Deliverable D3.9
5G-PPP security enablers technical roadmap (Final)

Project name	5G Enablers for Network and System Security and Resilience	
Short name	5G-ENSURE	
Grant agreement	671562	
Call	H2020-ICT-2014-2	
Delivery date	30.09.2017	
Dissemination Level:	Public	
Lead beneficiary	Thales Services (TS)	Pascal Bisson, pascal.bisson@thalesgroup.com Nizar Kheir, nizar.kheir@thalesgroup.com
Authors	VTT : Pekka Ruuska, Olli Mämmelä, Jani Suomalainen TS: Pascal Bisson, Nizar Kheir, Cyrille Martins, Edith Felix, Laurent Morel EAB: Alireza Ranjbar Håkan Englund ITInnov: Toby Wilkinson, Stefanie Cox, Gianluca Correndo, Mike Surridge LMF: Bengt Sahlin, Patrik Salmela NEC: Felix Klaedtke Nixu: Tommi Pernilä Orange: Jean-Philippe Wary, Ghada Arfaoui SICS: Thomas Carnehult, Nicolae Paladi, Ludwig Seitz TASE: Gorka Lendrino Vela, David Pérez Izquierdo TCS: Sébastien Keller, Frédéric Motte, Filippo Rebecchi TIIT: Luciana Costa, Madalina Baltatu UOXF: Piers O'Hanlon	

Executive summary

Deliverable D3.9 is the final update of the 5G-ENSURE security enablers Technical Roadmap, and completes the previous D3.5 deliverable. It briefly reminds the features that were developed in scope of the project and their relevance to the identified use cases. More importantly, it provides recommendations and further insights on future work to be conducted by interested parties (either partners or future projects), and this based on the expertise and experience acquired by the consortium through participation to the 5G-PPP. The contributions in this deliverable can be structured into three distinct categories:

- First, for each enabler developed in scope of 5G-ENSURE, this deliverable describes new relevant features to be further explored in order to meet new requirements that have been identified later in the project lifecycle.
- Second, for each of the thematic clusters (AAA, Privacy, Trust, Security monitoring, Security management), it also calls for additional enablers to be considered based on lessons that has been learnt during the project.
- Third, it highlights new research directions that we believe are of interest to the 5G community, contributing to further progress on 5G Security and satisfying the requirements that come from the 5G-PPP Community at large.

In overall, this deliverable is expected to further advance the 5G Security Vision within the 5G-PPP community and beyond, taking advantage of the work performed at the project level, but also at the program level, would it be through 5G-PPP Security Work group (e.g. Security WG Whitepaper) or other joint activities performed (e.g. ETSI or EuCNC workshop, Open consultations on 5G Security, …).

Foreword

5G-ENSURE belongs to the first group of EU-funded projects which collaboratively develop 5G under the umbrella of the 5G Infrastructure Public Private Partnership (5G-PPP) in the Horizon 2020 Programme. The overall goal of 5G-ENSURE is to deliver strategic impact across technology and business enablement, standardisation and vision for a secure, resilient and viable 5G network. The project covers research & innovation - from technical solutions (5G security architecture and testbed with 5G security enablers) to market validation and stakeholders' engagement - spanning various application domains.

Deliverable D3.9 is the final update of the Technical Roadmap that was initiated in D3.1, and updated in D3.5. In this scope, D3.9 leverages on both D3.1 and D3.5 in order to complete the Product Vision on 5G-Ensure security enablers that were specified or specified and developed during the project, and which led to the delivery of two enablers' software releases. Moreover, D3.9 goes beyond the work that has been realized in 5G-ENSURE in order to recommend new features for the 5G security enablers that were developed during the project, and also to advise new enablers to be considered by 5G security community at large, based on lessons that have been learnt, and experience that the consortium has acquired through its participation to the 5G-PPP. This deliverable leverages on latest update of the technical roadmap (aka D3.5) that it extends and complements..

D3.9 is organized into three levels of granularity.

First, while the 5G-ENSURE security enablers were mainly designed to achieve requirements collected during the project, new requirements that have happened during the project lifetime and that couldn't be taken into account in the software releases have been captured and reported in D3.9 to raise awareness of the 5G Security Community on them.

Second, some new requirements in scope of the thematic clusters that have been explored during the 5G-ENSURE project and not covered by any of the developed enablers call brand new enablers to be investigated. D3.9 discusses and motivates the need for such enablers, providing the rationale behind and justifying why those requirements could not have been anticipated early in the project (mainly because the 5G vision has been rapidly evolving and maturing over the last couple of years, shedding some light on new requirements that were not yet envisioned in the early stages of the 5G-PPP).

Finally, D3.9 also discusses open security issues that go far beyond the thematic clusters developed during the project, and that the members of the 5G-ENSURE consortium believe are of relevance to the wider 5G security community. We believe that these open issues deserve to be addressed in future projects, both in the scope of, and beyond the 5G-PPP.

Disclaimer

Copyright notice

Contents

1 Introduction

Deliverable D3.9 is the final update of the Technical Roadmap that was initiated in D3.1, and further updated in D3.5. In this scope, D3.9 leverages on latest update of the technical roadmap (i.e. D3.5) where the product vision of 5G-Ensure security enablers in scope of the project were specified and/or developed, and which led to the delivery of two enablers' software releases (i.e. v1.0 delivered on M11/Sep'16 and v2.0 due M22/Aug'17). Moreover, D3.9 goes beyond the work that has been realized in 5G-ENSURE in order to recommend new features for the 5G security enablers that were developed during the project, and also to advise new enablers to be considered by the large 5G community, based on lessons that have been learnt, and experience that the consortium has acquired through its participation to the 5G-PPP. This deliverable leverages on latest update of the technical roadmap (aka D3.5) that it extends and complements.

D3.9 is organized into three levels of granularity.

First, while the 5G-ENSURE security enablers were mainly designed to achieve requirements collected during the project, new requirements that have happened during the project lifetime and that couldn't be taken into account in the software releases have been captured and reported in D3.9 to raise awareness of the 5G Security Community on them.

Second, some new requirements in scope of the thematic clusters that have been explored during the 5G-ENSURE project and not covered by any of the developed enablers call brand new enablers to be investigated. D3.9 discusses and motivates the need for such enablers, providing the rationale behind and justifying why those requirements could not have been anticipated early in the project (mainly because the 5G vision has been rapidly evolving and maturing over the last couple of years, shedding some light on new requirements that were not yet envisioned in the early stages of the 5G-PPP).

Finally, D3.9 also discusses open security issues that go far beyond the thematic clusters developed during the project, and that the members of the 5G-ENSURE consortium believe are of relevance to the wider 5G security community. We believe that these open issues deserve to be addressed in future projects, both in the scope of, and beyond the 5G-PPP.

To achieve these objectives, this document is organized as follows:

- Section 1 is a general introduction.
- Section 2 is devoted to the AAA category of enablers.
- Section 3 is devoted to Privacy category of enablers.
- Section 4 is devoted to Trust category of enablers.
- Section 5 is devoted to Security monitoring category of enablers.
- Section 6 is devoted to Network Management & Virtualization category of enablers.
- Section 7 provides a summary of the Technical Roadmap (final update) stressing what has been achieved through R1 and R2, and what is recommended as future work for the wider 5G security research community.
- Section 8 Research directions (recommended for future work)
- Section 9 concludes the document, while References are provided at the end.

Each of the category descriptions of Sections 2-6 provides details on the security enablers in second release (i.e. R2) together with the features planned. For the sake of completeness, the features achieved in R1 and already being there are reminded as well.

1.1 Abbreviations

3G	3rd Generation
3GPP	3rd generation partnership project
4G	4th Generation
5G PPP	5G Infrastructure Public Private Partnership
AAA	Authentication, Authorization, Accounting
ABAC	Attribute-based access control
ABE	Attribute Base Encryption
AKA	Authentication and Key-agreement
API	Application programming interface
APPEL	A P3P Preference Exchange Language
BYOI	Bring your own identity
CDN	Content Distribution Network
DPI	Deep Packet Inspection
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAP-AKA	EAP-Authentication Key Agreement
EPC	Evolved Packet Core
eUICC	embedded Universal Integrated Circuit Card
FastData	Processing of Big Data in real-time to take action when it matters (FastData is linked to notion of temporary storage of collected data, for instance less than 4 hours).
GUTI	Globally unique temporary UE identity
HSS	Home Subscriber Server
IMEI	International Mobile Equipment Identifier
IMPI	IP Multimedia Private Identity
IMS	IP Multimedia Subsystem
IMSI	International mobile subscriber identity
IDP	Identity provider
IoT	Internet of Things
KEC	Key Escrow Component
KPI	Key performance indicator
KP-ABE	Key Policy ABE
LEA	Lawful Enforcement Authority
LI	Lawful Interception
MCC	Mobile Country Code
mMTC	Massive machine-type communication

MMS	Multimedia Messaging Service
MNC	Mobile Network Code
MSISDN	Mobile Subscriber ISDN Number
NAT	Network Address Translation
NESAG	Network Equipment Security Assurance Group
NFV	Network-Function Virtualization
NFVi	Network Function Virtualization Infrastructure
NIB	Network Information Base
OS	Operating System
P3P	Platform for Privacy Preferences
PDP	Policy decision point
PEP	Policy enforced point
PFS	Perfect forward secrecy
PKI	Public key infrastructure
RBAC	Role-based access control
RCD	Resource-constraint devices
SC	Secure Component
SDN	Software-Defined Networking
SECAM	Security Assurance Methodology
SIM	Subscriber Identity Module
SMS	Short Message Service
SO	System Operating
SSL	Secure Sockets Layer
S-TMSI	SAE-Temporary Mobile Subscriber Identity
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
UE	User equipment
UICC	Universal Integrated Circuit Card
USIM	Universal subscriber identity module
VMNO	Virtual mobile network operator
VNF	Virtual Network Function
VPN	Virtual Private Network

2 AAA Security Enablers

2.1 Security Enabler "Basic AAA enabler"

2.1.1 Product Vision

It can be assumed that 5G will utilize a basic 5G access authentication similar to what is employed by 2G, 3G and 4G. The Authentication and Key-agreement (AKA) procedures for these systems have mostly fulfilled the requirements present in each of these generations. 5G puts new requirements on the AKA procedure and certain new aspects to be considered when designing the 5G system. Examples of such new aspects are:

- Forward secrecy of the keys produced by the AKA procedure.
- AAA aspects of trusted micro-segmentation in 5G networks.
- Trusted interconnect and authorization.

Table 1: Mapping between enabler security features and relevant use cases

Enabler Security Feature	Relevant Use Case
Forward secrecy of the keys produced by the AKA procedure	Use Case 2.3: Enhanced Communication Privacy
AAA aspects of trusted micro-segmentation in 5G	Use Case 5.1: Virtualized Core Networks, and Network Slicing
Trusted interconnect and authorization	Cluster 9

2.1.1.1 Forward secrecy of the keys produced by the AKA procedure

There have been reports on compromised long-term keys in UICCs (The Register, 2015). In such situations, security against both passive and active attackers is lost. Since 5G aims to attract mission critical services, it would be beneficial to provide stronger protection against such threats. The vision for the enabler is not that it can ensure 100% elimination of key compromises but rather that it should

- Limit the impact of long-term key compromise in temporal and/or spatial dimensions
- Make it more difficult to exploit compromised keys
- Provide mechanisms to restore, to the extent possible, security after a key compromise

One ingredient in such a solution could be to add (perfect) forward secrecy (PFS) to current AKA protocols.

2.1.1.2 AAA aspects of trusted micro-segmentation in 5G networks

Micro-segmentation is a more fine-grained approach than traditional network segmentation. The network is divided into smaller parts which can be based on host, user, application or network identity information. These distinct security segments can be divided down to the individual workload level. For each unique segment, security controls are defined and services delivered. Only authenticated devices and network services can join the segment, additionally, traffic inside the segment should be monitored. The work on this enabler feature will consist of studying AAA aspects of trusted micro-segmentation by defining AAA functionalities required by the micro-segmentation, and propose an AAA solution (with required modifications, if any) to be used together with the developed micro-segmentation enabler attached to Network Management & Virtualization enablers Cluster, detailed in Section 6.5.

2.1.1.3 Trusted interconnect and authorization

A problem that has been growing the past years, and is likely to become a major issue for 5G, is authentication and authorization between operator core networks. To prevent unauthorized entities (e.g. 3rd parties or a compromised operator) from obtaining authentication vectors, sending spoofed SMS etc., the incoming request to one operator from another operator needs to be authenticated and authorized before being accepted. This becomes especially relevant if more dynamic interaction opportunities are provided, e.g., in the form of dynamic roaming, where it might not be so clear who the interacting parties are. There should be sufficient assurance that the interaction refers to authentic entities, even if the said entity is not explicitly a party to the protocol communication, e.g., two parties exchange information regarding a third party, i.e., in the form of authorizations. Thus, strong naming of entities needs to be studied in the context of suggested AAA protocols, whilst also making sure new privacy issues are not introduced. Granularity of authorization needs to be studied as well, so that actions with security or real world implications (such as charging) are properly authorized.

2.1.2 Features achieved in R1

Forward secrecy and AAA aspects of trusted micro-segmentation were both “early” specified and incorporated in deliverable D3.2 5G-PPP security enablers open specifications (v1.0) despite the fact they were not developed and release in software.

- **Feature name:** Forward Secrecy
- **Goal:** Limit and/or recover from impact of compromised long-term keys, preferably with backward compatibility. Provide a high-level description of which concepts to use for key agreement and authentication.
- **Description:** Enhanced AKA protocols and key management (recovery) mechanisms.
- **Rationale:** Offer very high levels of security for critical applications. Build strong 5G perception as being secure against “mass surveillance”.

- **Feature name:** AAA aspects of trusted micro-segmentation
- **Goal:** Provide a high-level description of micro-segmentation and its potential benefits for 5G.
- **Description:** A study of AAA aspects and requirements introduced with trusted micro-segmentation and proposal of AAA solution with the developed enabler in task 3.5, Network Management & Virtualization, detailed in Section 6.5.
- **Rationale:** A suitable AAA solution is an important aspect in trusted micro-segmentation for 5G. The existing AAA solutions might not suffice due to the new requirements introduced with micro-segmentation

2.1.3 Features achieved in R2

R2 of Basic AAA enabler includes mainly features continued from R1, which were not fully specified. No software release has been made for this enabler, but only open specifications.

- **Feature name:** Forward Secrecy
- **Goal:** Limit and/or recover from impact of compromised long-term keys, preferably with backward compatibility. Provide a detailed description on how protocols need to be adapter to support PFS. Investigate both classical DH as well as the protocol impact of quantum immune solutions.
- **Description:** Enhanced AKA protocols and key management (recovery) mechanisms.
- **Rationale:** Offer very high levels of security for critical applications. Build strong 5G perception as being secure against “mass surveillance”.

- **Feature name:** AAA aspects of trusted micro-segmentation
- **Goal:** Find a suitable AAA solution for micro-segmentation in 5G networks, and verify AAA aspects in trusted micro-segmentation of 5G networks.
- **Description:** A study of AAA aspects and requirements introduced with trusted micro-segmentation and proposal of AAA solution with the developed enabler in task 3.5, Network Management & Virtualization, detailed in Section 6.5.
- **Rationale:** A suitable AAA solution is an important aspect in trusted micro-segmentation for 5G. The existing AAA solutions might not suffice due to the new requirements introduced with micro-segmentation.

- **Feature name:** Trusted interconnect and authorization
- **Goal:** Ensure authenticity of interconnecting parties, provide explicit authorization to actions with security impact
- **Description:** Study of suitable naming and authorization schemes in the context of 5G network involving dynamic interaction
- **Rationale:** Expected dynamism of 5G networks requires more explicit security mechanisms instead of relying on implicit security

2.1.4 Recommendations for further research

In general, a major recommendation is to provide actual implementations of this enabler's features to consolidate their open specifications. In addition, an interesting future research work for this enabler is to investigate performance and security aspects of quantum immune algorithms for Perfect Forward Secrecy. Furthermore, Trusted interconnect and authorization. (TIA) as outlined in previous roadmaps has to be considered for further research due to other enablers' complexity that leads to a down prioritization of TIA.

2.2 Security Enabler "Internet of Things - IoT"

2.2.1 Product Vision

The vision of this enabler is to provide features in support of the Internet of Things (IoT). The collection of connected devices is likely to increase substantially and 5G is expected to fully support the connectivity of IoT devices.

As 5G aims to be the network of excellence for IoT, it must provide an adequate security level, without exposing others services and legal obligation, which in turn introduces novel security challenges for authentication of the IoT devices in 5G.

This enabler envisions four features:

USIM-less support: The USIM application and the pre-shared key based EPS-AKA procedures believed to remain important for many types of access to 5G systems. However, some use cases, may benefit from support of AKA procedures based on other types of credentials such as asymmetric keys and certificates. This would allow reuse of already deployed identity infrastructures also for access to 5G. A relevant use case is when a factory owner operates his own AAA server for 5G network access.

Group-based AKA: The Authentication and Key Agreement protocol (AKA) has a central role in the security of mobile networks as it bootstraps the parameters needed to form a security context that 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 is almost identical to its predecessor used in 3G, which was introduced in the late 90s. A limitation of EPS-AKA is that, for each device that requires network

access, the protocol requires signalling among the device, 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 when users are roaming. This represents a bottleneck for the development of 5G as a low delay and reliable network for IoT devices.

5G is expected to handle with an unpredictable number of heterogeneous connected IoT devices while guaranteeing a high level of security. This feature hence focuses on a group-based AKA protocol that contributes to reduce latency and bandwidth consumption, and scales up to a very large number of devices. A central aspect of group-based AKA is to provide a protocol that enables to dynamically customize the trade-off between security and efficiency. The protocol should be lightweight and resorts on symmetric key encryption only to supports low-end devices and to facilitate a smooth transition from the current standards with little effort.

Bring your own identity: As 5G wants to attract new user categories, i.e. industries (process/manufacturing) and societal functions (public safety, health), it is important to minimize costs associated with becoming "5G subscribers". It can be foreseen that in many cases, these types of "enterprises" may already have an existing AAA infrastructure in place for devices and/or employees. Our vision is to allow such user groups to re-use their pre-existing identities as a basis for 5G network access, i.e. a "bring your own identity" (BYOI) solution, thus reducing administrative tasks and the deployment of separate credentials for 5G access, which in turn will lower the overall cost. To deliver this type of functionality, a new architecture has to be investigated, thus the enabler will look into the technical solutions of delegating third-party access, liabilities and access control. A risk analysis should identify any eventual residual risks.

vGBA: The Generic Bootstrapping Architecture (GBA) is a 3GPP defined solution for re-using the 3GPP credentials and AKA for authentication also outside the 3GPP scope. GBA uses the 3GPP subscription credentials for authentication and key-agreement with any GBA enabled service regardless if the service is operated by an MNO or some other instance. For IoT device, operating autonomously, GBA provides a strong and proven authentication framework that relies on credentials stored and used in a physically secured way using (e)UICC, which could be used for authentication towards IoT services such as data aggregation and device management. However, as GBA is based on AKA it also means that an authentication vector needs to be fetched from the subscriber database. Vertical GBA (vGBA) minimizes the impact on the subscriber database by utilizing the AKA run from network attachment for automatically bootstrapping also the GBA security. In addition to optimizing the usage of the subscriber database, also the constrained IoT devices utilizing this feature benefit from the solution as it reduces signalling by removing the need for a dedicated AKA run for bootstrapping GBA security.

Table 2: Mapping between Basic AAA enabler security features and relevant use cases

Enabler Security Feature	**Relevant Use Case**
Group-based AKA	Authentication of IoT Devices in 5G (Use Case 3.1)
Specification of how to integrate an AKA procedure for one or more alternative credentials to USIM.	Using Enterprise Identity Management for Bootstrapping 5G Access (Use Case 1.2)
Authentication based on third party identities, i.e. bring-your-own-identity	Factory Device Identity Management for 5G Access (Use Case 1.1) Using Enterprise Identity Management for

	Bootstrapping 5G Access (Use Case 1.2)
vGBA	Authentication of IoT Devices in 5G (Use Case 3.1)

2.2.2 Features achieved in R1

- **Feature name**: Group authentication by extending the LTE-AKA protocol (Group-based AKA)
- **Goal**: Enable 5G to support massive deployments of IoT devices by adding explicit support for group authentication of devices.
- **Description**: A new protocol has been proposed in R1. The protocol is pivoted on the idea of using an inverted hash tree to manage a large number of devices efficiently. The cryptographic primitives of the protocol are based on MILENAGE so that the protocol can be adopted in the current standards. The implementation in OpenAirInterface (OAI) confirms that only minor modifications to EPS are needed to support the group-based AKA. A formal analysis of the protocol corroborates the security guarantees of the proposed solution (Giustolisi, Christian, Åhlstrom, & Holmberg, 2016), which proved to resist to threats due to colluding corrupted devices. The performance analysis yields promising results in term of latency and bandwidth consumption, with a remarkable gain, i.e., the group-based AKA consumes less bandwidth when already seven devices are considered.
- **Rationale**: The current protocols, e.g. AKA, must be enhanced to support the novel requirements introduced by massive deployment of IoT devices. As a result, 5G will be the network of excellence for IoT.

The theoretical solution of vGBA was presented but not implemented.

2.2.3 Features achieved in R2

- **Feature name**: Group authentication by extending the LTE-AKA protocol (Group-based AKA)
- **Goal**: Enable 5G to support massive deployments of IoT devices by adding explicit support for group authentication of devices.
- **Description**: The group-based AKA has been improved in R2. The direction we took was to modify the implementation with support of native multiple devices and to introduce a resynchronization procedure into the protocol.
- **Rationale**: The current protocols, e.g. AKA, must be enhanced to support the novel requirements introduced by massive deployment of IoT devices. As a result, 5G will be the network of excellence for IoT.
- **Feature name**: Non-USIM based AKA
- **Goal**: Enable 5G to support massive deployments of IoT devices by adding support for alternative AKA procedures than EPS-AKA (e.g. EAP-TLS, using certificates instead of USIM, etc.).
- **Description**: This feature will consist on a survey that investigates and identifies suitable alternative AKA procedure to USIM based EPS-AKA. The intention to find one or more suitable candidates and described impacts and how they can be integrated into the 5G.
- **Rationale**: For 5G to reach its full potential and be appealing for new industries, it is important to simplify the deployment of AAA infrastructures. It is hence beneficial if already deployed non EPS-AKA based authentication schemes can be reused for 5G access.

- **Feature name**: BYOI
- **Goal**: Allow enterprises that already have an existing AAA infrastructure in place for devices and/or employees to re-use pre-existing identities as a basis for 5G network access.

- **Description**: To deliver this type of functionality, a new architecture has to be investigated, thus the enabler will look into the technical solutions of delegating third-party access, liabilities and access control.

Rationale: Reduce administrative tasks and the deployment of separate credentials for 5G access, which in turn will lower the overall cost.

2.2.4 Recommendations for further research

Regarding the group-based AKA, further research includes the extension of the group-based AKA with support for secure handover among different MME. One approach is to use techniques from different areas, such as mobile cloud computing. Another research direction is to support dynamic groups with key forward/backward secrecy: linkable group signature schemes might be used on top of the protocol. Lastly, establishing how group-based AKA should behave during the Update-location procedure in LTE should be researched. An approach to this would be to leverage the grouping of devices and the inherit device information in the inverted hash trees in order to reduce signalling between MME and HSS. Another recommendation for future research concerning Group-based AKA is to modify the protocol to meet perfect forward secrecy for the session master key.

For vGBA it could be beneficial to do a more in-depth analysis of alternatives for handling GBA bootstrapping context lifetime expiry. In regular GBA, the network informs the UE of the bootstrapping context lifetime, after which the UE can re-bootstrap with the BSF. With vGBA, the UE does not get any indication of GBA bootstrapping context lifetime, but will instead notice lifetime expiry from authentication requests, e.g. HTTP 401, from GBA enabled services. As a reaction to this the UE could either perform a regular GBA (re-)bootstrap with the BSF or re-authenticate with the network, resulting in a new GBA bootstrapping context in the BSF. Furthermore, when GBA ME is used, various scenarios where vGBA is only enabled in part of the end-point (ME, UICC) result in scenarios that could be further studied.

2.3 Security Enabler "Fine-grained Authorization Enabler"

2.3.1 Product Vision

The role of interconnected resources, such as services and resource-constrained devices (RCDs), will be preponderant in the following years in the capabilities offered by systems. Today, a lot of RCDs, such as sensors, actuators, satellite modems and IoT devices in general, already exist but are not secured. Some standards have been specified and implemented (e.g. LoWPAN – Low power Wireless Personal Area Networks, RPL – Routing Protocol for Low power and Lossy Networks), but focusing on the communication level rather than the application level; hence, it is possible to establish a secure layer to communicate with them, but without fine-grained access control. Currently there is standardization work in progress at the Internet Engineering Task Force (IETF) on access control for RCDs[1]. This enabler will leverage the results of that work in order to align the resulting 5G standards with the future IETF standardization.

The owner *controls* access to the resources, while users may be *granted* access to them. The goal of this security enabler is to provide a secure fine-grained access control to such resources.

This enabler will research new methods to provide distributed authorization, suitable in resource-constrained environments. The goal of the enablers is to make 5G fully ready for Identity and Access Management (IAM) of IoT devices.

[1] https://datatracker.ietf.org/wg/ace

The security enabler should support:

- Multiple users with different rights.
- Decision per user, resource and action.
- Access based on dynamically changing parameters.
- Access control enforcement directly embedded in the device (i.e. without direct connection to an external Authorization server).
- Integration of different Authorization servers.

Such a security enabler is important to 5G because interconnected resources are becoming ubiquitous, and fine-grained authorization is an essential security requirement in this field. Therefore, 5G will benefit interconnected resources due to the evolution of the mobile telecommunication technology in terms of available bandwidth and minimized latency.

Table 3: Mapping between Fine-grained Authorization enabler security features and relevant use cases

Enabler Security Feature	Relevant Use Case
Basic Authorization in Satellite systems	Satellite Identity Management for 5G Access (Use Case 1.3) Authorization for End-to-End IP Connections (Use Case 4.2)
Basic Distributed Authorization Enforcement for RCDs Authorization and authentication for RCD based on ongoing IETF standardization	Authorization in Resource-Constrained Devices Supported by 5G Network (Use Case 4.1) Authentication of IoT Devices in 5G (Use Case 3.1)
AAA integration with satellite systems	Authentication of IoT Devices in 5G (Use Case 3.1)

2.3.2 Features achieved in R1

The features achieved in R1 in terms of design, analysis, implementation and test are the following:

- **Feature name:** Basic Authorization in Satellite systems
- **Goal:** To support access control of multiple users with different rights in satellite devices and services.
- **Description:** To provide an enabler that supports different authorization methods (RBAC/ABAC) and policies to provide basic access control to satellite devices and services. It will consist in a set of application programming interfaces (API), policies and an AAA server. The same AAA server will support RBAC to satellite services and ABAC to satellite modems**.**
- **Rationale:** 5G daily activities will need multiple authentication methods with multiple authorization policies that provide fine-grained access to a plethora of interconnected resources. This enabler will support 5G with these tasks.

  Additionally, this enabler will integrate existing AAA protocols in satellite and terrestrial communications, necessary to improve 5G use cases that can only be served by satellites (no terrestrial coverage), or for which satellites provide a more efficient solution (i.e. traffic congestion, cyber-attacks or natural disaster). Offering an “always on” service will be one of the 5G requirements.

While Satellite modems are directly connected to the satellite, 5G devices can be connected to a traditional eNodeB or to an eNodeB improved with a satellite link, which is connected to the core network.

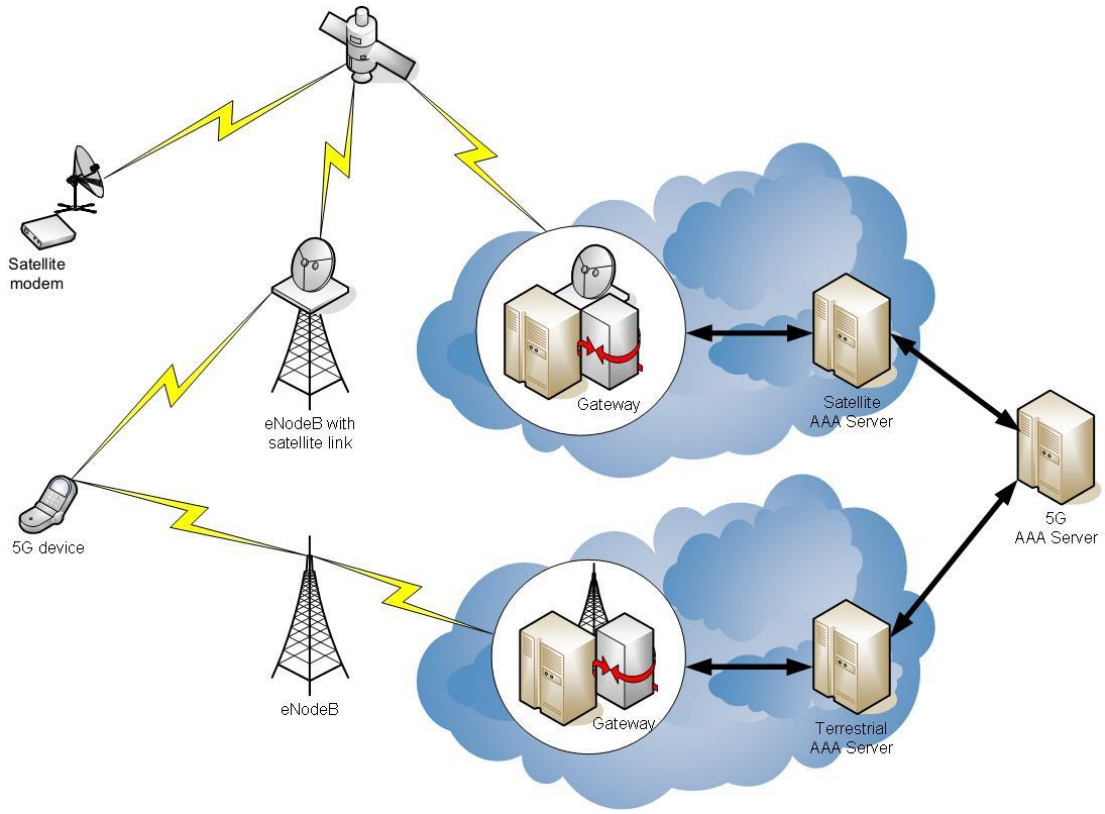


Figure 1 AAA system mechanism

- **Feature name:** Basic Distributed Authorization Enforcement for RCDs
- **Goal:** To support access control on RCDs based on existing http solutions using ABAC and adapted for these devices.
- **Description:** To provide a prototype that supports the different exchanges between the different actors (user/Authentication server/RCD) with simple access control policy and a simple PEP and PDP on RCD side. An evaluation of CPU, memory and latency cost will be delivered. The following schema gives the proposed architecture:

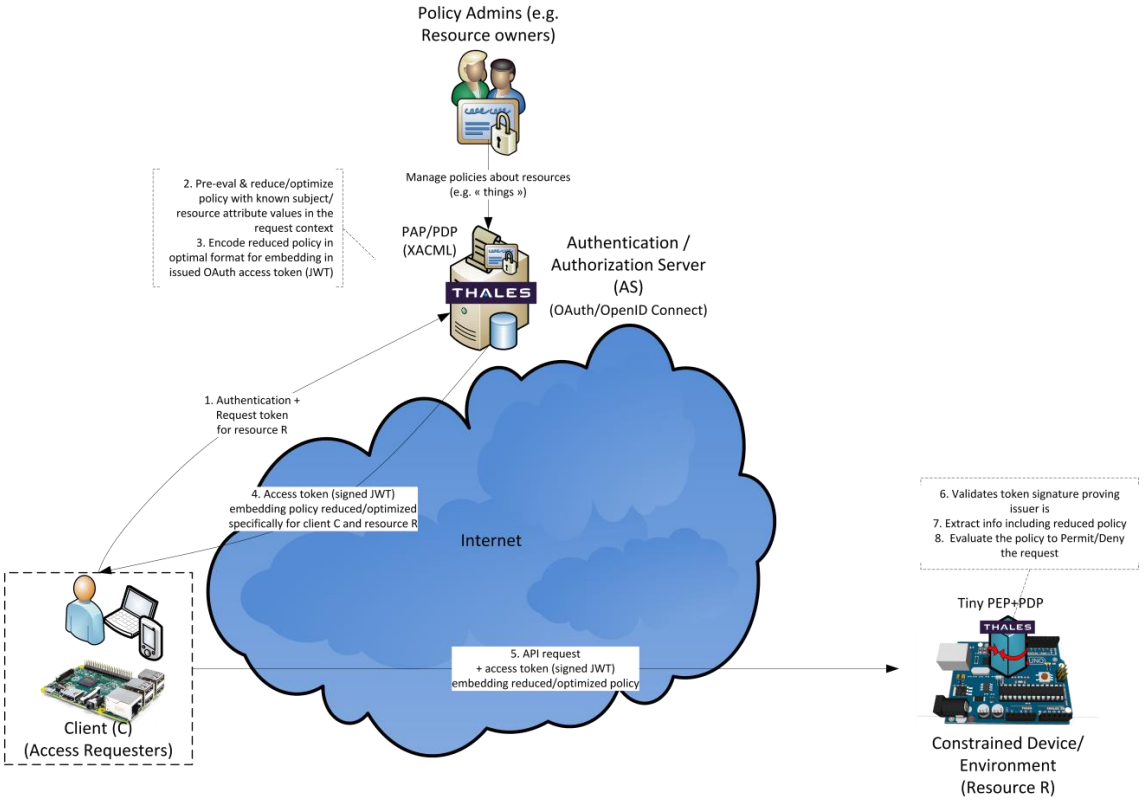


Figure 2 Distributed Authorization Architecture for RCDs

The main difference with common web technologies of centralized access control is that the Authentication and Authorization enforcement are embedded on the RCD. The access control policy is planned to be defined with XACML.

The solution is envisioned to rely on:

- Central OAuth-compliant Authorization service capable of:
  - On-the-fly XACML policy evaluation for specific client and resource,
  - Issuing signed OAuth tokens embedding a conditional access control decision (e.g. based on CWT[2]),
- Minimal PEP for enforcement of conditional access control decisions on constrained resource and supporting such tokens.

- **Rationale:** Authentication and Authorization for RCD ABAC access control based on http standard solutions. This basic authorization enforcement is a first step towards fine-grained access to the RCD.
  - This enabler is not about the access authorization to 5G network. Instead, it focuses on an authorized service on a higher layer offered by the 5G operator based on the 5G credentials.
  - Some devices are quite constrained that they cannot easily employ a full protocol stack but they are capable enough to use this enabler specifically designed for RCDs. Therefore, any 5G device can benefit from this light-weight enabler from consuming less bandwidth. Moreover, using fewer resources for networking leaves more resources available to applications.

[2] https://datatracker.ietf.org/doc/draft-ietf-ace-cbor-web-token/

2.3.3 Features achieved in R2

- **Feature name**: AAA integration with satellite systems
- **Goal**: To support policies for decision per user, resource and action; and integrate the authentication and authorization mechanism with the satellite system.
- **Description**: To implement the policies for decision per user, resource and action having a server with rationalities between all of them. Those policies should clearly be stated for each group or type of user, defining what accesses are permitted through the roles and the responsibilities of the different user groups. It will also be implemented an access control based on dynamic changing parameters and the final integration of the authentication and authorization mechanism with the satellite system.

  Finally, this release is expected to provide a version of PEP and PDP embedded on the RCD, and the Authentication server delivering a self-sufficient security token allowing decentralized authentication and authorization, compatible with RCDs in terms of performance.

  The final objective with that prototype is to support the different exchanges between the different actors (user/Authentication server/RCD) with simple access control policy and a simple PEP and PDP on RCD side. An evaluation of CPU, memory and latency cost will be delivered. A complete log with all the exchanges in the network should be stored in a file or displayed.

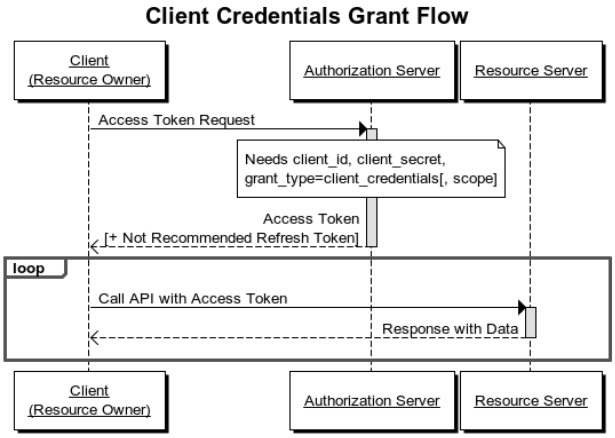


Figure 3 Client Credentials Grant Flow

- **Rationale**: At the end, this enabler will integrate existing AAA protocols in satellite and terrestrial communications, necessary to improve 5G use cases that can only be served by satellites (no terrestrial coverage), or for which satellites provide a more efficient solution (i.e. traffic congestion, cyber-attacks or natural disaster). Offering an "always on" service will be one of the 5G requirements.

  When the integration has been finished, the enabler will bring new features to 5G, enhancing the authentication and authorization protocol between mobile operations in order to mitigate the risk of malicious operators.

- **Feature name**: Authorization and authentication for RCD based on ongoing IETF standardization
- **Goal**: Enable standards-based, fine-grained access control and authentication on resource constrained devices connected at the edge via low power lossy networks.

- **Description**: To provide a prototype that supports the different protocols between the different actors (user/Authorization Server/RCD) as follows:
    - The user requests from the Authorization Server (AS) an access token authorizing specific requests to the RCD. The AS renders an access control decision using a PDP component based on XACML policies set by the RCD owner. This decision is encoded into a compact, cryptographically protected access token (e.g. JWT/CWT) and sent back to the user together with the necessary information allowing the user to authenticate or prove that it is the rightful owner of the access token (proof-of-possession).
    - The user transfers the access token to the RCD together with an access request to some resource hosted by the RCD (e.g. a sensor value) and preforms the proof-of-possession and/or authentication.
    - Using a PEP component, the RCD verifies the authenticity and validity of the token and the proof-of-possession, and whether it applies to the request the user sent. This must be possible to perform off-line, without invoking external services. If these verifications succeed, the RCD grants access to the desired resource.

  Rationale: Fine-grained, application layer authentication and authorization solutions, aligned with ongoing IETF standardization work. This enabler is not about access authorization to the 5G network, instead it focuses on providing authentication and authorization services to the application layer using the 5G credentials and facilitated by the 5G operators. This enabler is designed for IoT devices at the edge of the network that are constrained and need to save bandwidth, memory, CPU capacity and possibly even battery power.

- **Feature name**: Basic Distributed Authorization Enforcement for RCDs based on existing web standards
- **Goal**: Enable fine-grained access control enforcement based on web standards on resource constrained devices, using standalone proof of access rights to lower resource consumption of external connections requirements.
- **Description**: To provide a prototype of enforcement module, deployable on a resource-constrained device, relying on access tokens provided by enabler R1 Authentication server. This enforcement consists in:
    - Cryptographic signature validation in accordance with a trusted Authentication server source
    - Validity timestamp checking to ensure the token has been recently provided and lower the risks of using stolen standalone tokens by using an expiration time
    - Validation of the currently performed action regarding the token scope formally expressed using an embedded XACML access control policy
- **Rationale**: This feature does not relate to authorization to the 5G network itself, but demonstrates how, through 5G networks, IoT devices can securely provide services based on existing web standards and relying on existing web access control architecture using a trusted third party authentication server and centralized access control policy without requiring more resource consumption. This saving is ensured by the delivery of standalone access tokens containing a subpart of the central access control policy that can be fully enforced by the IoT devices themselves.

2.3.4 Recommendations for further research

Possible directions of further IoT authentication research:

- Dynamic client and RCD registration protocols at the Authorization Server
- Security parameter lifecycle management solutions for large IoT deployments (e.g. sensor networks)

Also, the further research can include improving the AAA integration with satellite systems module and converting it into AAA+, defined as a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to grant/deny/control access to satellite link to requests made by subscribers. Some of the requirements for this new module could be:

- The operator shall be able to authenticate at satellite system with secure and hierarchical access control.
- The audit function shall be able to record the identity of every access, privileged operations, unauthorized access attempts, and changes or attempts to change system security settings and controls.

A further research to improve the time and resource consumption of the enforcement of an access token is an optimization of the expression of the self-contained authorization.

2.4 Security Enabler "Federative authentication context usage enabler"

2.4.1 Product Vision

In the context of a slice based on different infrastructures, the end user connected to the slice wants to use different services. These services, offered by these infrastructures, need to trust the authentication mechanisms used by the end user in the context of identity federation. The goal of this enabler is to collect at 5G nodes the authentication context of an end user and to provide this information to service providers allowing them to adapt dynamically their security policy using their risks evaluation before delivering the service. The security enabler should support:

- Different authentication mechanisms (USIM Card, login/password, x509 certificates, PIN code for instance – list not exhaustive-) could be improved regarding the available access control features of the Testbed.
- Authentication mechanisms supported by the AAA server.
- Access control enforcement directly managed by the service provider depending on the type of authentication mechanisms.

Table 4: Mapping between Basic AAA enabler security features and relevant use cases

Enabler Security Feature	**Relevant Use Case**
Different authentication mechanisms (e.g. login/password, x509 certificates, pin code)	Using Enterprise Identity Management for Bootstrapping 5G Access (Use Case 1.2) Satellite Identity Management for 5G Access (Use Case 1.3) MNO Identity Management Service (Use Case 1.4)
Authentication mechanisms supported by AAA server.	Factory Device Identity Management for 5G Access (Use Case 1.1) Using Enterprise Identity Management for Bootstrapping 5G Access (Use Case 1.2) Satellite Identity Management for 5G Access (Use Case 1.3) MNO Identity Management Service (Use Case

	1.4)
Access control enforcement directly managed by the service provider depending on the type of authentication mechanisms.	Using Enterprise Identity Management for Bootstrapping 5G Access (Use Case 1.2) Satellite Identity Management for 5G Access (Use Case 1.3) MNO Identity Management Service (Use Case 1.4)

2.4.2 Features achieved in R1

None since this enabler was already announced in D3.1 (early version of Technical Roadmap) as specifically planned for R2

2.4.3 Features achieved in R2

- **Feature name**: Storage of authentication level
- **Goal**: To store in a dedicated database the authentication level (in LDAP for example)
- **Description**: Each time, a user authentication is performed (or updated) at AAA level, this information is registered, timestamped and stored for future usage in a specific database managed with the HSS database. This information could be used to contextualize the security environment of the user at Service level.
- **Rationale**: provide at any time the authentication level of a user in the network. This level is depending on the authentication mechanism used.

- **Feature name**: Usage of authentication level
- **Goal**: Usage, at node level, of the authentication level.
- **Description**: For specific nodes, to implement the usage of the authentication level.
- **Rationale**: Allow dynamic adaptation of service delivery regarding the security level of the access to 5G Network.

2.4.4 Recommendations for further research

In this section, "AAA Security Enablers ", different enablers have proposed different ways to open the authentication mechanisms. Deliverable D2.1 mention different use cases like UC3.3.1 and U3.3.2 where the identity has to be managed in a more open way.
Regarding the "Federative authentication context usage enabler", it makes sense to store the way a user (or a device) is authenticated in a 5G infrastructure. That's why this enabler should be concretely developed (at least the 2 features specified in R2) and could be extended to different other kinds of authentication, not only limited to AAA authentication.

3 Privacy Enablers

Privacy is an important 5G enabler since it has a high social impact and can be one of the fundamental requirements that can permit the creation of new services and new business models on top of 5G networks. If properly addressed, privacy can increase users' assurance and confidence in 5G networks.

The main objective of the 5G-Ensure Privacy enablers is to identify in advance 5G user privacy requirements and to provide security mechanisms able to prevent privacy violations by adopting a proactive, privacy-by-

design approach. Therefore, this section describes some privacy enablers which have been identified as relevant to 5G, i.e., needed by the use cases defined in Deliverable D2.1 (5G-Ensure Consortium, 2016) and/or by 5G stakeholders. These enablers should be integrated into the 5G security architecture overall design so as to be natively supported into the 5G systems, services and also business practices.

The privacy enablers result from the analysis of the 5G use cases and from anticipated privacy requirements needed in order to derive their design. For each use case, the privacy mitigation technology (e.g., anonymity by using temporary identity, access control mechanisms, new encryption system and procedures, etc.) was also investigated so as to satisfy privacy requirements. The 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.

The first enabler provides encryption 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 network. The enabler focuses on counteracting the vulnerabilities of current 3G and 4G attach and paging procedures. This enabler also extends protection of subscriber's identity for non-3GPP access such as WiFi/EAP-AKA.

The second enabler provides an anonymization mechanisms for protecting the privacy of device identifiers for both UICC and UICC-less devices attaching to 5G networks via various network technologies.

The third and fourth enablers are concerned with offering the 5G users the ability to be in control of his/her 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 mainly stored on the SIM by employing device-based anonymization techniques, while the fifth enabler provides a means to future 5G applications to define their own privacy policy and to check it against the servers' privacy policies in order to detect any possible privacy violations at the application level.

3.1 Security Enabler "Privacy Enhanced Identity Protection"

3.1.1 Product Vision

All previous generations of mobile devices, as standardized by 3GPP, have failed at providing proper privacy in regards of protecting device and subscriber IDs, i.e. current protocols have not successfully been able to prevent tracking of the location of devices and users (Shaik, Borgaonkar, Asokan, Niemi, & Seifert, 2015). Mobile devices engage in a number of AAA protocol interactions dependent upon their access to the network where the device and subscriber ID transmission is requested. As such, this privacy enabler was designed to provide protection against user's identity disclosure and unauthorized user tracking, and to defend against various types of IMSI (International Mobile Subscriber Identity) catching attacks and location tracking attacks. The enabler is an enhancement to subscriber privacy in 5G network, if compared to the level of protection provided in current 3G and 4G networks. Briefly, the enabler helps at:

- Increases privacy in protocol interactions
- Enhances anonymity properties
- Improves unlinkability.

The first privacy enhancement lays on the fact that the 5G user true identity is never transferred in clear text over the network during the attach procedure (when a security context is not yet defined) and as an answer to an Identity Request. This protects towards passive attacks aiming to intercept the transmission of the user identity over the air and also towards active attacks aiming to obtain the real user identity through

request sent by a fake base station. The second enhancement is provided by the generation of unique dynamic (pseudo) random pseudonyms used in the signalling procedures which follow the user's network access. A subsequent enhancement is provided by the method used to generate the dynamic random pseudonyms.

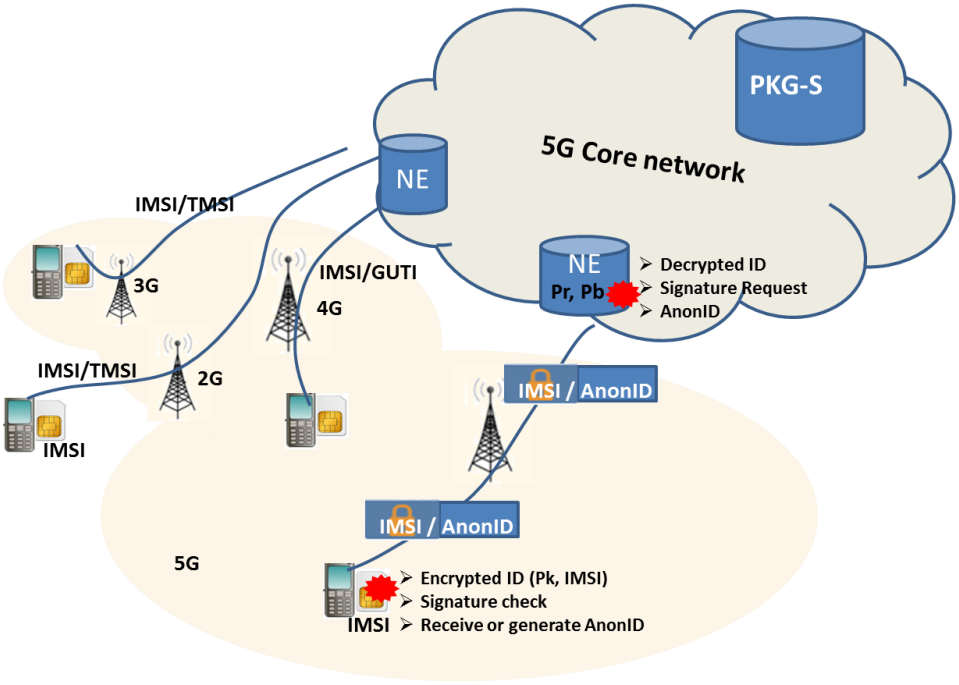


Figure 4: High level Privacy Enhanced ID Protection architecture.

Table 5 Mapping between Privacy Enhanced Identity Protection enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case
Encryption of Long Term Identifiers (all solutions)	Use Case 2.2: Subscriber Identity Privacy
	Use Case 2.3: Enhanced Communication Privacy
IMSI pseudonymization	Use Case 2.2: Subscriber Identity Privacy

3.1.1.1 Encryption of Long Term Identifiers

The feature "Encryption of Long Term Identifiers" provides an encryption scheme for the user permanent or long term identifiers (IMSIs) in messages unprotected by symmetric cryptography due to lack of security context. In such cases, since no session secrets are yet shared, asymmetric encryption is necessary, in order to avoid using the Ki (the secret key of the USIM/UICC). Solutions of this type were discussed in 4G standardization, for example Section 5.1 of (3GPP, 2008) (already in Rel-99 standardization of 3G). 3GPP (3rd Generation Partnership Project) decided against the usage of public key mechanisms because the implementation cost was deemed too high. However, recent findings (Shaik, Borgaonkar, Asokan, Niemi, & Seifert, 2015) and the increased computational power of present and future mobile devices, can justify the use in 5G network of a scheme where public/private keys are deployed only on network elements. The computational cost of the enabler related to the use of an asymmetric encryption scheme has been measured on some common UE devices to evaluate its effective impact.

The enabler encrypts the permanent or long term subscriber identifier when it has to be sent towards the network by using the public key of the network; therefore, the UE does not send the subscriber's permanent or long term identity in clear text in order to initiate the network attach procedure.

In order to cover other possible scenarios, like a LI (Lawful Interception) scenario, the Attribute-Based Encryption (ABE) (Goyal, Pandey, Waters, & Sahai, 2006) scheme is used, instead of traditional public key encryption. ABE enables the encryption of sensitive data by a single public key and decryption by different secret private keys according to access policies. For asymmetric/public-key ABE, access policies are expressed as access structures in terms of attributes and can be built in the private decryption keys (key-policy ABE (Goyal, Pandey, Waters, & Sahai, 2006)) or in the cipher text (cipher text-policy ABE (Bethencourt, Sahai, & Waters, 2007)). In this latter case, the access policy is built in the cipher text and the subsets of attributes are built in private decryption keys of the users. In the key-policy case, the set of attributes is built in the cipher text and the access policies in private decryption keys of the users.

ABE schemes should satisfy the collusion resistance, namely, it should be infeasible to obtain any advantage by pooling different private keys. The ABE schemes based on elliptic curve pairings are practical and inherently include message randomization for semantic security and personalized randomization for collusion resistance.

Examples of where the enabler applies are the Attach Request and Identity Response NAS messages.

In both cases the public key is stored on the SIM (Subscriber Identity Module), while the private key is either stored on the network element, such as the 5G equivalent of the MME in 4G networks. A dedicated network element may be set up which stores and handles the private key for decryption.

In order to implement an ABE cryptosystem in a roaming scenario, the participating MNOs have to be members of a PKI, managed by a trusted authority (e.g., the GSMA). All MNOs (home and serving) participating in the scheme have associated attributes bound to their private keys, allowing them to individually decrypt and avoiding the need for HN to transfer IMSI to SN (which is needed in case of the "home network centric IMSI" solution in order to respect the LI requirement). In all cases the implemented system respects the LI requirements.

3.1.1.2 Encryption of Long Term Identifiers (solution 2) a.k.a. Home Network centric IMSI protection

In this solution a traditional public-key scheme is implemented, in which the UE uses the public key of its home network to encrypt parts of the IMSI. The key can be stored on the UEs in advance (e.g. on the USIM card), given that it is static, so there is no need of deploying additional infrastructure for key management, such as a PKI, except possibly a revocation/update mechanism in case of key compromise, but that can be managed on per-operator basis.

The home network is responsible of performing the decryption and sharing afterwards the clear-text IMSI to the rest of the network elements on the system that may need it. An example can be a visited network (the MME), which has to maintain a copy of all IMSIs from users attached to the network due to Lawful Interception. Such a transmission of IMSIs will be done over a secure channel.

In order to allow a visited network to route the identifier to the correct home network, both the Mobile Country Code (MCC) and the Mobile Network Code (MNC) of the IMSI are sent in clear text, while the Mobile Subscription Identification Number (MSIN) of the IMSI will be sent encrypted.

The use of Elliptic Curve Cryptography is desirable given its computational efficiency, message size and key length compared to traditional schemes such as RSA or ElGamal. An example of an encryption scheme based on Elliptic Curve can be Elliptic Curve Integrated Encryption Scheme, ECIES [40]. The main idea of this scheme is to use public information of both parties in the communication in order to agree on a secret key, which will be used for symmetric encryption of the message.

The UE will generate an ephemeral key pair for the encryption which, combined with the home network's public information, will derive a secret key. This key together with the MSIN will generate a cypher text. The UE will send the cypher text and its ephemeral public key in the attach request (identity response, so that the home network can decrypt the cypher text and thus obtain the MSIN in clear text.

Due to the ephemeral key generation, the resultant encrypted identifier will be different every time it is created, so that it is infeasible for a third party (like an IMSI catcher) to link a given encrypted IMSI with another encrypted copy of the same IMSI or the true identifier or to guess it. Furthermore, the scheme is collision-free, because if two different users shared the same public key the resulted cypher text would look different as a consequence of having different IMSIs.

An encrypted identifier will be used every time a UE needs to send its identity over an insecure channel, such as in the Attach Request or Identity Response messages.

3.1.1.3 IMSI pseudonymization

This feature complements the “Encryption of Long Term Identifiers” feature by providing a way to generate random pseudonyms which are used in the signalling procedures which follow the user access to the network. The “Encryption of Long Term Identifiers” feature is only used during the first attach to the network and as a fault recovery mechanism. This is needed to avoid lock-out of a mobile device when errors occur, e.g., when the serving network and the mobile device are not synchronized. A current 3G/4G solution for protecting subscribers' identity is based on the serving network assigning a randomly generated Temporary Mobile Subscriber Identity (TMSI) (referred as GUTI in 4G) to the mobile device. However, prior work has demonstrated that TMSI/GUTIs are not randomly generated and they remain in use for long period (sometime 3 days).) (Shaik, Borgaonkar, Asokan, Niemi, & Seifert, 2015).

The “IMSI pseudonymization” feature applies to GUTI generation. It generates Pseudorandom dynamic pseudonyms, herein referred as RIMSI (Random IMSI)/dGUTI (dynamic GUTI), which are always used instead of real permanent or long term identities (IMSIs) in response to an Identity Request, in a Paging Request, etc., and are consumed by usage (they should follow a “one-time” scheme). This ensures they are frequently renewed avoiding the risk of user tracking. Two RIMSI/dGUTI generation mechanisms have been defined and implemented. The first mechanism runs on both the network and client (UE) side. By using a (standardized) pseudonym-derivation algorithm with a shared secret key, the network and the UE generate the next value for the RIMSI/dGUTI. The second mechanism is an alternative to the previous approach where the network generates the RIMSIs for the entire Tracking Area and maintains the state for each UE (the UE active RIMSI or RMSI window).

In both case, the permanent or long term identity (IMSI) is communicated only once to the network in the first Attach Request encrypted with the “Encryption of Long Term Identifiers” feature . Subsequently, RIMSI/RGUTIs are always used by UEs instead of permanent or long term identities and updated by the network after each usage (i.e., after being used in a message for UE identification).

3.1.2 Features achieved in R1

- **Feature name**: Encryption of Long Term Identifiers **(**IMSI KPABE-based encryption**)**
- **Goal**: Limit (preferably totally avoid) exposing user permanent or long term identities on (at least) the air interface (i.e., in Attach requests, Identity responses).
- **Description**: The release provides the open specification and a prototype software implementation of the main functions of the system (i.e., the libkpabe library with the main cryptographic functions: setup, key generation, encryption, decryption). The release did not foresee the integration of the provided functionality in any UEs or network elements; nevertheless, it has been integrated in the context of a 5G non-3GPP (WiFi) access scenario with EAP-AKA authentication.
- **Rationale**: Preserving the confidentiality of the mobile subscriber's identity in 5G network, thus preventing privacy violations, such as IMSI leaking and user tracking.

The feature's open specification was delivered in D3.4 together with the software implementation in D3.3 and a demonstration of the feature is also available and has been made in a major 5G event. This demo is also integrated on the project's testbed.

3.1.3 Features achieved in Release 2

- **Feature name**: Home Network centric IMSI protection
- **Goal**: Limit (preferably totally avoid) exposing user permanent or long term identities on (at least) the air interface (i.e., in Attach requests, Identity responses).
- **Description**: The release provides system definitions. Due to constraints that apply, this enabler can only be demonstrated outside the testbed and thus is not integrated/deployed on the testbed.
- **Rationale**: Preserving the confidentiality of the mobile subscriber's identity in 5G network, thus preventing privacy violations, such as user tracking.

- **Feature name**: IMSI Pseudonymization
- **Goal**: complement the "Encryption of Long Term Identifiers" feature to totally avoid exposing user permanent or long term identities on (at least) the air interface (i.e., in Attach Requests, Identity Responses, Paging Responses) by avoiding user traceability.
- **Description**: The release provides the open specification and a prototype software implementation of the main functions of the system (i.e., the librtmsi library containing the two main cryptographic functions for the pseudonyms generation). The release does not provide the integration of these functions in any UEs or network elements.
- **Rationale**: Improving the confidentiality of permanent and temporary identities used in current network (the GUTIs in LTE), preventing in 5G network privacy violations, such as permanent identity (IMSI) recovery through sniffing and user tracking due by the use of stationary temporary identity.

3.1.4 Recommendations for further research

- **Feature name:** Home Network centric IMSI protection.
- **Goal:** Limit exposing user permanent or long term identities on the air interface in the wake of quantum computing
- **Description:** Current solution uses ECIES which is not quantum computing safe.
- **Rationale:** It is expected that Quantum computers can break public-key cryptography like ECIES therefore a post-quantum solution needs to be found which is also format-preserving.

- **Feature name**: Authentication of Identity Requests and Paging requests.
- **Goal**: To provide enhanced privacy for the corresponding 5G procedures, in the sense that the user sends his/her identity only to authorized network entities

- **Description**: It would be useful to provide public-key based authentication (signatures) for this kind of messages.
- **Rationale**: It is essential that user's privacy is guaranteed not only through the protection of the identifying data itself but also by protecting the access to this data. Only authorized authenticated network entities can request the user to send his/her identity over the network.

- **Feature name:** authentication of radio signalling
- **Goal:** to prevent access to fake access node by ensuring the authenticity of the radio messages carrying service and system information.
- **Description:** the use of solutions based on a public key have to be evaluated, since they give the possibility to digitally sign the radio broadcast messages, such as MIB and SIB packets, or the sensitive information carried within.
- **Rationale:** a very large number of radio control plane (signalling) messages are transmitted without authentication, integrity and cyphering protection. The RRC protocol in LTE includes various functions needed to set up and manage over-the-air connectivity between the eNodeB and the UE. The eNodeB periodically broadcasts SIB messages which carry information necessary for UEs to access the network, to perform cell selection, and other information. Such broadcast messages are neither authenticated nor encrypted. Therefore, anyone owning appropriate equipment can decode them and can exploit these messages to create a targeted DoS to users or to track users' movements by setting up a rogue access point. Mobile devices do not have the means neither to authenticate nor to validate the messages received from the access node before the authentication phase and NAS (Non Access Stratum) security activation, therefore they inherently and implicitly trust all messages coming from anything that appears to be a legitimate base station.

3.2 Security Enabler "Device Identifiers Privacy"

3.2.1 Product Vision

The Device Identifier Privacy (DIP) enabler provides privacy enhanced network attachment, offering protection against unauthorized device tracking and device location disclosure. The main focus is to offer improved privacy protection of device identifiers, on IP-based networks, for access to 5G services via non-3GPP access mechanisms, such as via Generic Access Network (GAN), or to operator services. It also provides enhanced device identity privacy for access to third party Internet-based resources when utilising authentication schemes. These privacy mechanisms are built upon the Detection of Network Attachment protocol (Aboba, Carlson, & Cheshire, Detecting Network Attachment in IPv4 (DNAv4), 2006), which provides for reduced handover latency when moving and reattaching between network access points.

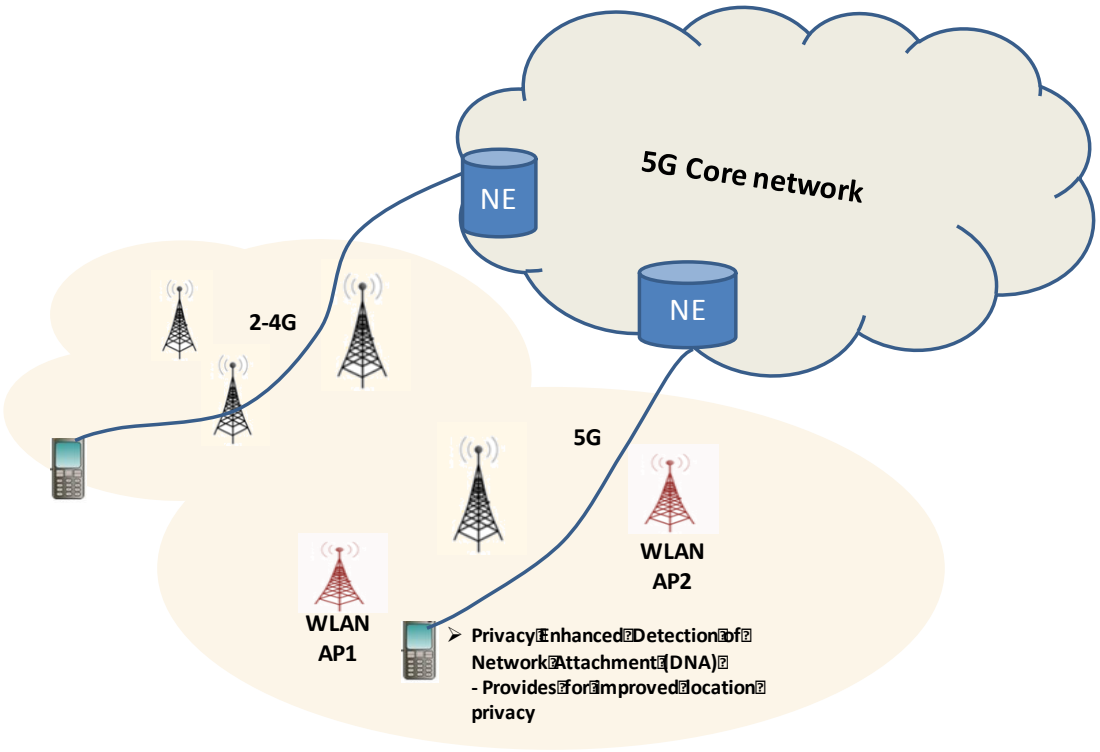


Figure 5: Privacy Enhanced Attachment

The enabler addresses two use-cases, within the Enhanced identity protection and authentication cluster, specifically the Device identity privacy and the Subscriber identity use-cases.

Table 6 Mapping between Device Identifiers Privacy enabler security features and relevant use cases

Enabler Security Feature	Relevant Use Case
Enhanced privacy for network attachment protocols	Use Case 2.1: Device Identity Privacy
	Use Case 2.2: Subscriber Identity Privacy

3.2.2 Features achieved in Release 1

- **Feature name**: Enhanced privacy for network attachment protocols.
- **Goal**: Limit exposure of device identifiers and prior points of attachment, and therefore, limit the ability to track a device.
- **Description**: The first release provided protocol enhancements and architecture definitions and a prototype implementation. This release primarily targets IP-based network attachment protocols, specifically the Detection of Network Attachment (DNA) protocol (Aboba, Carlson, & Cheshire, Detecting Network Attachment in IPv4 (DNAv4), 2006).
    - **Randomised ordering**
        - This mechanism provides for randomised delivery of candidate link layer addresses in the DNA reachability tests, so as to enhance the location privacy with respect to the location and time-based analysis of the device's movement patterns.
    - **Dummy addresses**

        - This mechanism allows for the introduction of dummy addresses into the DNA reachability tests to enhance location privacy, with respect to location identification and time-based analysis of the device's movement patterns.

- **Rationale**: To ensure that users consider 5G as a privacy preserving technology during network attachment.

The feature's open specification was delivered in D3.4 together with the software implementation in D3.3 and a demonstration of the features is also available on the project's testbed.

3.2.3 Features achieved in Release 2

In Release 2 we developed approaches to provide for anonymised and optimised address selection for network attachment protocols which build upon release one features.

- **Feature name**: Anonymous and optimised address selection for network attachment protocols
- **Goal**: Enhanced address anonymity providing for protection of device identifiers and prior points of attachment, and therefore, limit the ability to track a device.
- **Description**: The second release provided the following enhancements to the release one features:
    - Pre-analysis phase of the address anonymity metrics
        - This mechanism allows for the set of existing candidate link layer (MAC) addresses for DNA to be analysed before use to ascertain their privacy metrics with release R2. Specifically, we provide for the option to check and filter geolocatable candidate MAC address pairs.

    - Dynamically optimised choice of dummy addresses
        - With the R2 release, we introduced a new option that provides for automated choice of the number of dummy addresses.
- **Rationale**: To ensure that users consider 5G as a privacy preserving technology during network attachment.

3.2.4 Recommendations for further research

We have two recommendations for future features - firstly:

- **Feature name**: Geo-fencing for candidate network attachment address selection
- **Goal**: This would enable users to enjoy increased location privacy protection in their specified geo-fenced locations.
- **Description**: The feature would provide for the use of geo-fencing of specified geographical areas when the device performs candidate network attachment address selection and thus provide for enhanced location privacy.
- **Rationale**: To ensure that users consider 5G as a privacy preserving technology during network attachment.

And secondly:

- **Feature name**: IPv6 support for the enabler features with IPv6 network attachment protocols
- **Goal**: This would enable users to enjoy increased location privacy protection when utilising IPv6
- **Description**: The feature would provide for the enablers features on IPv6 networking protocols and thus provide for enhanced location privacy.

- **Rationale**: To ensure that users consider 5G as a privacy preserving technology during network attachment.

3.3 Security Enabler "Device-based Anonymization"

3.3.1 Product Vision

This enabler provides anonymization techniques on the user's device, offering protection against disclosure of sensitive information stored mainly on the SIM. The privacy/anonymization configuration (or profile) is directly controlled by the user, who can activate different anonymization profiles stored on the device. The user's device hosts a configuration tool which enables the user to activate and configure his/her privacy profile.

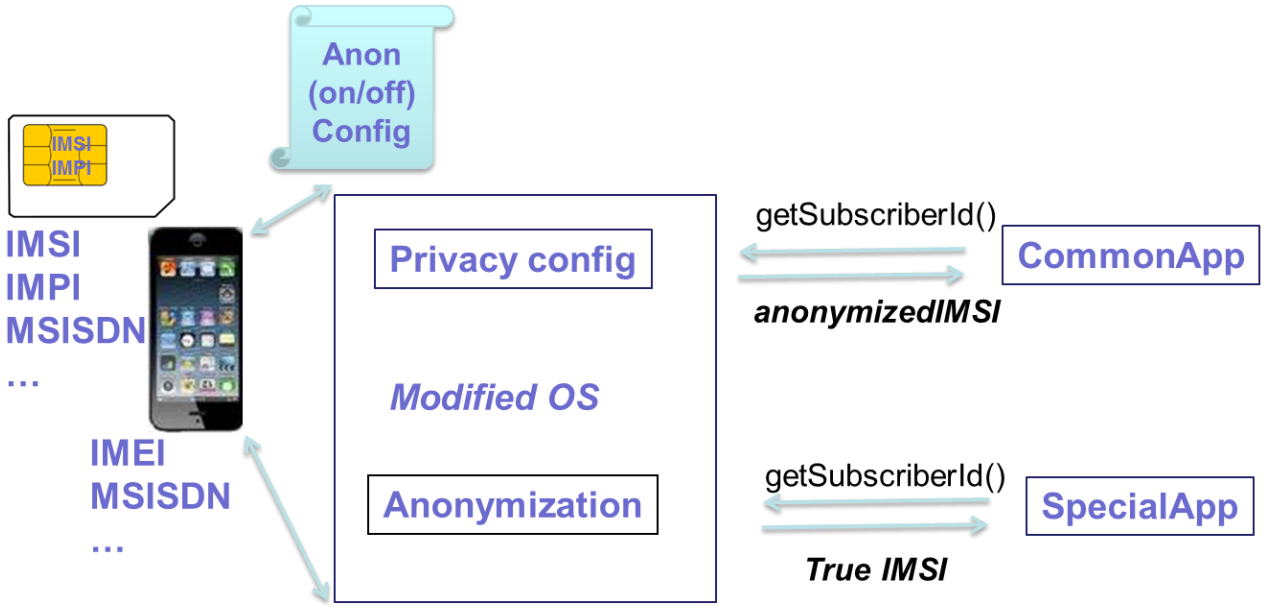


Figure 6 Device-based Anonymization.

The device implements a specific anonymization algorithm at the lowest possible layer in the device OS stack and offers the means to the user to activate and deactivate the anonymization. As illustrated in Figure 6 whenever a user space application requires access to SIM data protected by an active privacy profile/configuration, the request is managed by a privacy provider, which returns an anonymized version of the sensitive data to the caller, therefore activating this specific data protection with the configured anonymization algorithm. Therefore, the requesting application obtains the anonymized piece of data instead of the original one.

Table 7 Mapping between Device-based Anonymization enabler security features and use cases.

Enabler Security Feature	Relevant Use Case
Privacy Configuration tool for device-based anonymization	Use Case 10.3: SIM-based and/or Device-based Anonymization
Format preserving anonymization algorithm	Use Case 10.3: SIM-based and/or Device-based Anonymization

3.3.2 Features achieved in R1

No features were planned or delivered for R1, since this is a R2 enabler.

3.3.3 Features achieved in Release 2

- **Feature name**: Format preserving anonymization algorithm
- **Goal**: provide an anonymization algorithm for data received in input (e.g., the IMSI, IMEI, telephone number, etc.), with the preservation of the input data format.
- **Description**: The release provides the algorithm implementation. The algorithm preserves the format of the input data (e.g., IMSI, IMEI, phone number, etc.).
- **Rationale**: Avoid disclosure of sensitive information to all or selected user space applications.

- **Feature name**: Privacy configuration
- **Goal**: the mediator between the caller and the anonymizing SIM.
- **Description**: The release provides the prototype implementation of the agent. This prototype application receives the data to be anonymized, checks the configuration, applies the appropriate anonymization methods to the data and returns the anonymized data to the caller.
- **Rationale**: Make active use of the anonymization capabilities to protect sensitive data in order to avoid its disclosure to user space applications if user desires so.

3.3.4 Recommendations for further research

The device should be able not only to turn on and off the anonymization, but also to apply different algorithms on different sensitive data like IMEI, IMPI (IP Multimedia Private Identity), MSISDN, etc. For data residing on the SIM the anonymization algorithm should be ported to/implemented by the SIM itself, or into the radio proprietary binary blobs in order to maximize security (the data is protected at its source or as close as possible to its source).

- **Feature name**: Format preserving anonymization algorithm on the SIM or on the device's proprietary binary blob
- **Goal**: provide an anonymization algorithm for data received in input (e.g., the IMSI or the telephone number), with the preservation of the input data format.
- **Description**: based on the type of data (e.g., phone number, etc.) that have to be concealed, specific anonymization algorithms have to be specified ensuring the format preserving of the input data. To maximize security these anonymization algorithms have to be implemented directly into the radio or device proprietary binary blobs.
- **Rationale**: Avoid disclosure of sensitive information to all or selected user space applications.

- **Feature name**: Privacy agent
- **Goal**: the mediator between the caller and the anonymizing SIM/proprietary code.
- **Description**: The agent receives the data to be anonymized, checks the configuration, applies the appropriate anonymization methods to the data and returns the anonymized data to the caller.
- **Rationale**: Make active use of the anonymization capabilities to protect sensitive data in order to avoid its disclosure to all or selected apps if user desires so.

3.4 Security Enabler "Privacy Policy Analysis"

3.4.1 Product Vision

Nowadays, users of networked services are confronted with a plethora of services and applications that may put their privacy at risk right through the stack from the core network (potentially) to over-the-top application services. Currently it is difficult for a user to understand the privacy implications of using a mobile service or application: privacy policies (where they exist) are often not easy for users to read and commonly not presented upfront to the user.

The core support for SDN and NFV in 5G networks raises the expectation of new virtual MNO's (VMNOs) being able to easily enter the market and bring innovative new business models. For instance, it may be that a VMNO chooses to charge its customers very little for services by selling the users' personal information (such as location and usage patterns) to advertisers. Users however, need to be able to make an informed choice about such a trade-off.

This enabler provides the user a way to analyse the privacy policy of a service or a (V)MNO and compares it to their pre-defined preferences. Ideally, the analysis would be carried out prior to the service being used, for example, at the client application installation time or at the point of connecting to a 5G network.

Figure 7~~Figure 7~~ describes the high level architecture of "*Privacy Policy Analysis"* enabler.

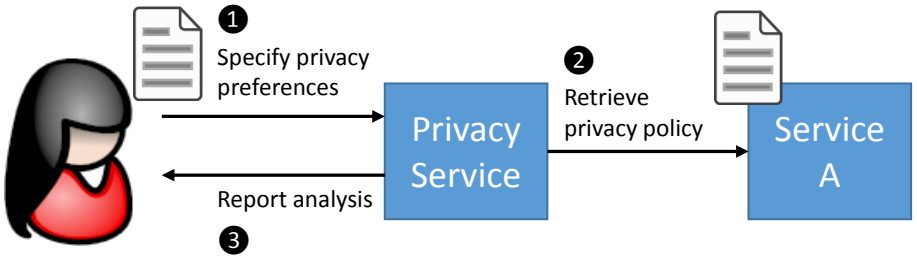


Figure 7: High level architecture of Privacy Policy Analysis Enabler

This enabler allows the user to specify their privacy preferences including what type of data they are willing to share, for what purpose and for what period. This allows the user to make privacy aware decisions regarding use of 5G networks and over-the-top 5G services. The enabler may be of interest to all 5G users.

The privacy policy enabler could be integrated with the SIM-based anonymization enabler for the specification of the user's privacy policy preferences which would then be translated into the format required for the SIM-based privacy agent configuration file.

The table below illustrates the mapping between the enabler features and the 5G-ENSURE use cases.

Table 8 Mapping between Privacy Policy Analysis enabler security features and relevant use cases

Enabler Security Feature	Relevant Use Case
privacy policy specification	Use Case 10.2: Privacy Violation Mitigation
privacy preferences specification	Use Case 10.2: Privacy Violation Mitigation
comparison of policies and preferences	Use Case 10.2: Privacy Violation Mitigation

3.4.2 Features achieved in R1

No features were planned in R1 since this enabler was planned for R2 only.

3.4.2.1 Features achieved in Release 2 (R2)

For release 2 (R2) three features are released:

- **Feature name**: privacy policy specification.
- **Goal**: encoding service privacy policy.
- **Description**: support the loading of a privacy policy into the enabler.
- **Rationale**: this is required for a privacy analysis of service offerings.

- **Feature name**: privacy preferences specification.
- **Goal**: encoding users' preferences.
- **Description**: allow the user to define their privacy preferences. The preferences offered to the user are generated by the amount of policy-affecting actions described in each policy, making the process flexible and able to cope with multiple domains and varying services managed.
- **Rationale**: this is required for the comparison with service offerings.
- **UI**:

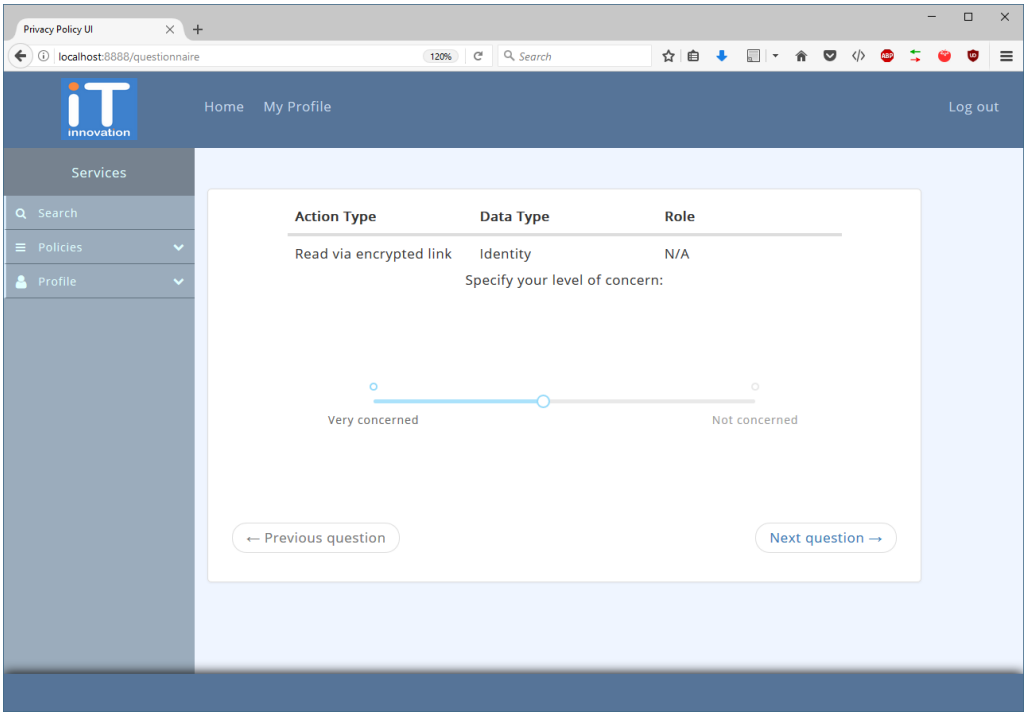


Figure 8 Privacy preferences questionnaire

- **Feature name**: comparison of policies and preferences.
- **Goal**: compare the managed service policies with the user's expressed preferences.
- **Description**: the service policies managed by the system are compared with a user's expressed preferences and the analysis is presented to the user in a clearly understandable form where the policies with offending actions (i.e. actions which do not comply with the user's preferences) are classified as noncompliant, and all the policies are given, and ordered by, a preference score which is produced taking into account the user's preferences.
- **Rationale**: privacy based analysis of service offerings.

- **UI**:

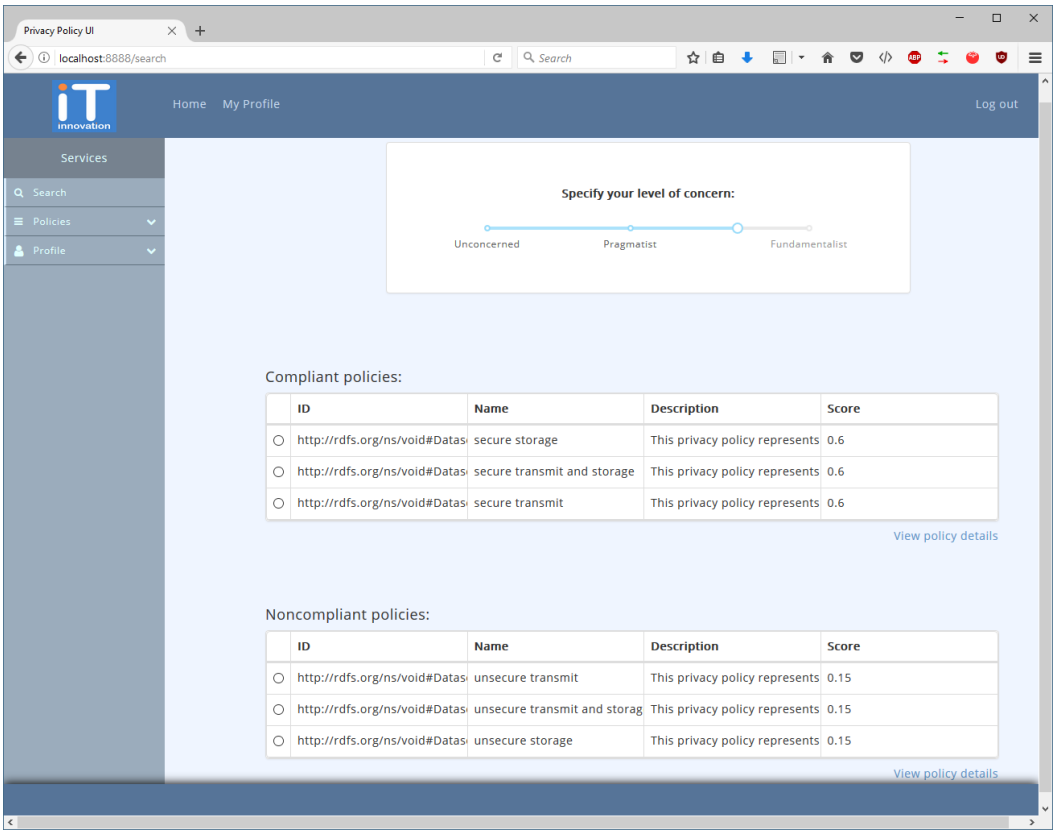


Figure 9 privacy policies' search

3.4.3 Recommendations for further research

Multiple layers of privacy policy specification could be further modelled and investigated. For instance, in the case of a mobile phone owned by a company but issued to a member of staff, the company would mandate certain (immutable) privacy policies and any user-defined policies would have to be layered below the corporate policy. Moreover, a more generic scenario could be studied where the privacy policy specification for services which are composed of sub-services, carrying their own privacy policy, is the result of the collaboration of multiple parties.

3.5 Additional enablers

The overall trend towards encryption of network communications may prevent the application of certain security services, such as in-depth threat monitoring and fine-grained access control. Therefore, the conciliation between privacy requirements in terms of encryption/anonymization, and security requirements in terms of monitoring and threat detection, is becoming increasingly challenging.

- **Enabler name**: security services over encrypted traffic
- **Goal**: to provide value-added security services to vertical domains in the context of encrypted network communications.
- **Description**: investigating existing cryptographic tools such as searchable encryption, format preserving anonymization and privacy respectful key escrow.
- **Rationale**: perform data analysis without compromising user privacy to provide security services such as in-depth threat monitoring and fine-grained access control

Another area that should be investigated is the privacy in the contest of IoT scenarios and the applicability of new privacy protection techniques. Internet-of-Things (IoT) devices are capable of capturing physiological measures, location and activity information, hence sharing sensed data can lead to privacy implications. Data anonymization provides solution to this problem, however, traditional anonymization approaches only provide privacy protection for data stream generated from a single entity. Since a single entity can make use of multiple IoT devices at an instance, IoT data streams are not fixed in nature. As conventional data stream anonymization algorithms only work on fixed width data stream they cannot be applied to IoT, therefore new anonymization approaches has to be studied for publishing IoT data streams.

The application of some well-known anonymization techniques, like k-anonymity, may also be studied in order to evaluate its suitability in the IoT context.

Many envision nowadays the use of IoT devices in the context of blockchains. The main characteristic of the blockchain is to offer a fully-decentralized repository of data of events, where information is validated, stored in a precise order, and timestamp. The side effect connected to the use of this technology, initially designed for economic transactions, is the computation required, the high bandwidth overhead and delays, which are not suitable for most IoT devices. Taking into account these limits the research should investigate how to design a lightweight blockchain optimized for the application in an IoT scenario, where, for example, the validity of an IoT output data is validated by means of distributed blockchain computation. Nevertheless, the privacy issues are to be carefully taken into consideration. While blockchains are a powerful technology that allows for a large number of interactions to be codified and carried out in a way that greatly increases reliability, removes risks associated with the process being managed by a central entity, and reduces the need for trust, they are known to have two primary issues: scalability and privacy. Privacy is of course fundamental in all IoT application scenarios where sensitive data are treated. Therefore, there is a need to convert current IoT blockchain implementations to fully privacy-preserving applications, allowing users to benefit from the security of a blockchain, using a decentralized network to process the transactions, but “encrypting” the data in such a way that even though everything is being computed in plain sight, the underlying “meaning” of the information is completely obfuscated.

4 Trust Security Enablers

4.1 Trust Builder

4.1.1 Product Vision

5G networks will introduce new actors and roles. The extended concept of “operator” could include e.g. a car manufacturer that embeds 5G devices into their cars at production time. This new type of operator may need roaming agreements with traditional MNOs for the purpose of remote management of their products after they leave production line. New usage scenarios could bring changes to core responsibilities such as authentication, meaning that the traditional MNO may need to evaluate the trustworthiness of assertions made by a variety of new actors. For instance, if a factory owner wishes to use a local system to authenticate production robots but have those robots communicate on a 5G network.

Increasing virtualisation brings further complexities with slices introduced but not fully yet defined complicating the trust relationships further. An operator may wish to outsource its ICT hardware needs to a 3rd party Cloud provider as software on top of IaaS or PaaS cloud service models. Conversely, an operator who still owns dedicated hardware could choose to make core or radio access nodes available to VMNOs.

Parts of network resources might also be dynamically allocated using SDN according to current needs and sourced or outsourced based on these needs. The enabler helps the network operator understand the threats and potential countermeasures to be deployed in these more complex situations.

5G also brings in new devices types in IoT scenarios and the threats brought by these new network elements and the associated authentication mechanisms need to be understood. Finally, it is not always the network operator who needs to understand threats to the system. SDN scenarios and the more dynamic markets they may bring mean that third party service operators will need to understand the trustworthiness of operators to make an informed choice and out contracting their services; end users of 5G networks need to understand the trust implications of Lawful Interception features.

Designing a trustworthy system and making informed trust decisions are both challenging in such an environment. The Trust Builder enabler addresses the automated identification of threats that may compromise such a multi-stakeholder system. Our approach (based on work done in the OPTET[3] project) is defined in terms of the automated and systematic identification of risks to the assets within the (5G) system (both human and technological) as well as their knock-on consequences and countermeasures to mitigate these risks. The identified threats depend not only on what assets are involved but also on how they are related to each other. Addition or removal of an asset, or changing the composition of existing assets may result in different threats being identified. This goes beyond the current risk management methodologies in terms of usability and applicability to dynamic and adaptive multi-stakeholder ICT systems. We apply this approach to the 5G domain where a 5G asset model has been developed and associated threats and trust relationships encoded to enable repeatable, systematic threat and trust identification in the network. This also provides an advantage when run-time aspects are considered in future phases.

The Trust Builder enabler comprises a set of linked ontologies describing the asset types, relationships, threats to assets (taking into account their relationships) and countermeasures along with the software tools required to create, validate and use the ontologies.

Table 9: Mapping between Trust Builder enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case
5G Asset model 5G Threat knowledgebase v1 5G Threat knowledgebase v2 A graphical editor for describing systems using the knowledgebase	1.1: Factory Device Identity Management for 5G Access Cluster 3: IoT Device Authentication and Key Management 5.1: Virtualized Core Networks, and Network Slicing 5.5: Control and Monitoring of Slice by Service Provider 9.3: Authentication of New Network Elements 11: Lawful Interception

4.1.2 Features achieved in R1

- **Feature name**: 5G asset model v1.

[3] www.optet.eu

- **Goal**: allow the modelling of 5G networks using the information gathered.
- **Description**: the 5G asset model is a first draft of an ontology which contains the typical assets in a 5G network and the different possible relations between them.
- **Rationale**: an asset model is the basis for modelling a system and then identifying the threats and required controls.

- **Feature name**: Graphical modelling tool v1
- **Goal**: Allow the mapping of the threats to the designed 5G system
- **Description**: the editor will allow system designer to model their system and analyse the potential threats and their mitigation through controls.
- **Rationale**: an editor will provide an easy to use interface for system threats and controls analysis.

4.1.3 Features in R2

- **Feature name**: 5G asset model v2.
- **Goal**: allow the modelling of 5G networks using the information gathered.
- **Description**: the 5G asset model is an ontology which contains the typical assets in a 5G network and the different possible relations between them. The second version has been updated with information (specific assets and relationships) from the architecture defined in D2.4 and through further discussion in the architecture task.
- **Rationale**: the asset model has been updated with new information to match the architecture.

- **Feature name**: Graphical modelling tool v2.
- **Goal**: provide a tool to analyse the threats present in a 5G system design.
- **Description**: the editor allows system designer to model their system and analyse the potential threats and their mitigation controls. The second version of the tool includes usability enhancements for dealing with complex models, a re-architected back-end for persisting and processing the models and user management facilities.
- **Rationale**: the modelling tool has been updated to support more complex scenarios.

- **Feature name**: 5G threat and trust knowledgebase.
- **Goal**: encode threat and trust data so that it can be inferred from the models and displayed in the modelling tool.
- **Description**: a second part of the ontology, the threat and trust knowledgebase, includes a first pass at the description of the threats and how they apply onto a 5G system alongside descriptions of trust relationships. Moreover, the threats are mapped to some of the controls that can be used to manage them. The information encoded in the ontology comes from an analysis of D2.2 (5G-ENSURE, 2016) and D2.3 (5G-ENSURE, 2016) but also includes additional detail from the work performed on Trust Model and Risk assessment, Mitigation& Requirements.
- **Rationale**: a threat knowledge base supports the automated identification of threats in designed or existing 5G systems. The trust data highlights trust relationships between assets and stakeholders.

4.1.4 Recommendations for further research

In combination with the System Security State Repository, this enabler could become part of a suite of tools to support the design lifecycle in 5G systems. Trust Builder supports the design of a system configuration, highlighting potential threats and showing available control options. The System Security State Repository uses the same model, and when combined with other monitoring enablers, ingests data from a live system to understand what assets and controls are actually in place, and compares this with the design. A future

development would be to integrate the two more closely, allowing the System Security State Repository to ingest data about active misbehaviours and use machine reasoning facilities from Trust Builder to infer which threat(s) are the most likely causes of the observed misbehaviour. Trust Builder could then be used to review the design and incorporate additional controls. This type of coupling has been done by IT Innovation in the past, but at that time the computational performance of general purpose semantic reasoning tools was insufficient to make use of it. The research challenge will be to develop optimised reasoning algorithms that can provide the inferences needed for threat diagnosis.

4.2 Trust Metric Enabler

4.2.1 Product Vision

We consider economic benefits, user experience and energy efficiency as the three high level drivers of 5G system development. These three drivers have often conflicting interests which leads to compromises in system design and deployment, including 5G security enablers. Security community is well exercised in making compromises as the solutions that improve security in a system often lead to additional costs, worse user experience and higher energy consumption. Security professionals are also well aware that in practice a perfect security cannot be achieved. Therefore, the security solutions strive to provide 'good enough' security to the system they are protecting. The hard question is: what is 'good enough'. The Trust Metric enabler is developed to tackle that question from end-user and trust perspectives.

5G system is hugely complex including unprecedented actors, access technologies, network domains and services, for instance. Therefore, the system consists of multiple security technologies and the overall security from the end-user perspective may change also over time leading to different levels of securities within the system and to different setups for 'good enough' security. The end-user is able to affect the security of the used applications, e.g. by choosing among different end-user devices, access networks, network services and security enablers. However, the average end-user does not have the skills to assess the security impact of the previously listed decisions so there is natural tendency to select the best user experience which could often be the option of least security. And still the IT-professionals, such as system administrators, who may often do the selection for the real end-users, face exactly the same problems. So there is a need to provide the end-user with security information in easily understandable format and at other hand to provide evidence that 'good enough' security could be achieved when some security controls are disabled to improve the user experience.

Our hypothesis to realize this vision is that end-user (by which we mean first of all the system administrator) needs objective evidence to make a better decision related to trust. The evidence is gathered in real-time through objective measurements related to components of trust and presented as an aggregated trust metric in a user-friendly format. This concept can also be applied to M2M system in which case the focus will be in monitoring that will provide the evidence that the required security levels are maintained and enable dynamical management of security enablers. These functions should of course be automated and any violation of trust should produce alarms or interrupt communication.

The enabler is applicable in a wide variety of use cases of which some specific examples can be found from the use cases listed in D2.1. Among these the ones for which the Trust Metric Enabler clearly has potential to provide support are Use Case 3.1: "Authentication of IoT Devices in 5G" and 5.5: "Control and Monitoring of Slice by Service Provider" as the enabler controls maximum number of simultaneous connections and may limit the traffic. Especially the Use Case 5.5: "Control and Monitoring of Slice by

Service Provider", may get support as the enabler monitors network's security status and provides trust metrics for micro-segments.

The first release (Release 1) of the enabler, offers a feature named "trust metric based network domain security policy management". It provides basic functionalities to calculate and output a trust metric value based on the trust model and existing trust related measurement capabilities of a network system. The second version of the enabler (Release 2) supports "improved trust metric based on extended data" which enables collecting of detailed information from different data sources, particularly from eNodeB and Security Monitoring Enabler. Chapter 4.2.5 Technical Roadmap describes these features in more detail.

Table 10~~Table 10~~ illustrates the use cases that are relevant to the enabler's security features.

Table 10: Mapping between Trust Metric enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case
Trust metric based network domain security policy management (Release 1)	Use case 5.5: Control and Monitoring of Slice by Service Provider
Improved trust metric based on extended data (Release 2)	Use Case 3.1: Authentication of IoT Devices in 5G Use case 5.5: Control and Monitoring of Slice by Service Provider

4.2.1 *Features Achieved in Release 1*

The first release (R1) was a prototype for calculating a trust metric value from (static) simulated input data.

Through the first release (i.e. R1), the following feature was in scope and achieved:

- **Feature name**: Trust metric based network domain security policy management
- **Goal**: Enable service providers to offer trust based services for customers in mass market and industry.
- **Description**: The first release will integrate a trustworthiness model derived from trust model defined, into network management functionalities to enable network segmentation based on different trust levels. The functionalities of the first release will be limited and concentrate on the integration of trust model:
    - Enabler will calculate and output a trust metric value to a complex event processor based on the trust model and existing trust related measurement capabilities of the 5G-system. Based on the trust metric value the complex event processor can make network management decisions such as guide micro-segmenting of the network.
- **Rationale**: To enable UEs to offload security mechanisms to the network and to help 5G architecture to meet industrial Internet delay requirements by eliminating overlapping security features.

4.2.2 *Features Achieved in Release 2*

The second release of the enabler provided near real-time monitoring and dynamic operability. Clients were allowed to provide trust policies at any time using a new trust policy model which was defined in R2. The R2 of the enabler monitors changes in the 5G network continuously and immediately reports detected trust level changes to the clients.

The second release (R2) of this enabler included the following additional feature:

- **Feature name**: Improved trust metric based on extended data

- **Goal**: Collecting monitoring data and KPI from the micro-segment to enable near real-time operation
- **Description**: The feature enables collecting of information from different data sources, particularly the Security Monitoring Enabler for 5G Microsegments. Interfaces to counters and KPIs of eNodeB within the 5G-ENSURE testbed (in VTT's testbed node) will be provided. Event information from Micro-Segmentation Enabler and Security Monitoring Enabler is gathered, and trust metrics is delivered to the Security Monitoring Enabler and to the clients of the Trust Metric Enabler.
- **Rationale**: Quick detection of trust level changes (e.g. due to attacks and risks) in 5G networks.

4.2.3 Recommendations for further research

Anonymization and access control over shared trust metrics information - To increase accuracy of monitoring and security awareness in distributed, multi-domain scenarios, information must be shared. However, such sharing introduces a new challenge: the shared information may reveal details of the operator's network or the operator's clients. The clients may trust the operator to handle this information but do not wish it to be shared with other parties. Hence, solutions are needed e.g. to enable sharing of monitoring information between different parties without revealing any secrets of the measured party. These solutions can be based on privacy (e.g. anonymization) and access control mechanisms that enable sharing of sensitive information across administrative domains. The solutions could be autonomous so that the system can itself determine whether the information can be shared.

Increasing trust towards metric provisioning - Trust metrics are shared access domains and networks and services are orchestrated using this information. If such metrics are not reliable or trustworthy, the user of the network may experience significant losses. This issue has different layers. Firstly, the trust metric enabler may not be able to collect correct information from the network. Secondly, the trust metric enabler itself may not be trustworthy. For instance, the enabler may claim that the network is more trustworthy than it actually is in order to gain subscribers for the network. Hence, new mechanisms are needed for verifying trustworthiness of monitoring information that is coming from potentially hostile or compromised sources. A potential solution for further studies is approaches based on blockchains. These could be used to verify that a trust metric enabler cannot later on deny or tamper metrics it has provided.

4.3 VNF Certification

4.3.1 Product Vision

The shift of network functions into a data centre ("Virtualized network functions" – VNF) and new network control methods ("Software Defined Networking" - SDN) lead to risks for attacks on Network Elements (NE) within communication infrastructure. Virtualization of network functions allows agile recovery from attacks and faults through dynamic re-deployment of the network functionalities. The challenge is to design fault-resilient VNF services, built over SDN, to ensure critical services that must remain operational even after massive disasters (e.g., earthquake) or major security attacks.

The virtualization of network functions and network equipment enable to instantiate several of them on commodity servers, thus sharing physical resources (CPU, RAM, memory and network) with other hosted virtual machines (VMs). Nowadays, the infrastructure provider manages its own VNF on its own infrastructure.

In 5G architecture, we anticipate that the VMNOs (Virtual Mobile Network Operators) could have the possibility to manage directly their own VNF(s). The infrastructure provider will monitor these VNF(s) and will guarantee the hardware usage.

In case a VMNO wants to use a proprietary VNF (developed by itself for example), how could the VMNO provide trustworthiness assurance to the infrastructure provider? The idea of this enabler is to deliver, through a certification process, a Digital Trustworthiness Certificate (DTwC). This certification process will be lighter than existing certification process envisaging even self-certification. The different information would be:

- VNF environment;
- Threats and controls for the VNF;
- Trustworthy characteristics of the VNF.

The information would be based on automatic evaluation of the VNF and on the compliance to a part of the trust model defined in 5G-ENSURE (only the part related to trust in VNF and so how to make VNF trustworthy).

This enabler offers a good opportunity to reuse existing results of OPTET[4] FP7 project. OPTET has proposed a trust model for STS applications and has defined the trustworthy properties for an application. Based on that, OPTET has defined a certification process giving as output a certificate listing the certified properties of the application. This enabler contributes in one of the project major motivations, "*5G requires a new Trust model"*. 5G-ENSURE will provide, through the different use cases, a new trust model trying to address the multiplicity of actors and also considering the M2M interaction characterising new generation networks. On the basis of this trust model and attached deliverables (namely D2.2 Trust Model "Initial" (5G-ENSURE, 2016) and D2.5 Trust Model "final" (5G-ENSURE, 2017) , 5G-ENSURE will provide appropriate trustworthiness elements in order to be able to take into account trust concerns and to offer (or specify) new tools or requirements. This enabler will provide assurances for the trustworthy elements that specifically apply for VNF.

Table 11: Mapping between VNF Certification enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case
VNF Trustworthiness Evaluation	5.2: Adding a 5G Node to a Virtualized Core Network 5.4: Verification of the Virtualized Node and the Virtualization Platform 5.5: Control and Monitoring of Slice by Service Provider

4.3.2 Features achieved in R1

- **Feature name**: VNF Trustworthiness Evaluation.
- **Goal**: to certify the trustworthy implementation of the VNF and to expose their characteristics through a Digital Trustworthiness Certificate.
- **Description**: The first release will provide different elements coming from OPTET project with their adaptation for VNF and 5G environments:
    - Format of the DTwC
    - Tools for certification workflow
    - A certification process

[4] http://www.optet.eu/

4.3.2.1 Features in R2

The work in scope of Release 2 for this enabler is to provide a more complete prototype for the VNF certification and for the Digital Trustworthiness Certificate which translates into the following feature:

- **Feature name**: VNF Trustworthiness Certification
- **Goal**: Delivery of a trustworthy Digital Trustworthiness Certificate
- **Description**: This release will complete the first release by adding:
  - New trustworthiness evidence like “VNF hardening”, “kind of communication” (secured or not) and “Runtime environment reference”.
  - A complete certification process
  - A secured repository (especially with access control addition)
- **Rationale**: Offer a secured and a more complete Digital Trustworthiness Certificate for external usage.

4.3.3 Recommendations for further research

This enabler, developed in the context of 5G ENSURE, delivers trustworthy information about VNFs. Future work could be to develop or to extend NFV infrastructure for using this information (at the orchestrator level for example).

The main idea is to set the NFVO configuration to select the different VNFs answering the security needs requested by the Virtual Infrastructure provider. For that the NFVO should be able to select the best appropriate VNF in a repository and after that to deploy it. The following figure highlights how the enabler could be used. For a future work, a new feature selecting the most appropriate VNF could be developed and would be strongly associated with a NFVO orchestrator.

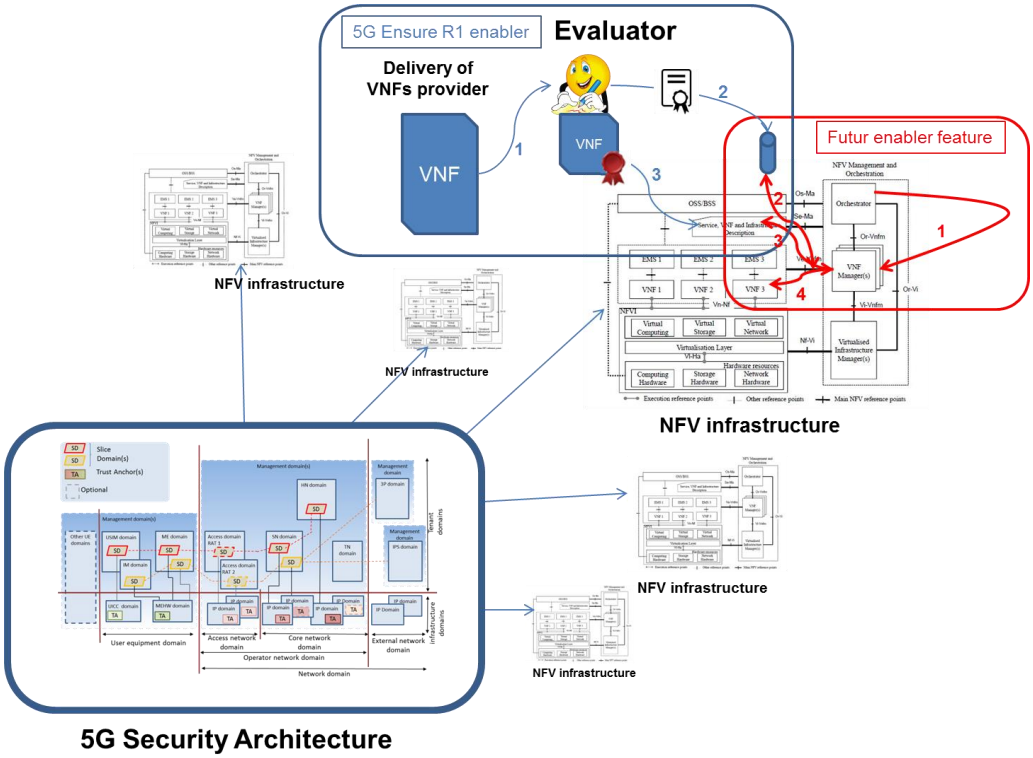


Figure 10 : Overview of enabler usage in a multi party infrastructure

In the context of 5GENSURE, the detailed scenario was defined and is illustrated by the following figure.

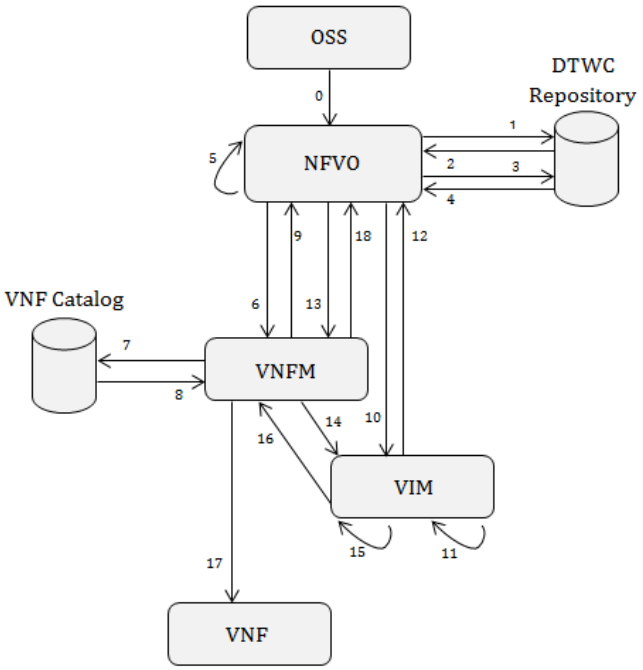


Figure 11 : Detailed scenario of VNF selection

This scenario could be implemented with Tacker as NFVO orchestrator. The scenario could then be:

0. OSS sends a request to NFV Orchestrator for deploying a VNF for a specific function (for example: router, firewall, etc.).
1. NFV Orchestratorr sends a request to DTWC Repository to obtain the different hashes of the VNFs covering this function.
2. DTWC Repository provides the list of hashes to NFV Orchestrator.
3. For each hash, the NFV Orchestrator sends a request to DTWC Repository in order to receive the associated DTWC.
4. DTWC Repository sends the DTWC
5. NFV Orchestrator selects the most appropriate VNFs by scoring the different VNFs using the Trustworthiness metrics.
6. NFV Orchestrator sends a request to VNF Manager for deploying this VNF. This request contains the VNF id : vnf_id.
7. VNF Manager receives the request and interacts with the VNF Catalog.
8. VNF Catalog provides the VNFD to the VNFD.
9. VNF Manager sends a request to NFV Orchestrator about the needed resources for deploying the VNF.
10. NFV Orchestrator sends a request to the VIM to obtain theses resources.
11. VIM allocates the needed resources and the VMs.
12. VIM informs the NFV Orchestrator that all resources are available.
13. NFV Orchestrator informs the VNF Manager that all resources for the VNF are available.
14. VNF Manager sends a request to the VIM for creating and starting the VMs.
15. VIM creates and starts all VMs.
16. VIM informs the VNF Manager that all VMs are available.
17. VNF Manager configures the VNF and deploys it.
18. VNF Manager informs the NFV Orchestrator that the VNF was deployed.

NB: The scenario described above is representative of the work that Thales plan to achieve in the context of Celtic+ SENDATE-TANDEM project leveraging on VNF certification enabler developed in 5G-ENSURE project.

4.4 Security Indicator

4.4.1 Product Vision

This enabler aims at increasing trustworthiness of serving mobile network operator, offering network security indicators, which supports one of the primary security visibility features of 5G networks [33.401]. The main focus is to offer a means to add new network security indicators to those proposed in 3GPP TS 22.101 [22.101] to be displayed on mobile devices. This enabler not only addresses mobile subscriber's trust in the serving mobile network but also adds new security indicators into the UE for adaptive security policy management for various operational needs.

The enabler addresses two use-cases, within enhanced security services and trusted core network and interconnect cluster, specifically authentication of new network elements and privacy violation mitigation use-cases.

Table 12. Mapping between trust security enabler features and relevant use-cases.

Enabler Security Feature	Relevant Use Case
Security Indicator	Use Case 9.3: Authentication of New Network Elements
	Use Case 10.2: Privacy Violation Mitigation

4.4.2 Features achieved in R1

None since enabler here presented not planned in early description of Technical Roadmap and so R1.

4.4.2.1 Features in R2

- **Feature name**: Security indicator subscriber display.
- **Goal**: Provide a new security indicator to be displayed to subscribers, whilst complying with operators' requirements to local regulations.
- **Description**: The release will provide a mobile application utilizing a new security indicator received via an API.
- **Rationale**: Increase the visibility security in the serving network, and improve the trust in the network.

4.4.3 Recommendations for further research

The current version of enabler supports Android OS version 4.1.2 due to limited support of certain APIs. Hence, we investigate new methods to access baseband information without requiring root access to the device in future. Certain baseband vendors are adding similar security features to increase trustworthiness of serving network (Xiaomi). However, their security features are not transparent to end users. In future, we would be aiming to work in this direction to provide transparent security features of serving network with the help of a mobile network operator or a mobile equipment manufacture. In addition, we focus on making such a security enabler available across all mobile platforms including iOS and Windows Mobile.

4.5 Reputation based on Root Cause Analysis for SDN

4.5.1 Product Vision

We proposed here an enabler targeting the exposal of responsibilities based on reputation values of partners of a service delivered across different domains.

The goal was to describe a methodology to evaluate and then expose reputation values from the different domains involved in a service. The goal then was to have an estimation of the domain responsible for a given service failure.

The service chain considered was delivered across two or more domains, and this work was to establish a methodology and a procedure to pinpoint when a given domain was responsible for a given service failure, any degradation or service unavailability.

Each domain was composed of a single SDN controller which was the only intelligent entity in the domain, whose role was to establish and control the interconnection among the different hosts in that domain. The infrastructure was then composed of the controller, the intermediate switches, connected to this controller and the different hosts embedding vNFs or other applications such as streaming applications.

We used a self-modeling based RCA (Root Cause Analysis) (J. Sanchez I. G., THESARD: on The road to resiliencE in SoftwAre-defined network-ing thRough self-Diagnosis, 2016), (J. Sanchez I. G., "Self-Modeling Based Diagnosis of Software-Defined Networks, 2015), (J. Sanchez I. G., 2014), (J. Sanchez I. G., "Self-Modeling based Diagnosis of Services over Programmable Networks, 2016) which was going to calculate the a posteriori probability of failure for all the elements in the infrastructure domain given any symptom of failure in the service. This module had been conceived for one single domain. A high-level view on this module can be seen in the next Figure, which had three main steps:

Step 1: Transformation of the network topology into a machine-readable format containing the classified network elements in each domain.

Step 2: On-the-fly construction and continuous update of the fault propagation model from the machine-readable format and running applications. This model contains the network nodes, their internal logical and physical components such as ports or running applications to ensure a fine-granular diagnosis.

Step 3: Root cause analysis (RCA) to calculate the probability of faulty networked elements with component-level granularity by exploiting this generated fault propagation model.

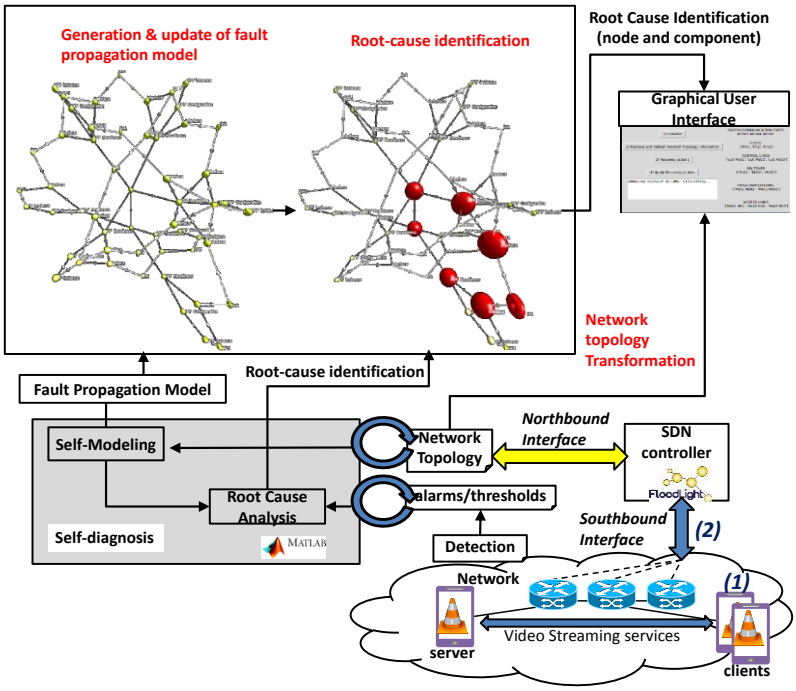


Figure 12: High-level view on the RCA for one single domain

The results of the RCA were which network component n in the domain d was responsible for the service failure. The reputation calculation block domain d received the RCA output with their timestamps t_n associated to the service failure. Thanks to the pair of values (n,d, t_n), a reputation r_n value could be calculated for every network component within the domain d. The timestamps values were necessary because the reputation calculation block needed to calculate the availability of that network component, defined here as the amount of time the resource was not operating correctly (m) in a given time window W.

The reputation values from the network components r_n in each network domain d were sent up to the overlying layers, calculating the reputation of the domain d in a hierarchical manner. As it can be seen in the figure, each domain was continuously running a RCA module with updates the reputation value of their resources (including the SDN controller).

A high-level view on this hierarchical approach can be seen in Figure 13.

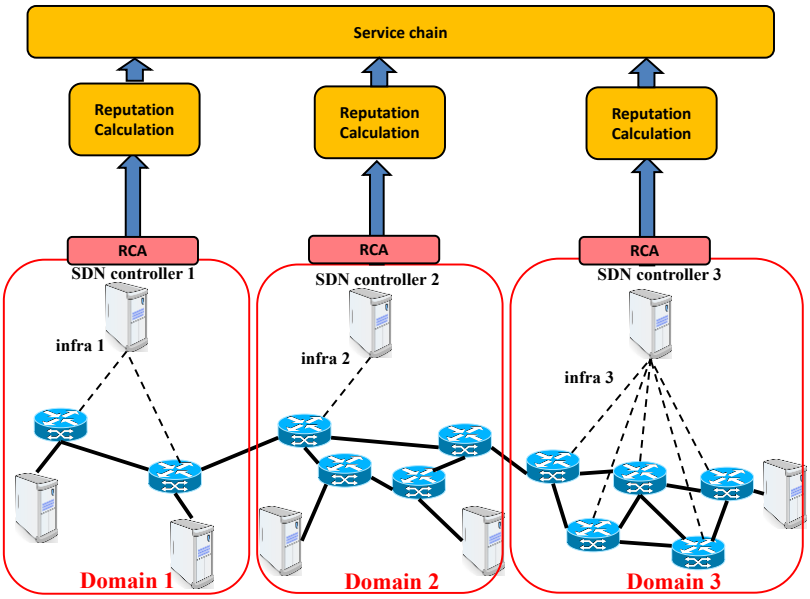


Figure 13. Hierarchical reputation propagation mechanism.

Table 13. Mapping between enabler features and relevant use-cases.

Enabler Security Feature	Relevant Use Case
Reputation based on Root Cause Analysis for SDN	5.5: Control and Monitoring of Slice by Service Provider

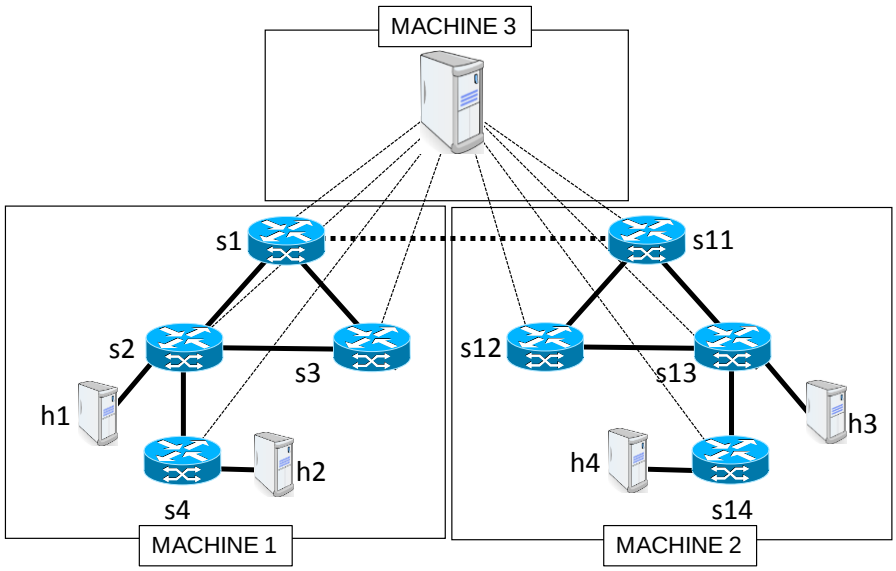
4.5.2 Features achieved in R1

None, since the enabler was not planned in early description of Technical Roadmap and so R1.

4.5.3 Features in R2

This enabler was matured in R2 with the overall objective to show how it could enable to pinpoint the responsible domain of several services failures through several simulated domains in Mininet (Mininet: an instant virtual network on your laptop).

We considered two domains and a video streaming application traversing both domains as a proof of concept, as shown in the figure:



- **Feature name**: Root Cause Analysis for SDN
- **Goal**: reputation calculation block based on a RCA, taken into account all changes at physical and virtual resource level
- **Description**: The reputation calculation mechanism is based on a RCA mechanism, which will have to take into account the topological view given by the different SDN controllers. This is only possible in SDN because this network architectural paradigm allows to centralize the intelligence within those nodes. This RCA is based on model-based fault propagation techniques such as Bayesian networks which can pinpoint the root cause with enough fine-granularity.

Only open specification were planned to be released in R2 for that enabler.

4.5.4 Recommendations for further research

Objective would be to further mature the enabler based on product vision and early specifications delivered in R2 in order to come up with more detailed specifications for anyone interested to come up with an implementation of it.

5 Security Monitoring Security Enablers

5.1 System Security State Repository

5.1.1 Product Vision

Organizations currently deploy different tools in order to monitor their socio-technical systems (where a system is composed of people, servers, network equipment and software that constitute a coherent sub part of an infrastructure). Monitoring helps to identify attacks and threats, react to security incidents, raise events and correlate them. These tools may need to analyse huge amounts of data in order to identify previous or on-going attacks, identify cost efficient remediation and in certain cases automatically apply them. The results of such remediation work are reflected in the new monitoring data from the system. However, this overview of the system is commonly dispersed across different tools, which makes it hard to get a consistent comprehensive understanding of the state of the system.

The enabler makes use of knowledge base encoding information about the assets, trust relationships, threats and controls in the 5G architecture. This knowledgebase is used to addresses the need to enrich the system view with information about the system's assets, the threats, incidents, and analysis results in order to understand the state of the whole system. The enabler allows querying and analysis for a higher-level view of security incidents and trends.

Such a model of the system documents in a sense the security practice within an organization including the system architecture, decisions about control deployment and their effect on the system.

This System Security State Repository enabler is the foundation of a more advanced visualization dashboard to show user-friendly and comprehensive information to the system administrator or for compliance related audit activities.

Table 14: Mapping between System Security State Repository enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case
Deployment model ontology System Security State Repository service	Use Case 5.1: Virtualized Core Networks, and Network Slicing Use Case 5.4: Verification of the Virtualized Node and the Virtualization Platform Use case 5.5: Control and Monitoring of Slice by Service Provider

5.1.2 Features achieved in R1

- **Feature name**: Deployment model ontology (also known as 5G asset model)
- **Goal**: Enable modelling a system at deployment stage.
- **Description**: a system to be deployed requires a clear plan on what assets it involves and also what controls to be deployed in order to manage the identified threats. Using the Trust Builder, the above are achieved at design time at an abstract level (e.g. asset types, roles rather than instances). This deployment model allows capturing the asset and control instances information in a semantic model that bridges the design phase and the operation phase later.
- **Rationale**: Need a clear reference security model for a deployed 5G systems.

5.1.3 Features in R2

- **Feature name**: System Security State Repository service
- **Goal**: software to create, update and query the runtime model
- **Description**: the software ingests monitoring data from other monitoring enablers via the Generic Collector and uses the data to build a model of the assets and controls present in the system which is compared with the design-time model from the Trust Builder. The SSSR itself detects any deficiency in the security configuration of each asset, checking that security controls specified in the design-time Trust Builder model are present, and sending alert events via the GCI if they are not. The 5G threat knowledgebase from Trust Builder R2 can then be used to discover possible uncontrolled threats. The SSSR enabler provides a query interface to allow other enablers' access to asset status, and a visualisation interface showing the location of any deficiencies in the system.

5.1.4 Recommendations for further research

These enablers are the first step towards runtime threat monitoring and cover the modelling of basic system information (assets, controls), the comparison with the intended design and the analysis of

potentially uncontrolled threats. The next stage of work involves the monitoring of possible asset misbehaviours which can be used to determine the likelihood that a threat is on-going.

Also of interest is the possibility of coupling an asset-based risk analysis capability with dynamic adaptation facilities in virtualised infrastructure including cloud services as well as 5G networks. There are two situations where this may be of value:

1. Dynamic adaptation is required to meet some business objective not related to security (e.g. cost reduction or energy efficiency). The adaptation may lead to an increased exposure to risks (e.g. by creating relationships between previously unrelated assets that could be exploited).
2. An internal system failure (e.g. a configuration error), or an external change (e.g. in the behaviour of attackers) may cause the level of risk to rise to an unacceptable level. Adaptation may provide a possible response to reduce risk by breaking relationships that could be exploited by attackers, or by moving assets away from danger.

Using risk analysis in this way leads to some potential challenges, including how one should automatically balance risk reduction against other business objectives, and how to perform machine reasoning calculations fast enough to be used in an autonomously managed system.

5.2 Security Enabler "Security Monitor for 5G Micro-Segments"

5.2.1 Product Vision

Security monitoring is needed to increase awareness and responsiveness of network security (to learn networks' security situation, to detect on-going attacks, and to quickly deploy appropriate countermeasures). However, attacks will be difficult to detect from 5G networks, which will be heterogeneous and will have massive amount of users and data flows. Micro-segmentation[5] increases the accuracy of monitoring by enabling focus to particular isolated applications and to restricted amount of users. Consequently, security monitor for micro-segments enables: 1) more accurate incident detection (by focusing on fewer data streams, we can study more parameters and correlations from homogeneous data flows), 2) customization of security monitoring based on 5G customers/end-users preferences, and 3) adaptation of 5G networks' (micro-segments') defences based on monitored/inferred security awareness.

The security monitoring enabler is based on the framework that is defined in the first release (**R1**). The framework enables distributed monitoring, inference, and reactions to security incidents. It enables development of components that will detect selected on-going attacks in micro-segments, in order to adapt 5G networks or segments' defences and topology. Particularly, Release 1 of the enabler provides a Complex Event Processing (CEP) tool chain, which is based on the state-of-the-art 'big data' technologies: Apache *Kafka* and Apache *Spark*. The framework can be used when constructing different monitoring setups. It

[5] Micro-segments are isolated parts of 5G network that have been dedicated e.g. for particular applications or organizations. For instance, a micro-segment may be dedicated for IoT communication of an industrial organization. They are created using software networking and virtualization techniques. Micro-segmentation addresses the scalability challenges of 5G networks, which consist of large amounts of heterogeneous devices and traffic. Micro-segments ease the development and configuration of focused and fine-grained security, as the amount of subscribers and type of communication can be limited. Each micro-segment may have its own security functions that target both 5G specific generic threats as well as micro-segment specific threats.

The concept of micro-segment is similar to slice or sub-slice. However, here we consider micro-segment to be controlled by single authority whereas an end-to-end slice can consist of elements belonging to several operator / authority domains.

provides a mechanism to collect and share events from various sources and to distribute them to security inherence components. The framework increases *scalability* and *flexibility* of 5G security monitoring by:

- Enabling new heterogeneous event sources (switches, logs, IDSs etc.) to be easily added.
- Reusable components to be used for processing of event streams (e.g. merging, aggregating).
- Enabling different 'inherence components' - such as pattern detectors, machine learners, correlation analyzers… - to be integrated to the system when a need arises in different micro-segments (the solution provides efficiency as events are provided only to those components that are interested on them).
- Deploying *'big data' technologies* for analytics. S*tate-of-the-art* software components - that implement CEP, publish-and-subscribe and cluster computing paradigms - are utilized to handle large amounts of event streams in near real-time.

The security features developed in the second release (**R2**) extend the monitoring framework by

- Integrating it with the micro segmentation enabler (KPIs, counters, and network configuration data related to traffic flows and software network).
- Adding inference and control logic for adapting micro-segments by utilizing analysed risk-information.
- Integrating it with Trust Metric Enabler (TME).

Security monitoring could be offered as a service by micro-segment providers (i.e. by mobile and virtual mobile network operators) for different organizations needing high-security level. It can be also deployed as a third-party service (by a security monitoring company that is employed by the user of the micro-segment). The enabler enables opening of the monitoring interfaces so that monitoring service provider may introduce customised monitoring analytics for 5G micro-segment users/customers. Potential customers include e.g. companies needing higher security assurance for industrial IoT, automotive, or e-health related services.

The enabler can be utilized to capture different security threats that exist in different 5G-ENSURE use cases. The security monitoring enabler does not aim to provide a comprehensive solution for any single use cases. Rather it may be used to address specific threats and problems in several use cases. Some relevant use cases have been listed in Table 15. The framework can be customized to detect and react to security incidents in virtualized 5G software networks (hence it is related to 5G-ENSURE use case 5.5). As it enables monitoring of communication flows, it may be used to detect attacks caused by botnets (use case 10.1). In the release 2, the enabler has been integrated with micro-segments and thus enables monitoring of virtualized network function platform (use case 5.4). Release 2 will also provide control functions to autonomous adaptation of micro-segments' topology and defences (use case 5.5).

Table 15: Mapping between Security Monitor for 5G Micro-Segments enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case
Complex Event Processing Framework for Security Monitoring and Inferencing (Release 1)	Use case 5.5: Control and Monitoring of Slice by Service Provider
	Use Case 10.1: Botnet Mitigation
Extended data gathering (Release 2)	Use Case 5.4: Verification of the Virtualized Node and the Virtualization Platform
Risk-based adaptation of micro-segments	Use case 5.5: Control and Monitoring of

(Release 2)	Slice by Service Provider
Cross-domain information exchange (Release 2)	Use case 5.5: Control and Monitoring of Slice by Service Provider

5.2.2 Features Achieved in R1

- **Feature name**: Complex Event Processing Framework for Security Monitoring and Inferencing
- **Goal**: Enable distributed security monitoring and reactions to security incidents.
- **Description**: The first release provides a more detailed design and a prototype that supports collection and sharing of monitored information. The first release provides a CEP framework enabling development of use case and threat specific monitoring applications / inference logic. However, the monitoring and inference capabilities, in release 1, were limited to few example cases.
- **Rationale**: Enable scalable and extensible security monitoring in 5G networks.

5.2.2.1 Features Achieved in R2

- **Feature name**: Risk-based adaptation of micro-segments
- **Goal**: Dynamic control of micro-segments topology and defences based on determined security threats and risk levels
- **Description**: The feature provides algorithms for determining risk-levels related to selected threats. Machine learning techniques (anomaly detection, correlation analysis) will be utilized in the process. The algorithms are also able to autonomously request the micro-segmentation enabler to adjust its topology and defences according to the inferred risk-levels (e.g. remove suspected nodes from the segment).
- **Rationale**: Fast security responses to attacks/risks in 5G micro-segments

- **Feature name**: Extended data gathering
- **Goal**: Collecting monitoring data and KPI from the micro-segment.
- **Description**: The feature will collect information from different data sources, particularly from micro-segment. Capabilities to collect topology and configuration information as well as traffic statistics from micro-segmentation enabler are provided.
- **Rationale**: Enable extensive awareness over security state of 5G application

- **Feature name**: Cross-domain information exchange
- **Goal**: Exchanging monitoring data - collected from the micro-segment - between the GCI enabler and micro-segmentation enabler
- **Description**: Release 2 provides export functions for delivering reports in XML-format to the GCI server. The micro-segmentation enabler collects data about a given micro-segment. Currently available information from micro-segment contains identifiers of nodes in the data layer (switches). When 5G VNFs are integrated to micro-segment, these export functions may be adapted to support VNF specific monitoring.
- **Rationale**: Enable interconnection between heterogeneous administrative domains that support different monitoring enablers

5.2.3 Recommendations for further research

Intelligent monitoring - Future research is needed to enable to cover more security threats - to enable extensive awareness and responsiveness over security state of 5G applications. New algorithms are needed for inferring security incidents and security threats from wide amount of information available from 5G network. To enable more efficient autonomous security, different machine learning mechanisms should be leveraged to correlate and infer monitored information. Machine learning algorithms for analysing monitored data should be scrutinized to enable autonomous mitigation actions. Further, potential of multi-access edge computing approaches should be studied for lowering latency of monitoring and mitigation actions.

Extended monitoring coverage over 5G functions - In Release 2, the monitoring is focused on the data layer of the micro segment / SDN. Information is collected only from switches and data flows as well as on authentication events. In the future, the monitoring should cover also different VNFs which may be relevant for 5G services (such as PWG, SGW, MME, HSS). This information could then be shared to other domains using e.g. GCI interface.

5.5 Security Enabler "PulSAR: Proactive Security Analysis and Remediation"

5.5.1 Product Vision

The Proactive Security Analysis and Remediation (PulSAR) enabler provides a cyber-security monitoring tool based on an attack graph engine to analyze and prevent cyber-attacks at run-time and to detect and counter on-going attacks. Its main capabilities are the following:

1. Attack graphs used at design time for static risk analysis
2. Technical vulnerability analysis to assess the paths that may be followed by attackers (e.g.. CVEs).
3. Remediation propositions.

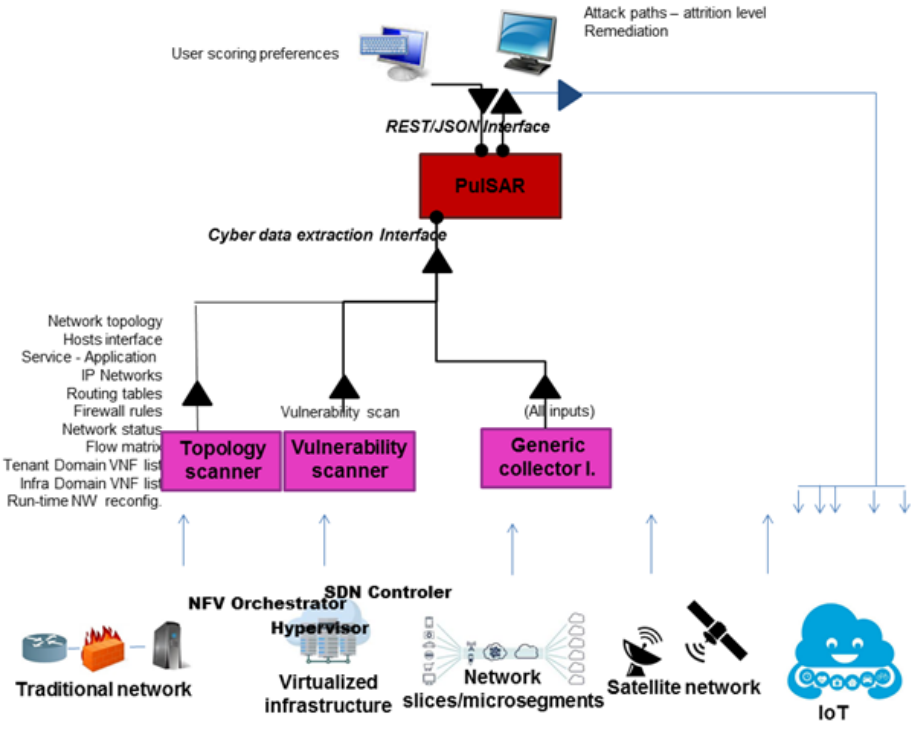


Figure 14. PulSAR overview

Thales Security analysis and remediation enabler builds upon CyberCAPTOR enabler (https://github.com/fiware-cybercaptor/) that has been developed within the FI-PPP FIWARE project. The main goals of CyberCAPTOR are to better understand the actual risk exposure of a Future Internet system through the detection of potential attacks based on NIST vulnerability database, or non-authorized usage in order to propose possible remediation.

For PulSAR, components have been slightly redesigned in the following way; a comparison with the initial CyberCAPTOR components is presented in the synthetic table of the technical roadmap section:

- Cyber data extraction: Topological and vulnerabilities data
- Attack graphs and scored attack paths: The security operator can enter her own scores.
- Remediation: To remediate possible attack paths
- Visualization

Table 16: Mapping between PulSAR enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case
5G specific vulnerability schema implementation	UC5.1: Virtualized Core Networks, and Network Slicing UC5.5: Control and Monitoring of Slice by Service Provider
PulSAR interface with Generic Collector	UC5.5: Control and Monitoring of Slice by Service Provider

5.5.2 Features achieved in Release 1

- **Feature name**: 5G specific vulnerability schema
- **Goal:** Extension of the Cyber-attack modelling.
- **Description:** This feature benefits from 5G-ENSURE work on 5G specifics threats and security enablers capabilities to further develop the several layers of the cyber-attack models.
- **Rationale:** 5G networks will face novels complex cyber-attacks that will combine vulnerabilities of its different management components and systems.

Details of the 5G specific vulnerability schema achieved in R1 are given in Annex of this deliverable.

Together with the 5G specific vulnerability schema, software has been delivered in Release 1 with a first implementation of the schema.

5.5.3 Features achieved in Release 2

Feature name: 5G specific vulnerability schema implementation

- **Goal**: Implementation of an extended Cyber-attack modelling for 5G.
- **Description**: This feature implements the 5G specific topology and vulnerability schema. This release provides an enhanced version of the 5G vulnerability schema, according to 5G architecture principles (links instead of IP networks) and the new attacks methodology discovered during the project lifetime.
- **Rationale**: 5G networks will face novels complex cyber-attacks that will combine vulnerabilities of its different management components and systems.

Feature name: PulSAR interface with Generic Collector

- **Goal**: provide an integration with Generic Collector enabler
- **Description**: This feature provides an implementation of the PulSAR interface with the Generic Collector enabler in order to analyse more data on going attacks.
- **Rationale**: benefit from Generic Collector means of data collection to analyse more data.

5.5.4 Recommendations for further research

In order to provide the best coverage for cyber-attacks at run-time, it would be useful to provide countermeasures which could be enforced by a dynamic reconfiguration of the VNFs at run-time. This implies that orchestrators can send reconfiguration commands to the VMs they orchestrate. State-of-the-art orchestrators are not ready yet to support such dynamicity. A modification in the VNF configuration implies as far a restart of the VNF.

The recommendation would be to develop a security monitoring component working tightly with the controller/orchestrator of the network or slice in order that the security monitoring component could send reconfiguration commands to the orchestrator.

5.6 Security Enabler "Satellite Network Monitoring"

5.6.1 Product Vision

This enabler takes its origin from 5G satellite Business needs and 5G-ENSURE use case "5G integrated satellite and terrestrial systems security monitor". 5G integrated satellite and terrestrial systems are constituted by the following components:

- Satellite Hubs.
- Satellite Terminals (Ka band).
- Satellite Modems.
- 5G EnodeB: traditional EnodeB improved with a satellite link and dynamic beams.
- 5G devices.

Components that are subject to active security analysis are identified. Security metrics, counter measures and the mitigation level they provide are determined.

This security enabler provides pseudo real-time monitoring and threat detection in these systems. Several indicators (including security metrics) are collected from the listed 5G integrated satellite and terrestrial systems and are periodically delivered to the monitoring system in a secure way.

An active security analysis has been used to detect, investigate and response to the threats identified.

It can be mentioned that Satellite Network Monitoring can contribute to AAA enablers with respect to Identity Management use cases, and can contribute to Network Management & Virtualisation Isolation enablers in use cases such as "Verification of the Virtualized Node and the Virtualization Platform" and "BotNet activity".

Table 17: Mapping between Satellite Network Monitoring enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case
Pseudo real-time monitoring	Use Case 5.6: Integrated Satellite and Terrestrial Systems Monitor

Ultra-Reliable Operations	Use Case 8.1: Satellite-Capable eNB

5.6.2 Features achieved in R1

- **Feature name**: Pseudo real-time monitoring
- **Goal**: Provide pseudo real-time monitoring of the satellite network
- **Description**: provide a prototype to monitor the indicators (including the credentials management) in a quick, effective and intuitive manner. These indicators are collected in a heterogeneous 5G satellite system and are periodically delivered to the monitoring system in a secure way.
- **Rationale**: Monitor of heterogeneous 5G wide-area network.

- **Feature name**: Threat detection
- **Goal**: Include rules in the monitoring system that correlate different incidents to detect specific threats and vulnerabilities in the satellite network.
- **Description**: provide a prototype with information on the likeliest cause of failure and course of actions to follow by the operator.
- **Rationale**: Response to threats and vulnerabilities in satellite networks conveying data or signalling in heterogeneous 5G system.

5.6.3 Features achieved in R2

- **Feature name**: Active security analysis
- **Goal**: Provide the complete solution including the active security analysis to detect, investigate and response to the threats identified.
- **Description**: Using the R1 features (Pseudo real-time monitoring and Threat detection) together can be implemented an active security analysis. The first prototype monitors the indicators, including credentials. Those indicators are used to improve the real-time monitoring in order to collect in a heterogeneous 5G satellite system. With the second system, the threats detected into the system following different rules in a monitoring system are collected to retrieve the vulnerabilities in the satellite network. Monitoring those rules in the monitoring system can be detected the likeliest cause of failure and course of actions to follow by the operator.
  The security level shall be configurable. Some of the threats currently identified are: Attack to network components, attack on the SNM and denial of service.
- **Rationale**: Integration of the R1 features in order to enable a threat and monitoring system to detect possible failures and be preventing/informing the operator. Incorporating satellite network monitoring as a 5G Security Monitoring enabler will benefit other 5G enables:
  - AAA enablers: The Satellite Network monitoring enabler is expected to detect changes in the configuration of the network, keeping a log of each movement on it.
  - Identify abnormal activity at mobile devices and report this activity.
    - The end user will get an historical data of the activity of terminals connected to Satellite Network in order to improve the user experience and give security, because the user will know every moment his movements.
    - Giving specific restrictions and privileges to 5G satellite terminals.

- **Feature name:** Pre-emptive mitigation security actions.
- **Goal:** Provide predictive capabilities to the system in order to execute mitigations actions before possible security threats happened.

- **Description:** Using some of the R1 features available for pseudo real time events gathering, we establish a subset of configuration actions focus in block or mitigate the impact of security threats happened in an autonomous way.

  The main idea is provide to the system of no-human intervention mitigation actions, operators defines previously what kind of events and actions could be applied at configuration level and even define another suggested actions that needing just human authorization could be applied in real time, this feature suggests specific actions in order to decrease the response time and prevent a possible service lost.

- **Rationale**: R1 features offer the information sources necessary to determine some of the expected conditions to identify and alert a security threat. R2 feature improves the security capabilities by determining and preparing the system to mitigate attacks, some of the main advantages among others are:

  - Increase the Service Availability, service level agreements are the main focus on any TELCO subscriber agreement, an autonomous system with a subset of actions defined to mitigate possible threats increase the possibilities to avoid any service lost, enhancing the solution availability.
  - Mitigation autonomous actions, the operator is free to determine the subset of actions and configuration options available for the system, a different level classification of the threats and actions could be defined in function of the possible service impact or complexity.

5.6.4 Recommendations for further research

Some of the features previously implemented could be improved, for example the log file, which stores all the data into a server, could be encrypted using a known encrypted method. It can also be done a monitoring of those log files. Monitoring the logs can be done in order to improve the speed of the network because at some points if the logs are enough bigger could affect to the network generates those data. Also, it can be split into different network in order to avoid this effect.

With the security monitoring enabler, the system will be protected against internal and external threats coming from the heterogeneous 5G networks, to meet security requirements from the 5G-ENSURE trust model.

One of the main challenges in the developments that should be kept in mind is a resource optimized approach, between the layers and domains and the possibilities to combine another aspects as energy optimization and the security requirements at end user level in the solution.

5.7 Generic Collector Interface

5.7.1 Product Vision

The origin of most fraudulent accesses or security breaches could be formalized:

- By some technical identity alteration (after an illegal or illegitimate privilege augmentation)
- Through signalling messages received outside of the normal sequences (meaning that the finite state automata in charge of a connection management or service transaction received an abnormal message regarding its internal state).

In order to collect this added value information, a Generic Interface has been proposed to allow each subsystem to provide authorized parties with large amounts of data including internal logs and events and

which can be associated to incidents of virtualization, Identity Management, communication protocols, layers or stacks, and some specific Operating System privileges augmentations.

5.7.2 Features achieved in R1

- **Feature name**: Log and Event Processing
- **Goal**: Interoperability between events and logs format, in order to allow FastData technologies to be deployed inside the 5G Network
- **Description**: A format was proposed with a Proof-of-Concept (PoC) to be embedded in the TestBed in the release (R1)
- **Rationale**: 5G networks will face novel complex incidents, cyber-attacks, and frauds in a multi-tenant and technology environment.

5.7.3 Feature achieved in R2

There is no release R2. We supported others partners to generalize the usage of this enabler R1 to several 5G-ENSURE Enablers R2, in order to efficiently monitor the 5G Networks and infrastructures.

The integration of the Generic Collector Interface R1 is a feature release in the following enablers R2.

- System Security State Repository enabler R2: System Security State Repository service
- PulSAR: Proactive Security Analysis and Remediation enabler R2: PulSAR interface with Generic Collector

5.7.4 Recommendations for further research

The generalization of Generic Collector Interface on each 5G components leverages the implementation of efficient FastData inside 5G Networks.

After the evaluation of R2 Security Monitoring enablers over the TestBed (if the efficiency evaluation demonstrates the added value of GCI), we may investigate standardization of the Generic Collector Interface.

5.8 Malicious traffic generator for 5G Protocols

5.8.1 Product Vision

Stronger adoption of Software Defined Networks (SDN´s) and Virtualized Network Functions (VNF´s) is expected of the 5G network. This will increase opportunities for malicious use. Furthermore, increased use of open standards with a myriad of implementation options makes the 5G network more susceptible to mistakes and attacks to bypass security controls compared to previous mobile networks. Therefore, the effect of malicious traffic and malformed packets against different network elements should be investigated and tested.

An SDN controller will forward or compile received network commands either to the physical network or to the virtualized network. Such software may have bugs and misconfigurations. For example, an SDN controller provides APIs to the more abstract network views (northbound API) and might expose vulnerabilities to the network´s control plane (southbound API). A vulnerability can be exploited by a malicious attacker or an application by sending dedicated network packets. Furthermore, a controller's east- and westbound APIs might be exposed to vulnerabilities in case where network control plane comprises multiple controllers.

As virtualized networks share the same physical hardware and network resources, applications running on different virtualized networks might compete for the same physical network resources. Misconfigurations in the network can occur when conflicts from resource competition are mishandled. This can lead to a situation where network packets are transferred to the wrong endpoint.

This enabler provides protocol implementation testing by generating malformed packets or a traffic overload to network components in a 5G network. The enabler can also be used for testing the appropriate functionality of other 5G enablers.

Enabler Security Feature	Relevant Use Case(s)
Traffic generator engine	• Use Case 5.3: Reactive Traffic Routing in a Virtualized Core Network; network reconfiguration messages • Use Case 5.4: Verification of the Virtualized Node and the Virtualization Platform; attacking the SDN controller • Use Case 6.1: Attach Request During Overload • Use Case 7.1: Unprotected Mobility Management Exposes Network for Denial of Service
Malicious pattern library	• Use Case 1.1: Factory Device Identity Management for 5G Access • Use Case 1.2: Using Enterprise Identity Management for Bootstrapping 5G Access • Use Case 1.3: Satellite Identity Management for 5G Access • Use Case 1.4: MNO Identity Management Service • Use Case 4.1: Authorization in Resource-Constrained Devices Supported by 5G Network; attacks against the AAA servers' vulnerabilities • Use Case 4.2: Authorization for End-to-End IP Connections; direct IP connection without authorization • Use Case 4.3: Vehicle-to-Everything (V2X) • Use Case 5.1: Virtualized Core Networks, and Network Slicing; significant attack surface • Use Case 5.2: Adding a 5G Node to a Virtualized Core Network • Use case 5.5: Control and Monitoring of Slice by Service Provider • Use Case 5.6: Integrated Satellite and Terrestrial Systems Monitor; signalling messages outside of the normal sequences • Use Case 6.2: Unprotected User Plane on Radio Interface • Use Case 9.1: Alternative Roaming in 5G; spoofing of signalling messages • Use Case 9.2: Privacy in Context-Aware Services; User traffic can be enriched in various ways • Use Case 9.3: Authentication of New Network Elements
Fuzzing engine	• Generic use case: Any use case may contain a vulnerability when the interface is flooded with random traffic, the aim is to investigate whether an interface is vulnerable to the interface overload.

5.8.1.1 Traffic Generator Engine

The Traffic Generator Engine is a device that generates large amounts of syntactically correct messages to overload a node interface.

5.8.1.2 Malicious Pattern Library

The Malicious Pattern Library is a collection of protocol anomalies that are accepted by the message parser but will cause malfunction or let malicious messages to be transferred to later interfaces.

5.8.1.3 Fuzzing engine

The Fuzzing Engine is a random data generator.

5.8.2 Features achieved in R2

This enabler has features to emulate:

- **Hostile Evolved Node B (eNodeB) and Hostile User Equipment (UE)** which generates malicious, unusual or Denial of Service (DoS) type of traffic to 5G network.
- **Hostile client** against targeted server endpoints.

The enabler works in the following modes:

Traffic Generator Engine

- **Goal:** To generate an overload of traffic to the gNB or eNodeB in order to cause a DoS attack on the radio interface by flooding it with connects, or to generate traffic overload by a rogue gNB or eNodeB to UEs to prevent connectivity.
- **Description:** Traffic Generator Engine generates a large amount of formally correct messages in rapid succession to overload network interfaces i.e. performing a DoS attack.
- **Rationale:** To test network resilience to DoS attacks.

Malicious Pattern Library

- **Goal:** To compose a collection of syntactically correct messages in protocols supported by the 5G node protocol stacks that would cause the node to either malfunction, drop, or surrender to unauthorized access.
- **Description:** A library of message anomalies of accepted protocols.
- **Rationale:** To test the node interface protocol parsing and resilience to protocol message anomalies.

Fuzzing Engine

- **Goal:** To generate random input to node interfaces in order to crash the interface or induce a memory leak.
- **Description:** The Fuzzing Engine generates random input to a node interface.
- **Rationale:** To test the interface resilience to garbage input.

5.8.3 Recommendations for further research

While this enabler is subject to considerable workload, the topics to be researched are familiar from other current areas of security research:

- Reliably implementing a fuzzing solution that creates anomalies in 5G related protocol parsing.
- Implementing the entire set of protocols and technologies for anomalies and building a library of attacks for each of them. Modularity of the enabler provides easy way of adding new protocol templates.

- Exploring ways to overload 5G network elements and cause Denial of Service or significantly lowered QoS by abusing protocol parsing or application logic.
- Relating to performance. Part of the enabler that is creating the network frames and packages is implemented as a Python library. This is because the current implementation has focused on flexibility and not on network level performance. This network level performance might be preferred in some cases. There are some alternatives to this library that are implemented with C programming language which can be quite a lot faster, though some flexibility might be lost with it.

5.9 Additional enablers

Monitoring confidential traffic flows - The trend in networks security is encryption and obfuscation. With traditional monitoring approaches, this may result in a non-valuable collected data, hence, not detecting threats and vulnerabilities. This is why improving monitoring mechanisms to be able to treat encrypted traffic is of main interest.

- **Enabler name**: enhanced network monitoring
- **Goal**: to provides mechanisms that are able to treat any kind of traffic and network such as encrypted traffic.
- **Description**: we propose to study existing techniques in the state of the art like homomorphic encryption or searchable encryption, then, enhance it to be used in 5G network context.
- **Rationale**: provide enhanced service to verticals

Increasing Trust towards Monitored Information - Security awareness depends on the accuracy and trustworthiness of available event information. There is a risk that bogus information coming from untrustworthy (hostile or compromised) parties will cause network to behave in unwanted manner. Therefore, mechanisms for verifying trustworthiness of information should be integrated to the security monitoring enablers. Knowledge on the trustworthiness of monitoring sources should be utilized when planning and executing mitigation actions (that are based on monitored data). For instance, less weight should be given for event notifications that are coming from a node that has out-dated software or that has previously sent large amount of false alerts.

- **Enabler name**: Trust management for monitored information
- **Goal**: to provide mechanisms that increase trust towards monitoring
- **Description**: Different approaches can be utilized to increase trust. Trusted computing technologies provide one approach as they enable verification of software platforms used for monitoring. Security monitoring enablers could attest the reliability of information source. Alternatively, misbehaving information sources may be detected by monitoring their behaviour. For instance, correlation analysis may reveal anomalies raised by two sources providing contradictory monitoring data.
- **Rationale**: enabler collecting and using information on the trustworthiness level of monitoring source

6 Network Management and Virtualization Isolation Security Enablers

The management of 5G networks will fundamentally change through applying the principle of software-defined networking (SDN). While 4G networks already have a clear split between data plane and

management plane, the adoption of SDN in 5G networks will further evolve network management with a more (logically) centralized approach. Centralized control of the overall network infrastructure has a huge potential of simplifying network management and for offering new, richer, and more flexible network services. This potential is complemented by the programmable nature of SDN networks, which in turn eases the virtualization of networks. This is also often termed “network softwarization”. However, centralized control represents a valuable target for attacks and a single point of failure. Furthermore, software is vulnerable, e.g., because of bugs and misconfigurations.

The aim of the security enablers provided in this section is twofold. First, some of the enablers aim at securing a network’s control plane and the virtualized networks on top of it. Second, some aim at securing network services and providing new security services. To this end, we propose the following security enablers, which we describe in detail in the forthcoming subsections.

- Anti-fingerprinting interactions between switches and network controller.
- Access control mechanisms for the network’s control plane.
- Auditing the interactions between network components.
- Network management enabler (utilizing the SDN architecture) that facilitates micro-segmentation. Create secure network segments for fine-granular network flow policies.
- Bootstrapping trust in virtualized network environments between network endpoints and also between (SDN) network components.
- Flow control for in-network threat detection and mitigation for critical functions in virtual networks.

6.1 Security Enabler “Anti-Fingerprinting”

6.1.1 Product Vision

The separation of the network planes (e.g., the data plane and control plane as in SDN) opens the doors for a remote adversary to fingerprint the network. For instance, in an SDN network, whenever packet forwarding is performed in hardware, then packets at the data plane are processed several orders of magnitude faster than at the software-based control plane. This discrepancy acts as a distinguisher for a remote adversary to learn whether a given probe packet is handled just at the data plane or triggers an interaction between the data plane and the control plane. An interaction provides evidence that the probe packet does not have any matching flow rule stored at the switch's flow table (or it requires special attention from the controller). This knowledge empowers an adversary with a better understanding of the network's packet-forwarding logic and it even might reveal some information about the network’s topology. A network operator wants or is even required to prevent the leakage of such kind of information, since it exposes the network to a number of threats. In particular, with this additional knowledge it is possible to launch more powerful denial-of-service (DoS) attacks.

This security enabler prevents fingerprinting attacks in networks with separated planes like in an SDN network. More concretely, certain packets of a network flow are delayed at a switch before the switch forwards them. Such a delay mimics an interaction between components at different network planes. In an SDN network, this would be the interaction between the switch and the network controller. With this enabler in place, a remote attacker (active or passive) cannot distinguish anymore whether a real interaction took place or an artificial delay. Note that the impact on the network performance is insignificant, since the enabler only delays a few packets of a network flow. Experiments have shown that this is already effective against fingerprinting attacks.

The relevant uses cases from (5G-ENSURE Consortium, 2016) of this enabler's feature are listed in the following table.

Table 18: Mapping between enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case
Controller-Switch-Interaction Imitator	Use Case 5.3: Reactive traffic routing in a virtualized core network

6.1.2 Features achieved

The anti-fingerprinting enabler comprises one feature, which we describe in the following. As part of the technical roadmap for the first release (see the project deliverable D3.1 (5G-ENSURE Consortium, 2016)), it has been developed and analyzed in the first year of the project. It has however not released as software in the project deliverable D3.3 (5G-ENSURE Consortium, 2016) for reasons explained below.

- **Feature name:** Controller-Switch-Interaction Imitator.
- **Goal:** Prevent the leakage of timing information that would reveal whether a network packet received by a data plane component (e.g., a switch) triggers an interaction with the control plane (i.e., the SDN controller).
- **Description:** Based on the occurrence of the last packet of a network flow a switch decides whether the forwarding of the currently processed packet should be delayed. The additional delay depends on the actual network characteristic (switches, network load, controller, etc.). The impact on the network's performance is almost negligible since only a few network packets are delayed, namely the ones that match an already existing network flow that has not appeared for a while. Furthermore, there is no additional overhead on the network's control plane.
- **Rationale:** The introduced delay of a packet mimics the interaction with the SDN controller. This obfuscates timing measurements done by a remote attacker to determine the processing times of packets in the network.

Since the implementation of the enabler requires the modification of current hardware switches, it is not in the scope of 5G-ENSURE to deploy and evaluate the enabler in the project's testbed. Note that although an implementation in software, e.g., an extension of the OpenVSwitch (OVS) (Pfaff, Petit, Koponen, Amidon, Casado, & Shenker, 2009) (Open vSwitch - a production quality, multilayer virtual switch) would be rather straightforward to realize, an evaluation under realistic conditions would still not be possible, since hardware switches process packets several orders of magnitudes faster as software switches. It is, however, possible to emulate the security enabler by installing predefined flow rules in a switch and delay packets by a software component.

In our experimental evaluation of the feature, we used a small network with hardware and software switches. It mimics the structure of data center networks. We exchanged probe packets with the network from locations all around the globe and measured their round-trip times and packet dispersion. Our measurements were taken from 20 different hosts located across the globe (Australia, Asia, Europe, and North America) and spanning a period over several months. Overall, the experiments first demonstrate that fingerprinting attacks to SDN networks are feasible. Second, they demonstrate the enabler's effectiveness against fingerprinting attacks. More concretely, a remote adversary has in our experiments only a fingerprinting accuracy close to 50%. Intuitively, this means that the adversary is not much better than just

blindly guessing whether there is a controller-switch interaction for a network packet. In contrast, without the enabler, the fingerprinting accuracy is over 90%. Further details of this feature and its evaluation are found in the paper (Cui, Karame, Klaedtke, & Bifulco, On the fingerprinting of software-defined networks, 2016).

Currently, there are no further releases planned of this enabler with additional features.

6.1.3 Recommendations for Further Research

Similar to the fingerprinting attacks described here, recent work [Achleitner, S. et al. (2017), Conti, M. et al. (2017), Liu, S. et al. (2017), Lin, P-C. et al. (2017)] has shown that other types of attacks are possible to SDN networks that also reveal information about a network's data plane configuration. In general, SDN networks are exposed to attacks that exploit the information leakage between the different distributed planes (i.e., data, control, and application) and their APIs. Note that one reason for the information leakage is due to the softwarization of networks. Further general insights in this new kind of attacks, their feasibility, and the quantification of the leaked information are needed to design effective protection mechanisms against these new attacks.

6.2 Security Enabler "Access Control Mechanisms"

6.2.1 Product Vision

In 5G, a much stronger adoption of SDN and NFV is expected than in current networks. For example, for SDN, it is expected that various network applications will run at a network's control plane on top of the SDN controller. These applications will manage the network's data plane and offer a wide range of network services. Examples of such applications are routing applications, load balancer, and monitoring and analysis tools for network traffic. The diversity of network applications and their large-scale deployment actually applies to SDN in general. The network applications, however, might not be trusted by the network operator. Reasons for this are: (1) they might be from different network tenants or service providers, (2) they might be developed by third parties, or (3) they might contain bugs—as any complex software—and the control plane is therefore vulnerable to various kinds of attacks. It is also expected that a 5G network will comprise several service providers, each providing network functions that run in virtualized environments of a data center. These virtualized network functions (VNFs) will be managed by an orchestrator, which is, e.g., responsible for starting, terminating, and mitigating containers for these VNFs. Similar to SDN network applications, the access to network resources of the processes that run in these containers should be controlled. Analogously, these containers themselves should have only the permissions that are needed for their network tasks.

Related to untrusted network applications and VNFs because of software bugs is the following. Note that in the following description, we focus on SDN networks to ease readability. However, our comments carry over and remain valid in the context of VNFs and 5G networks.

First, note that even if a network application runs in a virtualized network, the SDN controller must compile network commands down to the physical network or up to the virtualized network. Such a compilation step is in general nontrivial and might be buggy or misconfigured. Furthermore, the API to the virtualized network might be buggy and not be trusted. More generally, any northbound API that the controller provides for more abstract network views (e.g., the intent framework of the ONOS controller (Berde, et al., 2014)) might expose vulnerabilities to the network's control plane, which can be exploited by malicious applications or network users by sending dedicated network packets. In case the network's control plane

comprises multiple controllers then the controllers' eastbound and westbound APIs might expose vulnerabilities.

Finally, different network applications might compete for network resources. Again, even if the applications run in different virtualized networks, they might still compete for the same physical network resource. Not resolving such conflicts can result in misconfigurations of the network, e.g., network packets are shipped to the wrong endhost because a network application overwrites a flow rule of another network application in one of the switch's flow tables.

Current state-of-the-art SDN controllers fall short in restricting the access of network applications to network resources. For example, a network application can send any OFPT_FLOW_MOD OpenFlow message to any switch (i.e., write any flow rule to a switch's flow table). This is analogous to a database user that can arbitrarily modify the tables of the database, or the root user of a computer that can write to any file. Another example concerns OpenFlow messages that request information about the current network configuration. If the controller maintains a network information base (NIB), not every application should have full read permissions to this database. For instance, not every application should be allowed to see all the currently installed flow rules at the switches.

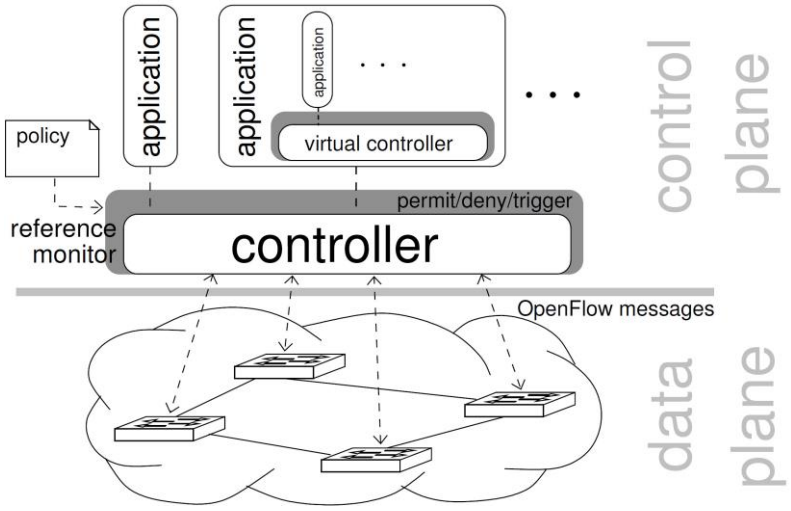


Figure 15: SDN controller extension with a reference monitor.

The security enabler described in this section applies the *principle of least privilege* to the network applications, that is, the enabler enforces that each network application must be able to only access the information and resources that are necessary for performing its tasks. To this end, the security enabler adds *reference monitors* to the network's control plane. See Figure 16 for an illustration, where a reference monitor is added to an SDN controller and limits the sending and receiving of OpenFlow messages, i.e., the network abstraction provided by the OpenFlow protocol. In general, a *reference monitor* permits and denies actions of the network applications according to a given *security policy* with respect to a network abstraction. For instance, the policy might only permit certain network applications to modify a flow rule or install new flow rules. The owner of the flow rule or the flow table, respectively, specifies how the network applications can access these network resources.

Analogously to the reference monitor for SDN controllers, this enabler targets to restrict access of virtualized environments that host VNFs. Furthermore, it also focuses on checking requirements for these environments. For example, a container hosting a VNF or parts of it is only allowed to connect to a specified socket or containers hosting VNFs from different owners must not run on the same physical machine.

The relevant uses cases from (5G-ENSURE Consortium, 2016) of this enabler's feature are listed in the following table.

Table 19: Mapping between enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case(s)
Southbound Reference Monitor	Adding a 5G node to a virtualized core network (Use Case 5.2)
Access Requirements for VNF Container Resources	Adding a 5G node to a virtualized core network (Use Case 5.2)

6.2.2 Features achieved

This security enabler will comprise the following two features, which we describe below. The first feature of this security enabler targets SDN networks. More concretely, the feature is an additional component of an SDN controller. Its development started in the first year of the project, where a first running prototype of the reference monitor for the ONOS controller (Berde, et al., 2014) (ONOS - a new carrier-grade SDN network operating system designed for high availability, performance, scale-out) was developed and evaluated in a Mininet environment (Gkounis, Klaedtke, Bifulco, & Karame, 2016). Its development will be continued in the second year of the project.

- **Feature name:** Southbound Reference Monitor.
- **Goal:** Enforce access control policies that account for the southbound API of an SDN controller.
- **Description:** The reference monitor is a component at the network's control plane. It permits or denies, for a given OpenFlow message, whether the message can be sent to a switch. This decision is based on the given access control policy and the initiator of the message (i.e., the network application). Similarly, for a message that is sent to the controller, the reference monitor decides whether a network application that is running on top of the controller can receive this message.
- **Rationale:** The sharing of resources in an SDN network is effectively realized by empowering network tenants at the control plane with permissions for administrating network components. However, since the different tenants can have competing objectives, mechanisms are needed to protect the network resources from unauthorized access. The reference monitor is such a mechanism, which restricts the access to the network components according to a given policy.

The second feature of this security enabler is as follow, which is specifically in the scope of the enabler's second release.

- **Feature name:** Access Requirements for VNF Container Resources
- **Goal:** Enforce policies for containers that host VNFs and restrict their access to other network resources.
- **Description:** This feature will provide additional security checks for Docker containers (Docker) that host VNFs. An example of such an additional check is whether the container can connect to another container or whether it can be migrated to another physical machine.
- **Rationale:** VNFs will run in the cloud in virtualized environments like Docker containers. The physical infrastructure on which the VNFs are executed is not necessarily owned and operated by the VNF owners. In fact, multiple service providers may use same physical infrastructure for their VNFs. To ensure strong isolation guarantees, a VNF owner may want to restrict the access to the containers hosting parts of its VNFs. Furthermore, the VNF owner may require that its containers do not share the same physical infrastructure with containers of other VNF owners. The cloud provider needs to put mechanisms in place to ensure such isolation guarantees.

The first prototype of this feature will be able to limit the network connections of Docker containers that host VNFs. Furthermore, it will allow one to specify and enforce simple requirements and policies for container instantiation and migration.

6.2.3 Recommendations for Further Research

Forthcoming releases of this security enabler will support network abstractions at higher levels. More concretely, the developed access control mechanisms will target the northbound APIs of SDN controllers like the intent framework of the ONOS controller. Furthermore, it is also planned that future releases of this security enabler will include mechanisms for multitenant networks, where, for example, multiple SDN controllers act together for managing the network's control plane. In particular, the enabler will account for the westbound and eastbound APIs of a controller.

Complementary to extending the access control to other network abstractions and APIs, we recommend to provide a trustworthy reference monitor, which is however not in the scope of the project. Note that the simplicity of the access control scheme supports its trustworthiness as a reference with a small code base can be verified and certified. However, the verification and certification of the reference monitor is not in this task of the project. Nevertheless, we want to point out that the trustworthiness of a reference monitor overlaps with enablers in scope of Trust area and detailed in Section 44.

6.3 Security Enabler "Component-Interaction Audits"

6.3.1 Product Vision

A network comprises various types of components, e.g., endhosts and switches, and a controller in case of an SDN network. The network components interact with each other in one way or the other. For example, in an SDN network, the controller interacts with the switches by sending and receiving messages according to the OpenFlow protocol. How components must and must not interact with each other is often stipulated by policies. There is a wide spectrum of policies, targeting various aspects of a network like correctness, performance, reliability, and security. Note that these aspects are not necessarily disjoint. In addition to policies, workflows may specify how, e.g., an SDN controller must react to events that trigger the reconfiguration of network components. Policies and workflows can be stated at different levels of abstractions.

The proposed security enabler checks compliance of the interactions concerning the network management between components in networks with respect to a given policy or workflow. The enabler checks policy compliance or workflow compliance either at runtime or offline during an audit. For online checks, whenever a network component performs an action relevant for the configuration of the network, it must send a corresponding message to the compliance checker about the performed action. For an offline audit, each network component must log its relevant actions, which are later collected, merged with the logs of the other components, and inspected by the compliance checker during the audit.

One focus of the enabler is SDN networks and the OpenFlow protocol. Recall from Section 6.26.2 that SDN will play a major role in managing 5G networks and a wide range of network services will be provided by network applications that run at the network's control plane on top of the SDN controller. In the online case, the compliance checker can here be understood as a monitor that checks compliance of security policies about the exchanged OpenFlow messages between network components in an SDN network. In addition to SDN and OpenFlow, the enabler focuses on policies and workflows for NFVs and their reconfigurations.

We remark that the proposed security enabler in this section complements the security enabler proposed in Section 6.2~~6.2~~. The enabler of this section focuses on ongoing interactions between network components. It *checks* their compliance with respect of a given policy and *reports* the policy violations. In contrast, the enabler in Section 6.2~~6.2~~ grants or prevents a request of a network component of accessing network resources. It *enforces* a given access control policy (Schneider, 2000). In general, policy compliance checking is an "easier" problem than policy enforcement. Hence, the enabler in this section targets a wider range of policies than the enabler in Section 6.2~~6.2~~. In particular, it accounts for policies that stipulate requirements and regulations on how network components should and must not interact with each other. Furthermore, the compliance check supports external offline audits.

A simple policy on the interaction of network components in an SDN network, which is in the scope of this enabler but not of the enabler in Section 6.2~~6.2~~ is that network flows from 1.2.3.4 to 5.6.7.8 must be established quickly. More concretely and in terms of OpenFlow messages, this policy stipulates that whenever the controller receives an OFPT_PACKET_IN OpenFlow message from a switch for a packet with source address 1.2.3.4 and destination address 5.6.7.8, then all the relevant switches must receive—within 10ms—corresponding OFPT_FLOW_MOD OpenFlow messages that establish the network flow. Another policy example is that whenever the master controller of the SDN network is down then within 50ms a new master controller is elected among the slave controllers.

The relevant uses cases from (5G-ENSURE Consortium, 2016) of this enabler's feature (see Section 6.3.2~~6.3.2~~) are listed in the following table.

Table 20: Mapping between enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case(s)
Basic OpenFlow Compliance Checker	• Adding a 5G node to a virtualized core network (Use Case 5.2) • Verification of the virtualized node and the virtualization platform (Use Case 5.4)
Basic NFV Reconfiguration Compliance Checker	• Adding a 5G node to a virtualized core network (Use Case 5.2) • Verification of the virtualized node and the virtualization platform (Use Case 5.4)

6.3.2 Features achieved

This security enabler comprises the following two features, which we describe below. The first feature of this security enabler targets SDN networks. Its development already started in the first year of the project and wascontinued in the project's second year.

- **Feature name:** Basic OpenFlow Compliance Checker.
- **Goal:** Verification of the interaction between multiple network components with respect to policies about the components' exchanged OpenFlow messages.
- **Description:** The Basic OpenFlow Compliance Checker is an additional component at the network's control plane. The network components (e.g., controller, switches, and network applications) are instrumented such that they send messages to the compliance checker whenever they receive and send OpenFlow messages. Alternatively, the network components can provide logs about the sending and reception of the exchanged OpenFlow messages. The Basic OpenFlow Compliance Checker processes these messages from the network components and checks whether they comply

with the given policy, provided by the network operator. In case of a violation, the compliance checker outputs a warning, e.g., it sends a corresponding message to the network operator.

- **Rationale:** SDN networks comprise several components, which interact with each other. Furthermore, these components use different network abstractions. Identifying non policy compliant behavior about the components' interactions across different network layers makes a network less vulnerable to intended or unintended misconfigurations.

A first running prototype of the Basic OpenFlow Compliance Checker was developed in the first year of the project. It was evaluated in a Mininet (Lantz, Heller, & McKeown, 2010) (Mininet: an instant virtual network on your laptop) environment, identifying performance bottlenecks. In the second year of the project, we focused on optimizing the compliance checker to overcome the bottlenecks we identified in with our evaluation in the first year.

The second feature of this security enabler is as follow. It was developed in the second year of the project.

- **Feature name:** Basic NFV Reconfiguration Compliance Checker.
- **Goal:** Verification of reconfigurations on NFV deployments with respect to policies or workflows.
- **Description:** The Basic NFV Reconfiguration Compliance Checker is similar to the Basic OpenFlow Compliance Checker. However, it targets VNFs and their reconfigurations. Namely, it receives the actions performed by other network components that concern the reconfiguration of VNFs (e.g., the NFV orchestrator and the virtualization environment). This compliance checker processes the received messages (either online or offline) and checks whether these actions are compliant with respect to given policies or workflows, provided by the network operator. In case of a violation, the compliance checker outputs a warning, e.g., it informs the network operator.
- **Rationale:** Various VNFs with different requirements will be managed in a 5G network by an orchestrator entity. Such an orchestrator will act upon triggers that, e.g., request the starting, terminating, and migrating of VNFs. The orchestrator actions must comply with policies or workflows. This feature will identify incompliant behavior to triggers by the orchestrator, making a network less vulnerable to intended or unintended misconfigurations.

This feature comprised a proof-of-concept of the compliance checker of the basic NFV reconfiguration that is able to check the compliance of simple workflows for reconfiguring VNFs. To this end, we instrumented Docker (Docker - Build, Ship, and Run Any App, Anywhere) to send messages to the compliance checker about the performed actions that are relevant for containers that host VNFs. Furthermore, we provided a simple NFV orchestrator that also sends messages about its performed actions to the compliance checker.

6.3.3 Recommendations for Further Research

Additional features can be added to the enabler's prototype, e.g., a more expressive policy specification language, accounting for different APIs. The extensions canalso account for different network abstractions. Furthermore, algorithmic improvements are a continuous effort for this enabler.

Additional mechanisms for the trustworthiness of the messages sent to the compliance checker are needed, e.g., mechanisms that guarantee the integrity of the messages. Note that it does not suffice to only provide a secure channel from a monitored component to the compliance checker. A malicious component could still suppress the sending of a message about its action performed. The component could even misinform the compliance checker about the component's actions by sending bogus messages. Potential solutions could be based on trusted computing technologies and remote attestation.

6.4 Security Enabler "Micro-segmentation"

6.4.1 Product Vision

The security enabler described in this section is a network management enabler for single and multi-domain software networks that will facilitate dynamic arrangement of micro-segmentation, i.e., creation deletion, of micro-segments. With micro-segmentation, it would be possible to create secure segments where more granular access controls and stricter security policies can be enforced.

The Network Slice concept has been recently introduced for the upcoming 5G mobile networks and it is considered to be an integral part of 5G. Network slice is a logical instantiation of a network, with all the needed functionalities. In the context of 5G, micro-segments can be considered as isolated parts of the 5G network dedicated for particular application services or users. Compared to network slices, micro-segments can provide more fine grained isolation and segmentation, specific access controls and tuned security policies based on unique trust models of respective use cases and application services. A micro-segment instance is not necessarily required to form a complete logical network. By focusing on smaller, less heterogeneous parts in the network, better accuracy can be achieved for e.g. anomaly detection.

Within the mobile network, the minimum requirements could be to include virtualized instances of both the Serving Gateway (SGW) gateway and the Policy Control Resource Function (PCRF) in a network slice or micro-segment (Ericsson, 2014). For applications or services requiring Internet access, the network slice or micro-segment should include also the Packet Data Network (PDN) gateway (PGW). For applications requiring mobility, Mobile Management Entity (MME) and SGW is needed. Each slice or micro-segment could also have its own AAA entity. All these entities would be virtualized resources or functions.

Figure 16 shows an example of the micro-segmentation approach in a single domain (single operator) that could be built on top of existing 4G architecture. Network slices and micro-segments are created by the use of virtualization. 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 is typically 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 domain, the segments should typically lay within a single network slice.

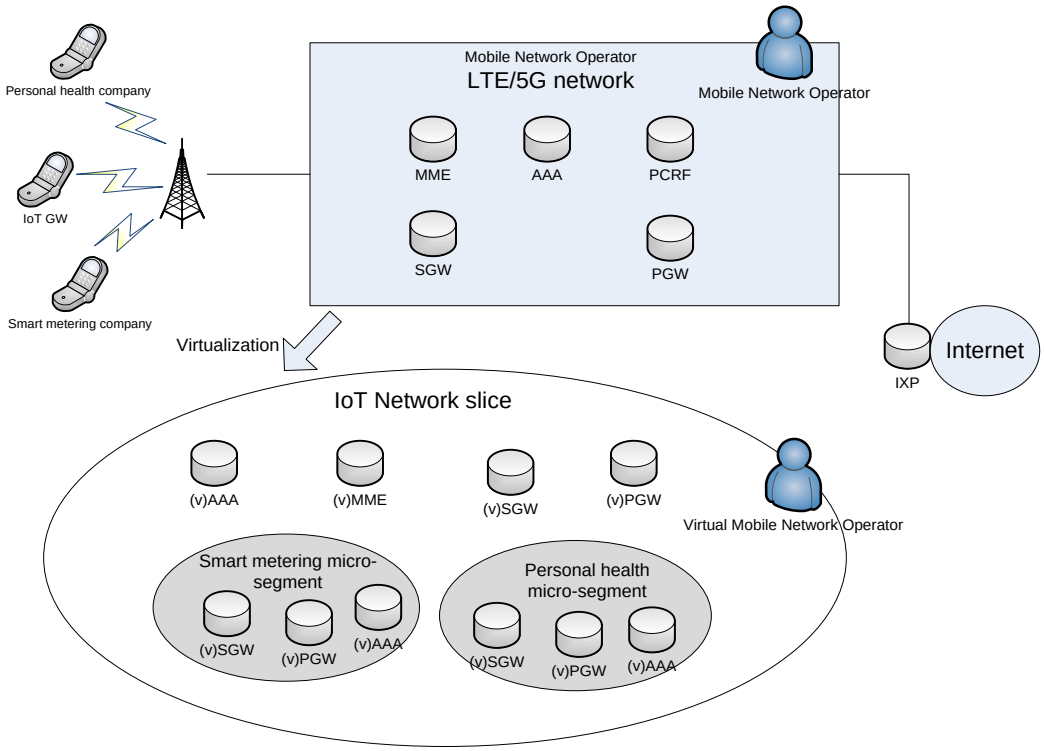


Figure 16 Micro-segmentation in a single domain network

In a multi-domain/multi-operator setting, end-to-end security could be achieved by chaining micro-segments from multiple network slices. Figure 17~~Figure 17~~ depicts an example of how micro-segmentation might be deployed in a multi-domain network based on the existing 4G architecture. There are two network slices: one located in the city of Helsinki, and one in the city of Oulu. In both network slices there is a micro-segment for "Personal Health". The two micro-segments could be chained together by the use of VPN or IPSec to provide end-to-end security. VMNO may have control over both network slices.

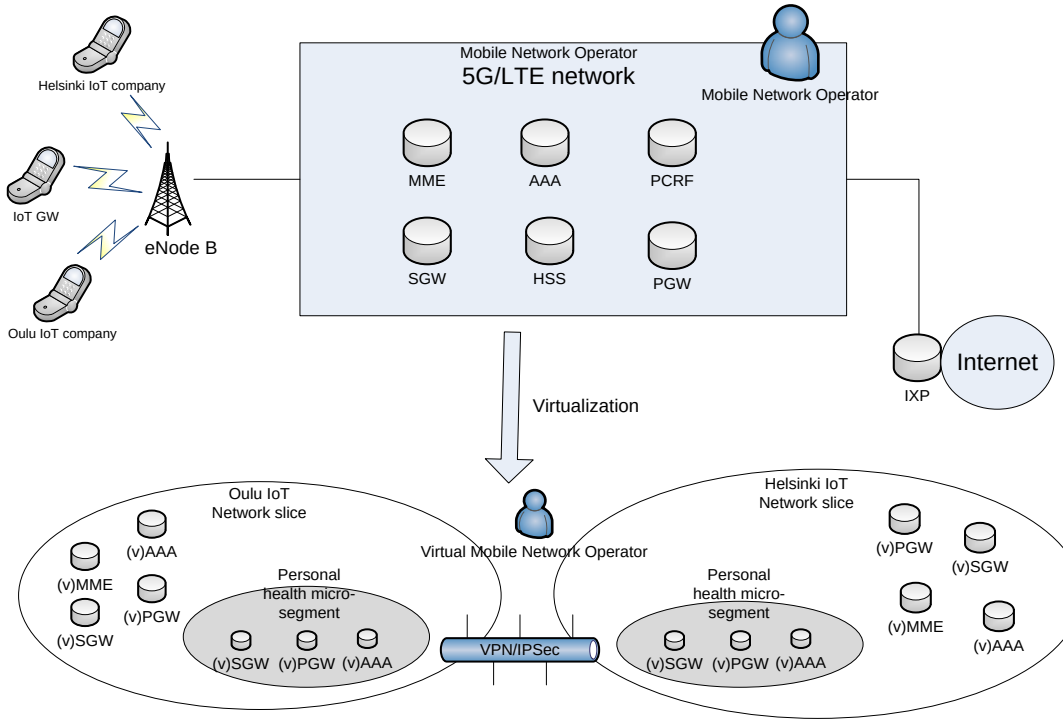


Figure 17 Micro-segmentation in a multi-domain network

Micro-segmentation could be a good security solution especially to mMTC, M2M or Industrial Internet based companies, which require a high level of security for their application services and service isolation. Also 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 also used to provide customers with micro-segments that have different security levels depending on the used service. For example, 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.

Micro-segmentation needs to take into account different trust models for different micro-segments. Some micro-segments may require a 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. Such a trust model can be, e.g., provided to micro-segments with critical services. Such a case could be an authority network in a crisis situation, in which trust would not be self-evident and the micro-segment should be highly secure. A suitable trust model shall be developed for the enabler that incorporates network segmentation based on different trust levels. This trust model will be utilized together with this enabler.

The following table shows the mapping between the enabler security features and the uses cases which are relevant for the enabler. As the enabler uses virtualization and is related to network slicing, two directly related use cases are Virtualized core networks and network slicing (Use Case 5.1) and Adding a 5G Node to a Virtualized Core Network (Use Case 5.2). For the second release, Use Case 5.5: Control and Monitoring of Slice by Service Provider is also relevant.

Table 21 Mapping between enabler security features and relevant use cases.

Enabler Security Feature	**Relevant Use Case**
Dynamic arrangement of Micro-Segments (R1)	Use Case 5.1: Virtualized core networks and network slicing Use Case 5.2: Adding a 5G node to a virtualized core network
Extended Northbound API (R2)	Use Case 5.1: Virtualized core networks and network slicing Use Case 5.2: Adding a 5G node to a virtualized core network Use Case 5.5: Control and Monitoring of Slice by Service Provider
Adding support for multi-domain micro-segments (R2)	Use Case 5.1: Virtualized core networks and network slicing Use Case 5.2: Adding a 5G node to a virtualized core network

The implementation of 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. We shall also analyze where to implement micro-segmentation in the mobile network architecture and what kind of threats can be solved by micro-segmentation.

6.4.2 Features achieved

The implementation of the first release (R1) was done in a single domain, using virtualized switches and IEEE 802.1X access control. The development started in the first year of the project and wascontinued in the second year of the project.

Through the first release (i.e. R1), the following feature was in scope and achieved:

- **Feature name:** Dynamic arrangement of Micro-Segments
- **Goal:** Enable dynamic arrangement (create, delete) of micro-segments in the network.
- **Description:** Implementation of micro-segmentation in an SDN environment. Micro-segmentation requires isolated parts of the mobile network, which are dedicated for particular services or users. The isolation is possible by the use of SDN and virtualization technology. Each micro-segment is a virtualized instantiation of the network and SDN is used for controlling that micro-segment.
- **Rationale:** Enable dynamic arrangement (create, delete) of micro-segments, i.e., smaller parts of the network so that monitoring of anomalous behavior or threats and responding to them would be easier.
- **Roadmap:** A first running prototype of the Micro-segmentation enabler was developed in the first year of the project. It was evaluated in a Mininet (Lantz, Heller, & McKeown, 2010) (Mininet: an instant virtual network on your laptop) environment and used IEEE 802.1X access control. The prototype used OpenVirtex (OpenVirteX Network Virtualization Platform) software based virtualization and Ryu SDN controller (Ryu SDN Framework).

The second release (R2) of this security enabler focused on the following two additional features:

- **Feature name:** Extended Northbound API
- **Goal:** Northbound micro-segmentation API extension
- **Description:** The northbound micro-segmentation API is extended, which makes it possible for other security enablers, namely **Security Monitor for 5G Micro-Segments** and **Trust Metric**, to utilize micro-segments.
- **Rationale:** Security Monitoring can include specific methods for monitoring micro-segments and responding to threats and anomalous behavior. By opening up northbound interfaces and publishing monitoring data it is thus possible to dynamically control micro-segments. The Trust Metric enabler is able to compute a trust metric value for a dynamic micro-segment in real time using monitoring data.

- **Feature name:** Support for multi-domain micro-segments
- **Goal:** Add support for multi-domain micro-segments and include secure communication between two micro-segments (and different operators).
- **Description:** This feature will add support for micro-segments located in different domains and a secure communication between the micro-segments.
- **Rationale:** The first release was done in a single domain. Micro-segments can, however, reside in different domains and support for them is needed. Also, the communication between the micro-segments needs to be secure.

6.4.3 Recommendations for Further Research

Micro-segmentation as a Docker container services – Possible approach for further research would be to include the micro-segmentation approach running as a service in a Docker container. This means that

micro-segmentation would be one micro-service that can be part of a complete security service. Other security micro-services could be encryption, access control, and security monitoring.

Micro-segmentation for 5G Mobile Edge Computing – Micro-segmentation approach could be part of 5G Mobile Edge Computing, in which there is an entity, such as a server or group of servers, located between the base station (eNodeB) and the core network. This entity brings the mobile network functions closer to the edge of the network and user. In this way, it is possible to enhance the performance of the applications and reduce the delay. Micro-segmentation could thus be a single Mobile Edge Computing application to ensure the security of a certain service.

6.5 Security Enabler "Bootstrapping Trust"

6.5.1 Product Vision

The SDN architectural approach – which is expected to be widely used in 5G network deployments – challenges many of the network infrastructure rules and best practices that have evolved over the previous decades. Likewise, many security best practices are becoming obsolete and must be adapted to the SDN model, in order to adjust to the emerging risk factors and threat vectors. New risk factors are introduced through the proliferation of virtual network components (such as *virtual switches and virtual network functions*) executing on full-fledged commodity operating systems (OS), often assigned the same trust level and privileges as specialized, hardware network components with compact embedded software. Considering that commodity OS with large code bases are likely to contain multiple exploitable security flaws, such components can be attacked and modified to *not* follow the protocol, manipulate traffic and hijack other network edge components or even the entire SDN deployment [1].

This enabler addresses attacks on network components by attesting the integrity of data plane components and virtual network functions prior to enrolling them into the SDN deployment. Attestation in this context means measuring and reliably recording the security configuration of the component – done by a trusted computing base – and reporting the measurement to a verifier for inspection. Furthermore, this enabler protects authenticity, confidentiality and integrity of control plane communication, by facilitating the deployment of secure communication channels among the SDN components. The enabler consists of a suite of protocols and additional software components, which can either be deployed independently, or integrated as a module of deployment orchestrators or network controllers. The high-level security features of this enabler, as well as the corresponding use cases identified in the deliverable D2.1 "Use Cases", are shown in Table 22 while a high-level architecture is presented in Figure 18.

This enabler prepares the foundation for secure execution combined with protected end-to-end communication in a cloud environment, which relies on a hardware root of trust (RoT), verifiable by an external authority. In this context, a *hardware RoT* means a minimal trusted computing base implemented in either a discrete specialized hardware component or integrated into the platform CPU. The RoT is responsible for measurement and recording of the component integrity, cryptographic operations as well as storage of cryptographic material.

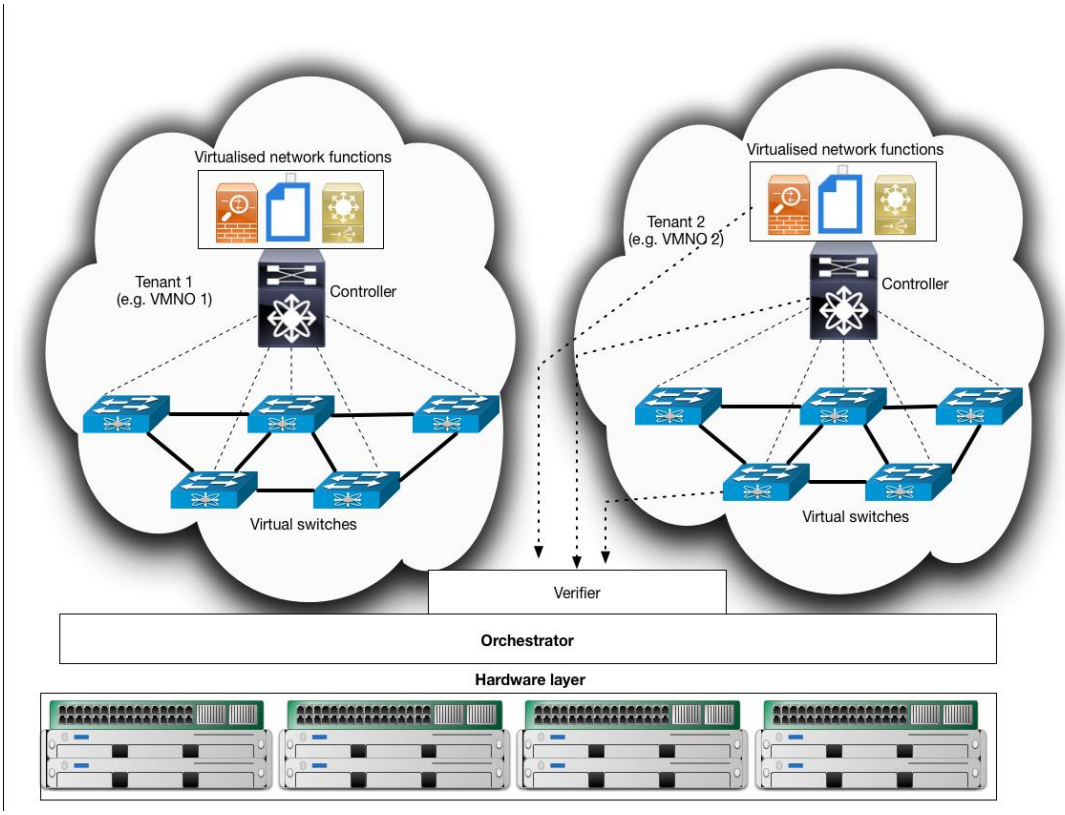


Figure 18: Integrity verification of virtual network components.

Furthermore, **this enabler strengthens the isolation between network slices,** by allowing the network infrastructure provider to verify that the configurations of the deployed network management components belong to the set of configurations defined by a pre-determined policy. For example: a traffic shaper virtual network function (VNF) enabled for a Virtualized Mobile Network Operator (VMNO) *A* may only have the configurations *C = {TS-A.1, TS-A.2, TS-A.3}*. Assume VMNO *A* attempts to redeploy the virtual network component, with a new configuration (potentially with extended capabilities) *TS-A.4;* the Virtualized Infrastructure Provider would then be able to observe that the reported configuration **is not** one of the allowed configurations – i.e. does not belong to the set *C* – and invalidate the actions of the VMNO.

Table 22 Mapping between enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case(s)
Integrity Attestation of Virtual Switches	• Adding a 5G node to a virtualized core network (Use Case 5.2) • Verification of the virtualized node and the virtualization platform (Use Case 5.4)
Integrity Attestation of Virtual Network Functions	• Virtualized Core Networks, and Network (Use Case 5.1)

6.5.2 Features achieved

- **Feature name:** Integrity Attestation of virtual switches.
- **Goal:** Verification of the virtual switch configuration using trust agents running in trusted execution environments.
  Description: A trust agent running in a trusted execution environment verifies the integrity of certain specified, security-critical software components (assets) on platforms hosting the virtual

switches in the tenant's domain. Assets may include virtual switch binaries, kernel modules, libraries and related configuration files, etc. Measurement, verification and remote attestation is done before the network controller enrolls the virtual switches into the SDN deployment.
Integrity measurement can be implemented using an open-source tool – such as the *Linux Integrity Architecture* utility or similar – and will be limited to detecting *modifications* of the assets compared to an initially known state, recorded at deployment time. The trust agent can run in an isolated execution environment, such as the ones enabled by Intel SGX. Additional software components – such as a security orchestrator for integrity attestation of platforms and virtual switches prior to enrollment in the deployment – may need to be developed or extended based on existing software.
This enabler aims to detect alteration attacks on the assets, ensuring that they not have been modified since deployment time.

- **Rationale:** SDN deployments may become dysfunctional if managed by a network controller with a distorted view of the network topology, caused by malicious virtual switches enrolled into the deployment, or by spoofed network management commands. Furthermore, malicious virtual switches can compromise the network controller (Thimmaraju, et al., 2016). Hence, it is essential to verify the integrity of virtual switches and related assets prior to enrollment in the SDN deployment, similar to the principles introduced in (Paladi & Gehrmann, 2016).
- **Roadmap:** A first limited prototype of the *Bootstrapping Trust* enabler that validates the concept was developed in the first year of the project. The first release made use of hardware emulation for SGX, called OpenSGX [5], due to the unavailability of an official SDK.

The second feature of this security enabler is described below. It has beendeveloped in the context of the second release (R2), planned for the second year of the project.

- **Feature name:** Integrity Attestation of VNFs running in Docker containers.
- **Goal:** Verification of VNF container integrity using trusted agents running in trusted execution environments.
  Description: The *Integrity Attestation of VNFs* feature is similar to the *Integrity Attestation of virtual switches* feature, but targeting VNFs deployed in lightweight virtualization containers. The goal of this feature is to verify the integrity of specified, security-critical software components (assets) on platforms hosting the lightweight containers with NVFs. Such assets may include lightweight virtualization isolation code and data (such as kernel configuration options or cgroups configuration files), lightweight virtualization middleware and configuration files, already deployed containers with VNFs, etc. Integrity measurement can be implemented using an open-source tool – such as the *Linux Integrity Architecture* utility or similar – and will be limited to detecting *modifications* of the software switch binaries compared to an initially known state. An integrity verification agent can run in a trusted execution environment – such as the ones enabled by Intel SGX – and verify the measurements of the assets against a whitelist provided by the security orchestrator. Before enrolment, the security orchestrator remotely attests the verification agent and queries the integrity verification result to establish trust in distinct VNF containers.
  This enabler aims to detect alteration attacks on VNFs, related configuration files and lightweight isolation infrastructure, ensuring that the assets have not been modified since deployment time.
- **Rationale:** Malicious VNFs enrolled with an SDN controller have the potential to incur significant damage to the entire SDN deployment. Furthermore, devastating attacks on the SDN deployment infrastructure – such as described in (Thimmaraju, et al., 2016) – cannot be excluded, considering that the northbound API is less mature than the OpenFlow protocol commonly adopted as the southbound API. It is therefore necessary to verify the integrity of both the lightweight virtualization isolation layer and of the VNF containers prior to enrolling the VNFs into the network deployment. *Integrity Attestation of VNFs* can check the integrity of specified assets and communicate the result through a secure channel to the network controller.

- **Roadmap:** A prototype was developed during the second year of the project. It focuses on the *Integrity Attestation of VNFs and* is able to verify the integrity of a limited set of assets and reliably report the verification results to the security orchestrator. To this end, the prototype measures security-critical Docker assets using Linux IMA, verifies them using a trust agent running in an SGX isolated execution environment, and reports the verification results to a security orchestrator.

6.5.3 Recommendations for Further Research

Improved versions of the enabler can be further developed and integrated with one of the popular SDN controllers, such as ONOS or Floodlight. A primary goal for future releases is to combine authentication of components in the data plane with integrity measurement and distribution of keys to protect confidentiality and integrity of information, by e.g. sealing keys to the integrity configuration of trust agent.

- **Feature name:** Shielding controllers from malicious data planes
- **Goal:** Sanitize – in a secure execution environment – all packets sent to the controller from the data plane components (e.g. switches/virtual switches).
- **Description:** In order to protect the network controller from potentially malicious packets issues by network data plane elements (switches), all traffic must be sanitized and verified to conform to the OpenFlow protocol prior to reaching the network controller. This can be done by deploying trusted agents on the virtual switch hosts that can verify switch-issued traffic before it reaches the controller.
- **Rationale:** Recent attacks (Thimmaraju, et al., 2016) have shown that in the SDN model the data plane – and eventually the control plane -- can be compromised by an unsophisticated attacker with limited resources. Given the central importance of the network controller in the SDN model, there is a need for additional layers of protection between the data plane and the control plane

- **Feature name:** Intra-domain data plane protection
- **Goal:** Contain compromise of data plane components
- **Description:** In order to protect the data plane in the event of a virtual switch compromise, there is a need to increase intra-domain network security, by e.g. identifying mechanisms to securely open and share network services, components and resources between multiple security availability zones of the network deployment.
- **Rationale:** Recent attacks (Thimmaraju, et al., 2016) have shown that in the SDN model the data plane – and eventually the control plane -- can be compromised by an unsophisticated attacker with limited resources. Data plane components – such as virtual switches have currently little or no protection against neighbor malicious virtual switches. It is therefore important to limit the extent of a potential data plane component compromise.

6.6 Security Enabler "Flow Control: in-network Threat Detection and Mitigation for Critical Functions in Virtual Networks"

6.6.1 Product Vision

5G will greatly benefit from the concept of Network Functions Virtualization (NFV) to make the provisioning of new services more flexible, detaching network providers from hardware appliances, and reducing CAPEX and OPEX. NFV coupled with other 5G enabling technologies, such as SDN and cloud computing, will greatly contribute in alleviating these problems. NFV capitalizes on virtualization technologies by abstracting software applications from the real hardware used to make them work, thus making them deployable network-wide by demand **without the need for new specialized hardware**. Typical applications that can be deployed through NFV are: firewalls, CDNs, NATs, DPI probes, VPN, IMS, and packet gateways.

However, when deploying VNFs, network operators should take into account the security threats that come with and that may severely affect them, given also that the virtualized applications may run over data centres not directly owned by them. The introduction of new logical elements such as service orchestrators and hypervisor represent **vulnerability points** that can be exploited by attackers to severely harm overall network functionalities. For some critical network functions, such as firewalling, load balancing and packet gateway, an attack may have a catastrophic impact, taking down most of the network functionalities. Among the approaches to make virtual networks more robust to attacks, one proposes to proactively adopt proper means to minimize network disruptions and data loss in the case of attacks.

The security enabler described in this section **applies a flow control for in-network threat detection and mitigation for critical functions in virtual networks**, by protecting the VNFs at runtime from malicious network-based attacks that can severely harm the proper functioning of the overall network. To this end, the security enabler proposes an ***enhanced Virtual Switches (eVS)*** embedding the capability to protect the virtual network interfaces of critical VNFs. In particular, *eVSs* are capable of automatically detecting network-based security threats and act appropriately to minimize their impact i.e., applying flow control (e.g. rate limiting), black holing or discarding certain flows.

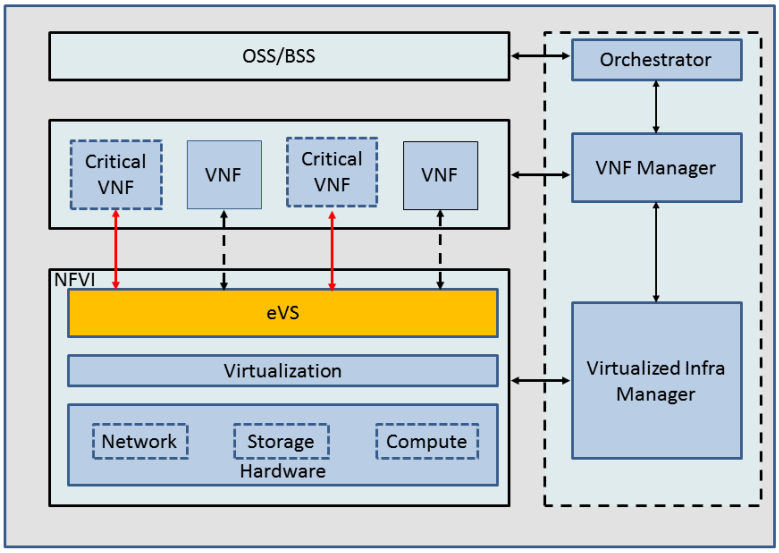


Figure 19: ETSI NFV Architectural framework comprising an eVS protecting critical VNFs from network-based threats.

Table 23 Mapping between enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case(s)
Detection of malicious behaviours in virtual networks	Verification of the Virtualized Node and the Virtualization Platform (Use Case 5.4)
Mitigation of detected network threats	Verification of the Virtualized Node and the Virtualization Platform (Use Case 5.4)

6.6.2 Features achieved in R1

None since this enabler was only planned for second release (i.e. R2).

6.6.3 Features achieved in R2

- **Feature name:** Detection of malicious behaviours in virtual networks.
- **Goal:** Detection of malicious network-based attacks.
- **Description:** The proposed enabler is a virtualized function operating to detect threats on the network's data plane. The *eVS* is instrumented by the network controller in order to automatically detect network-based security threats. The detection software deployed in *eVS* processes network messages and automatically checks whether they comply with a given security policy provided by the network controller.
- **Rationale:** VNFs could be harmed by malicious network-based attacks. Furthermore, some VNFs are critical for the overall network functions. For some network functions, such as firewalling, load balancing and packet gateway, an attack may have a catastrophic impact, taking down most of the network functionalities. Identifying network-based menaces without resorting to a continuous supervision by the network controller makes the virtual network less vulnerable and more responsive to network-based threats.

The second feature of this security enabler is described below. It works in conjunction with the detection enabler in order to react to the identified network threats.

- **Feature name:** Mitigation of detected network threats.
- **Goal:** Take actions to mitigate at runtime network-based attacks.
- **Description:** The proposed enabler permits to act appropriately whenever a menace is identified in order to minimize its impact on critical VNF. In case of one or multiple menaces detected by the detection enabler, the eVS automatically takes the mitigation mechanisms planned by the network operator (i.e., applying flow control, rate limiting, black holing or discarding certain flows).
- **Rationale:** Once identified as a menace, a threat must be processed by taking the most appropriate mitigation steps. For instance, malicious traffic originated by a distributed attack must be blocked without affecting legitimate traffic. Also, fast mitigation strategies must ensure and improve the service availability in case of core network functions.

The enabler is implemented, in order to be integrated with one of the most popular SDN controllers (Ryu).

6.6.4 Recommendations for Further Research

Further research is planned in order to study the best splitting of tasks and computations between the controller and the eVSs. While, the benefit of offloading tasks from the controller is evident, in order not to overload the control plane, data plane switching performance could be harmed by the additional burden required for threat detection. Moreover, threat detection can be improved whenever several eVSs are involved. In this case a refined orchestration policy should be studied at the controller.

6.7 Additional Enablers

The management of the network and its services will drastically change in 5G. One reason is that there will be multiple actors in the network, each of them possibly acting in different roles. Actors may also need to interact with each other to configure, orchestrate, and maintain network services. Another reason is that various and rich network services will be offered, some of them will be mission critical for verticals. Finally, the network services will be implemented through various virtualized network functions that will dynamically allocate and free network resources.

The security enablers of this task target to secure individual network services. For example, the micro-segmentation enabler allows one to isolate its service in the network and the bootstrapping trust enabler allows one to check the integrity of a network component or function. However, additional enablers will be required to securely manage chains of network services. Recall that such chains might comprise virtualized network functions that are interacting with each other and that are possibly operated by different actors.

For instance, a software update, a reconfiguration, or the migration of one of the virtualized network functions in the chain may have consequences on the security of the network service. These problems become even more challenging when network functions are outsources to third parties.

Network slices will play a dominant role in a 5G network. However, their technical implementation is far from trivial. Since a network slice will share physical hardware with other slices, additional security enablers will be needed that provide strong isolation and quality-of-service guarantees for each of these slices. For instance, information leakage between slices needs to be prevented.

Another consequence of the multi-domain character of 5G networks is that changes to the network state must be reliably traced to the originating actor both *prior* being applied (in order to verify their compliance to security policies) and afterwards (for forensics purposes or state rollbacks). Additional enablers will be required to implement the collection and reporting of traces.

Likewise, actors of a multi-domain network may have incompatible security policies with regards to the underlying resources, based on either their functional properties (e.g. hardware or software support for certain security functionality) or non-functional properties (e.g. policies with regards to security patching). Additional enablers will be needed both to implement an automated security classification of network resources and to implement their scheduling and utilization according to policies that take into account such a security classification.

7 Summary of Technical Roadmap final update

The section provides a global summary of all enablers released in scope of 5G-Ensure, and their features, both as delivered in the two software releases R1 and R2, and as recommended by the consortium to the wider 5G security community, beyond what have been released in the project.

First, the Table 24~~Table 24~~ below summarizes the final update of the 5G-ENSURE Technical Roadmap. It shows what has been in scope through the two successive releases and provides insights on what additional features and requirements need to be considered by anyone interested to further progress them. Indeed, this roadmap shows for each of the 5G security enablers in each of the categories addressed by the project (i.e. AAA, Privacy, Trust, Security Monitoring, and Network management & virtualization isolation) what was in scope of Release 1 versus Release 2. It shows that each of the enablers in scope of the project has been investigated and/or developed taking advantage of the two iterations proposed by the model (i.e. some enablers being continued between R1[6] & R2[7] whereas some others added and so fully new in R2) to deliver the features announced also recognized as of topmost priority.

Overall, the Table 24~~Table 24~~shows the extent and coverage of security-related enablers and their features that have been developed and released in scope of the 5G-ENSURE project. Moreover, it recommends feature extensions for those enablers, which can be developed in the future by stakeholders and interested parties.

[6] R1 aka Release 1 corresponds to the first software release of 5G-ENSURE enablers delivered by end of September 2016

[7] R2 aka Release 2 corresponds to the second software release of 5G-ENSURE enablers delivered by end of August2017

Table 24: 5G-ENSURE Technical Roadmap final update (reminding R1 and R2 features and providing insights on what could come next)

Category	Security enabler name	Security features		
		R1 features	**R2 features**	**Recommended features**
AAA	Basic AAA Enabler	Forward secrecy AAA aspects of trusted micro-segmentation	Forward secrecy AAA aspects of trusted micro-segmentation Trusted interconnect and authorization	Performance and security aspects of quantum immune algorithms for Perfect Forward Secrecy
	Internet of Things –IoT Enabler	Group authentication by extending the LTE-AKA protocol (Group-based AKA)	Group authentication by extending the LTE-AKA protocol (Group-based AKA) Non-USIM based AKA Bring Your Own Identity (BYOI)	Secure handover among different MMEs GBA bootstrapping context lifetime expiry
	Fine-grained Authorization Enabler	Basic authorization in satellite systems Basic distributed authorization enforcement for RCDs	AAA integration with satellite systems Authorization and authentication for RCD based on on-going IETF standardization Basic distributed authorization enforcement for RCDs based on existing web standards	Dynamic client and RCD registration protocols Security parameter lifecycle management for large IoT deployments
	Federative authentication context usage Enabler	None	Storage of authentication level Usage of authentication level	Evolve communication protocols to integrate authentication characterization and usage/exploitation
Privacy	Privacy Enhanced Identity Protection	Encryption of Long term identifiers (IMSI KPABE-based encryption)	Home network centric IMSI protection IMSI pseudonymization	Home network centric IMSI protection Authentication of identity requests and paging requests Authentication of radio signalling
	Device Identifiers Privacy	Enhanced privacy for network attachment protocols	Anonymous and optimized address selection for network attachment protocols	Geo-fencing for candidate network attachment address selection IPv6 support for the enabler with IPv6 network attachment protocols
	Device-based	None	Format preserving	Format preserving anonymization

	Anonymization		anonymization algorithm Privacy configuration	algorithm on the SIM or on the device's proprietary binary blob Privacy agent
	Privacy Policy Analysis	None	Privacy policy specification Privacy preferences specification Comparison of policies and preferences	Multi-layer privacy policy specification Collaborative / Composite sub-services privacy policy specification
Trust	Trust Builder Enabler	5G asset model v1 Graphical modelling tool v1	5G asset model v2 Graphical modelling tool v2 5G threat and trust knowledge base	Coupling with the system security state repository
	Trust Metric Enabler	Trust metric based network domain security policy management	Improved trust metric based on extended data	Anonymization and access control over shared trust metrics information Increasing trust towards metric provisioning
	VNF Certification Enabler	VNF trustworthiness evaluation	VNF trustworthiness certification	Most appropriate VNF selection feature
	Security Indicator Enabler	None	Security indicator subscriber display	Transparent security feature of serving network
	Reputation based on Root Cause Analysis for SDN	None	Root cause analysis for SDN	None
Security monitoring	System Security State Repository	Deployment model ontology	System Security State Repository service	Dynamic adaptation and risk handling
	Security Monitor for 5G Micro Segments	Complex event processing framework for security monitoring and inference	Risk-based adaptation of micro-segments Extended data gathering Cross-domain information exchange	Intelligent monitoring Extended monitoring coverage over 5G functions
	PulSAR: Proactive Security Analysis and Remediation	5G specific vulnerability schema	5G specific vulnerability schema implementation PulSAR interface with Generic Collector	Cyber-attacks at runtime requesting dynamic reconfiguration of VNFs
	Satellite Network Monitoring	Pseudo real-time monitoring Threat detection	Active security analysis Pre-emptive mitigation security actions	None
	Generic Collector Interface	Log and event processing	None	Generalization of GCI on each 5G components
	Malicious traffic Generator for 5G protocols	None	Hostile eNodeB and hostile user equipment emulation	Node

			Hostile client emulation	
Network management and virtualization isolation	Anti-fingerprinting	None	Controller-Switch interaction imitator	SDN-based Information leakage attack protection
	Access control mechanisms	Southbound reference monitor	Access requirements for VNF container resources	Higher-level network abstraction support West/East-bound SDN controllers APIs Trustworthy reference monitor
	Component interaction audits	Basic OpenFlow compliance checker	Basic NFV reconfiguration checker	Expressive policy specification language
	Micro-segmentation	Dynamic arrangement of Micro-Segments	Extended northbound API Support for multi-domain micro-segments	Micro-segmentation as a Docker container services Micro-segmentation for 5G Mobile Edge Computing
	Bootstrapping trust	Integrity attestation of virtual switches	Integrity attestation of VNFs running in Docker containers	Shielding controllers from malicious data planes Intra-domain data plane protection
	Flow control: in-network threat detection and mitigation for critical functions in virtual networks	Detection of malicious behaviours in virtual networks	Mitigation of detected network threats	Support for offloading of detection tasks from the controller to the enhanced virtual switches

To complement the final technical roadmap summarized in Table 24~~Table 24~~, Table 25~~Table 25~~summarizes the recommended new enablers that the consortium considers as of interest to the wider 5G security community following work achieved by 5G-ENSURE also advancement of the 5G Security Vision inherent to the work done. .

Table 25: Recommended new enablers per Category/Cluster

Category	Enablers description
AAA	- Enablers detailing security and trust for Vehicle-to-vehicle and vehicle-to-other communication
Privacy	- security services over encrypted traffic
Trust	further develop enablers that evidence “trustworthiness” of 5G systems at various level and make it actionable to make informed decision (automated or semi-automated).
Security monitoring	- Monitoring confidential traffic flows and provide mechanisms able to treat any kind of traffic, including **encrypted** traffic - Increasing trust towards monitored information
Network management and virtualization isolation	- Secure management of chains of network services that comprise virtual network functions operated by different actors - Strong isolation and quality of service guarantees among different network slices - Collection and reporting of traces coming from different 5G domains - Automated, policy-based security classification of network resources, and their scheduling and

	utilization

The last table gives the coverage of 5G-ENSURE security enablers with respect to Use Cases as anticipated and defined in D2.1. Overall it shows the wide coverage that 5G security enablers have in R2 through their developed features. Indeed, most of the clusters and use cases are covered with some being covered by enablers from various categories addressed.

Table 26: Use cases coverage of 5G-ENSURE security enablers in R2

Cluster	Use Case	Labeling	Supporting enablers
C1	UC1.1	Factory Device Identity Management for 5G Access	IoT Federative authentication context usage enabler Trust Builder Malicious traffic generator
	UC1.2	Using Enterprise Identity Management for Bootstrapping 5G Access	IoT Federative authentication context usage enabler Malicious traffic generator
	UC1.3	Satellite Identity Management for 5G Access	Fine-grained Authorization Enabler Federative authentication context usage enabler Malicious traffic generator
	UC1.4	MNO Identity Management Service	Federative authentication context usage enabler Malicious traffic generator
C2	UC2.1	Device Identity Privacy	Device Identifiers Privacy
	UC2.2	Subscriber Identity Privacy	Privacy Enhanced Identity Protection Device Identifiers Privacy
	UC2.3	Enhanced Communication Privacy	Basic AAA enablers Privacy Enhanced Identity Protection
C3	UC3.1	Authentication of IoT Devices in 5G	IoT Fine-grained Authorization Enabler Trust Builder Trust Metric Enabler
C4	UC4.1	Authorization in Resource-Constrained Devices Supported by 5G Network	Fine-grained Authorization Enabler Malicious traffic generator
	UC4.2	Authorization for End-to-End IP Connections	Fine-grained Authorization Enabler Access Control Mechanisms Malicious traffic generator
	UC4.3	Vehicle-to-Everything (V2X)	Malicious traffic generator
C5	UC5.1	Virtualized Core Networks, and Network Slicing	Basic AAA enablers Trust Builder System Security State Repository Micro-segmentation Bootstrapping Trust PulSAR: Proactive Security Analysis and Remediation Malicious traffic generator
	UC5.2	Adding a 5G Node to a Virtualized Core Network	VNF Certification Access Control Mechanisms Component-Interaction Audits Micro-segmentation Bootstrapping Trust Malicious traffic generator
	UC5.3	Reactive traffic routing in a virtualized core network	Anti-Fingerprinting Malicious traffic generator
	UC5.4	Verification of the Virtualized Node and the Virtualization Platform	VNF Certification System Security State Repository Security Monitor for 5G Micro-Segments Root Cause Analysis Component-Interaction Audits Bootstrapping Trust PulSAR: Proactive Security Analysis and Remediation Flow Control: in-network Threat Detection and Mitigation for Critical Functions in Virtual Networks Malicious traffic generator
	UC5.5	Control and Monitoring of Slice by Service Provider	Trust Builder Trust Metric Enabler VNF Certification System Security State Repository Generic Collector Interface Security Monitor for 5G Micro-Segments Reputation based on Root cause analysis for SDN Micro-segmentation Malicious traffic generator
	UC5.6	Integrated Satellite and Terrestrial Systems Monitor	Satellite Network Monitoring Malicious traffic generator
C6	UC6.1	Attach Request During Overload	Malicious traffic generator
	UC6.2	Unprotected User Plane on Radio Interface	Malicious traffic generator
C7	UC7.1	Unprotected Mobility Management Exposes Network for Denial of Service	Malicious traffic generator
C8	UC8.1	Satellite-Capable eNB	Satellite Network Monitoring
C9	UC9.1	Alternative Roaming in 5G; spoofing of signalling messages	Malicious traffic generator
	UC9.2	Privacy in Context-Aware Services; User traffic can be enriched in various way	Malicious traffic generator
	UC9.3	Authentication of New Network Elements	Basic AAA enablers Trust Builder Security Indicator Access Control Mechanisms Malicious traffic generator
C10	UC10.1 UC10.2 UC10.3	Botnet Mitigation Privacy Violation Mitigation SIM-based and/or Device-based Anonymization	Security Monitor for 5G Micro-Segments Privacy Policy Analysis Security Indicator Device-based Anonymization
C11		Lawful interception	Trust Builder

8 Open research directions

8.1 Consolidated 5G architecture for (renewed) security requirements

Due to the wide spectrum of 5G verticals and use cases, the 5G security architecture is expected to be "metamorphic" in essence, coping with diverse and frequently changing requirements from diverse verticals. Future work should extend the security architecture initiated in 5G-ENSURE, addressing new

challenging aspects such as high availability and resilience, while also embedding the following important characteristics:

- The 5G Security Architecture from 5G-ENSURE has significantly advanced the trust model towards a novel concept capturing and evaluating trustworthiness. The wider 5G research community is now required to further investigate metrics and solutions that assess the trust at different levels of the architecture (software, virtual resources, hardware, etc.) taking into account the multiple administrative domains that are involved in the offering of an end-to-end service.
- The 5G Security Architecture from 5G-ENSURE offers solutions to meet numerous security requirements that were discussed in the past, but never implemented. A notable example is the protection against IMSI-catching. Future work must leverage complementary solutions to ensure security and resilience for different verticals with potentially different requirements.
- The 5G Security Architecture from 5G-ENSURE comprises a number of security enablers that can run as independent, yet complimentary, modules. This modularization feature of the 5G Security architecture can largely help in customizing the security offerings as per the needs of verticals and across multiple administrative domains. This is a requirement that must be carefully addressed by the wider 5G research community.

The 5G-ENSURE consortium strongly recommends extending the 5G Security Architecture introduced in the project and most importantly shared and agreed with 5G-PPP Security and Architecture WGs , in order to sustain security while tailoring its features to the needs of verticals, and to leverage the challenges stemming for operations across multiple administrative domains.

8.2 End-to-end security and privacy guarantees

Providing end-to-end security for future 5G networks and services is very challenging. Multi-domain software networks, where physical infrastructures are shared, will be exposed to a larger attack surface, because of the new emerging control plane that will be subject to new software flaws and the heterogeneous implementation of software services across all domains. Software networks will also experience new failure modes at higher rates, which in part derive from the added complexity and the lack of unified control. In this scope, the advent of SDN/NFV technologies provides a unique opportunity to develop innovative management paradigms that release the full potential of the distributed control plane in order to dynamically manage and guarantee security despite the evolving security threats.

To further enrich and expand - *beyond what has been realized in 5G-ENSURE* - the end-to-end security and privacy requirements of 5G via secure and robust orchestration of network services, future work should advance the state of the art in multiple directions, including:

- The integrity of 5G services and their placement over heterogeneous, multi-domain physical platforms;
- Tying security to elementary services and automate the security provisioning mechanisms;
- Conciliating privacy and security monitoring requirements, through enabling value-added security services, such as threat diagnosis over encrypted traffic; and
- Advancing machine learning algorithms to enable proactive and fine-grained 5G threat detection and trust measurement.

8.3 High availability and resilience of multi-party 5G systems

Achieving resiliency and high availability in 5G systems is a challenging and complex problem. It mainly depends on different heterogeneous and decentralized devices/entities that may be owned and managed by multiple parties. Besides, while 5G networks promise to achieve unforeseen performances, dynamicity and complexity of these infrastructures makes anomaly detection very challenging in such environments. In particular, current anomaly detection and root cause diagnostic techniques consider per- component (VM) analysis and lack an end-to-end analysis of failures.

Future research should devise high-availability and fault-tolerance solutions to proactively detect and automatically contain the potential failures. In the event of a service failure, detection and remediation of the failure should be performed using automated policy-based mechanisms along with event correlation to detect the root cause. Moreover, advanced trust techniques should be leveraged at both hardware and VNF levels to ensure that 5G services are launched on trustworthy platforms, enhancing their resilience and ensuring their high availability. Note that resiliency and high availability must be studied as a multi-dimensional problem, and will need to integrate different techniques, spanning from mechanisms that ensure trust of the underlying infrastructure to SDN/NFV-based solutions that take into account the multi-tenancy and multi-domain features of 5G systems, and finally provision adequate VNF redundancy, placement, and chaining strategies to ensure a high level of availability.

9 Conclusion

This document provides the final update of the 5G-ENSURE security enablers Technical Roadmap. It reminds the features that were developed in scope of the project, and that were released at two stages through two software releases R1 and R2. More importantly, this document provides recommendations and further insights on future work to be conducted by interested parties and 5G Security community at large, and this based on the expertise and experience acquired by the consortium through participation to the phase 1 of the 5G-PPP.

We believe that this deliverable contribute to further advance the 5G Security Vision within the 5G-PPP community and beyond, taking advantage of the work performed at the project level, but also at the programme level, would it be through 5G-PPP Security Work group (e.g. Security WG Whitepaper) or other joint activities performed (e.g. ETSI or EuCNC workshop, Open consultation of 5G Security, …). Overall we claim this deliverable is actionable to further advance 5G security the way needed.

10 Bibliography

Hennebert , C., & Dos Santos, J. (2004). Security protocols and privacy issues into 6LoWPAN stack: A synthesis. *Internet of Things Journal, IEEE, 1(5):384–398.*

3GPP. (2008). *Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE).* 3GPP TR 33.82.

3GPP. (2016). *TS44.318 Generic Access Network (GAN); Mobile GAN interface layer 3 specification (Release 13) .* 3GPP.

5G-ENSURE. (2016). *Deliverable D2.1 - Use Cases.* Récupéré sur http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.1-UseCases.pdf

5G-ENSURE. (2016). *Deliverable D2.2 Trust Model (draft).* Récupéré sur http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.2-TrustModel.pdf

5G-ENSURE. (2016). *Deliverable D2.3 Risk Assessment, Mitigation and Requirements (draft).* Récupéré sur http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.3-RiskAssessmentMitigationRequirements.pdf

5G-Ensure Consortium. (2016). Deliverable 2.1 Use Cases. [Online]. Available: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.1-UseCases.pdf.

5G-ENSURE Consortium. (2016). Deliverable 2.1: Use Cases. [Online] Available: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.1-UseCases.pdf.

5G-ENSURE Consortium. (2016). Deliverable 3.1: 5G-PPP security enablers technical roadmap (early vision). [Online] Available: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D3.1-5G-PPPSecurityEnablersTechnicalRoadmap_early_vision.pdf.

5G-ENSURE Consortium. (2016). Deliverable 3.3: 5G-PPP security enabler software release (v1.0).

Aboba, B., Carlson, J., & Cheshire, S. (2006). Detecting Network Attachment in IPv4 (DNAv4). *RFC4436, IETF.*

Aboba, B., Carlson, J., & Cheshire, S. (2006). *Detecting Network Attachment in IPv4 (DNAv4). RFC 4436.* IETF.

Anderson, J. (1973). *Computer security technology planning study.* Technical Report ESD-TR-73-51, US Air Force Electronic System Devision.

Arkko, J., & Haverinen, H. (2006). *RFC4187 Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA).* IETF.

Berde, P., Geralo, M., Hart, J., Higuchi, Y., Kobayashi, M., Koide, T., et al. (2014). ONOS: Towards an open, distributed SDN OS. *Proceedings of the 3rd SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN).* ACM Press.

Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. *Proc. IEEE Symp. Security and Privacy (S&P '07).*

Bifulco, R., Cui, H., Karame, G. O., & Klaedtke, F. (2015). Fingerprinting software defined networks. *Proceedings of the 23rd International Conference on Network Protocols (ICNP).* IEEE Computer Society.

COWL. (s.d.). Récupéré sur http://w3c.github.io/webappsec-cowl/

Cui, H., Karame, G. O., Klaedtke, F., & Bifulco, R. (2015). *Fingerprinting of software-defined networks.* Récupéré sur http://arxiv.org/abs/1512.06585

Cui, H., Karame, G. O., Klaedtke, F., & Bifulco, R. (2016). On the fingerprinting of software-defined networks. *IEEE Transactions on Information Forensics and Security, 11*(10), 2160-2173.

Docker. (s.d.). Récupéré sur http://www.docker.com

Docker - Build, Ship, and Run Any App, Anywhere. (s.d.). Récupéré sur https://www.docker.com/

ElGamal, T. (1985). A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory 31 (4): 469-472.*

ELISS. (s.d.). *Regulatory Status of Lawful Interception in Italy*. Récupéré sur http://www.eliss.org/index.php/sicurezza-e-giustizia-regulatory-status-of-lawful-interception-in-italy-g-nazzaro/

Ericsson. (2014). *Network functions virtualization and software management.* Récupéré sur http://www.ericsson.com/res/docs/whitepapers/network-functions-virtualization-and-software-management.pdf

Foo Kune, N., Koelndorfer, J., & Kim, Y. (2013, August 8). *Location Leaks on the GSM Air Interface.* Récupéré sur http://www-users.cs.umn.edu/~foo/research/docs/fookune_ndss_gsm.pdf

Gemalto. (s.d.). Récupéré sur http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx

Giustolisi, R., Christian, G., Åhlstrom, M., & Holmberg, S. (2016). A Secure Group-Based AKA Protocol for Machine-Type Communications. *19th Annual International Conference on Information Security and Cryptology.* Seoul.

Gkounis, D., Klaedtke, F., Bifulco, R., & Karame, G. O. (2016). Cases for including a reference monitor to SDN. *Proceedings of the 2016 ACM SIGCOMM Conference*, (pp. 599-600).

Goyal, Pandey, Waters, & Sahai. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *ACM CCS'06.*

Hewlett Packard. (s.d.). *SDN App Store*. Récupéré sur https://saas.hpe.com/marketplace/sdn

Huffingtonb Post. (s.d.). Récupéré sur http://www.huffingtonpost.com/2013/10/24/nsa-world-leaders_n_4158922.html

J. Sanchez, I. G. (2014). “Softwarized 5G networks resiliency with self-healing. *1st Internation-al Conference on 5G for Ubiquitous Connectivity (5GU).*

J. Sanchez, I. G. (2015). “Self-Modeling Based Diagnosis of Software-Defined Networks. *1st IEEE Conference on Network Softwarization.* London.

J. Sanchez, I. G. (2016). “Self-Modeling based Diagnosis of Services over Programmable Networks. *2nd IEEE Conference on Network Softwarization.* Seoul, Korea.

J. Sanchez, I. G. (2016). THESARD: on The road to resiliencE in SoftwAre-defined network-ing thRough self-Diagnosis. *2nd IEEE Conference on Network Softwarization.* Seoul, Korea.

Klaedtke, F., Karame, G. O., Bifulco, R., & Cui, H. (2014). Access control for SDN controllers. *Proceedings of the 3rd SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN).* ACM Press.

Klaedtke, F., Karame, G. O., Bifulco, R., & Cui, H. (2015). Towards an access control scheme for accessing flows in SDN. *Proceedings of the 1st IEEE Confernce on Network Softwarization (NetSoft).* IEEE Computer Society.

Lantz, B., Heller, B., & McKeown, N. (2010). A network in a laptop: rapid prototyping for software-defined networks. *Proceedings of the 9th ACM Workshop on Hot Topics in Networks (HotNets).* ACM Press.

Luoto, M., Rautio, T., Ojanpera, T., & Makela, J. (2015). Distribueted decision engine - An information management architecture for autonomic wireless wetworking. *IFIP/IEEE International Symposium on Integrated Network Management*, (pp. 713-719).

Mantere, M., Sailio, M., & Noponen, S. (2014). A module for anomaly detection in ICS networks. In A. Press (Ed.), *the 3rd international conference on High confidence networked systems - HiCoNS '14*, (pp. 49–56). New York.

Mantere, M., Uusitalo, I., Sailio, M., & Noponen, S. (2012). Challenges of Machine Learning Based Monitoring for Industrial Control System Networks. In IEEE (Ed.), *26th International Conference on Advanced Information Networking and Applications Workshops*, (pp. . 968–972).

Mininet: an instant virtual network on your laptop. (s.d.). Récupéré sur http://mininet.org/

OASIS. (s.d.). *JSON Profile of XACML 3.0 Version 1.0*. Récupéré sur http://docs.oasis-open.org/xacml/xacml-json-http/v1.0/xacml-json-http-v1.0.html

ONOS - a new carrier-grade SDN network operating system designed for high availability, performance, scale-out. (s.d.). Récupéré sur http://onosproject.org/

Open Networking Foundation. (2012). *OpenFlow switch specification - version 1.3.0 (wire protocol 0x04).*

Open vSwitch - a production quality, multilayer virtual switch. (s.d.). Récupéré sur http://openvswitch.org/

OpenVirteX Network Virtualization Platform. (s.d.). Récupéré sur http://ovx.onlab.us/

Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. *Eurocrypt'99, LNCS 1592, pp.223-238.*

Paladi, N., & Gehrmann, C. (2016). TruSDN: Bootstrapping Trust in Cloud Network Infrastructure. *12th EAI International Conference on Security and Privacy in Communication Networks.*

Pfaff, B., Petit, J., Koponen, T., Amidon, K., Casado, M., & Shenker, S. (2009). Extending networking into the virtualization layer. *Proceedings of the 8th ACM Workshop on Hot Topics in Networks (HotNets).* ACM Press.

Podgursky, B. (s.d.). *GitHub - bpodgursky/jbool_expressions: jbool_expressions is a simple open-source library for creating and manipulating propositional logic expressions in java*. Récupéré sur https://github.com/bpodgursky/jbool_expressions

Privacy Level Agreements. (s.d.). Récupéré sur https://cloudsecurityalliance.org/group/privacy-level-agreement/

Ryu SDN Framework. (s.d.). Récupéré sur https://osrg.github.io/ryu/

Schneider, F. B. (2000). Enforceable security policies. *ACM Transactions on Information and System Security, 3*(1).

SDN Market Sizing. (2013). Récupéré sur https://www.sdxcentral.com/wp-content/uploads/2015/02/sdn-market-sizing-report-0413-4.pdf

Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., & Seifert, J. (2015). Practical attacks against privacy and availability in 4G/LTE mobile communication systems. *Cryptography and Security, arXiv:1510.07563.* Cornell University Library.

The Guardian. (s.d.). Récupéré sur The Guardian: http://www.theguardian.com/us-news/2015/feb/19/nsa-gchq-sim-card-billions-cellphones-hacking

The OpenDaylight Platform. (s.d.). Récupéré sur https://www.opendaylight.org/

The Register. (2015). *Did NSA, GCHQ steal the secret key in YOUR phone SIM? It's LIKELY.*

Thimmaraju, K., Shastry, B., Fiebig, T., Hetzelt, F., Seifert, J.-P., Feldmann, A., et al. (2016). *Reigns to the Cloud: Compromising Cloud Systems via the Data Plane.* arXiv.

Van den Broek, F., Verdult, R., & de Ruiter, J. (2015). Defeating IMSI Catchers. *ACM CCS 2015.*

Wright, J. (2009). Characterising Anonymity Systems. *York University.*

Xiaomi. (s.d.). *https://www.lowyat.net/2017/126154/xiaomi-unveils-surge-s1-soc/* . Consulté le 2017

A Annexes

A1.1 PulSAR 5G specific vulnerability schema

To explain shortly the extension of the Cyber-attack modelling schema, SDN and NFV bring new attack path types, due to three aspects:

- A centralized control plane
- A mutualized data plane
- 3-party interaction rule for VNF vulnerability exploitations: (NFV allows placing middle boxes between A and B, that can be targeted by the attacker)

We extended the classical IP based schema with specific concepts of links, orchestrators, VNF managers, VIM, hypervisors, to automatically generate a corresponding physical infrastructure to support virtual functions.

We identified seven additional rules to cope with these threats:

- VM on host + vuln in hypervisor + vulConsequence == privEscalation => exec code in hypervisor (host compromised):
    - If a VM runs on a host, and a vulnerability exists on the Hypervisor which enables privilege escalation, then malicious code can be executed on the hypervisor which compromises the host.
- exec code on host + VM runs on host => exec code on VM
    - If code can be executed on a host and a VM runs on that host, then malicious code can be executed on the VM.
- exec code on host + VM runs on host => read VM FS
    - If code can be executed on a host and a VM runs on that host, then the File System of the VM can be read.
- exec code on orchestrator + VM in orchestrator domain => exec code on VM
    - If code can be executed on an orchestrator and a VM is in the orchestrator domain, then malicious code can be executed on the VM.
- exec code on host1 + VM on flow host1->host2 + Vuln on VM + vulConsequence == privEscalation => exec code on VM
    - If code can be executed on host1, and a VM is on a flow between host1 and host2, and there is vulnerability on the VM which enables privilege escalation, then malicious code can be executed on the VM.
- exec code on host1 + vuln on vnf management protocol => exec code on vnfm
    - If code can be executed on host 1, and a vulnerability exist on the VNF Management protocol between the VM and the VNFM which enables privilege escalation, then malicious code can be executed on the VNFM.