sustainable in 5G which rests on management and orchestration of virtualization. Third, for mission critical services (health, transport, industrial automation, etc.) a completely *new threat and risk situation* occurs. The damage done by cyber-attacks to safety (potential loss of life) goes way beyond the impact on the "mobile broadband" type services that we see today.

3.2 Design Principles for a 5G security architecture

To build a viable security architecture for 5G then, several *design principles* for such an architecture can be identified as discussed in the following sub-sections.

3.2.1 A logical rather than physical security architecture

5G networks will heavily rely on network virtualization, implemented by VNFs, forming network slices running on shared infrastructure. The 5G security architecture cannot be built independently of the overall architecture, but must follow its design principles. The 5G security architecture needs to be logical rather than physical [5G-Ensure]. Slicing must isolate resources and data even on shared infrastructure.

In the RAN, a high degree of heterogeneity is expected with a significant part of the functions still implemented by non-virtualized equipment. The RAN security architecture must support flexible allocation and dynamic relocation of functions between different implementation domains (like edge cloud deployments versus all-in-one 5G base stations).

3.2.2 A distributed, hierarchal and recursive approach

The need for a distributed security architecture will in 5G be more challenging due to the need for end-to-end coordination across multiple domains [COGNET]. For example, probes that distil security events/threats from a tenant's data plane need to be distributed across administrative domains. A hierarchy of security controls allows trade-off between centralized and distributed functions and provides defence in depth [Selfnet].

As orchestration takes place there will appear choices concerning how and where to instantiate security mechanisms. A recursive approach can be used, where a high-level security objective is gradually broken down into a set of complementary enforcement mechanisms, dispatched at different layers/locations, ensuring a coherent instantiation of the proper security controls [Selfnet].

3.2.3 Multi-domain and vertical support

Central to the vision of 5G is to provide a secure SDN/NFV industrial network architecture, supporting coordination and orchestration both *intra- and inter-domain interactions* between a mix of verticals' and operators' domains Cross-operator/domain damages must be mitigated [VirtuWind, 5GEx]. Slices may extend across several domains and a consistent security view still must be maintained [5GEnsure].

3.2.3.1 Security-as-a-Service

Much of the attractiveness of 5G is presumed to lie in the ability for vertical industries to improve cost/efficiency by using shared infrastructure. Some verticals may wish to remain in control of security while others may opt for further savings by "outsourcing" selected security services to the 5G network. This could include placing policy enforcement (firewalls, device access control) in the network and/or relying on authentication/geo-location assertions provided by the network.

3.2.3.2 Industry grade SDN and NFV

Research done in the 5G-PPP envisions a framework for (de-facto) standardized controller architecture and interfaces for SDN/NFV based solutions supporting industry-grade QoS and security, see e.g. [4], opening up a huge space for solution providers, e.g. SDN controller variants, or specific VNFs for industrial applications, see e.g. [5]. Various security elements are necessary for this vision, especially when considering the criticality and intricacies of specific business applications (e.g. installing/upgrading network devices, SCADA systems, policies, etc).

Specifically, the architecture should provide AAA mechanisms for all actors involved in intra- and inter-domain deployments. Appropriate interfaces should be included to provide means for the designation of the access control policies. Furthermore, industrial and other critical applications require an automation of security monitoring, analysis, and incident response. These features can exploit the flexibility of SDN/NFV deployments, e.g. by Service Function Chaining.

The SDN control plane (in particular the controller itself) must be fault tolerant. Additionally, architectural provisions such as controller clustering for fault tolerance and localization provides reliable and consistent network control even if some controllers are faulty or compromised.

3.2.4 Bringing (security) management into scope

There are two main aspects here: *securing the management* (e.g. securing orchestration) and *managing the security* (e.g. preventing unwanted traffic).

The complexity of security mechanisms in 5G networks grows not only due to virtualization but also due to security requirements at different levels, e.g. associated with a slice, a service, or a resource. Security management needs to provide a holistic system view, supported by monitoring/analytics, guided by programmable security policies, to ensure SLA security levels [CHARISMA].

To support DevOps, service platforms needs to validate the services submitted to that platform. DevOps components will have to be linked with some type of manifest describing the functional scope of DevOps component, existing API and log, and related external interface to permit proper authorization and liability of the supplier [SONATA].

Unwanted traffic detection in the tenant's data plane could in 5G context be enhanced by machine-learning based detection, coupled with SDN/NFV-based deployment of countermeasures. An example of a real-time automated, security management framework following a closed-loop inspection-analysis-decision-actuation regime is described in [6].

3.2.5 Flexibility and extensibility

To support the diverse needs of different user groups and to provide a future proof architecture, we must cater for *flexibility and extensibility* [5GEnsure]. An extensible set of authentication methods and cryptographic algorithms must be supported; broken cryptographic algorithms must be easily replaceable, etc. Flexibility should also include the option for users to choose end-to-end application layer security rather than network-terminated security. Backward compatibility must not result in the possibility of 'down-grade attacks'. The *flexibility* should prevent any fraud or security issues, in which attacker could exploit and benefit from heterogeneity of security levels in subparts of the 5G infrastructure.

3.2.6 Support for massive and critical MTC

The MTC space can be divided in two main dimensions, the scale of the MTC service and the criticality. Each have different implications on security.

For *massive MTC*, existing authentication mechanisms may be non-suitable due to heterogeneity among mobile wireless devices, and scalability issues [SPEED5G]. An authentication component for massive IoT communications, managing devices as a group instead of individual entities should be provided. This component could support a proxy authentication mechanism performed by a user gateway. Delegation of authentication rights to the gateway should be at the discretion of network operator, who holds the control on the authentication rights.

A flexible choice of crypto-algorithms with different properties to support the variety of expected services, in particular energy-efficient crypto for massive IoT deployments, also becomes essential [5GNORMA, 5GENSURE].

In *critical MTC*, access to actuators needs to be secured, as these devices actively ‚do' something and potentially can do wrong things. This point will have to be carefully investigated regarding above mentioned security *flexibility* [SELFNET, CHARISMA].

Common to both dimensions is, as mentioned, the potential and opportunity of the network itself to enhance security and/or reduce verticals' cost by offering "Security-as-a-Service" [SELFNET, CHARISMA]. Concretely, for MTC one can envision the network answering questions such as: Is actuator connected at the right place? Is the path to the actuator working?

3.2.7 Regulatory compliance

A number of already existing, as well as potentially new regulatory requirements obviously must be satisfied. Among the existing requirements one can note those related to Lawful Intercept, user privacy, and customer notification of security breaches. 5G security features must also meet trade compliance regulations. Potential future requirements could arise in the need for infrastructure and service provider to demonstrate their provided level of security [5G-ENSURE].

3.3 Draft high level security architecture

This initial architecture is, at the time of writing, in its first "iteration" and while many design principles discussed above (e.g. a logical architecture, multi-domain support, management aspects, etc) are visible, other aspects are (yet) not visible at the current level of detail[1].

3.3.1 Rationale and Background

A sound principle is to not re-invent the wheel. While the current 3GPP security architecture fails to meet all the 5G needs, it has undisputedly created a huge, trusted ecosystem and provides a proven basis to build on. The current security architecture is defined in TS33.401 [3] and in turn builds on the 3G architectures in TS23.101 and TS33.102, [1] [2], namely the so called *strata*, where a stratum is a "grouping of protocols and functions related to one aspect of the network services". The five defined strata are: access, transport, serving, home, and application stratum. For each of these strata, TS33.401 defines security mechanisms and protocols grouped into five *security feature groups*: access (I), network (II), user (III), application (IV), and visibility & configurability (V).

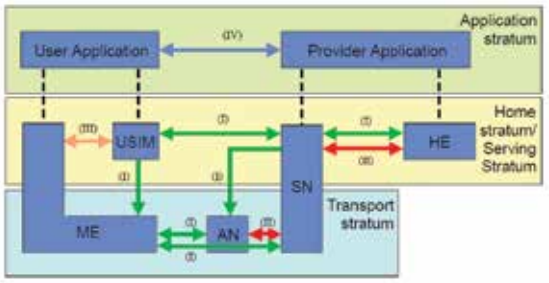


Figure 1: The 3GPP TS 33.401 Security Architecture

A main component missing in 5G context is the support for (multiple) *domains*. Domains are fundamental also to model trust between actors. Though lacking in TS33.401, such domain concepts can however be found in TS23.101, which defines two "top-level" domains for *user equipment* and *network infrastructure*. These are then further sub-

1 The work in the 5G-PPP Security WG has resulted in an agreement vision for a reference security architecture framework based on [ed2.4]. Of course, further analysis in the Security WG may result in additions and/or modifications.

divided as depicted in Figure 2 below.

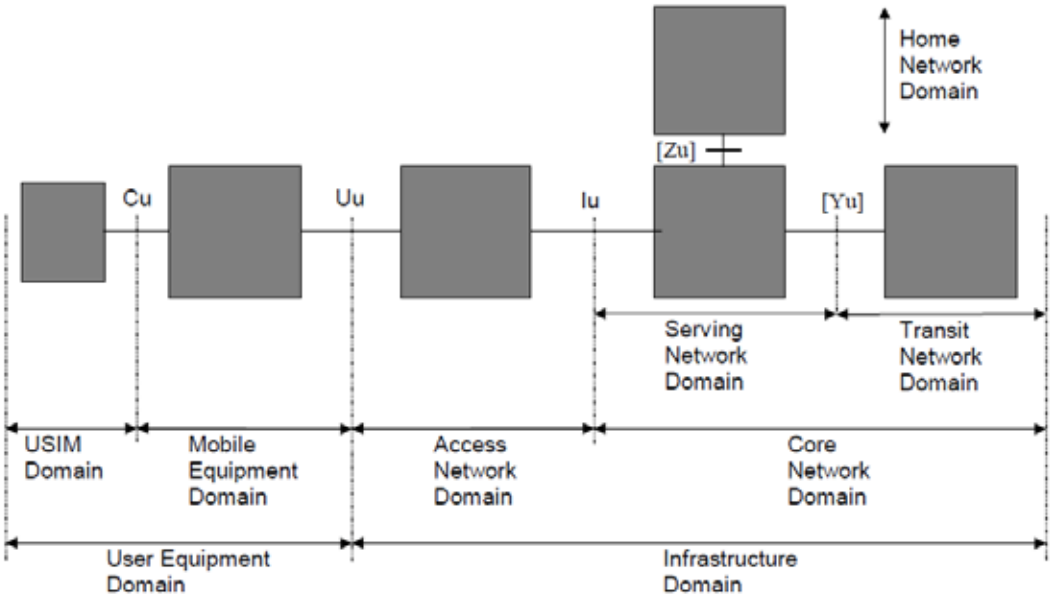


Figure 2: Domains from TS23.101

We refer the interested reader to TS33.401 and TS23.101 for further details.

3.3.2 Architecture Extensions for 5G

We here summarize the approach taken to extend the current architecture to a 5G setting, building on strata, security feature groups and domains. Further details are found in [7].

3.3.2.1 Strata

The strata can be largely re-used as-is. However, an additional stratum for management is proposed. In this stratum we place functionality and protocols related to e.g. orchestration, security monitoring etc.

3.3.2.2 Security Feature Groups

All the security feature groups are valid also in a 5G context. However, a feature group related to management appears missing from the map so an additional sixth "Security Management (VI)" feature group is added, comprising e.g. securing orchestration, key management etc. Additionally, the "Visibility & configurability (V)" feature group in 4G contains only one single feature: an indication to the user if ciphering is switched off over the radio access. This is really a special case of *trustworthiness* indication. Trustworthiness will have many more facets in 5G setting (e.g. 'Is the platform trusted to run my VNF?') and thus we have chosen to widen the scope of this feature group and rename it "Trustworthiness (V)".

3.3.2.3 Domains

The domains require more changes to be adopted to a 5G context. First, TS23.101 defines a domain to be a *physical grouping*, which we (due to e.g. virtualization) need to generalize to a *logical or functional grouping*. There will certainly still be physical entities in a 5G setting and we therefore define (akin to ETSI NFV) a distinction between the set of physical domains which we call Infrastructure Provider Domains (IP Domains) and the logical/ functional domains which we call *Tenant Domains*.

Second, one can observe that slices (that may extend across both access and core domain) form a kind of transversal "domains-across-domains". We model this by special *Slice Domains*.

Third, we have chosen to define special *Management Domains* for management functionality. Modelling this by a domain as well as a stratum has the advantage that it allows us to think of a setting where management is (partly) performed by a third party. For example, a vertical industry may be allowed to manage certain aspects of the network slices they use. For the same reason we also add the *3rd Party (3P) Domain* and the *Internet Protocol (IP) Service Domain*. The 3P Domain allows us to capture a vertical industry that provides authentication and identity management functions for their own devices As a consequence, we also add an *Identity Module Domain* in the device (UE) that complements USIM for industry/MTC use cases. The IP Service Domain is used to model external IP networks such as the public Internet or various enterprise networks.

The final extension captures so called direct-mode, UE-to-UE communication by adding the *(Additional) UE Domain* (which internally has the same de-

composition as the UE domain). The proposed 5G domains are visualized in Figure 3 below (we omit the strata and security feature groups since the changes in those areas as quite small compared to TS33.401).

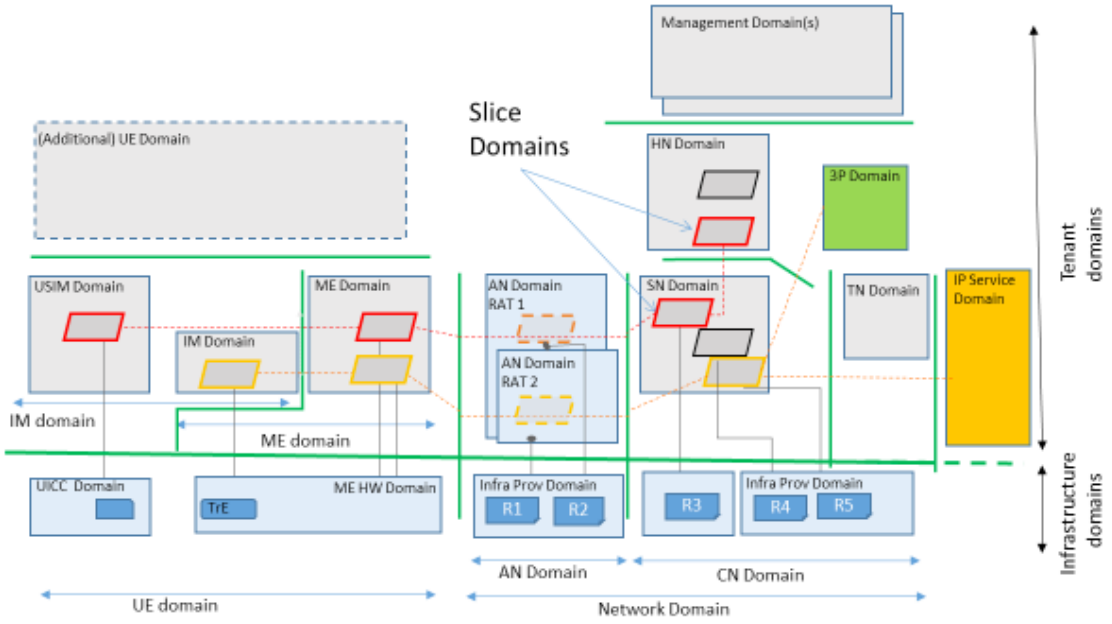


Figure 3: Proposed domains for the 5G security architecture. (Note that not all IP Domains are shown.)

In the figure, the green lines denotes interfaces/ reference points between domains and identify points where security contextualization and continuity needs to be securely propagated between domains, where security monitoring features has to be deployed to manage security from and end-to-end perspectives.

Home and Serving Domains (HN, SN) are example Tennant Domains making use of underlying Infrastructure Domains. Among the Infrastructure Domains, we show a number of Infrastructure Provider Domains and highlight some exemplary (physical) resources as R1, R2, etc. We show two Slice Domains, the red slice domain could correspond to some "traditional" service such as a VoLTE equivalent and the orange slice might correspond to some industry/enterprise service (using separate AAA). Note that the slices are carried over separate ANs (e.g. 3GPP access and WLAN) and extend all the way into the UE. While this may not be a typical case, the architecture allows us to model it.

The architectural principles laid out are a first step toward a common 5G security framework. Many details of implementation of the architecture (how to enforce/uphold it, which parts to standardize, etc) are for further discussion in the 5G-PPP community and SDOs such as 3GPP, and in particular for those aspects related to cross domains orchestration (see section 2, 5GEx requirements).

Access Control to 5G

4 Access Control to 5G

Authentication, Authorization and Accounting (AAA) services play a central role in 5G security, at least to protect frequency and radio/communication resources, to deliver 5G networks services on demand and comply with different regulation constraints.

Up to 4G, the mobile network access control is homogeneous, secure (thanks to the hardware component: USIM Card), and interoperable worldwide over visited network infrastructures. The access control model is also interoperable in the access to services, as each 2/3/4G device or handset accepts USIM Card (under different physical formats, but with the same interface). In order to allow M2M and industry to use 4G Data Network more easily, GSMA has developed the concept of embedded UICC[2], a soldered component, owned by third parties, certified under Common Criteria EAL4+[3], on which operator could remotely provision their credentials to allow 4G access to Machines. The eUICC is today a soldered equipment (see specification ETSI MFF2[4]), but it could evolve to be directly integrated in future 5G based band processors. The User Equipment credentials required to access to a 5G Licenced Mobile Network infrastructures will have to be securely stored, managed and used in secure elements to fulfil the security state of the art regarding the incapacity of Software technology to prevent Identity theft and clone.

The Authentication and Key Agreement protocol (AKA, between the USIM card and Core Network HSS component) plays a central role in the security of mobile networks as it bootstraps the parameters needed to form a security context containing what is agreed by the parties. The protocol provides mutual authentication between device and serving network, and establishes session keys. The state-of-the-art protocol used in 4G (EPS-AKA) is almost identical to its predecessor used in 3G, which was introduced in the late 90s. A limitation of EPS-AKA is that, the protocol requires signalling between each device that requires network access, the local serving network and the device's remote home network. In particular, the signalling between serving network and home network may introduce a major delay when they are distant, which is the case for roaming users.

Regarding anticipated 5G use cases, analysts forecast more than 25 billion of devices to be interconnected in 2020 (Ericsson, 2015). Providing connectivity to such a large amount of devices, which may require simultaneous network access, may lead to a potential signalling overload. Signalling data is growing 50% faster than data traffic in mobile networks (Nokia Siemens Networks, 2012) and is expected to surpass the global IP traffic growth within three years (Oracle, 2015). An increased level of signalling would affect the speed and data capacity of 5G. Therefore, the contemporary architecture of the mobile network should be investigated, including the aspects related to security to fully support IoT connectivity use cases.

In the 5G use case "Massive Internet of Things", IoT device locations can either indoor or outdoor. In addition, IoT devices can be connected towards small cells and/or to macro cells, depending on the availability. Small cells are connected to the mobile operator using either a broadband connection through an evolved-Home-NB (eHNB) device, or based on radio resource units that constitute a front haul connection to the evolved-NodeB (eNB), carrying both data and control data. This signalization amount increase is one of the major bottlenecks for 5G development as a low delay and reliable network for IoT devices.

To circumvent the signalization bottleneck, two approaches are currently being investigated. One first approach is a family of *lightweight authentication and key agreement protocol for massive IoT communications* [SPEED-5G], while the second approach investigated is a family of protocols that allows to group devices together allowing the reduction of signalling and communication latency through a *family of group-based AKA protocol* [5G-ENSURE].

2 http://www.gsma.com/connectedliving/embedded-sim/
3 https://www.commoncriteriaportal.org/
4 http://www.etsi.org/deliver/etsi_ts/102600_102699/102671/09.00.00_60/ts_102671v090000p.pdf

Lightweight authentication and key agreement protocol family

Authenticating the continuously increasing number of IoT devices over the 5G network is of paramount importance to ensure security in the upcoming 5G communications systems, which will be the target of many known but also unknown security threats [6]. In this context, the *lightweight authentication and key agreement protocol for massive IoT communications* meets the requirements in terms of computational complexity, communication and storage overhead.

Proposed approach: Initially, the mobile device authenticates to the MME and the sensors form N groups based on their similarity (e.g., type of app). Afterwards, the group authentication process is performed for each group of sensors with the mobile device using WiFi technology. If the authentication process succeeds, the authenticated sensors are able to send data to the IP-based service networks via the Femtocell Access Point. [SPEED-5G]

Group-based AKA protocol family

The *group-based* AKA protocol family allows the serving network to authenticate a group of devices reducing the signalling and communication latency with the home network.

Proposed approach: Groups may consist of devices sharing similar features such as functions, locations, or ownership. These group-based AKA protocols contribute to reduce latency and bandwidth consumption, and scales up to a very large number of devices. The group-based AKA protocol is designed with a novel mechanism based on an inverted hash tree that allows the network operator to dynamically adapt the requirements of security and efficiency of the designed protocol. More details can be found in [5G-ENSURE]. A ProVerif analysis (CHARISMA) demonstrates that the first implementation of the protocol meets mutual authentication, key confidentiality, and device privacy also in presence of corrupted devices. The protocol is on its early stage and future extensions could be envisaged. One possible extension is the support for secure handover among different MME and the support of dynamic groups with key forward/backward secrecy.

Although those proposals circumvent some intrinsic bottlenecks of future 5G infrastructures, they imply some heterogeneity in the level of Access Control security delivered to the 5G network. It seems crucial to propagate evidences of user equipment or stakeholders' trustworthiness and risk indices from the access control (performed at the edge of the 5G network) to the verticals services (operated in some slice). Several 5G PPP Phase 1 projects have already anticipated this need of security contextualization propagation and sharing from an end to end perspective. For instance, there is a proposition of Federation of Identity over multi-tenant infrastructures [5G-ENSURE] and an infrastructure of Federated Authentication via a trusted third party, which acts as an Identity Provider [VirtuWind] to protect access to network's controllers (like SDN controller). In the former case, all entities that want to access a controller's functions (e.g. to insert flows or negotiate parameters) must have credentials on the said controller to authenticate locally. An alternative approach is for all entities have accounts at the Identity Provider, where they authenticate remotely.

This perspective faces another technical challenge to unify the two standards based on 3GPP AKA based approaches for mobile access and the ETSI NFV framework for the slicing concepts of 5G. Those two levels of trust models could be unified through 'Virtualized–AAA' approach [5G-NORMA]. This approach can be implemented with NFV and the elasticity of storage, which can be based on tenant's end-user volume. It also allows the tenant to provide the mobile subscriber billing and accounting system, which makes this 3GPP and ETSI NFV unification become a new characteristic of AAA. The model may provide flexibility in security management, the accuracy of tracking information (i.e. mobility and billing information etc.) and the isolation of a tenant's end-user based on its own geolocation database [5G-NORMA]

An open point not solved today concerns AAA and potential heterogeneity of access control security levels. A multi-tenant 5G infrastructure could be composed of many different types of slices i.e. RAN slice, Vertical slice, Core slice. Then, the Access controls performed at each of those sub-parties may be heterogeneous and not easily interoperable with the others sub-parties of the 5G infrastructure (access control to: the RAN slice, the slices interconnection between the RAN/Core level and the slice interconnection between the Core Level and the Verticals services itself). Indeed, the security level for authentication may vary between slices, which also implies a need for a high level of isolation between slices within the multi-tenant 5G Infrastructure.

New innovative approaches to predict and counter these challenges need to be considered, taking into account the nature of AAA performed at the edge of the network and inside the whole 5G infrastructure. These will need to deliver vertical services (multi-operator and multi-domain AAA on management, at control and user plane, for instance in case of interworking SDN and legacy domains). [5G-Ex].

Another point to be investigated in the near future is to qualify if a Licenced Mobile Network Operator could delegate or not some of its regulation constraints to a third party, in particular in the area of AAA (see Section 2.2.5).

Privacy

5 Privacy

Society as a whole, and users of digital services particularly, are becoming aware of privacy. This is a trend that is expected to increase as the new, fifth generation of networks and services is introduced (Ericsson, June 2015). The root cause of privacy awareness is two-fold. Firstly, recent developments in governmental and corporate **mass surveillance** and the emergence of prolific whistle-blowers (e.g., Edward Snowden) have made people realize that their personal data and communications are no longer safe, potentially affecting their everyday lives. It is also evident that the frequency of illegal activity and malicious attacks targeting personal data or private communications is increasing (e.g., IMSI-catchers). Since data is extremely valuable, such attacks and leaks are expected to be commonplace and increasingly impactful both financially and privacy-wise. Secondly, we are entering the **age of big data** with huge opportunities for digital service providers and other actors for the legal collection of data and metadata through their respective services. These opportunities will increase as concepts such as Internet of Things (IoT), connected vehicles, smart homes and smart cities leave the research labs and become reality. With the advances in machine learning and the lack of proper data management and mathematically sound anonymization practices, personally identifiable information (PII) is bound to be leaked, thereby harming users.

Elements of **subscriber privacy** have been around in 2G, 3G and 4G systems focusing on using randomly assigned temporary identifiers making it harder to track and identify subscribers. While certainly a step in the right direction, foreseen 5G systems need a much more thorough approach to privacy. Not only have the expectation and awareness of users about privacy increased but 5G networks will also serve individual users but **complete industry verticals** with stringent business-related requirements on both the personal data of their users and the sensitive data of service providers themselves. Furthermore, as a response to the big data deluge and associated privacy issues, the new **General Data Protection Regulation (GDPR)** will come into effect in May 2018. In order to comply with the GDPR, any company which collects, stores and processes personal data (i.e., relating to an identified or identifiable natural person) has a number of obligations. Failure to comply with the GDPR can incur hefty fines. As actors in the 5G ecosystem will be many and interacting with personal data on many different levels, only a **privacy-by-design** approach to 5G can ensure the satisfaction of users, operators, industry verticals, third party businesses and European lawmakers.

Privacy concerns and privacy-by-design aside, any future 5G system should be able to answer **Lawful Interception (LI)** requests. Therefore, LI should be performed in a secure way without compromising the privacy of network users, and the information provided by the LI function must be provably trustworthy and securely delivered. An LI request can consist of control or network management information and even the content of the communications. An envisioned common LI functionality is needed for all services delivered via the 5G network. There will be **new service delivery models** including anything-as-a-service using cloud and virtualization technologies, to reduce costs, deployment time and to optimize services. This approach can only work if telecom networks expose application programming interfaces (APIs) towards users and third-party service providers to a higher degree. This means that parts of service delivery will sometimes be provided by third-party software executing on shared hardware platforms. Thus, it is clear to see, that the nature, complexity and variety of 5G services (including industry verticals and composite services provided by multiple entities) make the design and realization of such LI functionality an extremely challenging task. Given the packetized and dominantly encrypted network traffic delivery, a must-have technical building block of LI is **Deep Packet Inspection (DPI).** Without DPI, no analytic insights can be derived from live or recorded user traffic, thus rendering LI powerless.

5.1 Stakeholder concerns: users, service providers and law enforcement

Here we provide a list of privacy concerns from the perspective of various 5G stakeholders. While this list is not exhaustive, it illustrates well the many facets of privacy in 5G.

Users

Due to the pervasive nature of 5G it is essential that **users** have control over their own and their devices identifiers' privacy. Three use cases can be established,which address the area of enhancements to **identity protection and authentication** in 5G compared to existing 3G and 4G networks (5G-ENSURE, Deliverable D2.1: Use Cases, February 2016.). Specifically, the first use case tackles privacy for device identifiers which need to be appropriately protected and/or anonymized. The second use case addresses the area of subscriber identity privacy, which also needs to be suitably protected and/or anonymized, particularly when traversing access networks. The third use case tackles the provision of perfect forward secrecy to combat the threat of passive attacks, particularly in the case of subscriber key compromise. Through these use cases it becomes clear that a 5G system is required to provide (at a minimum, if feasible in compliance with LI and Data Retention regulation): confidentiality of subscriber and device identities, untraceability of user location, perfect forward secrecy for encrypted communications and unlinkability between the user subscription information and the device and subscriber's identity.

Service providers

Proposed **5G verticals** are projected to be delivered as a service chain (Service Function Chaining, SFC) potentially with **multiple, independent business entities** contributing virtual resources; either for maintaining flexibility in resource allocation or for the lack of geographical footprint. Cross-domain orchestration of resources over multiple administrative domains enables collaborative service delivery, i.e., services can be realized via chaining of VNFs (Virtual network functions) over domains of multiple operators. In this use case, the contract structure, the lack of trust and SFC (the path and VNFs which customer data passes through) create a complex privacy situation; see Figure 1 for an example.

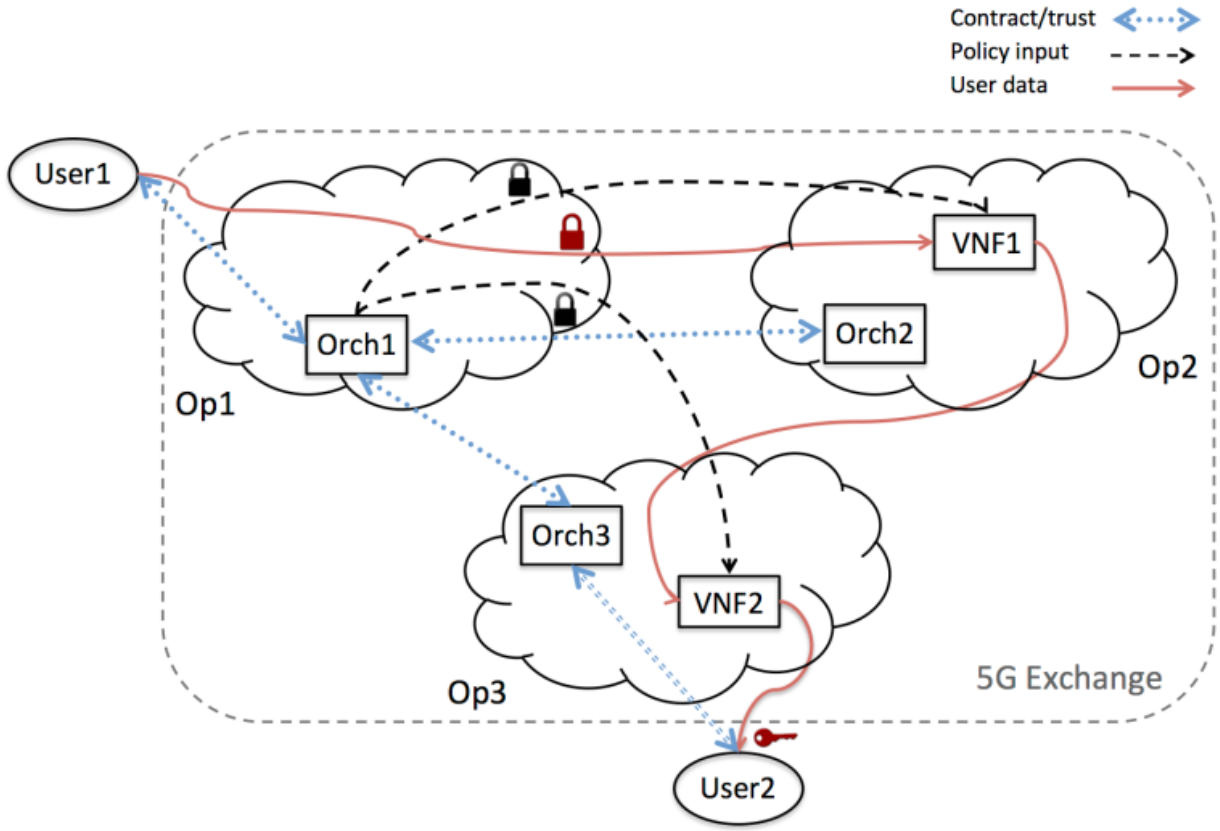


Figure 1 Multi-operator service chaining

First, the user forms a trust relationship with its customer-facing operator (Op1) upon buying a service and signing a contract (Service Level Agreement, SLA). Given that Op1 potentially

outsources some parts of the required service chain to other qualified operators (Op2 and Op3), user traffic will be steered through and potentially processed by VNFs in Op2's and Op3's administrative domains. Since the user does not have a trust relationship to the subcontractors Op2 and Op3, she might want to do something about the risk of Op2 or Op3 looking into her traffic. A logical step would be to apply encryption at the user side, or at the egress of Op1, before user traffic leaves the premises of the trusted domain. In this example, User 2 is the destination of User 1's traffic, therefore he is the one to decrypt it upon arrival. This scenario also has consequences for the trust model proposed in Section 6.

Second, VNFs usually have a policy input besides the data traffic. In the given setting, it is plausible to assume that policies (firewall rules, filter expressions, coding parameters, etc.) come from Op1, while the VNF is running on the infrastructure of another operator (Op2). Now, Op1 may have several reasons for not exposing its policies to Op2, including being competitors and hiding its cyber-defence strategies. Therefore, it could be beneficial for Op1 if encrypted policies could be interpreted by the VNF. Further complicating things, the VNF implementation could be provided by Op1, Op2 or a third-party VNF provider (not depicted in Figure 1). All three cases require a different approach if Op1 wants to keep its policies, or even the function the VNF implements, hidden and, at the same time, successfully outsource the operation to Op2. Even if there is a contract (and so some level of trust) between Op1 and Op2, an honest-but-curious Op2 could still pose problems to Op1. Thus, there is a need for security mechanisms and standards for enabling *private VNFs* (al. G. B., 2016).

Law enforcement

Law enforcement organizations and governmental agencies should have access to control and sometimes intercept user data in 5G networks in the regulated framework of **Lawful Interception**. The most pressing issues in this use case are related to Deep Packet Inspection (DPI) methods, enabling the analysis of information provided by the header and payload of traffic on communication networks. As indicated in (al. S. S.-B.), the main task that underlies in these technologies is recognition, which is directly related with manipulation and notification of information. The first facilitates the decision-making process about how to handle packets, thus enhancing among others, network traffic optimization or blocking certain contents. On the other hand, notification is a less direct form of invention involved in generating statistical reports, alert issue or espionage. With the advent of 5G technologies it is expected that the DPI methods will have a function similar to the functions performed so far. However, the complexity of this new scenario will have a direct impact on its processing capacity, hence exacerbating the challenges facing the research community nowadays.

There is great controversy about the ethical and legal implications of DPI. For critics, DPI calls into question Internet neutrality, since it could let public and private organizations modify, prioritize, monitor or filter network traffic. The adaptation of these policies to 5G networks is a problem that concerns both research and business. A clear instance of this preoccupation is observed in the popularly known "5G Manifesto", where operators claim that strict network neutrality rules will limit their ability and motivation to invest in 5G, requesting laws to specifically allow use DPI for "innovative specialized services". For the time being, even Lawful Interception-related laws are different on a country basis.

In addition to this problem, the deployment of DPI techniques in 5G networks also poses many technological challenges. The presence of a greater number of devices in the network, with the capacity to transmit more data in less time, presents important difficulty for the current DPI approaches. The four most important factors (al. R. A.) related to this problem are: 1) The large number of networked application signatures, 2) the complexity of the signature patterns, 3) the unpredictability of signature location in the network flow, as well as within the packet payload, and 4) the performance bottlenecks at OS and hardware levels.

5.2 Privacy-by-design, potential enablers and the way forward

The main objective of privacy enablers is to fulfil the various privacy requirements of major stakeholders by providing mechanisms able to prevent privacy violations via a proactive, **privacy-by-design** approach. Furthermore, the privacy enablers, to be relevant to 5G, need to especially address the threats and privacy requirements highlighted by the above-mentioned use cases. Last but not least, these enablers should also be integrated into the 5G security architecture overall design so as to be natively supported in 5G systems, services and business practices alike. For each use case, the privacy

enabling technology (ranging from anonymity by using temporary identity through homomorphic encryption to DPI virtualization) needs also to be investigated in order to satisfy privacy requirements.

Regarding **subscribers**, 5G privacy enablers aim to enhance user data protection by proposing solutions at several layers: at the network layer, as well as application layer, i.e., *privacy as a service*. In this respect, an initial set of privacy enablers (5) have been initiated by the 5G-ENSURE Project (5G-ENSURE, D3.1 5G-PPP security enablers technical roadmap (early vision), March 2016, http://www.5gensure.eu/deliverables.), (5G-ENSURE, D3.2 5G-PPP security enablers open specifications (v1.0), June 2016, http://www.5gensure.eu/deliverables). The first enabler proposes encryption, authentication and anonymization mechanisms to protect the privacy of the subscriber's identity (i.e., IMSI, but also temporal identities) in all the situations where it is currently sent in clear text over the access network. This enabler focuses on counteracting the vulnerabilities of current 3G and 4G attach and paging procedures. The second enabler proposes a 5G end-to-end encryption service able to guarantee the privacy of all users' communications from their source to their destination 5G devices. The service also defines a fair and collusion free key escrow mechanism needed to guarantee user privacy even under the constraints of LI. The third enabler proposes anonymization mechanisms for protecting the privacy of device identifiers for both UICC (Universal Integrated Circuit Card) and UICC-less devices attaching to 5G networks via various network technologies. The fourth and fifth enablers are concerned with offering 5G users the ability to be in control of their own privacy, which is configurable and controlled at the application level. Therefore, the fourth enabler provides a way to configure and protect the privacy of user data stored on the SIM by employing SIM- or device-based anonymization techniques. The fifth enabler provides a means for future 5G applications to define their own privacy policy and to check it against the servers' privacy policies to detect any potential privacy violation at the application level. This set of enablers, if designed, implemented and adopted, will be able to tackle pressing user data protection concerns. However, although some work and demonstrations have already been done (5G-ENSURE, D3.3: 5G-ENSURE_D3.3 5G-PPP security enablers SW release (v1.0), October 2016, http://www.5gensure.eu/deliverables), there still exist some technological and management challenges to overcome before these enablers are ready for integration into the 5G overall architecture. Firstly, the sheer predicted number of connected devices means that each enabler should scale extremely well in a carrier-grade, production environment. Secondly, some of these devices (e.g., in the context of IoT) have a very limited computational capacity; therefore, each enabler should be implemented in a way that allows adaptation to the characteristics of such devices. Thirdly, the abundance of verticals (value-added services built on top of the 5G infrastructure) makes the creation of a standard user privacy policy specification language a considerable endeavour.

With regard to the privacy expectations of **service providers**, including infrastructure providers, verticals and third-party software developers, a promising and certainly powerful enabler comes from the 5G-Ex project, which is considering homomorphic cryptography to enable the processing of encrypted data. Homomorphic encryption (HE) seems to be a fitting solution on how customer data, operator policy and VNF code might be kept private to the benefit of their respective owners. However, HE is known to be slow and resource consuming, which makes it less useful at high network throughput and/or real time. A potential game-changer is already envisioned: VNF class-specific encryption is a candidate solution, where HE characteristics can be satisfied via a restricted set of simpler but faster encryption schemes. With this proposed technique, even payload-intensive VNFs (e.g., media transcoding) may be realized somewhat homorphically, hence preserving privacy. Nevertheless, note that much research effort is still needed before this technique is ready for carrier grade operation.

Concerning the needs of **law enforcement organizations**, and DPI technologies especially, there is a plethora of tools already at our disposal aiming at addressing the challenge of ever increasing data traffic. Both commercial (*PACE*, *NBAR*, etc.) and open-source (*OpenDPI*, *L7-filter*, *nDPI*, *Libprotoident*) approaches have demonstrated their effectiveness in current networks [8]; but their performance in novel 5G scenarios is at best uncertain. As an alternative, the CHARISMA project works on improving DPI by integrating technologies inherent to 5G (SDN, NFV and SFC). An illustrative example of these approaches is in the progress toward providing DPI as a Service [8], where the classical DPI engine of the different middleboxes is instantiated around the network, orchestrated by a logically-centralized DPI Controller. Likewise, recent proposals are focusing on the implementation of single VNF like virtualized Deep Packet Inspection functions (vDPI), also offered as a cloud service. Thus, quite remarkably, upcoming 5G technologies go hand in hand with new technological challenges related to DPI, but also enable new mechanisms that might overcome them. Still, the complexity of 5G service delivery makes the design, integration, deployment and operation of the DPI functionality (and LI in general) a strongly non-trivial task for the near future.

Trust Model

6 Trust Model

The purpose of this chapter is to describe the security approaches based on trust model, liability model and trust matrix in the fifth generation (5G) telecommunication system. Envisioning the trust model and liability model in delivering a secure multi-tenancy and multi-network slice services in 5G, trust model, liability model and trust matrix are the key technologies to apply.

A trust model has been implicitly embedded into mobile telecommunication system since the first generation analogue telecommunications system. Trust models concern which stakeholders are responsible for what, and how stakeholders (or their technology components) depend on these responsibilities being met. Trust models can be used to gauge the security level of a telecommunication system, by capturing the level of dependency where there is no clear responsibility. Traditionally, a trust model may also help define security policy between entities and ensure all entities will respect the security policy.

In previous generation mobile networks, the trust model has always been implicit. In 5G networks, our goal is to make trust assumptions an explicit part of the architecture. This is being addressed in 5G-ENSURE, using automated methods to analyse the architecture and identify and specify trust relationships including those that might otherwise remain implicit and unacknowledged.

6.1 5G Trust Model

5G has been developed with two levels of trust models that are embedded into the 5G architecture. The first level of the trust model is in respect to stakeholders. The characteristics of the stakeholders trust model are: i) to evaluate the stakeholder's trustworthiness in the network, ii) to measure the security strength of stakeholder's network and services, iii) to quantify the stakeholder behaviour in the network, and iv) to migrate the risks and vulnerability autonomously through interactions between stakeholders. The second level of the trust model relates to network entities e.g. software-defined mobile networking controller/coordinator/orchestrator, physical and virtual network functions etc. The characteristics of the network entities trust model are: i) to evaluate the network entity's trustworthiness in the network, ii) to measure the strength level of security mechanism used in the network entities, iii) to quantify the network entities behaviour in the network, and iv) to migrate the risks and vulnerabilities autonomously through interactions between network entities.

For 5G stakeholders (i.e. end-user, consumer, tenant, mobile network operator, service provider and infrastructure provider) trust model is formed from multiple stakeholders in the 5G telecommunication systems, as shown in Figure 5. This trust model represents trust as an essential aspect of 5G architecture stakeholders to act dependably, reliably and securely within a specified service level agreement (SLA) and policies.

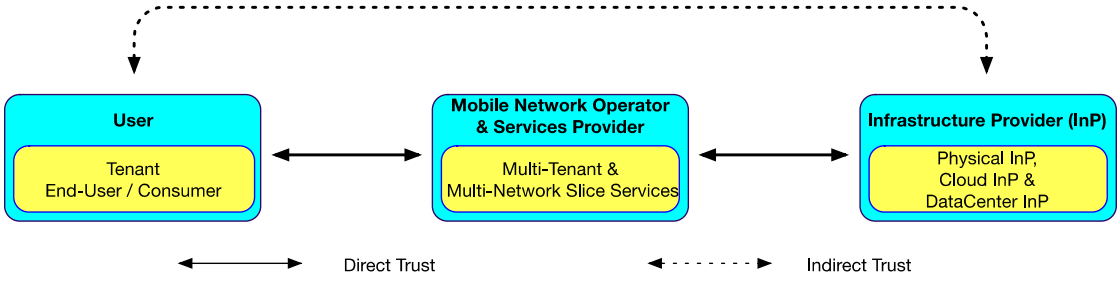


Figure 1: 5G NORMA telecommunication system trust model

6.2 5G Trust models in 5G

In 5G, machine trust models will be needed to support trust decisions over the selection of physical and virtualised assets and provisioning of (virtualized) infrastructure and applications. Machine trust models can be used in this context to provide quantified estimates of trustworthiness, and so enable automated decisions to accept or avoid specific interactions or dependencies.

As noted above, such estimates of trustworthiness may also be useful to provide decision support for human users, e.g. by using trust models to calculate the reliability of different network services, and providing feedback on this to a human through their UE devices.

6.2.1 Trust and trustworthiness by design models

Trust and trustworthiness by design models aim to capture the relationships between the architecture of a system and the types of risks that may be present. This in turn provides a basis for identifying and analysing the trust decisions that may need to be taken by system components and stakeholders.

Ultimately a decision to trust (in a system, stakeholder or component) is equivalent to accepting one or more risks. The alternatives are to avoid the risk (i.e. distrust and disengagement), transfer the risk (e.g. by making other stakeholders responsible for that risk through the terms of use, or by insuring against the risk so an insurance company pays for any damage caused), or to reduce the risk by introducing security measures. Consequently, trust(worthiness) by design models tend to start from the premise that risks can be reduced by using security controls, and the purpose of the model is usually to identify where this might be needed, and decide when it is appropriate.

Trust (as opposed to trustworthiness) comes into these models in two ways:

- as one of the two possible risk management responses (along with distrust) where the risk cannot be transferred, and security controls would be disproportionate or cannot be used at all; and
- as a property of (at least human) participants that allows them to engage in the system, whose loss could represent a source of risks to the system (if one considers users to be part of the system).

Among others major purposes these types of models can serve are to:

1. Enable design-time analysis of trust and trustworthiness in a vertical 5G application ecosystem, which can be used to support decisions about the design or configuration of security features.
2. Capture the (system-related) context for trust decisions by humans or automata, within which quantitative trust models can be used to assess specific concerns at run time.

Such models could also be used to provide a tangible measure of the effect of 5G security enablers on the trustworthiness (and where appropriate trust) in 5G networks. They may also be used to identify where additional security enablers might be needed, so consideration can be given to adding these to 5G Security Technical Roadmap (5G-ENSURE, 2016).

6.2.2 Trust model requirements

To construct a comprehensive trust model for 5G networks, we need to:

- Better define trust model in 4G networks to use as a starting point.
- Target comprehensive analysis of risks (to which trust is one possible response).
- Further progress on 5G security architecture.
- All aspects on which 5G-ENSURE is active and working collaboratively with other projects through the 5G PPP Security WG and beyond.
- The 5G trust model should allow stakeholders to answer the key questions about trust in terms of:
- In whom (or what) does one trust?
- For what does one trust, i.e. what is it the trustor expects from the thing(s) they choose to trust?
- How much should one trust?
- How much does anyone trust?

Identification of risks and trust dependencies during the design of a 5G service proposition: to understand what might go wrong in a specific scenario, e.g. providing a remote surgery service using a network slice with high guaranteed levels of service, or automobiles with built-in entertainment services, etc. This can be done by mapping potential threats onto the specific system under consideration, to find out where and how those threats might arise in that system. This is something designers of systems to deliver a scenario will want to do, so they can determine which risks are likely to be acceptable to users, and which must be mitigated in other ways by introducing security to increase trustworthiness, or by devising business models in which risks are transferred to stakeholders who can cope with the consequences.

During operation of 5G services: to estimate the trustworthiness of system components (including system stakeholders) so decisions can be made over which components to trust. This can be done with respect to the design-time model of threats to that system, by detecting which countermeasures

are deployed in the running system, and combining this with evidence from the behaviour of system components to assess their trustworthiness. This is really about using machine trust models as mechanisms for managing the network, or for providing guidance to human users over when and how they can trust the network.

6.2.3 Anticipating induces changes by 5G

In 5G, there will be more stakeholders involved in the delivery of any service, due to the opportunities created by virtualisation technology to create multiple virtual networks each of which may serve specific communities or applications. There will be also more recognition of who trusts whom to do what, driven at least in part by the need to manage risks associated with the complex and application-dependent interdependencies if the opportunities of virtualisation are to be seized.

At this stage, it is difficult even to enumerate the stakeholders and trust relationships in a 5G network. One side effect of virtualization is that the relatively static roles found in 4G networks are much more fluid, and services can be composed from other services in more complex ways. This leads to a more complex (and more application dependent) set of stakeholders and relationships. The 5G trust model should recognize a set of roles that stakeholders might take, based on the 4G actor model above plus some new roles such as Virtual Infrastructure Providers, Virtualized Network Function providers, Vertical Application Service Providers, etc. However, the relationships between these actors will not be fixed, but should be flexible enough to capture different configurations that may be found in different scenarios and value chains.

It is anticipated that stakeholders will want to define their roles and responsibilities to each other via Service Level Agreements, given that these responsibilities may vary depending on the scenario. To formulate such agreements, it will them be important to capture expectations and the ways in which things could go wrong.

6.2.4 Trust Enablers

5G-ENSURE is creating three enablers to help identification of trust relationships and management of trust and trustworthiness.

Trust Builder: this enabler provides the means to identify and analyze trust relationships, based on the observation that trust is a response to risk. Trust Builder allows a user to create a high-level model of a 5G network including the stakeholders responsible for managing network components in each 5G domain. The tool then uses machine reasoning to automatically identify potential threats in the network, and to identify stakeholders involved these threats: stakeholders that may be damaged by the threat, and stakeholders responsible for network assets whose security (trustworthiness) offers protection against the threat. Trust relationships can be assumed to exist between those who may be damaged (trustors) and those who could counter threats causing this damage (trustees). Trust Builder also supports the user to identify what security requirements should be met by each network component (and stakeholder).

The idea is that the Trust Builder can be used to analyze 5G network applications (vertical applications) and help the stakeholders understand their interdependencies and devise service level agreements that define their responsibilities to ensure mutual protection. Within 5G-ENSURE we also aim to use this enabler to analyse the proposed 5G architectural specifications and identify trust assumptions that should be acknowledged and specified as part of the architecture itself.

Trust Metrics: this enabler provides a way to define trustworthiness in an isolated 5G network segments, and continuously calculate trustworthiness using information derived from security monitoring of virtualised network functions (VNF).

The idea is that trustworthiness monitoring will be used to control whether or not isolated 5G segment should be used for communication i.e. whether it fulfils the trust related requirements made by participants in the communication. This is most likely to be used to automate the response of devices (e.g. in IoT scenarios) to changes in the security status of a network, or to support human decisions about which network to connect to and use for a given purpose.

VNF Certification or labelization: this enabler provides a certification or labelization process (compatible with industrial life cycles) that can be applied to virtualised network functions (VNF). These functions are critical to the trustworthiness of a 5G system, as they will be managed (at least to some extent) by tenants yet they affect (to some extent) the management of the underlying physical assets provided by a virtualised infrastructure provider (VIP). The concept of VNF certification has to be investigated and proposed in close cooperation with the applicable Trust models (slices and services dependencies).

The idea is that VNF developers will be able to have properties of their implementation certified, so a VIP operator can verify how the VNF might affect their network before deploying it on behalf of a tenant. The properties of the VNF can be expressed in terms of trust metrics related to measures that provide protection against potential threats.

6.3 Trust in Multi-Operator Services

6.3.1 Trust between Operators via Digital Certificates

A Certification Authority (CA) supports trust relationships by building, maintaining and revoking digital certificates. These processes can be used within any given NFV context (ETSI). It is important to note that a certificate verifies that a public key is owned by a particular entity, but **it does not imply the trustworthiness of the key owner**. This and other aspects of trust should be taken into account when using Public Key Infrastructure (PKI). Essentially this has to be done by the registration procedure used by a CA to verify a subject's claims before issuing a certificate referring to the claim.

Should PKI be used for trust, we refer to the ITU-T X.509 to address some of the security requirements. The ITU-T X.509 can be seen as a hierarchical trust model for authentication (Tyrone Grandison). It defines a certification authority tree in which a certificate within a local community is signed by a CA that can be linked into this tree. Such a rigid hierarchical structure could not be aligned with **NFV-specific trust objectives**. Thus, as far as trust is concerned, such objective should be defined before considering the use of PKI over the recommendations of ITU-T X.509.

6.3.2 PCEP Confidentiality in Multi-Operator Connectivity

In the context of 5G-Ex, a candidate mechanism for establishing inter NSP connectivity is the combined usage of Border Gateway Protocol-Link State (BGP-LS[5]) for abstracted topology dissemination at provider level and Path Computation Element (PCE) for the actual path computation and instantiation of connectivity. In the case of inter-domain path computation, the end-to-end inter-domain path is a concatenation of intra-domain path segments resulting from cascaded PCE-to-PCE cooperative communications. The PCE architecture can be considered as de-facto standard to effectively deploy TE in multi-domain networks (Francesco Paolucci). However, despite authentication, authorization and encryption mechanisms, confidentiality issues still might arise inherently due to the exchange of information on network resource availability (e.g., link bandwidth) aimed at the inter-domain LSP set-up. In fact, the information exchanged in inter-PCE communications can be used in a malicious way.

5 http://www.iana.org/assignments/bgp-ls-parameters/bgp-ls-parameters.xhtml

Security Monitoring and Management

7 Security Monitoring and Management

New innovative solutions for security monitoring and management are key to achieve and ensure the highest level of security and resilience as demanded for 5G networks.

5G brings many innovations from both a technical and a business point of view. On the one hand, this innovation will increase the number and variety of potential threats while at the same time providing enhanced mechanisms for protection. For instance, virtualization technologies have introduced an increase of attacks' surface and started generating a lot of new security issues, e.g. topology poisoning, potential leakage of data caused by isolation flaw among shared hardware, side channel attack between slices. On the other hand, virtualization can make it easier to contain or mitigate the effects of attacks, e.g. by making it easier to isolate critical functions or migrate them to safer parts of the network.

To cope with the new threats induced by 5G, it is important to include security monitoring by design and, even more importantly, to activate security monitoring during the 5G network infrastructure operations to (pro-actively) detect and efficiently respond to security threats in a dynamic and context-sensitive way. Overall effective and efficient security monitoring capable of producing clear evidence of threats and attacks is one the key ingredients for generating the necessary trust and confidence of various stakeholders to fully invest in/adopt it and ensure it realises its full potential. It is also a way to make the 5G network cyber resilient.

7.1 Security Monitoring in 5G Networks

Several research and development actions have been undertaken to study and achieve both effective and efficient security monitoring in 5G networks. Many projects of the 5G PPP phase I are active in this field, aiming at defining the foundations for network security for software defined 5G network towards the 2020 milestone.

The 5G threat landscape needs to be captured and continuously monitored. Introducing disruptive concepts,such as SDN and NFV to the communications network of critical infrastructures requires a careful investigation into new security risks since new threats not encountered in legacy systems will occur. More specifically, SDN is currently used only in closed environments, such as data centres. However, the use of SDN in cross-domain setups and the absence of multi-operator collaborative incident detection mechanisms brings new threats. The nature of software increasingly used in SDN and NFV environments come with additional security threats, such as data forging, application programming interface (API) abuse, controller and management exploitation that will need to be avoided by means of suitable mechanisms, e.g., strong authentication, access control, application isolation and sandboxing, flow integrity and conflict resolution as well as threat detection and encrypted interfaces.

7.1.1 Analytics applied to security operations

Due to the complexity and dynamic nature of network topologies, the fact that third parties could connect or leave the infrastructure at any time, the fact that those multi-tenant infrastructures completely modify the liability chain from an E2E perspective requires automatic and efficient tools to manage the dynamicity of the network, the control of the infrastructure owner on their resources, control of user requirements over the entire 5G infrastructures, etc. One approach that is agreed inside the 5G eco system is related to the use of Analytics.

Analytics applied to security operations are key in the 5G context, because they enable the analytical processing of a large number of logs produced at the network and application layers. These can provide essential inputs to learning processes

(based, for example, on Machine Learning or Artificial Intelligence approaches) that can steer decisions in automated network re-planning and threats prediction/preventions, maximizing the effectiveness of any adopted mitigation solutions. Furthermore, such tools could also help to manage the dynamic responsibility shared between parties and be able to proceed to forensic or post-mortem evaluation of Root Cause Analysis after security threat attacks.

CHARISMA is proposing a real-time, automated Security Management Framework for 5G telecommunications networking, by implementing a continuous and closed loop real-time environment inspection regime, based on analytics, policy-based decisions and actuation/enforcement via Cloud & SDN orchestration procedures. In particular, the virtualized nature of 5G networking itself allows the automated instantiation, deployment, configuration and management of Virtual Security Functions (VSFs) in real time, with a centralized orchestration approach. In CHARISMA, the introduction of Converged Aggregation Levels (CALs) enables the de-centralization of network intelligence, and also contributes to early detection and neutralization of attacks, placing the diagnostics and neutralizing systems as close as possible to the malicious entities originating the attack, and preventing hostile traffic from entering the network backhaul.

The COGNET project is also applying Machine Learning techniques, using a double closed-loop data streaming architecture, to threat detection, attack analysis, and security incident mitigation and response.

7.1.2 5G threats landscape

CHARISMA has analyzed and reported in [23] the different security threats associated to several typical 5G use cases and scenarios and extracted a set of security-related requirements for the 5G network. Moreover, CHARISMA foresees several key assets to deliver secure end-to-end services for 5G networks: security policy management, decision control for threat detection, orchestration, configuration and management of security services, virtualization isolation, access management and proactive traffic and resource monitoring.

SELFNET has made a detailed investigation into the new definition of perimeter security [24] [25] in virtualized 5G infrastructures, implications in workloads associated with multi-tenancy infrastructures, and how this perimeter security in virtual infrastructures can be protected against cyber-attacks by providing mechanisms to allow the inclusion of security control points along the 5G architecture. These control points allow the deployment of security monitoring components and the deployment of security enforcement components in key architectural places of the 5G infrastructure.

The 5G-ENSURE Project is active in the field through work engaged on 5G Trust model as well as risk analysis, not limited NFV/SDN threat only.

5G-Ex has compiled a list of security requirements specifically for 5G services jointly provided by multiple operators and the enabling orchestration framework. Furthermore, 5G-Ex is involved in establishing trust between multiple administrative domains in the context of multi-operator services [26].

7.1.3 Techniques for threat analysis and RT monitoring of 5G (industrial) systems

The aim behind this process is to reverse the imbalance of intelligence capabilities of the attackers versus the network infrastructures under attack, especially those considering SDN components. The cyber-adversaries prospective consists of: 1) developing knowledge on attack motivations, favoured techniques and known activities. 2) developing real-time security monitoring mechanisms, including mechanisms for monitoring network traffic will provide global visibility into actual conditions of an organization's operation as well as insight that can identify normal versus abnormal operation in the internal network infrastructure. 3) running automated security incident response mechanisms utilizing Virtualized infrastructure (Computing-NFV or Networking-SDN) architecture for joint intrusion detection, fraud management, and log and event management, while maintaining operational contact with the international CSIRTs (Computer Security Incident Response Teams) community.

When it comes to virtualization-powered infrastructures, the importance of successfully performing incident response becomes of paramount importance. The holistic nature of an SDN infrastructure with all its important advantages also demands state of the art security, monitoring and response procedures to maintain the necessary trust and optimum performance.

5G networks will go far beyond the networks of today. This is especially the case when it comes to 5G integrated satellite and terrestrial systems that will ensure high availability and service reliability with a 100% geographic coverage. This calls for new enabling technologies such as pseudo real-time monitoring of information collected to protect against internal and external threats coming from such type of heterogeneous and widely distributed systems.

CHARISMA has developed a generic Monitoring and Analytics system which captures information from multiple virtualized and non-virtualized resources, analyzes different preconfigured aspects of such information and provides alarms for subsequent policy-based decision and action. Apart from generic monitoring metrics, the Monitoring and Analytics system aggregates events and information coming from the deployed security services, such as intrusion detection systems, firewalls, etc. All generic monitoring metrics, events and logs collected will be used for the identification of potential security attacks and threats.

The 5G-ENSURE Project is one of the Phase 1 projects active in this field and is developing security monitoring enablers. One of them, the Proactive security analysis and remediation (PulSAR) enabler, aims at providing the means to protect against cyber-attacks. The motivation here is to enable complex attack detection, provide a clear view on an attack's progression by giving means to understand on-going attacks when a node is known as compromised, and also automatically compute possible remedies, potentially also their costs, depending on the company assets, e.g. sensitive data and resources, and the IT system vulnerabilities.

Another possible approach to monitor and respond to security threats on virtualization-enabled networks lies in machine learning algorithms that control security service function chains. One such method is to deploy security zones or networking islands, where the zones are deployed as service function chains (SFC) on the provider's network edge and administered via tailored security focused machine learning methods. This approach also needs to be dynamic in nature, tenant based, virtualized and distributed across the service providers network, thereby increasing network efficiency and network resource effectiveness. As cyber-security threats become more aggressive in the form of advanced persistent denial of service (APDoS), distributed denial of service (DDoS) and volumetric pipe threats, the possibility of manual intervention to detect and mitigate threats in a timely manner becomes less viable, and the need for automated responses increases.

A machine learning security threat detection system can be considered as an event, condition and action (ECA) rule based policy, where the event and action processes are considered to be part of a service function chain. The machine learning solution also has the advantage of being able to analyze past records from Big Data archives to evaluate how the tenants' network patterns functioned during normal network behaviour.

Multiple machine learning models acting in unison on streamed datasets can be used to provide an improved anomaly detection prediction. These predictions can also be combined together to boost the threat prediction accuracy rate. In conjunction with deep learning and neural network machine learning models, with their evolutionary programming adaptation process it is possible to iteratively deploy networks that become stronger at adapting to new aggressive automated network threats.

The COGNET project is actively working on a tenant based Distributed Security Enablement framework that uses machine learning to detect security threats on their corresponding network. NetFlow and sFlow probes reside on their Service Function Chains that will sample the tenant's data plane traffic. If an anomaly is detected the actuation section of the SFC implements a corrective security rule. The work is documented in [27] [28]

The SELFNET project is working on advance distributed architecture to allow efficient network probes to be deployed in the infrastructure to identify key metrics for threat detection and behaviour modelling associated with the different 5G Network Operators that will be sharing the infrastructure. This information together with the meta-data provided by the control and management plane of the different architectural layers of the 5G eco-system allows threat analysis to identify cyber-attacks. This threat analysis is performed by using close to real-time information provided by such probes to come with an effective detection of the attack and later on with an effective set of counter-measures (where possible) to protect against such attack.

7.1.4 Application and customer specific security configurations and monitoring

5G networks will connect substantial amounts of devices and serve different applications and customers with different security needs. This heterogeneity of applications and scale of communication is a challenge for the efficiency and accuracy of security controls and monitoring solutions. For instance, the heterogeneity makes it more difficult to detect application specific attacks or to dynamically react to perceived risks.

Software networking and virtualization techniques enable the deployment of security configurations for specific applications or users. By isolating application specific connections from each other, 5G network may for instance provide customized monitoring analytics and deep packet inspection for manageable amount of homogeneous data streams.

Application-specific isolation can be referred as network slicing or micro-segmentation. According to the (not yet fully standardized) network slicing concept [29] [30] [31], network slices can be

considered as isolated network resources serving specific types of E2Econnections. The micro-segmentation [32] [33] concept originated in data centres, and can be utilized as a short-term reference solution for providing fine-grained and dynamic configurations, and enable more customizable approaches to slicing. Micro-segments are isolated network resources dedicated for specific types of connections by one administrative domain. Going beyond the current view of large static network slices, micro-segments can provide more specific access controls and stricter security policies.

Micro-segmentation could be a good security solution especially for mMTC, M2M or Industrial Internet based companies, which require an elevated level of security for their application services and service isolation. In addition, mobile network operators and virtual mobile network operators would benefit from the solution, as they would be able to provide adequately secure segments of the mobile network for further use. Micro-segmentation could be used to serve customers that have different security levels depending on the used service. For example, in a micro-segment supporting "automotive" or "e-health", the security is of high concern while for a micro-segment supporting "general IoT" a lower security level may be acceptable.

The 5G-ENSURE project is working on 5G micro-segments and is investigating security monitoring to be associated with them. Compared to slicing that will offer basic security functions and basic security monitoring, micro-segments will offer the possibility of fine grained security monitoring or at least security monitoring tailored to meet specific needs.

The COGNET project is actively working on a tenant-based Distributed Security Enablement framework, this can be considered as a similar approach as the micro-segment one discussed above, but COGNET expresses these logical domains as SFC-enabled networking islands or security groups. The work performed is documented in COGNET [28].

7.2 Security Management in 5G Networks

7.2.1 Security management in a common logical/virtual layer

7.2.1.1 This section describes security management intended for a common logical and virtual layer, presenting also several challenges identified by phase 1 projects. Mechanisms for fast signature matching and fast processing at data plane

Many security VNFs require intensive CPU tasks and substantial amounts of memory (virtual RAM) which means data plane optimization techniques will be needed to achieve stable and high performance comparable to the standards of legacy physical network functions in terms of I/Os for traffic analysis, manipulation and forwarding [34]. Fast processing at data plane in a security context is typically needed to obtain fast packet processing and fast traffic inspection/signature matchingto promptly react with security enforcement.

Much more flexible are the software acceleration frameworks, which rely on a set of one or more optional software layers to increase network throughput and reduce operating overhead in a NFV deployment comprising Compute elements, Hypervisors, VNFs, etc.

Moreover, the growing trend towards pervasive E2E encryption will quickly invalidate all current techniques for signature matching and any other mechanism of traffic inspection at the data plane. The COGNET project is working on the application of Machine Learning techniques for attack identification in encrypted network flows.

Security services that analyze the incoming traffic, such as Intrusion Detection System VNFs can be configured to be off-path to avoid introduction of latency due to processing. This cannot be done for those security services that perform actions on on-going traffic, i.e. Intrusion Prevention Systems. These services need configuring in-line to perform actions on the passing traffic. CHARISMA is using both types of services, however, traffic analysis VNFs (vIDS) are preferably placed off-path. The re-acting VNFs that are placed in-line are selected in a way to introduce the less delay possible (e.g. virtual firewalls).

The SELFNET project is developing a Self-Protection use case [24] [25] into which the state of the art Network Intrusion Detection Systems are used by leveraging these techniques and in virtual functions. The SELFNET approach is in-line with the CHARISMA approach, but it is considering a two-loop innovation to reduce the amount of VNFs inserted along the data path with the idea of reducing delays and overheads and at the same time to allow for a distributed sensing of key metrics to be used for the detection phase of the treats. In terms of the reaction, SELFNET is also providing an innovative

security management where the deployment of VNFs is placed just in the position along the data plane where it is more convenient to stop or mitigate such attack.

7.2.1.2 Securing the network control plane

Centralized control of the overall network infrastructure and the use of open interfaces have an enormous potential to simplify and enrich network management. However, centralized control represents a valuable target for attacks and a single point of failure. Furthermore, the use of open interfaces and the accompanying 'softwarization' of networks pose new threats to a network. Software is difficult to get right, which makes it inherently buggy and vulnerable. Furthermore, opening the programming interface may break security assumptions of several network deployments, which assume operation in a controlled environment with exclusively trusted actors. Such [35] environments may not be well prepared for open APIs. They might, for example, lack authentication mechanisms and have only lax or even no input validation.

A wide variety of different mechanisms will be necessary to secure the control plane of a 5G network. For example, mechanisms that control the access to network resources and enforce access control policies are needed. Such mechanisms would prevent unauthorized reconfigurations of network components and would protect against intended or unintended network misconfigurations. This is a field where the 5G-ENSURE project is active in developing two enablers (access control mechanisms and component-interaction audit enablers).

The project SONATA has introduced the gatekeeper concept, a mediation service in charge of authorizing, validating, and logging service and function definition and deployment. The gatekeeper is an essential component for orchestration recursion, both vertical (service abstraction and slicing) and horizontal (multi-domain orchestration and federation), and to support DevOps and Continuous Integration.

The VirtuWind project is also active in the field, bringing two elements on the SDN controller: the Reference Monitor (coordinates the component sequence of operations, and verifies all entity operations/requests against the specified access control policies) and Security Manager (authenticates involved entities, keeps track of security-related activities for Accounting purposes and communicates pertinent data to the backend e.g. for more sophisticated analysis techniques). Moreover, provisions are made to employ techniques such as controller clustering for redundancy and fault tolerance technologies (e.g. Byzantine Fault Tolerance) to localize faults and secure the distributed control plane, providing reliable and consistent control of the network even in the case that some controllers have failed or are compromised [36].

Another example are mechanisms that uses trusted and/or trustworthy computing for the certification of network components and address the lack of a trust chain and traceability between management applications and data plane are also needed for enhancing the security the network control plane. The 5G-ENSURE Project is developing a VNF certification enabler.

The SONATA gatekeeper considers the inclusion of mechanisms for image verification and the incorporation of license management, with the goal to guarantee trustworthy deployment and seamless execution of software-based network infrastructures.

7.2.1.3 Coordination of security functions distributed across various VNF-Components

A typical security service in 5G networks is a composition of multiple, differentiated and specialized security Network Functions, both Physical (PNF) and Virtual (VNF) which are chained into an E2E service flow. Virtualization allows flexibility and automation of provisioning and re-planning processes, also enabling multi-tenancy of various isolated virtual infrastructures on top of a shared physical infrastructure.

Specific elements (potentially candidate VNFs) for this type of security scenario are split along the two major phases of the cyber-attack service lifecycle: a) sensing, where the system has to deploy traffic monitoring probes to collect and correlate traffic data to identify cyber-attacks and b) actuation, where the system has to deploy a chain of mitigation network functions and configure the appropriate traffic steering policies to let malicious traffic go through threat management systems and be mitigated/filtered.

Beyond the split of functional areas, a VNF is obtained from the composition of different service chain components, specialized in different processing aspects (e.g. distributed detection or prevention on flows, distributed firewall policy enforcement, distribute DPI, etc.).

CHARISMA implements two security related VNFs: a virtualised Intrusion Detection System (vIDS) equipped with advanced traffic analysis and monitoring capabilities for attack detection; and a virtualized firewall (vFW) able to filter the passing traffic based on a predetermined set of security rules. Both VNFs are comprised of a single VNF component (VNFC) and are offered as individual security services. Additionally, server applications were developed and instantiated within both VNFs to assist in real time policy enforcement. Policies

are communicated to external interfaces as HTTP requests sent to RESTful web APIs.

SELFNET is developing a control framework to manage and orchestrate the multi-tenant security service, capable of properly reacting to block and mitigate the attack, aimed at having zero effect for the end-users traffic and services. Possible reactions under study in SELFNET include: deployment of a new actuator VNF at the proper location in the security service chain (with re-configuration of the chain itself); and deployment of a new sensor VNF specialized for the given traffic pattern or intrusion type. Self-organization functions for automated re-configuration of service chains is key in the SELFNET reactions approach to cyber-attacks.

7.2.1.4 Run-time network adaptation mechanisms for incident response and mitigation

A framework of incident handling will usually form the basis of the mechanisms of monitor, detection and response/adaptation phases of a security incident. Mitigation strategies include decision making (prevention, remedial), changing roles of user privileges, and correcting system problems. The result of the response phase is improved security awareness.

The VirtuWind project is working on a Reactive Security Framework, equipped with SDN and SCADA honeypots, modelled on (and deployable to) an actual, operating Wind park, allowing continuous monitoring of the industrial network and detailed analysis of potential attacks, thus isolating attackers and enabling the assessment of their level of sophistication [36]. More specifically, the chaining of security functions enables the routing of unknown/suspicious traffic via Intrusion Detection and Deep Packet Inspection Service Functions, to classify it (as either legitimate or malicious), and forwarding it to the Wind Park or the honeypot, accordingly. Thus, malicious traffic can be isolated at the honeypot, allowing us to track the attacker, identify her purpose and keep her occupied. The honeypot itself is modelled after the actual operating Wind Park, fully emulating both the network (SDN-based) elements as well as the industrial application-related devices (e.g. SCADA systems), by combining the appropriate Honeypot/Honeynet security tools.

As a reaction to any botnet detection, a virtualized and personalized honeynet is being configured as an actuator network function in SELFNET to isolate potential cyber-attacks such as Distributed Denial of Service (DDoS) attacks, which can be triggered by the botnet owner. Such a honeynet acts as a fake network: the detected zombies are logically placed as cloned zombies to emulate the behaviour patterns of each real zombie, by contacting the Command & Control (C&C) Server, the main dashboard of the botnet owner, on behalf of the real, original zombie. From that moment on, the botnet owner will believe that the real zombie still exists, although it is not true. Subsequent cyber-attacks will not be carried out in reality [25].

7.2.1.5 Policy-based security management

Increased complexity of security mechanisms in 5G networks is not only due to the virtualization of resources but also to security requirements at different levels or domains such as network slice, network service, and network resource (physical & virtual) and RAN slice. Hence, a security management system, guided by a set of defined security policies, is essential to ensure that security mechanisms functions are enforced as planned.

This is not only applicable to one single administrative domain, but to several domains. The 5GEx project aims at establishing procedures for negotiating management boundaries in a multi-operator service delivery scenario. Such negotiation should result in an agreement between administrative domains on which operations a domain is allowed to do in another domain's network, whether per slice or per service. A related challenge is ensuring that slice management commands executed by one domain on another domain's infrastructure comply with this agreement.

7.2.2 Multi-layer security management

This section covers several challenges identified for multi-layer security management within Phase 1 projects.

7.2.2.1 Situational awareness for 5G security management

To tackle situational awareness for 5G security management problems, there is a tendency to assume more cognitive methodologies, thereby facilitating understanding of the environment through contextual analysis. Chief among this is the development of the Situational Awareness (SA) of the protected environment by applying the Endsley's model [35]. In accordance with this method, the perception, comprehension and projection of the system status needs taking into account. Because of the s, the Endsley's model has been specifically adapted the significant complexity of managing the security of current networks, leading to coining the term Network Security Situational Awareness (NSSA). Notwithstanding the extensive literature on this subject, there is not an NSSA general approach to the problem of security management on 5G networks. However, attempts have been made to implement the SA paradigm on recent uses cases

related to these technologies. A commonality is that they all consider three main stages of information processing on SA, i.e., perception, comprehension and projection. In broad terms, perception comprises the tasks of monitoring and identification of incidents, comprehension covers their analysis and association, and projection predicts the evolution of the state of the system.

7.2.2.2 Mixed integration of virtualized and physical security gateways/functions

Security network functions like IPsec Gateways, Firewalls, Load balancers, IPS, DPI, etc. are typically based on specialized architectures in which the flow processing at data plane is done by dedicated hardware acceleration tools and architectures. These are typically referred to as Physical Network Functions (PNF). The transformation of PNFs to VNFs may take several years because of the need to achieve high performance levels. Some PNFs may never be virtualized.

Therefore, hybrid network architectures in which PNFs and VNFs for security gateways/functions co-exist are fundamental to ease successful transformation and migration to NFV of existing network infrastructures. In this scenario, it is vital to have a unified network management system that manages both physical and virtual domains and provide unified view of the networks relying on:

- Common resource and service abstraction models (e.g. inspired by ONF Table Type Patterns through which to describe specific switch forwarding behaviours).
- Open interfaces for the configuration of the services (e.g. NETCONF, OpenFlow, etc.).

CHARISMA is currently investigating the use of closed-loop automation procedure in a hybrid 5G network comprising virtualized and non-virtualized network elements.

SELFNET is working on a control framework integrated with ETSI MANO capable of integrating sensors and actuators from both the physical and virtual domain.

7.2.2.3 Techniques for defining "isolation verticals" and runtime management/verification of isolation per tenant/user

The term "isolation vertical" is used to highlight the requirement of ensuring secure multi-tenant support across 5G infrastructures that rely on SDN and NFV practices to automate the deployment of services and functionalities. Secure multi-tenancy should primarily focus on traffic isolation among different tenant topologies as well as isolation of control plane functionalities with respect to the monitoring and management of network and virtualized components to avoid exposing to a tenant even the existence of forwarding or statistics pertaining to other tenants. Since this kind of mixed SDN and NFV based architecture spans across different layers starting from as low as the bare-bone machinery and physical network equipment and expanding up to complex and autonomous/automated OSS/BSS functional blocks, several different practices should be applied and synchronized to establish the required isolation per building layer. Each tenant is assigned a control space over the functionalities offered by a specific layer so that control policies are enforced only on the tenant's assigned resources and do not interfere with resources belonging to other tenants.

This kind of "silo-ing" of tenant control spaces over the logical and physical functionalities of each layer forms a logical overlay per tenant across all the involved layers. This can be considered as an isolation vertical that provides each tenant with full functionality over the autonomous/(semi-) automated and/or self-organizing features of a combined SDN, NFV and SON integrated platform. In this context, all the involved layers are identified along with the characteristics of the required per tenant separation that can be achieved. Each layer builds on the separation achieved by the layer below it and applies a higher layer separation so that at the top most layer of OSS/BSS, which is based on autonomous management, the full set of features of SON practices can be utilized by every tenant for easier deployment of added-value services.

One high-level objective of the CHARISMA project is to support the emergence of Virtual Network Operators (VNOs) in multi-tenancy environments. The virtualized physical resources of a 5G network infrastructure operator are shared by the VNOs enabling the rapid deployment of services, the flexible and efficient utilization of the required resources and the differentiation of the offered services against competitors. To achieve this, the created network slices must support complete traffic isolation between VNOs i.e., no traffic from one VNO should reach the other without explicit consent. Isolation will be achieved relying on a combination of two technologies, SDN, using virtual switches for each of the networks and VLAN segmentation (IEEE 802.1q).

VirtuWind aims to address the multi-tenant challenges in industrial applications, particularly Wind Parks. The design aspects of VirtuWind are enabled by the presence of a VTN Manager on the SDN Controllers and the multitenant functionality is driven by following principles: abstract the complex physical network configuration from administrators, form virtual users and customer networks, introduce security protection mechanisms for VTNSs, present a

transparent view on the network for critical tenants in the industrial infrastructure; and provide strict priority for mission-critical control and operational traffic [36].

7.2.3 Key Research Challenges in Security Monitoring and Management

In this section, we present additional challenges anticipated in the field. While this list is not exhaustive, it highlights some of the major points that remain open and for which additional research work is needed.

- How to combine the needs for E2E security monitoring with the need for strong isolation between slices (at Core and Access level) and how to prevent security shortcuts via a monitoring and management system.
- How to adapt in real time an E2E security monitoring system, if the logical or physical infrastructure and topology used to deliver the service evolve in real time (dynamic topologies).
- Regarding future dynamic topologies, virtualization (SDN/NFV), potential multi-tenant infrastructures and potential delegation of some network function to private entities, it seems we should have to migrate from a Trust concept to an E2E Liability concept. Relevant questions for consideration are: which entity will assume some risks or impact of a security flaw or who will pay in the end.
- How to define a security and management framework that allows centralized control but distributed over the network perimeter (fog and MEC approaches).
- Infrastructure sharing by multiple virtual network operators will require strict isolation at multiple levels to ensure absolute security. In particular, different aspects of the control-plane, data-plane and resource isolation have to be investigated and guaranteed to ensure zero correlation across the operations of different tenants. Tenant isolation is ultimately important to ensure a reliable and warranted service assurance, together with data and communication integrity and confidentiality.
- The security of VNF itself as an element, e.g., VNF hardening, VNF verification/attestation, VNF code robustness, etc. must be considered.
- A key question when considering Machine Learning is not whether a learning algorithm is superior to others, but evaluating under which condition a specific method can adequately outperform other methods for a given security problem (e.g. DDoS, fraud detection, customer assets abuse). The key challenge here is selecting appropriate machine learning algorithm and its learning styles for an accurate and efficient prediction; and not to under or over fit a machine learning classifier for a flexible prediction that can account for some noise in the dataset.
- The use of SDN in cross-domain setups and the absence of multi-operator collaborative incident detection mechanisms introduce new threats. This necessitates the development of intra- and inter-domain incident detection mechanisms including real-time detection, analysis and prevention for the trace-backs and audits enhancing root cause analysis during incident response, and failure analysis mechanisms.

The nature of software increasingly used in SDN and NFV environments comes with additional security threats, such as data forging, application programming interface (API), controller and management exploitation which need to be avoided using suitable mechanisms, e.g., strong authentication, access control, application isolation and sandboxing, flow integrity and conflict resolution as well as threat detection and encrypted interfaces. Intelligence-driven, proactive and reactive security capabilities are thus needed.

Slicing / Virtualisation and Strong Isolation

8 Slicing / Virtualisation and Strong Isolation

8.1 Motivation

The upcoming 5G networks are expected to comprise many heterogeneous devices, services, and generous amount of network traffic. This brings scalability challenges for the security of the mobile network. Having large segmented security zones can create significant attack surfaces and enable threats to move across large portions of the mobile network unrestricted. Thus, there needs to be a way to divide the mobile network into smaller parts to provide better scalability as fewer nodes need to be handled by security monitoring at a time. Also, by focusing on smaller parts in the network, better accuracy can be achieved for anomaly detection as the focus is on a less heterogeneous part of the network.

The Network Slice concept has been recently introduced for the upcoming 5G mobile networks and it is an integral part of 5G [31] [37] [11] enhancing 5G security by a divide and conquer approach to solving security problems. However, the effectiveness of this approach still depends on the selection of security mechanisms and their implementation. A network slice in the context of 5G consists of a collection of 5G network functions and specific RAT settings that are combined for a specific use case or business model [38]. In other words, a network slice is a logical instantiation of a network, with all the functions that the network needs to operate. A single, common physical network is separated into multiple complete, virtual, E2E networks. These virtual networks are logically isolated from each other, in terms of device, access, transport and core network, and are typically dedicated to different tenants and/or different types of services, considering the intrinsic characteristics and requirements of each one[30]. The aim is to guarantee, for each network slice, a minimum of dedicated resources, (e.g. computing resources), QoS parameters (e.g. low latency) and services (e.g. security or traffic shaping services), thus providing networks customized and optimized for different use cases/business models/market scenarios. This concept is depicted in Figure 6:

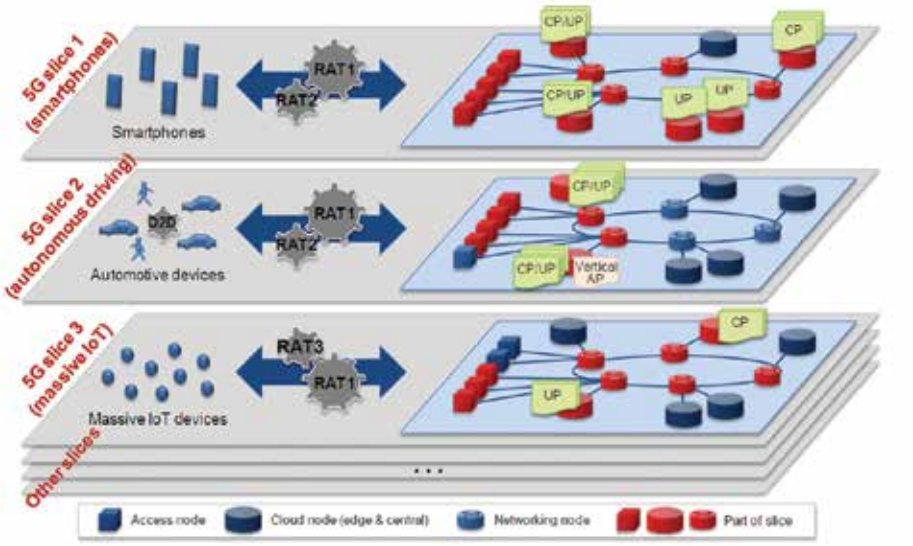


Figure 6: 5G Slicing – NGMN Alliance [39]

Network slicing is not a new concept, as Virtual Private Networks (VPNs) are a basic version of a network slice [37]. However, 5G networks have a wider scope and will need to cope with more challenging requirements, calling for an entirely new definition of slices. Slicing is an SDN/NFV-based alternative to VPNs (or 3G/4G Access Point name) for isolating traffic associated with a certain user or application from other traffic in the network. Network slices can be considered more as networks on-demand, which will be created, deployed and removed dynamically. For example, emergency communications could be isolated from the rest of the network with the goal of improving response time. Ultimately, with network slicing it is possible to implement different security measures and policies, facilitating the provision of certain level of quality and security to an application or a service.

8.2 Slicing in the Security context

Enlarging the perspective to security services for 5G networks, the concept of slicing enables many new options for managing network security in a more flexible, reactive and self-adapting way. Imagine multiple, differentiated and specialized security VNFs that can be chained in dynamic and rapidly adapting way within the logical instance of a network slice reserved for a tenant (owner and prime consumer of the slice resources). These logical functions allow to deploy tenant-scoped security functions that are needed to manage a cyber-attack reaction, i.e. for *sensing* via traffic monitoring probes that collect and correlate traffic data to identify attackers and their patterns, and for *actuation* via service function chains of security VNFs that allow to configure the appropriate traffic steering policies and threat mitigation/filtering rules (e.g. see [24]).

The logically dedicated and isolated resources within a network slice are key to developing distributed security services for 5G networks, capable of spanning edge and core virtual networks, featuring traffic attraction mechanisms to move attacks to a honeynet, which remain isolated from the legitimate traffic and traffic of other tenants in a shared infrastructure, threat/attack information gathering based on packet inspections, pattern recognition/detection engines, network monitoring and analytics, and distributing and running in parallel security functions (like rules, signatures, detection algorithms, etc.) across multiple and coordinated VNFs to implement highly performant security services. Thus, from the security perspective, it is essential to note that slices should be fully isolated and come with minimal but key security functions, i.e. core security functions, such as guaranteed E2E isolation, communications confidentiality & integrity, and AAA/traceability. Some key security issues in this context are highlighted in [40].

8.3 Slicing levels

Given the inherent flexibility of 5G networks, slicing has many approaches and applications. Slicing can be implemented and/or extended to various levels throughout the communication infrastructure, from the user equipment to the access and core networks, up to the virtualized applications; the Access Network can be common among slices; the network slices may include different network functions, optimized for a specific application or feature identical functions but dedicated to specific customers (i.e. subsets of UEs) who are able, via dedicated APIs, to set some parameters of the operation in their dedicated network functions. Some approaches investigated in 5G PPP Phase 1 research efforts are detailed below.

8.3.1 RAN network slicing

At the radio interface, the static assignment of frequency bands to different mobile network operators (MNOs) can be considered as a coarse-granular slicing. Resource isolation between these slices is based on collective agreement and good behaviour rather than enforced by technical means. Security isolation (in the sense that no interception or faking of traffic between these coarse slices is possible) can, however, be achieved by technical means, namely the use of cryptography.

For finer granular partitioning and efficient usage of radio resources between MNOs, 3GPP has specified a concept called MOCN (multi operator core network). Here, a common radio scheduler handles the traffic of several MNOs, allowing to assign not only frequency bands but even time slots within a frequency band individually to MNOs. By this, the radio scheduler creates fine grained and dynamically adaptable radio resource slices. Each slice may have a guaranteed amount of radio resources, their sum not exceeding the amount of available but unused resources of

one slice may be assigned other slices. Obviously, isolation and correct assignment of resources fully depends on the radio scheduler, which needs to be trusted by all participating MNOs. Again, security isolation is ensured with cryptography, which is specified for all mobile network generations in use today.

In current LTE networks, the RAN is typically implemented by bare metal equipment, i.e. proprietary hardware controlled by proprietary software. Multi-tenancy is not supported by such bare metal equipment, so the MOCN approach means that the complete RAN implementation must be shared. The new 5G network architecture proposed by 5G-NORMA, multi-tenancy is introduced into the RAN, allowing different MNOs to run individually tailored RAN functions on shared hardware, i.e. the edge cloud. Isolation between such operator slices can be ensured by existing NFV mechanisms, and the RAN slicing security will profit also from any future improvements of the existing techniques.

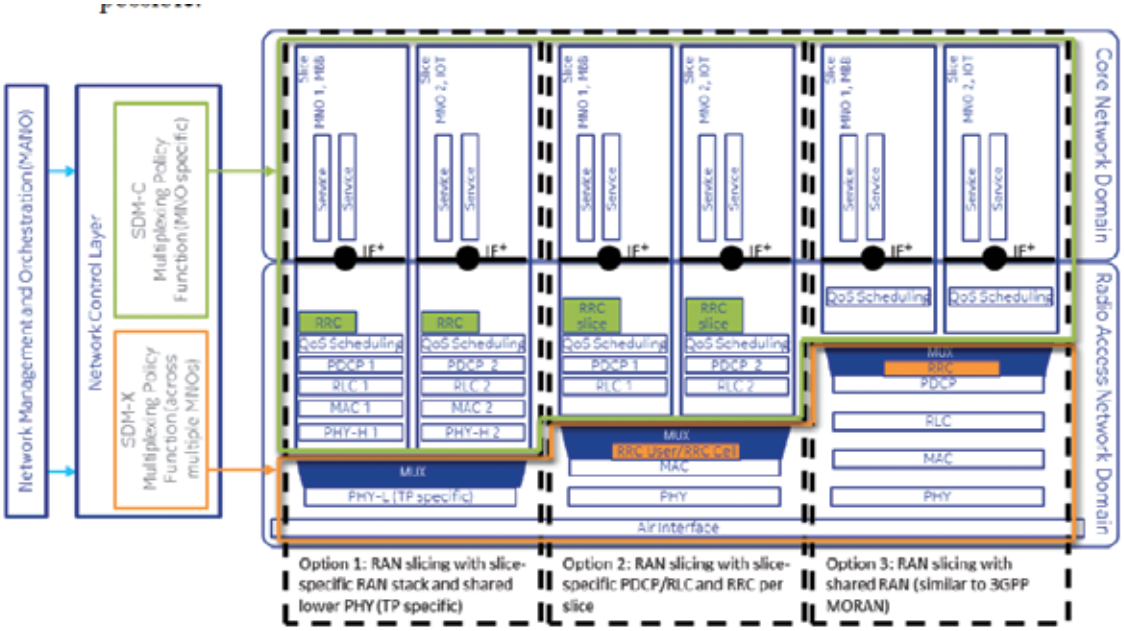


Figure 7: RAN Slicing (3 options) [41]

Note that with this approach, there will still be shared functions in the RAN. Inherently, there must be one instance that finally decides how to use each time slot in each frequency band on the radio interface. Also, even if not the functions themselves, but only the infrastructure, e.g. an edge cloud, is shared, a commonly trusted party is still required to provide this infrastructure. However, the 5G-NORMA approach supports efficient and flexible multi-tenant RANs while maintaining a high degree of security and isolation between the different RAN slices.

8.3.2 Core Slicing

A typical approach to slicing is for it to be realized at the core network, segregating across or parts of the control, management and/or data planes, as depicted in Figure 8:. Some approaches noted in current research efforts are detailed below.

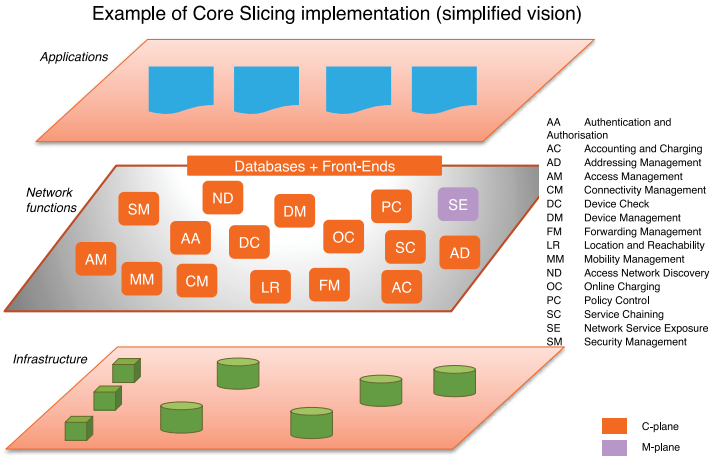


Figure 8: Example of Core Slicing implementation (source: Orange Internal)

8.3.2.1 Via Isolation at data plane but sharing of knowledge bases, signatures, monitoring KPIs for security, vulnerability intelligence

Whilst the resource and network isolation capabilities offered by network slices are key to implementing multi-tenant scenarios, it is similarly critical in the context of security to share threat and vulnerability information, reaction models, etc. More than the design and provisioning of an E2E security service, these aspects attain the design and operations of a cyber threat-management framework, in which a comprehensive threat intelligence is built leveraging per tenant functions (e.g. security monitoring and threat/vulnerability identification), and selection of reactive and proactive remediation actions derived from a shared, consolidated knowledge base.

The security service operator spawning the various network slices for the various security services of his tenants, can offer centralized cross-tenant/slice analytics and prediction services, based on the various information made available through the different sensors, deployed in the infrastructure and in each slice. This master analytics service is capable of correlating information on attacks from multiple slices and thus enhance the security services offered within each slice, e.g. by notifying alerts on potential attack approaching the tenant's network and triggering the configuration of preventive countermeasures, i.e. adaptation of security function chains, injection of ad-hoc traffic filtering rules, updates of threat identification patterns, etc.

8.3.3 Application-level Slicing

Slicing can also happen on the application-level, whereby its concepts are applied in application-specific deployments and the associated domain-specific network functions (typically virtualized). Some examples are provided below.

8.3.3.1 Via Network Virtualization

A characteristic example of application-level slicing the industrial network-focused approach comes from the VirtuWind project, where slicing is applied in the context of multi-tenancy in industrial, operational Wind Parks. The main design aspects of the multi-tenant functionality are to abstract the complex physical network configuration from administrators, form virtual users and customer networks, provide security protection mechanisms for VTNSs, present a transparent view on the network for critical tenants in the industrial infrastructure and provide strict priority for mission-critical control and operational traffic.

The basic design principles of multi-tenancy in industrial environments are described herein. A single physical communication network is rolled out as an industrial network infrastructure and offers the physical communication platform for all users, devices, sensors, administrators or customers. Virtualized networks are formed and implemented on top of this common physical network infrastructure. In the first step, the physical network must be identified and all core devices, interconnection points and access components are transferred in a logical view whereas this view will be stored in a common Network Topology Database (NTD). This process is called network bootstrapping and is a main prerequisite for the multitenant functionality. The bootstrapping itself is not a part of the multi-tenancy discussion but a pre-requisite. Each type of a network state change (e.g. link failures, devices shutdowns, introductions of new components etc.) should be automatically recognized and immediately introduced into the NTD. The NTD is the primary source of network state and guarantees consistency for VTNs and correspondent VTNSs. The VTN Manager as a core principal component of the multi-tenant architecture must have access to the NTD to construct the logical network views. If the VTN Manager is registered at the NTD a trigger mechanism should inform the VTN Manager instance about any kind of network state update. Such, the VTN Manager can update virtual tenant networks and their states accordingly. The VTN Manager forms a specific VTN for a dedicated tenant and performs mapping between physical and logical connection endpoints. An administrator can request a VTN creation for a specific application or user group. Automation of the creation of VTNs should be supported, e.g. via an uploaded pre-engineered template. A direct configuration of a VTNS must be possible for an administrator within a logical view of the VTN. It should be possible to show the full virtualized network view below the configured VTN. This ability should be considered for validation of the virtualization procedure. To separate VTN requests coming from an application or the administrator from requests of internal controller's modules, an abstraction layer must be designed. If the virtual tenant network is modified the VTN Manager should provide a VTN state update to respective components, e.g. Reference Monitor, SFC Manager. Once a VTN is implemented, the respective tenants and their internal members must be able to access the network access points, sensors and instances of virtual machines or containers. The capability of implementing dedicated forwarding rules within a VTN should be possible. VTNs are strictly separated and routing or switching between them is not planned. To offer a flexible and module-oriented VirtuWind industrial SDN architecture, the VTN Manager must be separated from the path calculation mechanism. This principal design guideline offers the capability to switch to

other types of path calculation modules without touching the abstraction functionality of network virtualization. A proactive flow instantiation mode is the preferred and most often required functionality within industrial networks to speed up packet forwarding and reduce packet delay. Nevertheless, a reactive flow installation to optimize network resource consumption is also needed. A single instance of the Path Manager should be responsible for all tenants.

Furthermore, the wind park network slicing detailed above can be extended to the Industrial IoT sensors residing in the wind turbines. In a Wind Park, different sensor devices can be found, with different criticality that needs to report data to different backbone services. By exploiting software defined architectures and virtualization we can map sensing channels to isolated data flows, managed by different tenants and orchestrating the data flows dynamically to meet the required QoS and service constraints. A key feature is to move the intelligence where is needed, most of the time in the IoT edge gateway where the sensors data flows can be proxied, labelled or forwarded according to dynamic policies. This approach provides access network technology independence and at the same time provides flexibility to the operators to select different IoT products to be installed at the edge. In this context, VirtuWind has elaborated on the ability to provide multi-tenant, isolated and virtualized access to a range of sensors gathering Wind Park data. The developed solution contains four main components: a GUI providing control of the infrastructure and visualization of tenant data; a gateway handling the sensors; the virtualized platform hosting the tenant VMs and the sensors themselves.

The approaches investigated in the context of VirtuWind are depicted in the figure below.

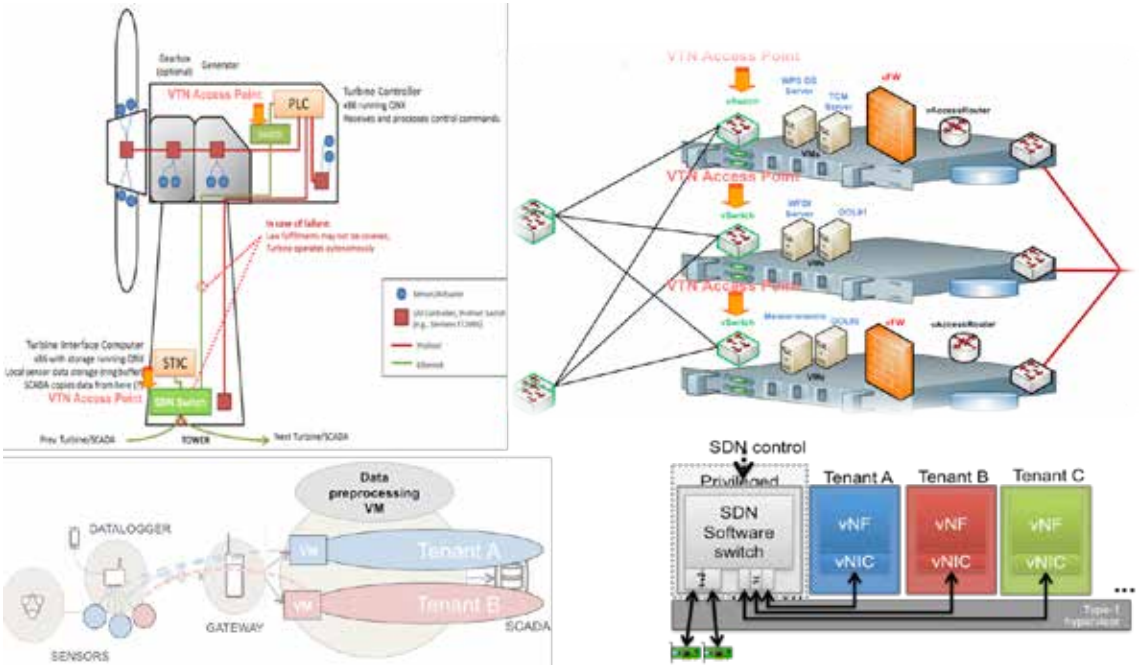


Figure 9:Multi-tenancy (Virtual Tenant Networks) in SDN-enabled Wind Parks. Wind Turbine & Substation Network – top – and virtualized IIoT sensor network – bottom (source: [36])

8.3.3.2 Via Microsegmentation

In addition to Network Slicing, micro-segmentation is a new security feature that has been introduced in data centres [32], but its use in mobile networks has not yet been considered. In data centres, the traditional security model is to regulate the north-south traffic at the edge of the data centre. This means that the data centre has a single firewall at the perimeter, where all incoming traffic to the data centre is considered untrusted and traffic inside the data centre is considered trusted. Consequently, once attackers gain access to the data centre through the firewall at the perimeter, they are free to move and carry out their attacks. Micro-segmentation aims to get rid of the single point of failure in data centre security by also considering the east-west traffic in the data centre, i.e., monitoring also the traffic inside the data centre. Micro-segmentation is generally an enabler for the Software Defined Data Centre.

In the context of 5G, micro-segments can be considered as isolated parts of the 5G network dedicated for application services or users. Compared to network slices, micro-segments can provide a finer grained isolation and segmentation, specific access controls and stricter security policies. The mobile network is generally divided into smaller parts, where each unique micro-segment can have its own security controls defined, and services delivered. Only authenticated devices and network services can join the micro-segment and traffic inside the micro-segment should also be monitored. A micro-

segment instance is not necessarily required to form a complete logical network.

For example, there could be one general network slice for IoT, but two micro-segments for smart metering and personal health. The user of a micro-segment could be an organization, service provider or a Virtual Mobile Network Operator (VMNO). The overall control of the micro-segments would be by (virtual) operators. The organizations and service providers that use the micro-segments may also have some control, especially related to the security functionalities within the micro-segment. Individual end-users would not have control over a micro-segment. Within a single network domain, the segments should typically lay within a single network slice. In a multi-domain/multi-operator setting, end-to-end security could be achieved by chaining micro-segments from multiple network slices.

In data centre networking, the micro-segmentation solution considers the Zero Trust model, which states that all nodes should be authenticated before attaching them into the micro-segment. The main principle of Zero Trust is "Never trust, always verify and authenticate". Zero Trust employs a least privilege and unit-level trust model that has no default trust level for any entity or object in the network. The entire mechanism is based on denying all communication until explicitly allowed (via explicit policies) and permitting only what is necessary from trusted sources. In the context of 5G, such a trust model could for example be provided to micro-segments with critical services. However, micro-segmentation in 5G needs to consider different trust models for different micro-segments, and a fully Zero Trust model may not be plausible.

The implementation of network slicing and micro-segmentation is possible with (SDN and virtualization technologies. In SDN, flow control policies can be defined at a very granular level such as the session, user, device, and application level. Generally, SDN would be used as a tool for monitoring each slice or micro-segment and virtualization technologies would be used for the creation of slices or micro-segments.

It is yet to be defined what specific components are included in a network slice or micro-segment. One possible solution could be to include the PDN gateway (PGW) and the policy control resource function (PCRF) in one slice or micro-segment [31]. For machine type communication (MTC) and machine-to-machine (M2M) solutions, the slice or micro-segment should, however, include also the Mobile Management Entity (MME) and the Serving Gateway (SGW). Each slice or micro-segment could also have its own AAA entity. All these entities would be virtualized resources or functions.

8.3.4 Slicing at Architecture level

For slicing at architecture level, please refer to Section 3 of this white paper, where such slicing is clearly depicted.

8.4 Open issues

Research on slicing in the security context include efforts from various Phase 1 projects, such as RAN network slicing and the security impact on bare metal equipment (without an NFV environment) and RAN functions shared between slices from 5G-NORMA; isolation at data plane but sharing of knowledge bases, signatures, monitoring KPIs for security, vulnerability intelligence from SELFNET; slicing via micro-segmentation & network management (including isolation guarantees between slices and used network services) in 5G-ENSURE; multi-operator/domain resource (network, compute, and storage) slicing in project 5GEx; and slicing to enable multi-tenancy via the deployment of Virtual Tenant Network in the context of software defined industrial networks (focusing on a Wind Park use case in specific) in VirtuWind.

An important open issue is the provision of isolation guarantees between slices and used network services, i.e. introducing mechanisms to deliver and maintaining a continuous chain of isolation evidence (from the user or infrastructure operator perspective) with respect to local regulation, also considering factors such as confidentiality, integrity, privacy, trust & liability, availability etc. These aspects will be considered in the contest of 5G-ENSURE's efforts. Moreover, multi-level isolation is expected to be needed, as infrastructure sharing by multiple virtual network operators will require strict isolation at multiple levels to ensure absolute security. In particular, various aspects of control-plane, data-plane and resource isolation must be ensured to achieve zero correlation among different tenants' operations. Tenant isolation is ultimately important to ensure a reliable and warranted service assurance, together with data and communication integrity and confidentiality. CHARISMA is active in this field. An important enabler for many of the above concepts will be the capability to monitor network activities across different domains, such as validating inter-domain SDN flow assignments, isolation and conflict resolution), also with respect

to cross-country regulation, which is a topic not adequately addressed by current research efforts. Part of the current landscape in this area is also covered in Section 7 (Security Monitoring and Management) above. Furthermore, for true E2E slicing the user equipment along its intricacies (e.g. lack of total control, multiple attack vectors and chances of compromise) will have to be included in the slicing, and this is a concept that has not been adequately addressed by current research efforts.

Security Standardization

9 Security Standardization

9.1 Introduction

5G will be even more reliant on standards than previous mobile telecommunications networks, due to the expected broad impact on society and the number of ways in which 5G networks will interact with each other and with external systems. To minimize exposure to risks, security must be built in from the designing phases rather then included later as an add-on feature. It is important to take into account a set of security, privacy and liability issues that must be addressed natively in the standardization and regulation processes according to the "Security by Design" approach. Moreover, security must be guaranteed both from the end-user's and the provider's standpoint, overcoming the mistaken belief that the final user's interest may contrast with the correct management of information from a public interest perspective, for example, privacy. However, 5G security is not just a technical issue but also a business opportunity, as well as an opportunity to educate on social risk management.

In order to provide a common agreement and encourage joint contributions, the Security WG should focus on:

- Security requirements that can impact all 5G aspects (e.g. radio, core, services).
- A minimal security baseline based on consistent technology and procedures by identifying the security functionality and mechanism required for 5G.
- Security architecture design based on the security baseline.
- Added security functionalities which can be instantiated based on the specific service/contest.

9.2 Motivation for Security Standardization

Security involves all aspects of 5G networks, from core and management systems, to all protocol layers from air interface to applications. Security standardization helps in several ways:

- Open, public standards allow scrutiny and analysis by a wide range of industry experts, academics etc., and therefore promote transparency and trustworthiness.
- Adherence to standards can help to ensure safety and reliable environment. As a result, users perceive standardized products and services as more dependable, which in turn raises user confidence, increasing sales and the take-up of new technologies
- Standards help ensure a minimal security baseline based on consistent technology and procedures by identifying the security functionality and mechanisms the 5G infrastructure need to support.
- They may also provide additional security functionalities which can be instantiated based on the specific service/contest.
- Standards are the best guarantee of interoperability. In a security context, this does not only mean that different systems can interact, but also that security levels are consistent on either side, so security is not undermined on either side by a lack of security in the other.
- Last, but not least, standardization brings business benefits such as:
  - Opening up market access.
  - Economies of scale.
  - Encouraging innovation.
  - Increased awareness of technical developments and initiatives.

9.3 5G Standardization and Industry Fora LANDSCAPE

A lot of work is on-going within several associations and standards organizations.

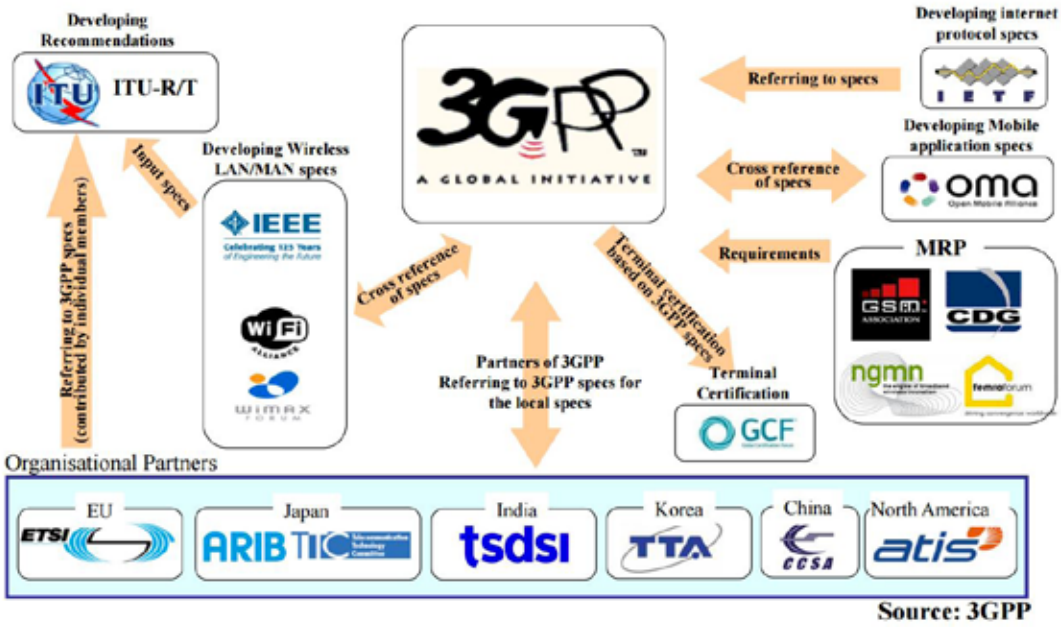


Figure 10: 5G standardization / the driving forces

The 3GPP is the key standardization organization for 5G standardization and it is the main target for 5G PPP projects, but other organizations can be considered relevant, such as ETSI, IETF and ITU. While not official standardization organizations, the GSMA and NGMN will also play an important role as drivers for 5G specifications across the industry.

9.3.1 3GPP

In March 2015, the 3GPP [S8] endorsed a timeline for the standardization of 5G, around the ITU's IMT 2020 deadline.

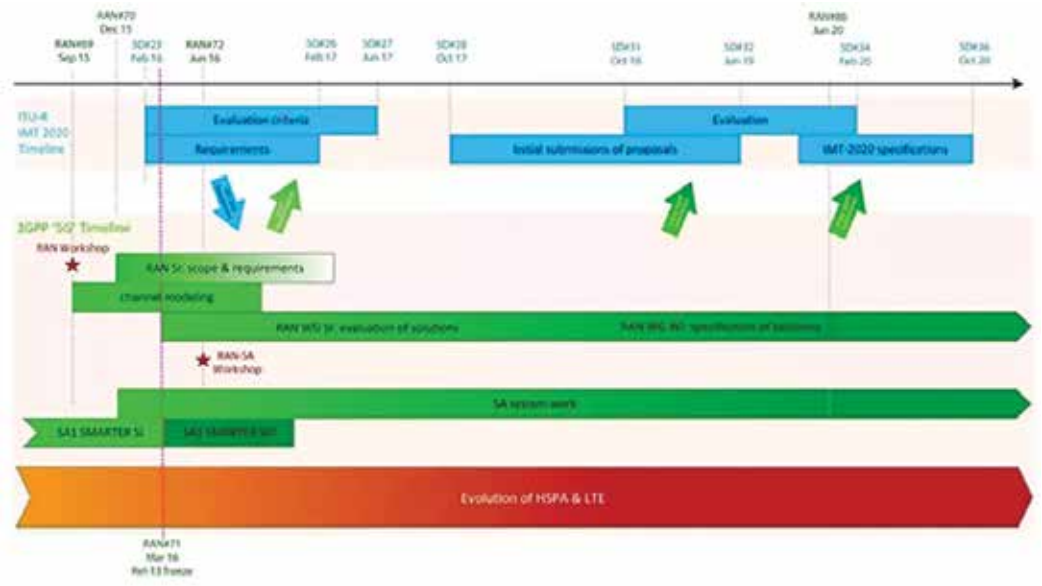


Figure 11: timeline for the standardization of 5G

This section provides a landscape of related 5G activities in standards bodies and industry forums.

In 2015, 3GPP began working on 5G. The 3GPP Services and Requirements Working Group has been working on the study phase for 5G service requirements, known as SMARTER work. It works also

on four technical reports that provide more detailed proposed service requirements for the four major categories 5G will touch on Massive IoT, Enhanced Mobile Broadband, Critical communication and Network operation. These are then be used as input for the development of the normative service requirements for 5G. These requirements are targeted for completion in June 2017.

In late 2015, the 3GPP System Architecture Working Group (SA2) approved a "Study on Architecture for Next Generation Systems". In scope is the design of 5G architecture, the support of at least the new RAT(s), the evolved LTE, non-3GPP access. The study has investigated high-level architectural requirements and is defining a common terminology. The expectation is to start normative work on a baseline 5G system in Release 15.

Standardization work on 5G security aspects started within the SA3 in January 2016 with the creation of an ad-hoc Work Item dedicated to study the security aspects of the next generation system. 5G-ENSURE project has supported the creation of the WI, where the scope of this study is to identify the threats, potential requirements and solutions for the security of next generation mobile networks. The work includes the:

- Collection, analysis and further investigation of potential security threats and requirements for the next generation systems, based on the service, architectural and radio related requirements for the next generation mobile networks.
- Investigation of the security architecture and access security.

The security areas cover relevant security topics such as the Security architecture, the Authentication, RAN security, the Subscriber privacy, the Network slicing security as well as the Network domain security. The approach taken by the study is to identify for each area the key issues, threats and potential security requirements that need to be satisfied by the solutions proposed. The complete or partial conclusions of this study are the basis for the normative work and/or for any further study. In this context, the SA3 group is working in conjunction with SA1, which focuses on 5G requirements. and SA2, which focuses on 5G architecture.

The 5G standardization time plan currently adopted by 3GPP, which is gradually realizing the full 5G capabilities in three consecutive releases spanning the period 2016-2019.

9.3.2 ETSI

ETSI TC CYBER Technical Committee [42] was established in 2014 to address the growing demand in the area of cyber security standardization. It works closely with relevant stakeholders within and outside ETSI to collect, identify and specify requirements, and thus develop appropriate standards to increase the privacy and security of organizations and citizens across Europe.

Although TC Cyber has not yet started a dedicated Work item on 5G security, it is considered a target group for the privacy aspects where it is more active with the delivery of guides and mechanisms for privacy assurance and verification. Last year, during the ETSI TC CYBER#7 meeting in Sophia Antipolis (June 2016), 5G-ENSURE co-signed a contribution for the creation of a new work item related to privacy aspect "CYBER; Application of Attribute-Based Encryption (ABE) for data protection on smart devices, cloud and mobile services". This work item specifies an application of ABE to implement ABAC for specific environments where access to data has to be given to multiple parties and under different conditions. The work item will describe the ABE encryption and decryption mechanisms, the boundary conditions relating to the underlying cryptography, the key distribution protocols and any related architectural aspect. Three main use cases will be addressed: Cloud, Mobile, and IoT. This is another target for 5G-ENSURE, which aims to contribute by presenting the work done on the use of ABE mechanism in the contest of user identity privacy protection enabler.

ETSI Industry Specification Group (ISG) for NFV [43] is the home for developing requirements and specifications for NFV. The main goal in forming ETSI ISG NFV was to produce the technical specifications to enable the development of an open, interoperable, commercial ecosystem based on virtualized network functions. In particular, ETSI NFV SEC is the working group responsible for security considerations throughout the NFV platform. The working group's main objectives, as presented in [44] [45], are to advice the NFV ISG on all matters of the relevant security technologies and develop a wide range of industry specifications that:

Identify both the NFV-specific security problems, as well as the technological advantages of the NFV environment that can be harnessed to improve the security of the network operators' services.

Provide specific guidance on various aspects of the NFV security in a systematic, holistic manner, building trust from secure hardware modules to software and covering identity management, authentication, authorization and secure attestation, as well as the means of global monitoring of the whole NFV environment and decisive operational security actions in response to security breaches.

Address in detail the security of the current Open Source-based platforms (such as OpenStack).

Contribute to solving the problem of implementing Lawful Interception (LI) in the NFV environment.

Work in close collaboration with other ETSI NFV WGs, Proog of Concepts, as well as external organizations

(ETSI TC Cyber, ETSI TC LI, Trusted Computing Group and contributing members of OpenStack).

To achieve these goals, NFV SEC WG is working on many different topics, ranging from defining a problem statement, defining the threat landscape, identifying potential areas for security vulnerabilities, hardening requirements, NFV specific use of security functionalities, identifying requirements to implement LI, providing certificate management guidance, regulatory concerns, etc. among others.

Currently 5G-ENSURE and CHARISMA are only monitoring the ETSI NFV SEC WG, which could be another standards group where the Security WG could participate with joint contributions.

9.3.3 IETF

In recent years, the Internet Engineering Task Force (IETF) [44] started a variety of activities to enable a wide range of Internet things to use interoperable technologies for communicating with each other, with the creation of working groups (WGs) focusing on IoT with constrained devices and networks.

Since 2010, most of the new IoT WGs have been added in the Security Area. The DTLS In Constrained Environments (DICE) WG (already completed) produced a TLS/DTLS profile that is suitable for constrained IoT devices. The Authentication and Authorization for Constrained Environments (ACE) WG is working on authenticated authorization mechanisms for accessing resources hosted on servers in constrained environments and a comprehensive use case document (RFC 7744 [46]) was recently completed.

Currently there is not a plan to provide contributions to the IETF WG related to IoT. Anyway these groups are monitored since they deal some aspects covered in several 5G-ENSURE enablers.

The IETF Detnet [47] WG aims to define an intra-domain architecture to support deterministic flows in heterogeneous networks. This architecture is based on open standards such as those developed at the IETF. The VirtuWind consortium is actively contributing to the IETF Detnet WG by providing a set of requirements derived from the wind farm industry and scenarios. These requirements are used to drive the standardization efforts of the IETF WG and guide the industry towards the improvement of communication protocols and technologies in the backbone of the network.

IETF Interface to Network Security Functions (I2NSF) [48] aims to define interfaces to the flow based network security functions (NSFs) hosted at different premises. NSFs are provided and consumed in increasingly diverse environments. Users of NSFs could consume network security services hosted by one or more providers, which may be their own enterprise, service providers, or a combination of both. Likewise, service providers of NSFs may offer their customers network security services that consist of multiple security products and/or functions from different vendors. NSFs may be provided by physical and/or virtualised infrastructure. Without standard interfaces to express, monitor, and control security policies that govern the behaviour of NSFs, it becomes virtually impossible for security service providers to automate their service offerings that utilize different security functions from multiple vendors. The goal of I2NSF is to define a set of software interfaces and data models for controlling and monitoring aspects of physical and virtual NSFs.

9.3.4 NGMN

The Next Generation Mobile Networks (NGMN [49]) Alliance has been focusing on 5G since 2015 and has established its intended role in 5G development in the white paper published in March 2015. The NGMN paper sets challenging technical and other requirements for 5G and accelerates the adoption of new emerging technology innovations. The paper's goal is to serve as a guideline for 5G definition, architecture and design, taking particularly into account the demand of consumers, enterprises, vertical industries and service providers.

NGMN continues working on the 5G work programme. Key tasks are the development of 5G requirements and design principles, the analysis of potential 5G solutions, and the assessment of future use-cases and business models. The key technical project is P1 Requirements & Architecture, which is sub-divided into the following Work Streams:

- End-to-End Architecture.
- Network Management & Orchestration.
- 5G Security.
- Work Stream on Requirements for Industry Verticals.

The NGMN P1 WS1 5G Security group objective is to guide standardization and implementation of 5G security features, based on but expanding as necessary, the security topics highlighted in the NGMN 5G White Paper covering, among others, radio architecture, virtualization, privacy, availability and IoT. The NGMN P1 WS1 5G Security group produces 5G security high-level requirements and recommendations. These have been used by 5G-ENSURE as insights for developing 5G security enablers.

9.3.5 GSMA

The GSMA [50] represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem, including handset and device makers,

software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors.

GSMA "Vision 2020" based on four pillars and a set of prioritized initiatives. One of the four pillars is "Network 2020" which intends to "create a network for secure, smart and seamless services" and includes 5G network requirements as an essential element.

As part of the GSMA Network 2020 program, GSMA published a paper titled "Unlocking Commercial Opportunities - From 4G Evolution to 5G" that argues for a continued evolution of 4G systems and suggest a number of technology drivers, such as NFV, as enablers to support existing services more efficiently and to start creating a market for emerging applications.

9.4 Large Scale Industry-Academic Research Projects Landscape

The scope of this section is to indicate the key standardization organizations addressing some of the security design/aspects related to 5G security and identified as the most relevant in this whitepaper.

The identified topics are the best candidate where all the funded H2020 projects on 5G should put more effort in order to propose co-signed contributions and so speed-up the specification processes on-going within the target standardization organizations.

9.4.1 Security Architecture

ETSI/3GPP has traditionally been the main SDO defining mobile network security architectures for 3G and 4G, and is expected to do so also for 5G. Security architecture aspects have mainly been concerned with design choices such as where to place termination points e.g. for user plane ciphering. The final design choice has also been driven by non-security aspects. 3GPP has concentrated most effort on more low-level security protocol and security mechanism design. As pointed out in Section 3, virtualization and multi-domain aspects, involving non-operator actors such as industry verticals, warrants a 5G security architecture which is logical rather than physical and which better reflects trust model, management, and slicing, etc. We also believe that the security architecture work should receive higher prioritization than in previous generations. A logical architecture with higher flexibility may also make physical allocation aspects of previous generations less critical.

At the time of writing, 5G work in SA3 is being developed through TR 33.899, which defines a number of key issues. However, architecture work has not progressed much so far. We therefore believe contributions on architecture from the 5G PPP should be a top priority. A number of contributions on specific topics have already been made to SA3 through co-signed contributions by partners of 5G-ENSURE. We believe contributions on architecture could also be handled this way.

Other standardization organizations of relevance for architecture include ETSI/NFV. Here, it is important to note that the draft architecture proposed in Section 3.3 has aimed for compatibility with existing ETSI/NFV work, e.g. through the definition on infrastructure and tenant domains.

9.4.2 AAA

The following standards are undergoing works for IoT networking and authentication. However, there are not ongoing standardization efforts on authentication in massive IoT communications.

- IEEE 802.1X-2010 [51]: IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control. It covers common architecture, functional elements, and protocols for mutual authentication and secure communication between the clients of ports attached to the same LAN.
- IEEE 802.1AR-2009 [52]: Standard for Local and metropolitan area networks: Secure Device Identity. It enables the secure association of locally significant device identities with manufacturer provisioned identities for use in provisioning and authentication protocols.
- IEEE project 15.9 [53]: IEEE Draft Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams. It provides guidelines for the support of key management in IEEE 802.15.4.

Note: key foreseen action is to engage at least with GSMA due to convergence needed at MNO level.

9.4.3 Privacy

Privacy and more specifically subscription privacy is a very important area for the Next Generation system and evident in the growing attention towards it, both inside and outside the 3GPP world.

NGMN is an alliance of mobile network operators, vendors, and universities, has identified security

and privacy as a 5G enabler and essential value proposition supporting the principle of privacy by design (NGMN 5G White Paper V1.0 [54]).

The FSAG group within GSMA has recently focused on Customer Privacy issues in mobile networks. Viable solutions to improve user privacy over the air interface have been presented and evaluated. The analysis was used to brief other GSMA working groups and to serve as the basis for viable solutions within theSA3 study item.

In the 3GPP, privacy is a topic that is addressed in several specifications. For example, the TR 33.849 [55] is a study on subscription privacy impacts in 3GPP that presents privacy key issues and risk mitigation approaches. The study highlights that the privacy needs addressing as a separate topic in its own. The TR 22.864 [56] also underscores subscription privacy as being very important. It is mentioned that the privacy of personally identifiable information needs to be protected, for example from a less trusted access or a rogue network element. The study contains several potential security requirements related to subscription privacy, e.g. protecting the user identifying information from active and passive attacks, protecting user location information from active and passive attacks, and not allowing UE location or application usage information to be related to an individual user identity. Similarly, the TR 22.891 [57] contains privacy requirements such as the possibility for the UE to hide its long-term identifier by using a temporary identifier even for initial attach and protecting the subscription privacy during system information collection. The TS 22.185 [58] has also identified privacy requirements in a V2X context, which needs further elaboration in the Next Generation system context as well, e.g. ensuring that a UE cannot be tracked or identified beyond over a short period of time [59].

In 3GPP SA3, Subscription Privacy is one of the Security Areas included in the "Study on the security aspects of the next generation system" (TR 33.899, not yet delivered). Subscription privacy itself is a wide area spanning many key issues such as identifiers, mobility patterns, location or presence information, data usage pattern, etc. Relevant privacy key issues and related high level requirements have been discussed and some solutions have also been proposed for evaluation.

Privacy is one of the key building blocks for the 5G-ENSURE project. Some 5G use cases affecting user privacy have been identified during the first year and some of the privacy issues have been presented to 3GPP SA3 as contributions to TR 33.899 which mainly relate to:

- *Refreshing of temporary subscriber identifier [S3-160957].*
- *Concealing of permanent or long-term subscriber identifier [S3-161285].*
- *Concealing of permanent or long-term device identifier [S3-160959].*
- *Using effective temporary or short-term subscriber identifiers [S3-160960].*
- *Transmitting permanent identifiers in secure interface [S3-160961].*
- *Transmitting permanent subscriber identifiers only when needed [S3-160962].*
- *Temporary device identifier [S3-160976].*

In addition, within 5G-ENSURE, a set of privacy enablers have been specified as part of Technical Roadmap [59] and are being software released. One of these, the "Privacy Enhanced Identity Protection" focuses on protecting the permanent subscriber identity (IMSI) from attackers on the air interface to avoid subscriber tracking. It proposes a solution based on the use of a global public key by each UE to encrypt the respective permanent or long-term subscriber identifier (IMSI) in any case where a pseudonym is not available (initial Attach Request). The solution was proposed for evaluation during SA3#85 meeting (Santa Cruz, November 2016). The contribution *"New privacy solution for concealing permanent subscriber identifier" [S3-161641]* has been accepted and included in the current version of TR 33.899 with the finalization of the study expected in spring 2017.

In the meantime, work on "WiFi-based IMSI Catcher has been presented to GSMA Fraud and Security WG, reporting on two issues discovered that can result in the exposure of the IMSI on WiFi networks. The results of this work are in part related to the activities conducted within the 5G-ENSURE project in the context of privacy issues in 5G network.

New privacy enablers and new security functionality for the ones already specified will be delivered as part of the second 5G-ENSURE roadmap. The plan is to continue working on the subscriber identity protection key issue by evaluating other solutions. In addition, the plan also focuses on the temporary subscriber identifier key issue by proposing a mechanism for the pseudonyms generation. The ultimate goal is to continue driving the privacy discussion ongoing in 3GPP SA3 study by presenting the new results from the project.

9.4.4 Network Slicing Security

The System and Service Aspects Architecture group (SA2) of 3GPP has a dedicated study item for next generation networks, TR 23.799 [60]. Taking as a starting point service requirements that 5G network must address [S19], the study identifies key issues for 5G networks, such as n meeting diverse use cases (e.g. Internet of things, Enhanced broadband, critical communication) on top of the same 5G network. The

support of network slicing is a key issue (solution) for this requirement. Several features related to network slicing in TR23.799 [61] have potential security implications such as the sharing of network functions and the isolation between the different slices. Moreover, network slicing security is another area under study within the SA3 WG Study Item TR 33.899., which has identified several issues such as the "Security isolation of network slices", "Security on management of slicing", "Security of inter slice communications".

Given the strategic importance of slicing for 5G, the Security WG will work on a common view of the security requirements and security functionalities/ mechanisms needed to address this security topic.

9.5 Final thoughts

The following security topics have common and shared interests, while also requiring investment and the effort by the H2020 funded projects:

» Security Architecture.

» AAA.

» Privacy.

» Network Slicing.

In 2017, the 5G PPP Security WG will encourage co-signed contributions to be elaborated by the H2020 projects and presented to the relevant standardization organizations/groups considered to be relevant. It is also important to should also strongly argue against the mistaken approach of projects making considerable contributions to standardization organizations without embracing 5G security challenges as this may lead to standards that do not appropriately address security by design.

The image below describes the current 5G-ENSURE standardization plan,which is aimed at ensuring that contributions to 5G standardization are both timely and targeted,with partners pursuing an industry-led approach and by down-streaming relevant research results into the standardization process. The 5G security standardization plan focuses on:

» Contributions to the most relevant standards bodies, particularly 3GPP and ETSI.

» Monitoring of on-going studies on 5G standardization.

The ultimate goal is help create some kind of harmonization within the standardization ecosystem.

5G-ENSURE has also undertaken actions with other standards bodies to share project results of interest. The on-going collaboration with NIST is one example of this, with contributions also to ITU Study Group 17

Figure 12: 5G-ENSURE actions undertaken with SDOs

References

References

[1] 3GPP, "General Universal Mobile Telecommunications System (UMTS) architecture (Release 13)", (TS 23.101).

[2] 3GPP, „Technical Specification Group Services and System Aspects; 3G Security; Security architecture", (TS 33.102)..

[3] 3GPP, „Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture", (TS 33.401).

[4] VirtuWind, Deliverable D4.1, "Detailed Inter-domain SDN Architecture.

[5] VirtuWind, Deliverable D2.4, "Techno-economic Framework and Cost Models", Aug 2016.

[6] CHARISMA, Deliverable D3.2 "Initial 5G multiprovider v-security realization: Orchestration and Management", June 2016, http://www.charisma5g.eu/wp-content/uploads/2015/08/CHARISMA-D3.2_v1.0.pdf.

[7] 5G-ENSURE, Deliverable D2.4, "Security Architecture (draft)", Oct 2016, http://5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.4-SecurityArchitectureDraft.pdf.

[8] Ericsson, «Ericsson mobility report,» 2015.

[9] Nokia Siemens Networks, «Signaling is growing 50% faster than data traffic,» 2012.

[10] Oracle, «Oracle communications lte diameter signaling index. 4th edition,» 2015.

[11] Ericsson, «5G Security - Scenarios and Solutions, White paper. Available: http://www.ericsson.com/res/docs/whitepapers/wp-5g-security.pdf,» June 2015.

[12] 5G-ENSURE, Deliverable D2.1: Use Cases, February 2016..

[13] G. B. e. al., „Private VNFs for collaborative multi-operator service delivery: an architectural case", In: Proc. of NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, 2016.

[14] S. S.-B. e. al., „From porn to cybersecurity passing by copyright: How mass surveillance technologies are gaining legitimacy ... The case of deep packet inspection technologies", Computer Law & Security Review, Vol. 30, Issue 6, pp. 670-686, Dec.

[15] R. A. e. al., "Deep packet inspection tools and techniques in commodity platforms: Challenges and trends", Journal of Network and Computer Applications, Vol. 36, Issue 6, pp. 1863-1878, November 2012.

[16] 5G-ENSURE, D3.1 5G-PPP security enablers technical roadmap (early vision), March 2016, http://www.5gensure.eu/deliverables.

[17] 5G-ENSURE, D3.2 5G-PPP security enablers open specifications (v1.0), June 2016, http://www.5gensure.eu/deliverables.

[18] 5G-ENSURE, D3.3: 5G-ENSURE_D3.3 5G-PPP security enablers SW release (v1.0), October 2016, http://www.5gensure.eu/deliverables.

[19] 5G-ENSURE, «Deliverable D3.5 5G-PPP security enablers technical roadmap (Update),» 2016.

[20] ETSI, GS NFV-SEC 003 V1.1.1 (2014-12): Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance.

[21] M. S. Tyrone Grandison, "A Survey of Trust in Internet Applications", IEEE Communications Surveys & Tutorials, Vol.: 3, Issue No.: 4, Year: 2000, Page(s): 2 -15..

[22] F. C. A. G. N. S. a. P. C. Francesco Paolucci, "A Survey on the Path Computation Element (PCE) Architecture", IEEE Communications Surveys & Tutorials, Vol.: 15, Issue No: 4, Year: Fourth Quarter 2013, Page(s): 1819.

[23] CHARISMA, «Deliverable D3.2: Initial 5G multi-provider v-security realization: Orchestration and Management,» [En ligne]. Available: http://www.charisma5g.eu/wp-content/uploads/2015/08/CHARISMA-D3.2_v1.0.pdf.

[24] SELFNET, «Deliverable D2.1: Use Cases Definition and Requirements of the Systems and its components,» October 2015. [En ligne]. Available: https://bscw.selfnet-5g.eu/pub/bscw.cgi/d18783/SELFNET%20Deliverable%202.1%20-%20Final%20v12.pdf.

[25] Manuel Gil Pérez, Giacomo Bernini, "Self-protection against botnet attacks - Solutions by 5G PPP project SELFNET," Eurescom message, Winter 2016. [Online]. Available: https://www.eurescom.

eu/news-and-events/eurescommessage/eurescom-message-winter-2016/self-protection-against-botnet-attacks.html.

[26] 5Gex, «"Deliverable 2.1: 5GEx Initial System Requirements and Architecture",» 2016. [En ligne]. Available: http://www.5gex.eu/wp/?page_id=55.

[27] CogNet, "Deliverable D5.1: Network Security & Resilience – Initial Design," June 2016. [Online]. Available: http://www.cognet.5g-ppp.eu/public-deliverables/.

[28] Cognet, Deliverable D5.1: Network Security & Resilience – Initial Design," June 2016. [Online]. Available: http://www.cognet.5g-ppp.eu/public-deliverables/..

[29] 3GPP, «Architecture Enhancements for Dedicated Core Networks. 3GPP TR 23.707 V13.0.0 (2014-12). Technical Report,» 2014.

[30] 3GPP, «Study on Architecture for Next Generation System. 3GPP TR 23.799 V14.0.0, Technical Report. Available: http://www.3gpp.org/ftp//Specs/archive/23_series/23.799/23799-e00.zip.,» December 2014.

[31] Ericsson, «Network functions virtualization and software management, White Paper. Available: http://www.ericsson.com/res/docs/whitepapers/network-functions-virtualization-and-software-management.pdf,» 2014.

[32] VMware, «Data Center Micro-Segmentation: A Software Defined Data Center Approach for a Zero Trust Security Strategy, White Paper,» 2014.

[33] O. Mämmelä, J. Hiltunen, J. Suomalainen, K. Ahola, P. Mannersalo, and J. Vehkaperä, «Towards Micro-Segmentation in 5G Network Security,» chez *European Conference on Networks and Communications (EuCNC 2016) Workshop on Network Management, Quality*, 2016.

[34] ETSI GS NFV-IFA 001 V1.1.1, "Network Functions Virtualisation (NFV); Acceleration Technologies; Report on Acceleration Technologies & Use Cases," December 2015.

[35] M. Endsley, «Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1), 32-64,» *32-64,* vol. Journa 37, pp. 32-64, March 1995.

[36] VirtuWind, «Deliverable D3.2: Detailed Intra-Domain SDN & NFV Architecture,» January 2017. [En ligne]. Available: http://www.virtuwind.eu/_docs/deliverables/VirtuWind%20Deliverable%20D3.2%20-%20Detailed%20Intra-Domain%20SDN%20&%20NFV%20architecture.pdf.

[37] Ericsson, «5G systems – Enabling Industry and Society Transformation, White paper. Available: http://www.ericsson.com/res/docs/whitepapers/what-is-a-5g-system.pdf,» January 2015.

[38] NGMN Alliance, «Description of Network Slicing Concept, Available: https://www.ngmn.org/uploads/media/160113_Network_Slicing_v1_0.pdf,» January 2016.

[39] NGMN Alliance, «5G White Paper. Available: https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf,» February 2015.

[40] NGMN Alliance, «5G security recommendations, Package #2: Network Slicing, V1.0. Available: https://www.ngmn.org/uploads/media/160429_NGMN_5G_Security_Network_Slicing_v1_0.pdf,» April 2016.

[41] 5G NORMA, «Deliverable D4.1: RAN architecture components – intermediate report,» November 2016. [En ligne]. Available: https://5gnorma.5g-ppp.eu/wp-content/uploads/2016/12/5g_norma_d4-1.pdf.

[42] ETSI, http://www.etsi.org/technologies-clusters/technologies/cyber-security.

[43] ETSI, http://www.etsi.org/technologies-clusters/technologies/nfv.

[44] IETF1, https://www.ietf.org/.

[45] W. S. C. -. Igor Faynberg, Presentation of the ETSI NFV SEC Working Group - Online: https://www.youtube.com/watch?v=uuwnovW92vI.

[46] IETF, https://tools.ietf.org/html/rfc7744.

[47] IETF, https://datatracker.ietf.org/wg/detnet/charter/.

[48] IETF, Internet Engineering Task Force Interface to Network Security Functions - https://datatracker.ietf.org/wg/i2nsf/charter/.

[49] NGMN, https://ngmn.org/home.html.

[50] GSMA, http://www.gsma.com/.

[51] IEEE, https://standards.ieee.org/findstds/standard/802.1X-2010.html.

[52] IEEE, https://standards.ieee.org/findstds/standard/802.1AR-2009.html.

[53] IEEE, https://standards.ieee.org/findstds/standard/802.15.9-2016.html.

[54] NGMN, https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf.

[55] TR 33.849: Study on subscriber privacy impact in 3GPP.

[56] TR 22.864: Feasibility study on new services and markets technology enablers for network operation; Stage 1.

[57] TR 22.891: Study on New Services and Markets Technology Enablers.

[58] TS 22.185: Service requirements for V2X services.

[59] 5G-ENSURE, 5G-ENSURE Project, Deliverable 3.5 5G-PPP security enablers technical roadmap (Update), http://www.5gensure.eu/deliverables.

[60] TR 23.799: Study on Architecture for Next Generation System.

[61] 3GPP, http://www.3gpp.org/news-events/3gpp-news/1786-5g_reqs_sa1.

[62] 5G-ENSURE, «Deliverable D3.2 - 5G-PPP security enablers open specifications (v1.0),» 2016.

[63] B. Blanchet, «An Efficient Cryptographic Protocol Verifier Based on Prolog Rules,» chez *CSFW*, 2001.

[64] 5G-ENSURE, "Deliverable D2.2: Trust model (draft)," November 2016. [Online]. Available: http://www.5gensure.eu/deliverables.

[65] 5G-ENSURE, "Deliverable D2.3: Risk Assessment, Mitigation and Requirements (draft)," August 2016. [Online]. Available: http://www.5gensure.eu/deliverables.

[66] A. V. Aho and M. J. Corasick, "Efficient string matching: An aid to bibliographic search," *Communications of the ACM,* June 1975.

[67] D. Brumley, J. Newsome, D. Song, H. Wang, and S. Jha, «Towards automatic generation of vulnerability based signatures,» chez *IEEE Symposium on Security and Privacy* , Oakland, California, May 2006.

[68] H. J. Wang, C. Guo, D. Simon, and A. Zugenmaier, «Shield: Vulnerability-driven network filters for preventing known vulnerability exploits,» chez *2004 ACM SIGCOMM Conference*, August 2004.

[69] S. Rubin, S. Jha, and B. Miller, «Language-based generation and evaluation of NIDS signatures,» chez *IEEE Symposium on Security and Privacy*, May 2005.

[70] R. Sommer and V. Paxson, «Enhancing byte-level network intrusion detection signatures with context,» chez *ACM Conference on Computer and Communications Security (CCS)*, 2003.

[71] «The OpenFlow eXtensible DataPath daemon,» [En ligne]. Available: http://www.xdpd.org.

[72] «TCAMs and OpenFlow – What Every SDN Practitioner Must Know,» 2012. [En ligne]. Available: https://www.sdxcentral.com/articles/contributed/sdn-openflow-tcam-need-to-know/2012/07/.

[73] CHARISMA, "Deliverable D3.2: Initial 5G multi-provider v-security realization: Orchestration and Management," [Online]. Available: http://www.charisma5g.eu/wp-content/uploads/2015/08/CHARISMA-D3.2_v1.0.pdf.

Editors and Contributors

Editors and Contributors

Name	Company / Institute / University	Project
Editorial Team		
Overall Editors		
Pascal Bisson	Thales / 5G-PPP Security WG Chair	5G-ENSURE
Jean-Philippe Wary	Orange / 5G-PPP Security WG Chair	5G-ENSURE
Contributors and Reviewers		
Mats Naslund	Ericsson	5G-ENSURE
Luciana Costa	Telecom Italia	5G-ENSURE
Felix Klaedtke	NEC	5G-ENSURE
Stephen C. Phillips	IT Innovation	5G-ENSURE
Paolo De Lutiis	Telecom Italia	5G-ENSURE
Nizar Kheir	Thales	5G-ENSURE
Jani Suomalainen	VTT	5G-ENSURE
Mike Surridge	IT Innovation	5G-ENSURE
Gergely Biczók	Budapest Univ. of Techn. and Economics	5G-Ex
Mateus Santos	Ericsson	5G-Ex
Zsolt Magyari	Berlin Inst. for Soft. Defined Networks	5G-Ex
Peter Schneider	Nokia	5G-NORMA
Stan Wong	King's College London	5G-NORMA
Carolina Canales	Ericsson	CHARISMA
Shuaib Siddiqui	i2cat	CHARISMA
Eleni Trouva	Demokritos	CHARISMA
Robert Mullins	Telecom. Software & Systems Group (TSSG)	COGNET
Joe Tynan	Telecom. Software & Systems Group (TSSG)	COGNET
Diego Lopez Garcia	Telefonica	SONATA
George Mantas	IT – Aveiro	SPEED-5G
Victor Sucasas	IT – Aveiro	SPEED-5G
Alireza Esfahani	IT – Aveiro	SPEED-5G
Jonathan Rodriguez	IT – Aveiro	SPEED-5G
Shahid Mumtaz	IT – Aveiro	SPEED-5G

Gregorio Martinez Perez	University of Murcia	SELFNET
Manuel Gil Perez	University of Murcia	SELFNET
Gino Carrozzo	Nextworks	SELFNET
Giacomo Bernini	Nextworks	SELFNET
Jose M. Alcaraz Calero	The University of the West of Scotland	SELFNET
Qi Wang	The University of the West of Scotland	SELFNET
Konstantinos Koutsopoulos	Creative Systems Engineering	SELFNET
Luis Javier García Villalba	Universidad Complutense de Madrid	SELFNET
Jorge Maestre Vidal	Universidad Complutense de Madrid	SELFNET
Marco Antonio Sotelo Monge	Universidad Complutense de Madrid	SELFNET
Konstantinos Fysarakis	FORTH	VirtuWind
Ioannis Askoxylakis	FORTH	VirtuWind
Nikolaos Petroulakis	FORTH	VirtuWind
Florian Zeiger	Siemens	VirtuWind
Vivek Kulkarni	Siemens	VirtuWind
Anton Matsiuk	NEC	VirtuWind
Simon Kuenzer	NEC	VirtuWind
Andreas Roos	Deutsche Telecom	VirtuWind
Xavi Vilajosana	WorldSensing	VirtuWind


LOCK

5G PPP Phase1 Security Landscape

This material is the result of collaborative work within the 5G PPP Work Group on Security, which is chaired by Pascal Bisson (Thales) and Jean-Philippe Wary (Orange) from the 5G-ENSURE project.
All contributing projects have received funding through the European Commission's Horizon 2020 Programme for 5G PPP Phase 1. The material has been designed and printed with support from the 5G-ENSURE project, which has received funding under grant agreement No 671562.

More information at
http://5gensure.eu

5G PPP

European Commission