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

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	30.11.2016	
Dissemination Level:	Public	
Lead beneficiary	Thales Services (TS)	Pascal Bisson, pascal.bisson@thalesgroup.com
Authors	VTT : Pekka Ruuska, Olli Mämmelä, Jani Suomalainen TS: Pascal Bisson, Cyrille Martins, Edith Felix, Theo Combe EAB: Mats Näslund, Håkan Englund ITInnov: Stephen C. Phillips, Stefanie Cox, Gianluca Correndo, Mike Surridge LMF: Bengt Sahlin, Patrik Salmela NEC: Felix Klaedtke Nixu: Tommi Pernilä Orange: Jean-Philippe Wary, Ghada Arfaoui SICS: Rosario Giustolisi, 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 D3.5 is the update of the 5G-ENSURE security enablers Technical Roadmap previously delivered (i.e. D3.1). Compared to previous deliverable which was only detailing the features of 5G security enablers in scope of the first release (i.e. v1.0 (R1) released on M11/Sep'16), D3.5 is more complete in the sense it provides all the details regarding enablers (either in continuation or fully new) in scope of the second (also last) release (v2.0 (R2) due at M22/Aug'17) detailing for each of them the targeted features, while showing excellent coverage they have, individually but most importantly conjointly, with respect use cases identified.

Overall D3.5 paves the way towards the second wave of 5G security enablers to be specified and then for most of them be software released by end of the project as part of v2.0.

It also contributes to further advance 5G Security Vision within 5G-PPP community and beyond.

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 D3.5 is the update of the Technical Roadmap previously delivered on M4 (i.e. D3.1) and which led to the delivery of the first software release of 5G-ENSURE Security enablers on Month 11 (Sep'16). As such D3.5 leverages on D3.1 and completes the product vision on 5G Security enablers in scope of 5G-ENSURE Project. Whereas D3.1 was providing an early vision of security enablers with details only regarding the features in scope of the first release, D3.5 provides product vision of each and every of the enablers either initiated in R1 and continued in R2, or fully new in R2 with all the details regarding their targeted features.

Those enablers will be fully specified in the next WP3 deliverable (i.e. D3.6 5G-PPP security enablers open specifications (v2.0)).

D3.5 (as D3.1 before) also takes advantage of deliverable D2.1 on Use Cases (issue on M2) to materialize relevance of enablers proposed in R2 with respect to use cases showing the broad coverage 5G-ENSURE enablers have achieved. It also feeds other WPs (especially WP2 & WP4) with information relevant in the context of their respective activities (e.g. security architecture, 5G security testbed).

Last but not least D3.5 targets to be a reference document to further increase exchanges and cross-fertilize within 5G-PPP (starting first with 5G-PPP Security WG) and beyond.

Disclaimer

Copyright notice

Contents

1 Introduction

This document provides an update of the Technical Roadmap previously delivered (namely D3.1) and which was scoping early description of security enablers and their features for the first release (namely R1). Deliverable D3.5 thus leverages and complements previous deliverable to provide Technical Roadmap with all the details regarding enablers in scope of the 5G-ENSURE project, adding to previous deliverable the enablers for second release (i.e. R2) and their planned features.

Whereas D3.1 was paving the way towards first software release of 5G-ENSURE security enablers (i.e. v1.0 delivered on M11/Sep'16), D3.5 targets the second and final release of them (i.e. v2.0 due M22/Aug'17).

Security enablers are presented as per categories defined within 5G-ENSURE and recognized by 5G-PPP Community as topmost priorities for 5G Security: Authentication, Authorization and Accountability (AAA); Privacy; Trust; Security Monitoring and Network management & virtualization isolation. They are also presented following a common template covering each of the following key aspects: product vision, technology area, security aspects, security challenges, technical roadmap (differentiating between achieved in R1 vs. planned for R2), recommendation for future work.

As such, this deliverable gives a complete overview of the enablers in scope of the 5G-ENSURE project, together with their rationale and their scheduling over the two major releases (reminded for R1/v1.0 and stated here for R2/v2.0). It also clearly shows the relevance of the enablers selected and their features from a Use Case perspective (here relying, although not uniquely, on 5G security use cases defined in D2.1).

Overall, this deliverable paves the way towards the second software release of 5G-ENSURE security enablers, whose open specifications will be one of the next steps. It also contributes to making further progress on 5G Security Vision through additions provided (i.e. new enablers, new detailed features), and also to the Technical Roadmap implementation that gives additional insights and shows progresses.

Last but not least, it also feeds the work of other WPs of the project (e.g. WP2 on Security Architecture where enablers could be mapped to building blocks envisaged; WP4 on Testbed to which it provides additional information on new enablers for the Testbed team to consider/adapt) and is also a source for further exchanges and cross-fertilization within 5G-PPP and beyond.

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 of security enablers in Release 2, also early plans for further technical work. This section is also the one that shows the coverage that 5G-ENSURE Security enablers in R2 have achieved with respect to the use cases defined in D2.1
- Section 8 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 [1]. 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 in T3.5, Network Management & Virtualization, 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 Technology Area

The Basic AAA enabler looks into security enhancement aspects of the existing AAA infrastructure utilized in third and fourth generation of 3GPP protocols. One area that will be studied is ways to recover from key compromise, e.g. on-line remote provisioning of new or updated long term keys. The second aspect of the enabler is focused on AAA aspects of trusted micro-segmentation in 5G networks. The third aspect is focused on improving authentication and authorization of inter-operator network communication.

2.1.3 Security Aspects

The forward security aspect primarily investigates three perspectives. The first is to limit effect of compromised keys in the temporal dimension, e.g. perfect forward secrecy. The second is to limit effect in spatial dimension, e.g. protect from passive attackers exploiting known keys. The final aspect is to consider recovery mechanisms.

The aim of the micro-segmentation is to divide the network into smaller parts, i.e., micro-segments so that monitoring of anomalous behaviour or threats and responding to them would be easier. This will likely also introduce new security aspects related to authentication, authorization and accounting. Secure authentication within each micro-segment should be possible and at the same time weak AAA solutions should be limited to be available only inside the particular micro-segment.

Authenticity of the interconnecting parties, i.e., operators, is required even in more dynamic setting. One cannot rely solely on the fact that messages are received on a certain network interface to be considered authentic. The message itself needs to include a way to securely identify the sender, and integrity, of the message. This is equally important in authorization, the authorization decision. Trust is an important aspect, as well, but it is not entirely a technical issue.

2.1.4 Security Challenges

The main challenge in the investigation of forward secrecy of AKA credentials lies in building a solution which does not add significant overhead, and is largely backwards compatible with the existing USIM AAA infrastructure. At some level, full backward compatibility may be difficult, but it shall nevertheless be a desired property.

Micro segmentation has similarities with the network slicing concept but it will provide more specific security services. Micro segments could be located inside a single network slice but it might also span over multiple slices through a hierarchical approach. If micro-segments are constructed using several slices, AAA aspects should also be considered. Due to this, utilisation of existing AAA solutions may not be

straightforward and new AAA solutions might be needed. The focus of this work will be on investigating if there are any issues related to AAA when micro-segmentation is introduced.

To achieve trustworthy interconnect and authorization, naming is important. However, the issue of who controls the naming arises. Like in the forward secrecy case above, it can be challenging to fully be backward compatible with the existing inter-operator AAA infrastructure, if new naming schemes are introduced. With simple naming schemes, binding authorizations to names might prove to be challenging.
From an architecture point of view, 5G networks' "distributed" realization approach (using cloud architecture principle) may imply challenges to maintain "synchronization" between AAA state across different locations within the network. However, this would mainly be an issue if control plane functionality is also to be distributed to the same degree as the user/traffic plane. While the enablers focus on functionality, they should to the extent possible ensure that the enablers can support a distributed implementation of the AAA control plane.

2.1.5 Features achieved in R1 (Reminder)

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

2.1.6 Technical Roadmap for Release 2 (R2)

Technical Roadmap for R2 of Basic AAA enabler includes both features continued from R1, which were not fully specified, and features specifically in scope of R2. No software release is planned 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

2.1.7 Early 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.

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 Technology Area

The IoT enabler provides new definitions of protocols for credential management and authentication of users and devices, such as sensors, actuators, and IoT devices in general. The enabler covers alternative authentication and key agreement protocols to the USIM based EPS-AKA procedure. The enabler investigates how such alternatives can be incorporated into the current protocols without causing major changes to the existing 3GPP transport protocols. As these devices are characterized by small size modules that embed low-power processors, limited memory and limited transmission capacities, the protocols are required to be as lightweight as possible.

To support new user categories, two main approaches to BYOI can be envisioned. One approach can be to simply allow enterprise AAA servers to be connected to a 5G access networks over an “S6-like” interface, i.e., the enterprise will basically act as a virtual mobile network operator (VMNO) for their own devices and users. As mentioned above, the enabler will investigate the technical solutions to enable third-party access. The second approach is to use already existing user/device credentials to bootstrap a 5G subscription, i.e., a USIM-credential. The exact technical realization of such an AAA interconnection to the operator network is for further study, but must obviously be performed to not jeopardize the security of the operator network.

The enabler may be partially dependent on security support in terms of network slicing, e.g. only allowing non-USIM devices in certain slices. Furthermore, the enabler might be dependent on micro-segmentation, in a similar fashion as to network slicing.

2.2.3 Security Aspects

IoT devices introduce several interesting security aspects that need to be addressed in 5G.

In USIM-less devices, the key security aspect is to provide alternative procedure that can provide a “sufficient” level of trustworthiness. It should be noticed that proposed solutions will have to be implemented in a way to sufficiently prevent at least cloning of credentials (see D2.1). In this aspect, sufficient may vary depending on the use case, hence a dependence to 5G network slicing may be an important ingredient in the realization of the IoT enabler, as USIM-less devices may not be sufficiently trusted devices to access the entire 5G network. The goal of creating 5G slices is to provide exclusively the requested functionality, thus isolating the devices to that specific level of trustworthiness. One result of this investigation will be to establish the dependencies between the security level of proposed solutions and the constraints imposed on the security of slices.

In a BYOI scenario, the main aspect lies in creating mutual trust between the enterprise and the serving network. This may require anchoring in a new business model and/or tight coupling to other technologies such as network slicing and trusted computing. Using slicing, a potential security compromise due to “weak” AAA solution can at least be confined to an individual slice. Relying on slicing to properly isolate devices who have been admitted to a specific slice based on relatively weaker AAA mechanisms of course has implications on the strength of the isolation mechanisms used for that slice. Conversely, access to special slices, e.g. “public safety”, might require an enhanced AAA solution, which provides a higher level of trust, which goes beyond basic solutions, e.g. “internet surfing” slices. One result of this investigation will be to qualify the needed isolation properties of the slice delivered in the infrastructure and the way for a device or client to evaluate if some slice is sufficiently isolated from slices allowing alternatives to USIM.

In group-based AKA, the security properties for the classical AKA should be enforced namely, confidentiality of the session master key, mutual authentication between device and serving network, and device identity privacy.

In the scenario of group-based AKA, the historical threat model concerning the traditional AKA should be extended with additional threats stemmed from the group approach. A comprehensive list of such threats is outlined below.

- The intruder is authenticated as a device by the serving network.
- The intruder is authenticated as serving network by the device.
- The intruder derives the session master key agreed between a device and the serving network.
- The intruder identifies and tracks a device.
- The intruder is authenticated as member of the group by the serving network.
- A corrupted member of the group is authenticated as another member of the group by the serving network.
- A corrupted member of the group is authenticated as serving network by another member of the group.
- Colluding corrupted members of the group derive the session master key agreed between a third group member and the serving network.
- Colluding corrupted members of the group identify and track a third group member.

Furthermore, the enabler will also investigate key protocols and algorithms which provide the necessary protective measures of the security aspects (e.g. backward and forward secrecy properties). Grouping algorithms, and group keying to each group for authentication, will be essential to mitigate the threat of malicious IoT devices in group based authentication scenarios.

vGBA optimizes the GBA based authentication and key-agreement solution both for the core network and the often constrained IoT devices. The security aspect lies in that vGBA makes GBA, a 3GPP specified security solution, more appealing for IoT scenarios. Thus, vGBA is promoting GBA over other, potentially less secure alternatives.

In general, A risk analysis of each feature of this enable should identify any eventual residual risks.

2.2.4 Security Challenges

The challenges for authenticating USIM-less IoT devices lie in finding an alternative that is more cost efficient to deploy and flexible than the well-proven USIM, yet providing a sufficient level of security. Indeed, defining “sufficient” (at least by mitigating sufficiently the cloning threat described in D2.1) may in itself prove to be a challenge. The enabler will investigate how suitable other well-proven alternatives, such as asymmetric key based PKIs, are for 5G. The overall reputation of 5G as a trustworthy system must not be put at risk. This work is dedicated to protocols, cryptography and credentials studies.

In BYOI and group authentication, the challenges are similar and lie in defining a suitable trust model. The trust model must be supported by various trustworthiness mechanisms, business models, and fundamental technologies such as slicing and trusted execution in devices. This is naturally correlated with the work on Trust security enablers, where different aspects of machine-to-machine and machine-to-human interactions are addressed.

For groups, a key point is to identify criteria for defining the group concept (e.g. based on geographical proximity and/or other forms of similarity between devices), the relation between “group”, “device” and “subscriber”, and the authorization level assigned to groups. For example, a group-based authentication may not be sufficient for all forms of services and may thus require complementing group-level authentication by individual authentication before granting certain 5G network services.

For group authentication in particular, the enabler must guarantee a high level of security with minimal communication and computational overhead (the reference will be based on existing EPS AKA for the device authentication). The list outlined in section 2.1.3 contains nine threats, five of which are novel because the group approach. The new threats involve an intruder with the ability to corrupt and control MTC that are members of the group. It follows that no member of the group should be trusted. Hence, it appears to be challenging how to ensure privacy and authentication in presence of one or several corrupted devices.

vGBA as such is only a quite small modification that happens on the network side by having the subscriber database provide the GBA network node (BSF), which resides in the same network domain, with some parameters from the network attach authentication vector. However, the implications of re-using the AKA run for both network attachment and GBA bootstrapping should be analysed so as to not e.g. violate existing policies of key usage.

2.2.5 Features achieved in R1 (Reminder)

- **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 [2], 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.

2.2.6 Technical Roadmap for Release 2 (R2)

- **Feature name**: Group-based AKA (continuation)
- **Goal**: Improve the support of group authentication of IoT devices in 5G.
- **Description**: The group-based AKA will be improved in R2. One direction is to modify the protocol to meet perfect forward secrecy for the session master key. Another direction is to provide an implementation in OpenAirInterface with support of native multiple devices.
- **Rationale**: The current implementation of OAI limits the deployment of multiple devices. However, OAI will fully support multiple devices from December 2016. Hence, the implementation of the

group-based AKA needs to adapt accordingly. In doing so, the IoT enabler will fully assume the characteristics of a prototype rather than a proof of concept.

- **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.

2.2.7 Early 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 and the resynchronization procedure of the sequence numbers. 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.

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.

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 **Technology Area**

This enabler is focused on authorization for two areas, which are expected to be strongly involved in 5G.

First, in addition to the authentication focus brought by the IoT enabler, 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. The enabler operates in a technology area of interconnected resources. Some of these resources, especially

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

RCDs, are characterized by small size modules that embed low-power processors, limited memory and storage resources, and absence of user interface. Additionally, these devices can be constrained by limited physical access and limited transmission capacities.

The second area is based on requirements from 5G satellite business needs and 5G-ENSURE use cases. The goal is to provide an integrated satellite and terrestrial approach, compared to the diverse methods existing today, to provide secure fine-grained access control to satellite resources (i.e. network element and services).

This technology area covers one of the 5G daily situations: multiple users with multiple authentication policies and multiple authorization policies that enforce fine-grained control of access to the system services and resources.

2.3.3 Security Aspects

Access control paradigms based on Role-based Access Control (RBAC) or Attribute-based Access Control (ABAC) are taken into account by different standards and are common today. This enabler proposes to reuse these existing technologies for services and interconnected resource access control, but with some adaptation depending on the constraints imposed by these resources and their widespread geographical distribution.

As introduced in Section 2.3.1, the main security goal of the enabler is to support fine-grained access control policies focusing on attributes related to user, resource, and action. Based on these policies an Authorization Server would render an access control decision that will be enforced by the embedded device. The decision may contain local conditions, evaluated by the device, such as device-state, position, time, etc. Moreover, the security enabler should be robust against an attacker who can physically access the environment where the resources are installed.

Another key goal is the decentralized access control using mainly existing standards (e.g. OAuth, OpenID Connect, XACML…). Authentication and Authorization can be ensured by a Policy Enforced Point (PEP) which is directly embedded on the RCD, without a connection to an AAA server. The access control policies that the Authorization Server uses to render access control decisions can be defined with XACML. These decisions can be transferred to the embedded device using last version's OAuth access tokens.

The enabler should integrate different Authentication and Authorization mechanisms using standard interfaces.

2.3.4 Security Challenges

Different security challenges for the enabler do exist. The main challenge to take into consideration is to find an appropriate format to formulate access tokens that encode conditional access control decisions. The enabler should also deal with anonymous accesses, whenever possible.

For group authorization in particular, the enabler must guarantee a high level of security with minimal communication and low computational overhead. Therefore, protection of the access control information itself is needed.

The location of the authorization server in the 5G network must be investigated with regard to the heterogeneous nature of the 5G architecture. Accordingly, the enabler will be focus on:

- Central server
- Embedded server

- Integration of different servers

In decentralized access control, the challenges are similar and lie in defining a self-sufficient access token allowing decentralized authentication and authorization, compatible with RCDs in terms of token verification and parsing on the one hand, and possibly high performance requirements on the other hand. The RCD should have embedded at least a secure storage for key material, an integrity protection algorithm, and a feature for the verification of origin for both the request and the access token in order to validate them before processing.

Finally, the enabler should improve the security of users/resources, while maintaining or increasing the level of productivity. In order to establish these points, an evaluation in terms of consumption of memory, CPU cycles and battery power, as well as network overhead will be provided (in theory and in practice over the testbed).

2.3.5 Features achieved in R1 (Reminder)

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.

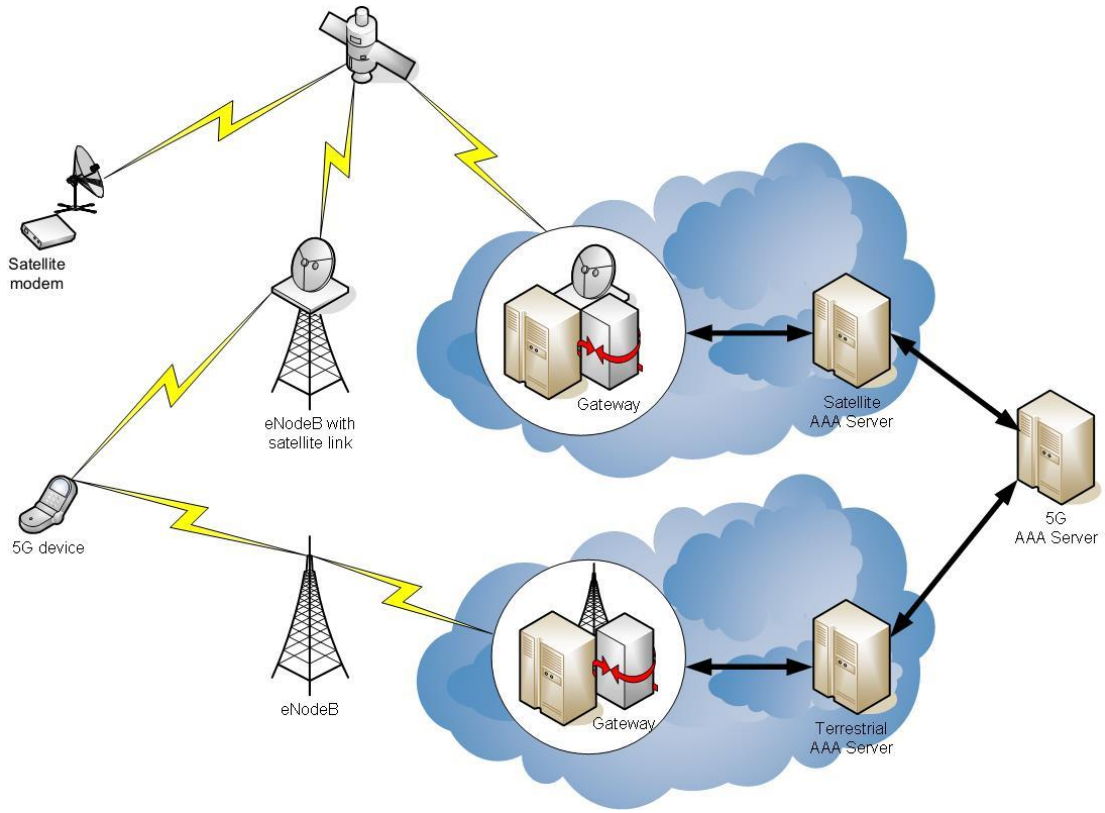

Figure 1 AAA system mechanism

- **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:

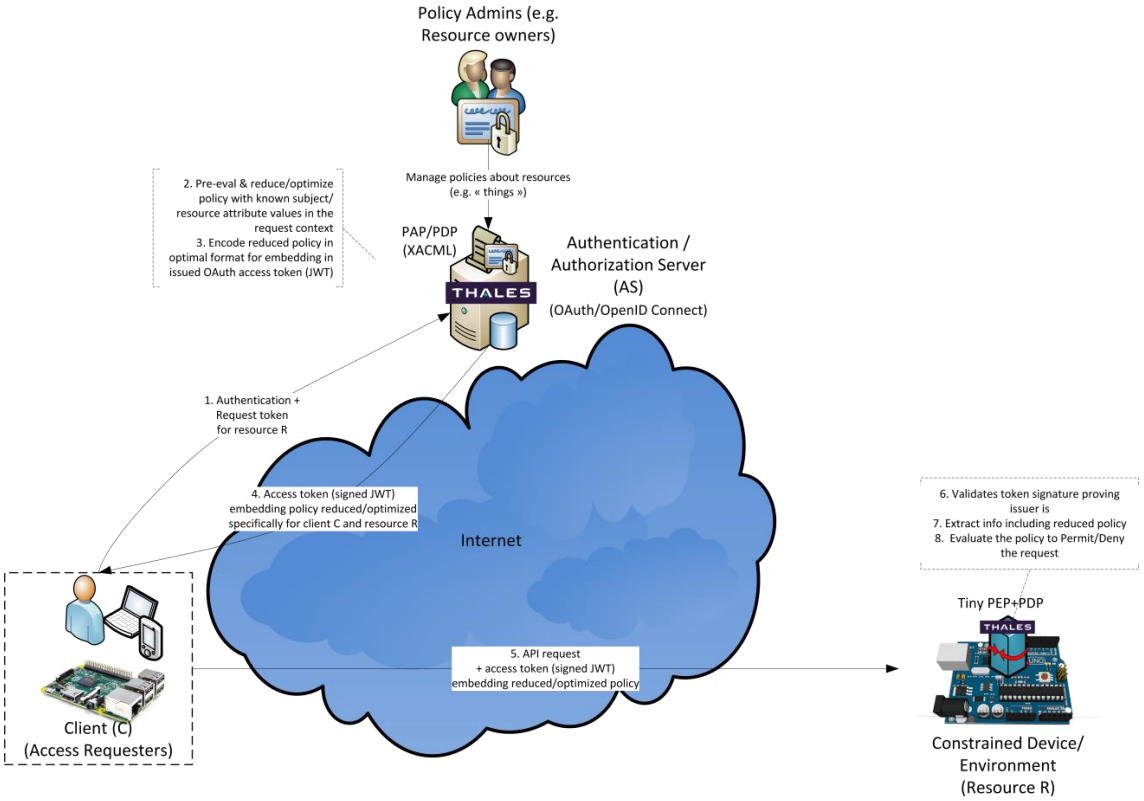

Figure 2 Distributed Authorization Architecture for RCDs

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/

2.3.6 Technical Roadmap for Release 2 (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.

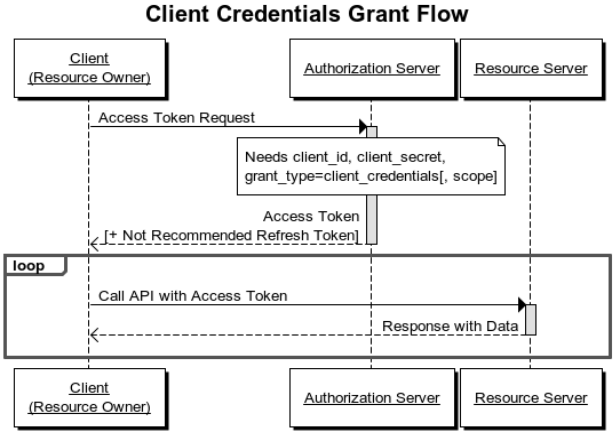

Figure 3 Client Credentials Grant Flow

- **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.

2.3.7 Early recommendations for further research

Possible directions of further research:

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

From the AAA enabler, it could be given new statements in order to protect the privacy of the users such as:

- To record in a text file or database the authorized access, privileged operations, unauthorized access attempts, system alerts or failures, and changes or attempts to change system security settings and controls.
- The identity of each terminal (workstation, computer) in the network will be registered in a database in order to improve the rules among users, terminals and policies. The register to those terminals will also be stored.
- Using Big Data to manage all this information in a better way, managing the previous statements with different servers dedicated to it. Using redundant servers this information can be backed up and the processing speed will be improved due the packages are segmented to work faster.

Also, the further research can include improving the AAA 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. Possible directions to achieve this are:

- A simple Boolean expression format that can be parsed and evaluated (e.g. using jbool expressions [3])
- The definition of a JSON Policy Format, relying or extending the JSON Profile of XACML [4].

The features achieved during R1 were a basic authorization in satellite systems and a basic distributed authorization enforcement for RCDs. Taking this in consideration, the further research will be focused into how to improve the authorization and authentication for satellite systems and time management. In order to have a complete AAA system, it would be required to synchronize all the elements in the network, using a time server (network device time).

2.3.8 Remarks

There are anticipated dependencies with “Internet of Things - IOT” enabler. In both cases they should support:

- Interconnected resources, such as sensors, actuators, satellite modems and Internet-of-Things (IoT) devices in general.
- AAA based on third party entities: bring-your-own-identity, integration of different servers…
- Efficient AAA in massive deployment scenarios

However, this enabler is focused in the authorization functionality, while “Internet of Things - IOT” enabler is mostly related to the authentication functionality.

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 Technology Area

This enabler is focused on authentication for two areas, which are expected to be strongly involved in 5G.

First, this enabler will propose a new way to define the level of authentication performed by a user and to store it. In 5G environment, a user can access a service by using different way to be authenticated, for example, with his PIN code by using his UE through his SIM card) or by a login/password by using an internet connection. This enabler will work to extend/complete the AAA authentication by adding information about the level of user's authentication and update it each time a new authentication is performed. This information could be stored in a separate storage than the AAA user database, this database will offer an API to provide it. This database will be collocated with the HSS and owned by the same provider.

The second area is based on the need to know how a user is authenticated in the network in order to provide or not some services. A typical example is for using bank payment. In this example, the bank could request a stronger authentication than only a login/password authentication. If a node (or a service) needs this kind of authentication, it needs to have this kind of information and to be able to interact with the user in order to obtain the desired level of authentication.

These two areas can be combined in the following steps:

- Nodes need to collect authentication context provided by the AAA server managing the end users.
- Depending on the authentication level, these nodes allow or not the access.
    - If not, the entity in charge of the end user has to strengthen the end user authentication by a new authentication mechanism.
        - With this new authentication, the authentication level of the end user is increased and the 5G node can allow his access.
        - If the end user is not able to provide a stronger authentication (due to a limitation of his UE for example), the access is denied.

These technology areas extend the 5G uses cases mentioned in Table 4. This enabler is not directly usable by the use cases but can complete their needs by allowing different services depending on the authentication performed.

2.4.3 Security Aspects

In 5G slice, the end user will enter in the slice through different access points. Depending on these access points, different authentication mechanisms will be used and will characterize the trust to be granted to this end user.

This enabler enforces the access control to critical services with:

- Authentication management
- Authentication level usage / propagation

2.4.4 Security Challenges

Different security challenges for the enabler can be envisaged. The first challenge to take into consideration is to find an appropriate way to store the authentication level and provide this information to different nodes. The second challenge is how to use this authentication level and to find a way to interact with the user so that he performs a new authentication with the desired level.

To store the authentication level, the challenge is to find the better way to use AAA authentication server for detecting the new (or update) authentication and to classify the authentication mechanisms. The information will be stored in a separate database linked with the HSS database.

To use the authentication level, the challenge is to retrieve this information through the AAA server and to find the better way to notify the end user if his authentication level is not well adapted.

2.4.5 Features achieved in R1 (Reminder)

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

2.4.6 Technical Roadmap for Release 2 (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.

2.4.7 Early recommendations for further research

This enabler will demonstrate only capabilities to characterize the authentication and the usage of this characterization. Further investigation could be to integrate this characterisation in the communication protocols, and to propose different evolutions of these communication protocols.

2.4.8 Remarks

The different features, mentioned for R2, integrate an important part of design and of research and not only of development. That's why simple mock-ups will be performed (developed) illustrating the complete design of the solution.

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 identifies some privacy enablers that are relevant to 5G, i.e., needed by the use cases defined in Deliverable D2.1 [5] 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 proposes 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 aims also to extend protection of subscriber's identity for non-3GPP access such as WiFi/EAP-AKA.

The second enabler proposes 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.

Each of the Privacy enablers in scope of the second release (R2) is detailed together with their features while features achieved in R1 are reminded whereas features specifically in scope of R2 are described. Next steps to come are also introduced in the form of early recommendations for further research.

3.1 Security Enabler "Privacy Enhanced Identity Protection"

3.1.1 Product Vision

This privacy enabler aims to provide protection against user's identity disclosure and unauthorized user tracking, by preventing or defending against various types of IMSI (International Mobile Subscriber Identity) catching attacks, paging attacks and location tracking attacks. The main goal is to offer stronger protection of user identity than in current 3G and 4G networks. The fundamental idea behind this enabler can be summarized in several simple concepts: 5G true identities shall not be transferred over the network but only unique dynamic (pseudo) random pseudonyms should be used during all normal operations. In

exceptional cases, if a true identity has to be sent from the UE to the network, it should be sent encrypted by means of asymmetric cryptography , and possibly all identity requests should be authenticated.

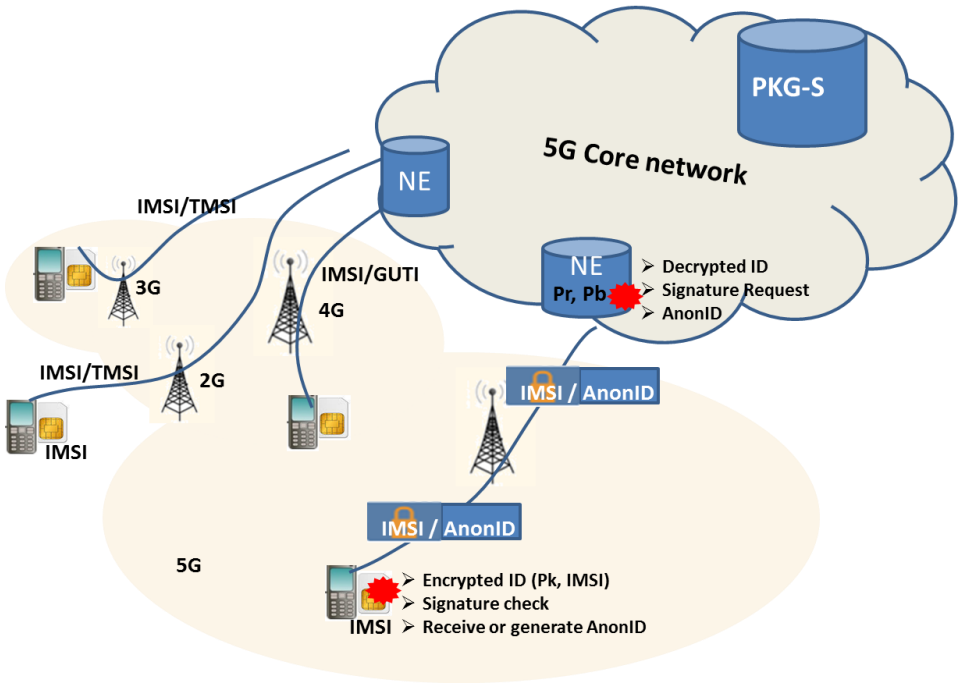

Figure 4: High level Privacy Enhanced ID Protection architecture.

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 [6]. Mobile devices engage in a number of AAA protocol interactions dependent upon their access to the network. In the case of mobile radio connection, assuming that AKA scheme (or similar) will be used also for 5G, the User Equipment (UE) obtains its temporary identity (e.g. S-TMSI, GUTI in current network). If the UE attempts to attach to WiFi then it may utilize the EAP-AKA protocol to authorize connection to the local network, or to the evolved packet core (EPC). The security enabler should therefore support:

- Increased privacy in protocol interactions
- Enhanced anonymity properties
- Improved unlinkability.

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 [7] (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 [6] 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. One of the goals of the present enabler is to measure the computational cost of asymmetric encryption schemes on some common UE devices. The compatibility of the approach with RCD devices will also be an object of study.

The fundamental idea of the enabler is to provide encryption of 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, UE shall not send the subscriber's permanent or long term identity in clear text in order to initiate the network attach procedure.

In a simple scenario where the UE only connects to its home network traditional public key encryption can be used. In order to cover other possible scenarios, like a LI (Lawful Interception) scenario, an Attribute-Based Encryption (ABE) [8] could be 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 [8]) or in the cipher text (cipher text-policy ABE [9]). 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 public key ABE encryption is needed 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 MME in 4G networks, or on a dedicated network element which stores and handles the private key for decryption. Randomized encryption schemes should be applied, such as, for example [10], or ABE encryption schemes in order to prevent linkability. Therefore, IMSI catchers cannot read or guess IMSI.

This approach (alone) does not protect against spoofed identity requests, but it always protects the long-term identifier against unauthorized access.
For implementing an ABE cryptosystem, the participating MNOs have to be members of a PKI, managed by a trusted authority (e.g., the GSMA). In all cases the implemented system should respect the LI requirements. All MNOs (home and serving) participating in the scheme will 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 second solution in order to respect the LI reqirement).

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 will be 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

The goal of this feature is to complement the “Encryption of Long Term Identifiers” feature to avoid exposing user permanent or long term identities on (at least) the air interface (i.e., in Attach Requests with GUTI, Identity Responses, Paging Requests). Some of the possible solutions identified at this stage are presented below, although the final choice could not be limited to the present ones.

Pseudorandom dynamic pseudonyms, herein referred as RIMSI (Random IMSI)/dGUTI (dynamic GUTI), can be generated in the same way both by the network and UE, by using a (standardized) pseudonym-derivation algorithm with a shared secret key.

These RIMSI/dGUTIs 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). The RIMSI/dGUTI generation mechanisms must guarantee collisions avoidance over a

Tracking Area. At the moment, there are some evidences that GUTIs are not random [6], therefore the proposed scheme can apply to GUTI generation.

As an alternative to the previous approach in devices which are not able to host a pseudonym generation algorithm, the network generates the RIMSIs for the entire Tracking Area and maintains the state for each UE (the UE active RIMSI or RMSI window). The permanent or long term identity (IMSI) is communicated only once to the network in the first Attach Request through the first feature of this enabler. The RIMSI can also substitute GUTI. The one-time pseudonym is updated after each usage (i.e., after being used in a message for UE identification).

The RIMSIs are univocal random numbers over the entire Tracking Area, they change periodically (short periods) and are always used where IMSI/GUTI are now used (except for the Initial Attach where the IMSI is sent encrypted). The RIMSI generation mechanisms must guarantee collisions avoidance.

These RIMSI/RGUTIs could always be used by UEs instead of permanent or long term identities IMSIs in response to an Identity Request and by the network in a Paging Request.

3.1.2 Technology Area

By design, current mobile networks need to occasionally expose permanent or long terms identities such as IMSI. Before network attach is complete, no protection can be offered in current 3G and 4G systems. Relevant technologies include ways to never expose clear text identifiers on the radio network, and, possibly to authenticate identity requests. Feasible solutions point in the direction of deployment of public key infrastructures with associated key and certificate management aspects.

3.1.3 Security Aspects

The main problem in current networks is that identifiers are exposed in situations where no security context (i.e., shared keys) is available; neither to authenticate identity requests, nor to protect (encrypt) the IMSI in the identity response messages, or in broadcast network messages sent by the network such as paging. In such messages the subscriber identity is included and is sent in an unprotected way, thus enabling UE tracking. Therefore, various ways to authenticate and encrypt such messages and/or to anonymize the IMSI are central to this enabler.

The main privacy issues in 3G and 4G systems that need to be addressed and overcome by 5G systems are:

- The permanent or long term identities (IMSI) are transmitted in clear text in the first Attach Request.
- Identity Requests are not authenticated and the user's Identity response contains the permanent or long term identities IMSI in clear text.
- Temporary identities, e.g., GUTI (Globally Unique Temporary Identity), TMSI (Temporary Mobile Subscriber Identity) protect only from passive attacks.
- Encryption of signalling is required to transmit temporary identities in a protected way. However, availability of encryption depends on the network configuration.
- Temporary identities reallocation depends entirely on network configuration.
- There are no explicit requirements on the randomness of temporary identities.
- Temporary identifiers are broadcasted over the air, e.g., during the Paging Procedure to locate the UE. Paging messages contain identities of UEs such as S-TMSI (SAE-TMSI) or IMSI. By means of a passive or semi-passive attack it is possible to locate and track the user.

This situation can be exploited by attackers as described in the literature [6], [11], [12].

3.1.4 Security Challenges

There are inevitably situations where identifiers (or at least parts thereof) need to be exposed, e.g., routing of AAA (Authentication Authorization Accounting) information, retrieval of subscriber data in data bases, lawful interception, etc. Therefore, a solution that provides a high degree of privacy even under these side conditions is challenging. In some cases, a reliable key escrow mechanism might also be necessary for lawful interception.

The enabler aims to protect subscribers' permanent or long term identifiers exposed over the air in all scenarios: when the UE is connected to the home network, as well as to the serving/visited network and in LI situations.

The enabler needs to address backward compatibility requirements as well, e.g., regarding the access of legacy terminals to 5G networks and vice versa. This can have a strong influence on the 5G security design and complexity, and so will requirements on mobility (seamless or not) between different generations of mobile systems.

3.1.5 Technical Roadmap

3.1.5.1 Features achieved in R1 (Reminder)

- **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 provided 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, a demo scenario was implemented in a 5G non-3GPP (WiFi) access 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 in integration phase on the project's testbed.

3.1.5.2 Features for 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 will provide system definitions and a prototype implementation. The prototype implementation touches protocol implementations and elements like HSS and MME. Changes in UE will be done in an emulated environment. Due to constraints that apply, this enabler can only be demonstrated outside the testbed and thus will not be 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 will provide the open specification and a prototype software implementation of the main functions of the system (i.e., a library with the main cryptographic functions for the pseudonyms generation). The release does not foresee 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.

3.1.6 Early recommendations for further research

- **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.

3.2 Security Enabler "Device Identifiers Privacy"

3.2.1 Product Vision

This enabler aims to provide state-of-the art end-to-end anonymization techniques on the user's device, offering *Privacy Enhanced Attachment (PEA)*, which provides protection against device identity (and possibly also user identity) disclosure and unauthorized device/user tracking. The main focus is to offer stronger protection of device (and related user) identity than on current networks, as compared to the Privacy Enhanced Identity Protection enabler which is aimed primarily at subscriber identity protection. Moreover, the privacy policy should be directly controlled by the user, who shall be provided tools for policy management. The enabler addresses both devices with and without UICC/SIM attaching via various network technologies.

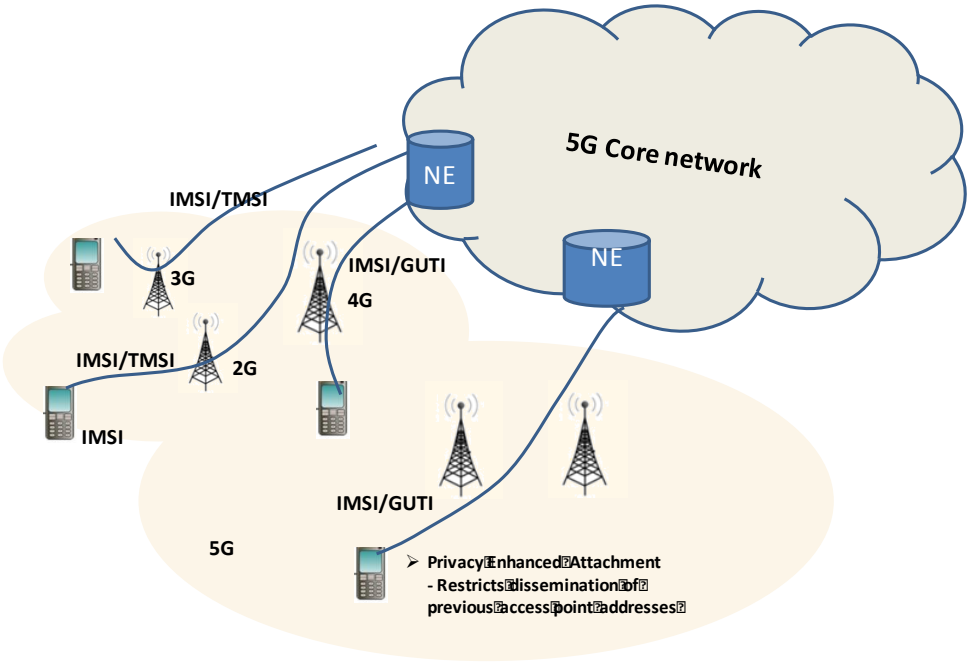

Figure 5: Privacy Enhanced Attachment

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 Technology Area

Users have an expectation of identity privacy and as such they assume that no device of theirs, including IoT devices, will leak any identifiers that can allow for unconsented tracking and attribution [13]. Relevant technologies include ways to securely anonymize identifiable device/user data in all or selected communications between the device and the network [14]. The range of network types employed in 5G is set to increase, particularly on IP-based network technologies such as WiFi, which may be utilised for 5G services, for example Voice over LTE, via Generic Access Network (GAN), or directly using applications such as chat or Voice over IP (VoIP). Furthermore, the enabler also aims to investigate the situation with respect to the proliferation of Internet connected devices for medical, industrial and personal monitoring. The solution points in the direction of using anonymization protocols and privacy protection profiles (c.f. Privacy Level Agreements [15]) directly on the device and at the network/server side.

3.2.3 Security Aspects

The enabler may be of interest to a number of 5G use case scenarios, like eHealth, smart home/office and traffic safety. The main privacy problem arises when the devices/sensors identities are often linked with the user's identity (e.g., a sensor on a car is ultimately linked to the identity of the car's owner, or a sensor which continuously monitors a patient condition is linked to the patient name in a hospital database). In

order to avoid exposing these identifiers in situations where there may be limited security mechanisms available, a trusted anonymization scheme may be useful. Therefore, various ways to anonymize the identities involved in the communication are central to this enabler. The enabler should also benefit from the implementation of a privacy management mechanism, where different levels of protection can be enforced on different data or different roles in the system can be given different access rules.

3.2.4 Security Challenges

The problem with a number of access protocols is that they can leak information that violates the user's privacy enabling third party tracking and monitoring.

There are inevitably situations where identifiers need to be exposed, e.g. to a law officer, emergency situation, and other situations which are very specific to the various 5G use cases. Therefore, a solution that provides high degree of privacy even under these side conditions is challenging.

The enabler aims to mainly protect identifiers exposed over the air, but it will also investigate if subscriber's anonymity may be improved for other user information flows across the network without compromising the usage of the collected data.

The enabler aims to address situations where different connection technologies are used (e.g., devices/sensors locally connected over various types of wireless networks like in an Internet of Things use case), and its general purpose is to be technology independent.

The enabler will consider policy management issues (configuration/negotiation/update) and possibly the backward compatibility requirements as well, e.g., regarding the access of legacy terminals to 5G networks and vice versa.

3.2.5 Technical Roadmap

3.2.5.1 Features achieved in R1 (Reminder)

- **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 will provide protocol enhancements and architecture definitions and a prototype implementation. This release will primarily target IP-based network attachment protocols such as Detection of Network Attachment (DNA) [16].
- **Rationale**: To ensure that users consider 5G as a privacy preserving technology for all types of 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 feature is also available to be integrated in the project's tesbed.

3.2.5.2 Features in Release 2

In Release 2 we will develop approaches to provide for anonymised and optimised address selection for network attachment protocols which builds on 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 will provide the following enhancements to the release one achievements: pre-analysis phase of the address anonymity metrics and dynamically optimised choice of address randomisation and dummy addresses.
- **Rationale**: To ensure that users consider 5G as a privacy preserving technology for all types of network attachment.

3.2.6 Early recommendations for further research

Possible directions for future work are:

- Analyse the application of geo-fencing to address selection
- Investigate the provision of support for the techniques in IPv6
- Consider extension of the techniques to other mobile network attachment protocols.

3.3 Security Enabler "Device-based Anonymization"

3.3.1 Product Vision

This enabler aims to provide 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) should be directly controlled by the user, who can activate different anonymization profiles stored on the device. The user's device will host a configuration tool which will enable the user to activate and configure his/her privacy profile.

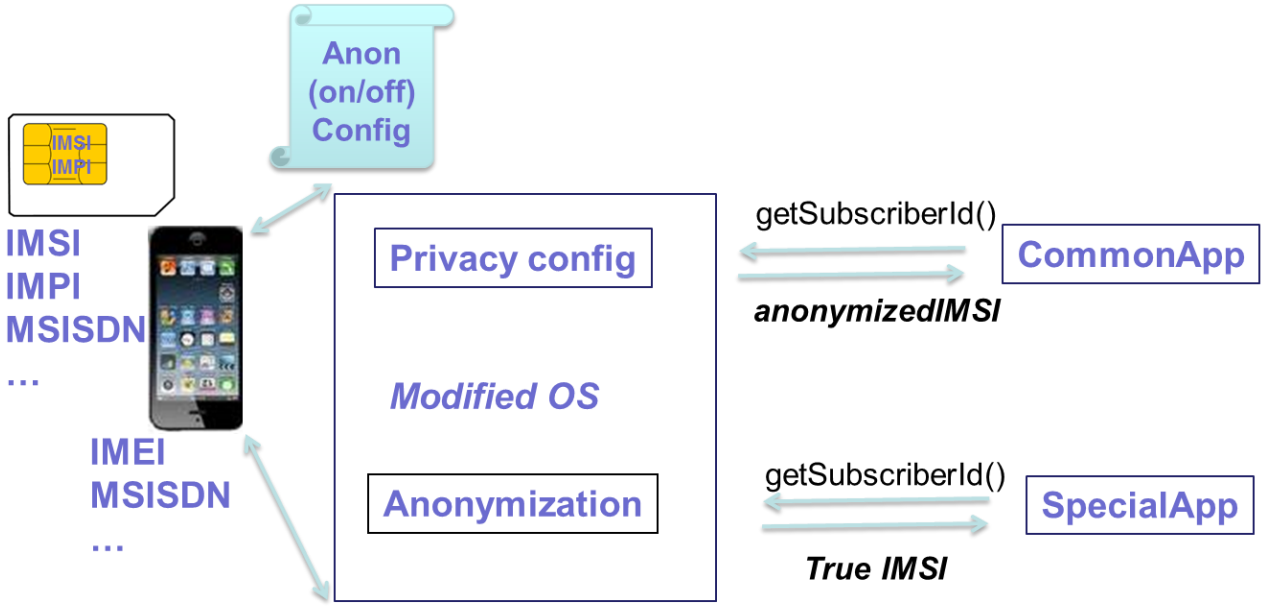

Figure 6 Device-based Anonymization.

Depending on the information to be anonymized, 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 will be managed by a privacy provider, which will return 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 will obtain 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 Technology Area

Relevant technologies for the enabler include light and efficient algorithms to anonymize data. A privacy configuration instrument should also be provided, in order for the user to be able to configure/select different anonymization profiles corresponding to different categories of data to be anonymized and to different applications.

3.3.3 Security Aspects

The enabler may be of interest to a plethora of 5G use case scenarios, for example whenever SIM identities are required by applications and probably sent over the network to remote entities. The anonymization technique can possibly be extended to other application data stored on the SIM or device, as specified by the user's anonymization profile/configuration.

3.3.4 Security Challenges

The user might want to configure a finer grained anonymization, i.e., to distinguish between the calling applications in order to disclose some data to some selected applications and thus avoid to disclose it to other applications. A solution that provides such flexibility is more onerous to provide. The privacy agent has to be able to distinguish the calls coming from different applications installed on the user's device, therefore modifications to the host OS are also needed. Additionally, the location of the privacy agent may also need to change.

As far as backward compatibility with Internet services is concerned, in many cases format preserving encryption should be enough to ensure transparency to these services. Probably for some services the algorithm should generate the same pseudonym for the same identifier received in input. This should be a configurable option/feature of the algorithm.

Some services (SpecialApp in Figure 6) might need to work on real identities (real IMSIs or MSISDNs). For example, there are apps that offer a mechanism to recover a lost password via SMS, therefore the real MSISDN in must be provided in the user's profile. Such apps have to excluded from the anonymization scheme through the configuration tool.

3.3.5 Technical Roadmap

3.3.5.1 Features achieved in R1 (Reminder)

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

3.3.5.2 Features for 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 will provide the algorithm implementation. The algorithm should preserve 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 will provide 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.

3.3.6 Early 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**: The release will provide the algorithm implementation. The algorithm should preserve the format of the input data (e.g., IMSI, phone number, etc.).
- **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 release will provide 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 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 aims to provide the user a way to analyse the privacy policy of a service or a (V)MNO and compare 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 describes the high level architecture of "*Privacy Policy Analysis"* enabler.

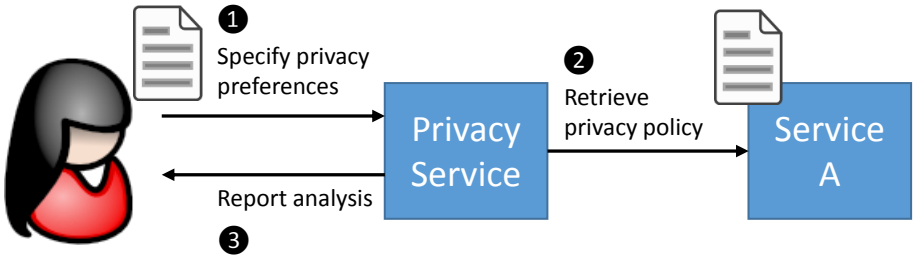

Figure 7: High level architecture of Privacy Policy Analysis Enabler

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 Technology Area

This enabler will be based on two complementary specification languages:

1. A privacy policy specification language that enables the expression of privacy policies of 5G network services and applications in a machine-readable format which may be analysed and compared. In addition to the specification of data-collection and data-usage practices, the privacy

policy language should provide a means of associating privacy policies with the target services as well as a mechanism for publishing, transporting and consuming these policies online.

2. Privacy preferences specification language is needed to allow users to express their privacy preferences in a set of rules which allows the user (or an agent) to make automated or semi-automated decisions regarding the acceptability of privacy policies and thus the mode of usage of the associated services (e.g. use, block, constrained usage without releasing sensitive data, etc.).

This enabler will include a matching engine in order to compare the privacy preferences to the service's policy. Matching rules need to be precise and clear in terms of how to compare the preferences with the actual policy (what is optional and what is mandatory).

The enabler requires service and application providers to make their privacy policy available such that it reflects the real behaviour of the service. The enabler compares the user's preferences against the privacy policies and indicates whether the policy is compliant with them or not. Specification languages like W3C P3P, APPEL and COWL [17] are candidates to be used by this enabler. Other constraints regarding interoperability with other privacy enablers may require transformation of the output to appropriate schemas. This is to be addressed later in the specification document.

3.4.3 Security Aspects

When users interact with services online, information (sometimes personal and sensitive) may be collected, aggregated and processed. This may be mentioned in the service privacy policy, but it is often not easily accessible or understandable by the user. This enabler will make querying and understanding the policy details and service behaviour easier for the user. The user can then make informed decisions on how to use the service or search for an alternative that satisfies their privacy requirements.

3.4.4 Security Challenges

Specifying service behaviour in terms of a privacy policy is a challenging topic especially in this case where the purpose is to structure such information in a way to query and reason on it. The semantics of policy constructs as well as those of the user preferences need to be specific and shared (at the service and the user side) in order to ensure a common mapping. Moreover, business models and the privacy policies of their services change and evolve implying that a flexible and extensible language is required and that the match between preferences and policies needs to be frequently re-checked.

3.4.5 Technical Roadmap

3.4.5.1 Features achieved in R1 (Reminder)

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

3.4.5.2 Features for Release 2 (R2)

For release 2 (R2) three features are planned:

- **Feature name**: privacy policy specification.
- **Goal**: encoding service privacy policy.
- **Description**: support the loading of a privacy policy into the enabler. Which particular standard to use for the privacy policy is yet to be defined.
- **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 particular standard to use for this is yet to be defined.
- **Rationale**: this is required for the comparison with service offerings.

- **Feature name**: comparison of policies and preferences.
- **Goal**: compare the selected service policies with the user's expressed preferences.
- **Description**: the selected service policies will be compared with a user's expressed preferences and the user will be presented with the analysis in a clearly understandable form.
- **Rationale**: privacy based analysis of service offerings.

3.4.6 Early recommendations for further research

Multiple layers of privacy policy specification could be imagined and will be 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.

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 will help 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 needs 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 will 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 will apply this approach to the 5G domain where a 5G asset model will be developed and associated threats and trust relationships will be encoded to enable repeatable, systematic threat and trust identification in the network. This will also provide an advantage when run-time aspects will be 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 Technology Areas for the Enabler

The enabler can be used in a variety of use cases and by a variety of users as indicated in the table above, both when designing new network configurations enabled by 5G technologies and when making trust decisions during the use and operation of networks.

4.1.3 Security Aspects

This enabler should provide system designers with a way to model and analyse their systems by automatically identifying the relevant threats and enumerating strategies to manage them.

[3] www.optet.eu

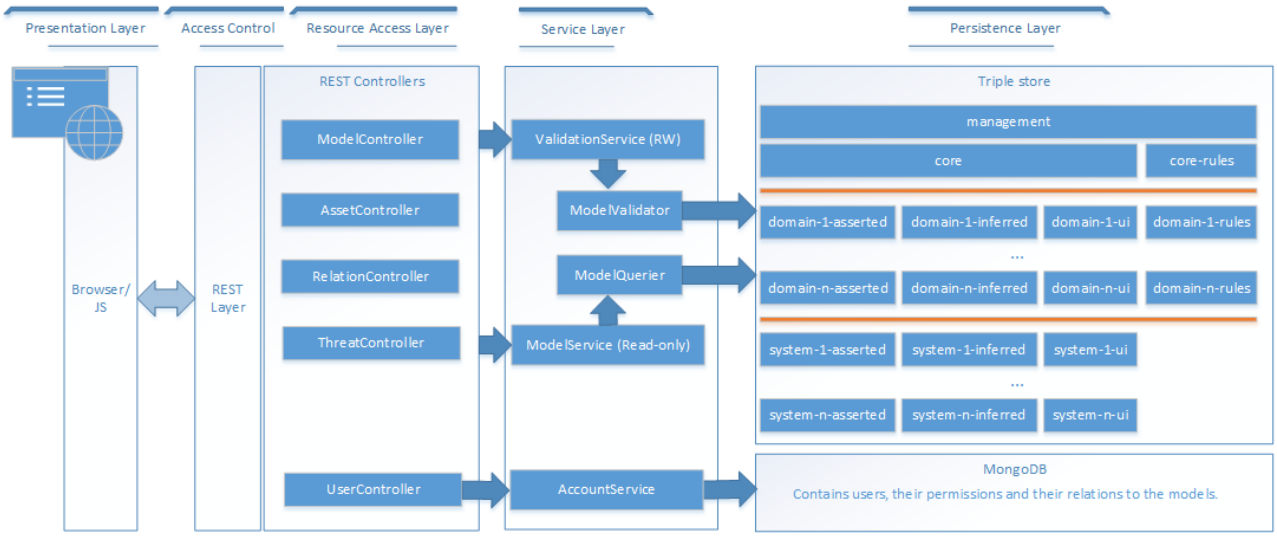

Figure 8: High level architecture of the Trust Builder enabler

The trust model will be realised as an ontology which will encode the identified assets, threats and controls in a knowledgebase. The architecture of the enabler is shown in Figure 8. The enabler will also provide a GUI for designing system models which specify the relationships between socio-technical assets in the system (see Figure 9). Based on the ontology and the system model, this enabler will be able to identify the relevant threats to the modelled system architecture, enriching the designed system model with the threat information. It will also allow the designer to select a management strategy based on controls automatically identified for a specific threat. All these decisions are also encoded in the system model and can be queried, analysed and updated as needed. In addition to the enriched semantic model, the enabler can provide a text report that can be used by different stakeholders e.g. system designers, components developers or risk managers to manage the identified threats.

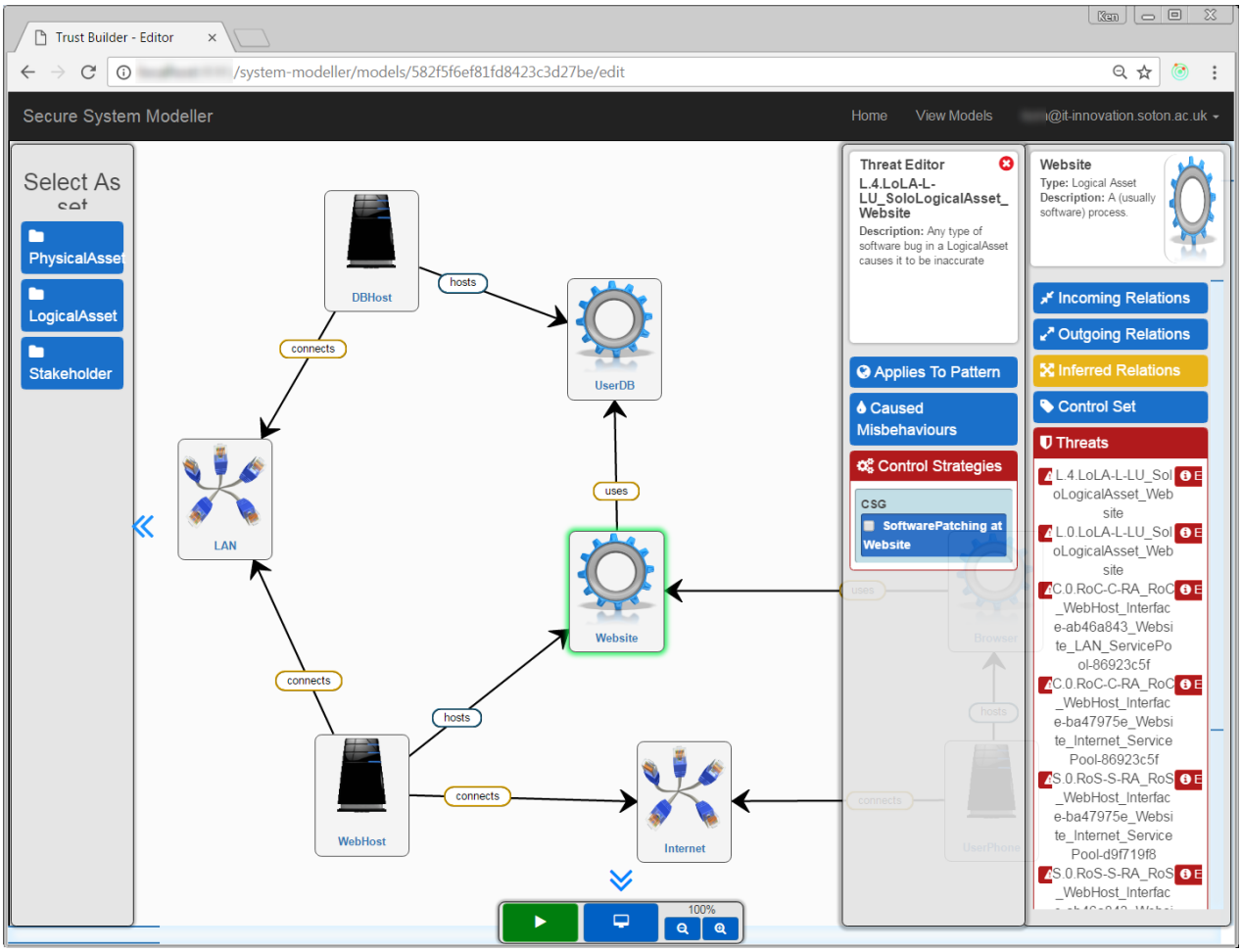

Figure 9: Trust Builder graphical user interface from R1.

4.1.4 Security Challenges

The knowledge base will be updated as new threats arise. This will require maintaining the link between the system model and the knowledge base used during the analysis. The graphical user interface will have to be designed to allow the user to interact easily with complex models and the performance of the model processing must be fast enough for the interface to remain useable.

4.1.5 Technical Roadmap (Update)

4.1.5.1 Features achieved in R1

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

4.1.5.2 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 will be updated with information (specific assets and relationships) from the architecture defined in D2.4 and through further discussion in the architecture task (T2.4).
- **Rationale**: the asset model will be 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 will allow system designer to model their system and analyse the potential threats and their mitigation controls. The second version of the tool will include 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 will be 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 would apply onto a 5G system alongside descriptions of trust relationships. Moreover, the threats will be mapped to some of the controls that can be used to manage them. The information encoded in the ontology will come from an analysis of D2.2 [18] and D2.3 [19] but will also include additional detail from the work of the project's tasks T2.2 and T2.3.
- **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.

4.1.6 Early 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. The Trust Builder will support the design of a system configuration, highlighting potential threats and showing available control options. The System Security State Repository uses the same model when, combined with other monitoring enablers, ingests data from a live system to understand what assets and controls are actually in place, in comparison with the design. A future version of the System Security State Repository could be able to ingest data about active misbehaviours and infer the most likely active threat. The Trust Builder could then be used to review the design and incorporate additional controls.

4.1.7 Remarks

The enriched model, developed at design-time, can later be used when monitoring the running system. The monitoring enabler, "System Security State Repository" uses the same ontology to describe the state of a running system.

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 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

4.2.2 Technology Area for the Enabler

This enabler is developed because of the general 5G network flexibility requirement and it supports the legacy requirements for security visibility and configurability defined in TS 33.401. The security visibility and configurability had a minor role in legacy 3GPP networks, e.g. ciphering indicator feature specified in TS 22.101 is not widely adopted and configurability is limited to enabling/disabling user-USIM authentication, but because of 5G network flexibility, these security aspects become more topical.

The network flexibility provides a challenge to define a general trust model utilized by the enabler. One approach is to extend the Network Domain Security for IP-based protocols framework (NDS/IP) specified in TS 33.210. The foreseen growth in the use of software networks, mobile edge computing and virtualization technologies provide the means to define network domains on-demand enabling sometimes to disable uncontrollable factors such as the Internet from the trust model. This can be carried on to the extreme by micro-segmenting the network for a single application which has a unique trust model.

The uniqueness of the trust model originates mainly from varying protection modes and application characteristics. Transport based hop-by-hop protection leads to service centric trust model to provide reliable services and access controls, for example. Media independent end-to-end protection leads to application based trust model which might be utilized dynamically and to form exclusive trust relationships. The application dependent part of the trust model is subject to varying threat profiles and business requirements. For example, if application does not handle sensitive information, the eavesdropping attacks are not of high importance or if the application pricing does not allow additional support infrastructure, a third-party providing the necessary security controls may be assumed to be trusted. Besides the aforementioned assumptive trust model, the two other major trust models, based on direct and transitive trust, are possible. NDS/IP provides an example of direct trust where a single network admin authority is clearly defined that may provide a single certificate authority within the domain. The micro-segmenting use case may implement advanced access controls that enable transitive trust in which any node's certificate can be validated by another node in the micro-segment.

Generally, the following factors are used in the trust metric aggregation:

- Application trust; level of end-to-end protection, level of platform protection, level of application protection, measurements of vulnerabilities
- Communication trust; level of transport protection, level of platform protection, QoS measurements, level of implemented security controls, measurements of vulnerabilities
- Identity trust; level of authentication mechanisms, reputation of the peers, transitive trust characteristics

The added value of the enabler comes from the improved user experience. It is assumed that the end-user experience is better if the end-user has evidence about the achieved level of trust when a specific application/service/network configuration is in use. The end-user utilizes the evidence to make decision whether or not to perform actions that require high trust. On the other hand, the security configurability requires visibility, i.e. the knowledge of the current setup and feedback about the status of the requested setup. A configuration could be applied that leads to low trust by disabling network security controls but it enables better network performance, e.g. real-time communications.

Another added value prospect is related to the network flexibility requirement which enables network operator third-party application programming (API) interfaces to control 5G services. It is evident that the network flexibility requirements enable diverse and sometimes complex network configuration and services that should be easy to utilize by the third-parties. This enabler aims to simplify the API by providing a readily usable trust metric, for example by outputting a single value (on a scale from 1 to 5) with related descriptions and mapping of use case examples. The third-parties using this API may also get competitive advantage by enabling dynamic operation of the developed application which could adapt to the underlying network configuration leading to better and/or more secure user experience.

4.2.3 Security Aspects

The enabler will provide means to achieve 'good enough' security by selecting the optimal security enablers and to enable visibility and configurability of 5G security controls. The optimal set of enablers depends on the application, current 5G setup and environment. New security features will not be developed as such but existing redundant security features may be disabled based on this enabler.

4.2.4 Security Challenges

The challenge to realize this enabler is the implementation of necessary measurements related to trust. A specific security challenge is to design an enabler that is resistant to insider threats. The safe-guards for trust enabler itself must also be well defined, e.g. what happens when the enabler is compromised, and the propagation of trust must be designed in a way which causes minimal damage in worst case. Also, the standardization of the security configurability and visibility requires formalization of security policy mapping to network security configurations.

The trust metric can be composed of vast amount of different measurements and it is not feasible to implement them all in every user case. Micro-segmentation enables scaling down the overhead of the measurements by focusing the extra efforts to specific use cases, e.g. to a specific service provided by a network operator.

4.2.5 Technical Roadmap (Update)

The first release (R1) was implemented and it can calculate a trust metric value from simulated input data. The development started in the first year of the project and it continues during the second year.

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.

During the second year, real-time monitoring of the 5G Test Network is utilized and the enabler's input data is delivered through the Kafka and Spark environment. The Trust Metric Enabler should support and interact with the Security Monitoring Enabler as well.

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

- **Feature name**: Improved trust metric based on extended data
- **Goal**: Collecting monitoring data and KPI from the micro-segment and from eNodeB to enable near real-time operation
- **Description**: The feature enables collecting of information from different data sources, particularly from eNodeB and Security Monitoring Enabler. Interface to counters and KPIs of eNodeB within the 5G-ENSURE testbed (in VTT's testbed node) will be provided. Traffic statistics from Micro-Segmentation Enabler and Security Monitoring Enabler will be provided, and trust metrics will be delivered to Security Monitoring Enabler.
  - Some missing but required basic trust related measurements may be developed and implemented.
- **Rationale**: Quick responses to attacks and risks in 5G micro-segments, support of extensive awareness of security status of 5G application

4.2.6 Early recommendations for further research

Following R2, the focus should be on enabling network segmentation based on different trust levels.

4.2.7 Remarks

This enabler is related to other enablers (Security Monitoring) and coordination has been planned. The R2 version of the Trust Metric Enabler provides its output for the Security Monitoring Enabler and it may utilize the same Kafka and Spark runtime environment as Security Monitoring.

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 provides 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 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 whose first draft has now been released through D2.2 [18], 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 for specifically 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] http://www.optet.eu/

4.3.2 Technology Areas for the Enabler

The enabler can be used in a variety of use cases and by different actors involved in designing new network configurations enabled by 5G technologies and when making trust decisions during the use and operation of networks. The table above gives some indicative examples taken from Use cases deliverable D2.1 [5]. The main actor could be the "5G Node Provider" in use case 5.2, the "Network Operator" in use case 5.4 and the VMNO in use case 5.5.

4.3.3 Security Aspects

The enabler will deliver a Certification process and tools to provide the Digital Trustworthiness Certificate (DTwC). The following schema illustrates the usage scenario of the enabler. This scenario describes the different mandatory roles, regardless of the implementations. For example, the evaluation laboratory could be instantiated inside the Software provider itself. Another possibility could be to have a Certification Body, only if an audit is requested; in this case, the certification would be a self-certification. The compliance with SECAM[5] methodology and NESAG[6] activity will be analysed.

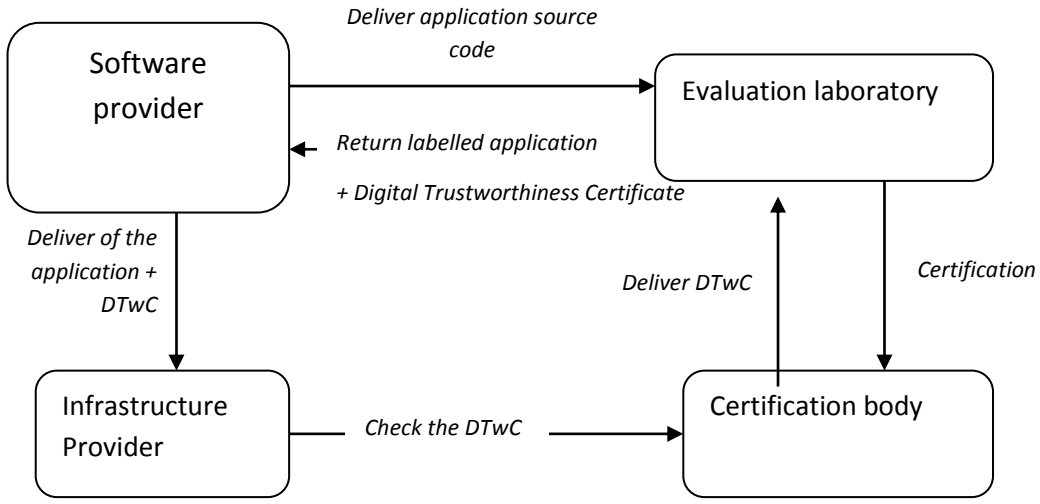

Figure 10 : Overview of Certification process scenario

This enabler will define especially:

- Certification process by favouring a lightweight certification process (based on automatic evidence production and on a self-certification).
- Format of DTwC
- Controls definition and parameters to provide information of the VNF allowing its monitoring at infrastructure level.

[5] http://www.3gpp.org/news-events/3gpp-news/1569-secam_for_3gpp_nodes

[6] https://docbox.etsi.org/workshop/indo-european%20dialogue%20on%20ict%20standards%20and%20emerging%20technologies/21_anand_prasad_nec.pdf

4.3.4 Security Challenges

The main security challenges to take into consideration are to define:

- The trustworthy characteristics for Virtualized Network Function VNF compliant to a part of the trustworthy model defined in 5G-Ensure (only the part concerning the VNF).
- A list of controls answering the main threats and a way to allow a monitoring tool to use them.

4.3.5 Technical Roadmap (Update)

4.3.5.1 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

4.3.5.2 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.

4.3.6 Early 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).

4.3.7 Remarks

This Enabler provides trustworthy information for external usage in the different use cases mentioned in Table 11 but the development in other components (NFV orchestrator for example) are not in the scope of R2.

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 Technology Area

For mobile communication networks, security visibility is one of the important security features identified by the 3GPP. This applies in today's operational networks from 2G to 4G. Indication of certain events during utilization of network services such as outgoing/incoming calls or data connection adds greater user visibility. In particular, during certain events the UE should include indication of whether encryption at radio access network is enabled or not, such as at connection set-up time. The 3GPP TS 22.101 describes in detail the proposed ciphering indicator feature to be used in 2G to 4G networks. This enabler adds new ciphering indicators that include state of network authentication, encryption algorithms in use, and temporary identity in use. These new detailed ciphering indicators assist in applying specific security policies as per the requirement of specific 5G application use-cases.

4.4.3 Security Aspects

This enabler may be of interest to a number of 5G use case scenarios, as depicted in the table above. The main trust issues arise when the device/subscriber is in a roaming area where the serving network has a different set of security features. In order to support operational or local regulatory requirements limited security features may exist in the serving network. Therefore, providing a new security indicator to enable the assessment of the trustworthiness of the serving network would be useful. In addition, this enabler may also benefit from an implementation of a security policy management mechanism, where different levels of protection can be enforced on different 5G specific applications or networks in case of weaker or stronger security of the serving network.

4.4.4 Security Challenges

Although the current UE's should support the ciphering indicator as a feature according to [22.101], however many vendors do not implement this mandatory requirement. Hence the primary challenge is to standardize an interface between the baseband OS and Mobile OS that enables access to signalling

messages carrying serving network security parameters. Technically it is possible to build such an API without affecting a device's performance and quality of service. In addition, such an interface may take the form of API that is mandatory to implement for UE manufacturers.

4.4.5 Technical Roadmap

4.4.5.1 Features achieved in R1

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

4.4.5.2 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.

4.5 Reputation based on Root Cause Analysis for SDN

4.5.1 Product Vision

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

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

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

Each domain is composed of a single SDN controller which is the only intelligent entity in the domain, whose role is to establish and control the interconnection among the different hosts in that domain. The infrastructure is 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 use a self-modeling based RCA [20], [21], [22], [23] which is 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 has been conceived for one single domain. A high-level view on this module can be seen in the next Figure, which has 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.

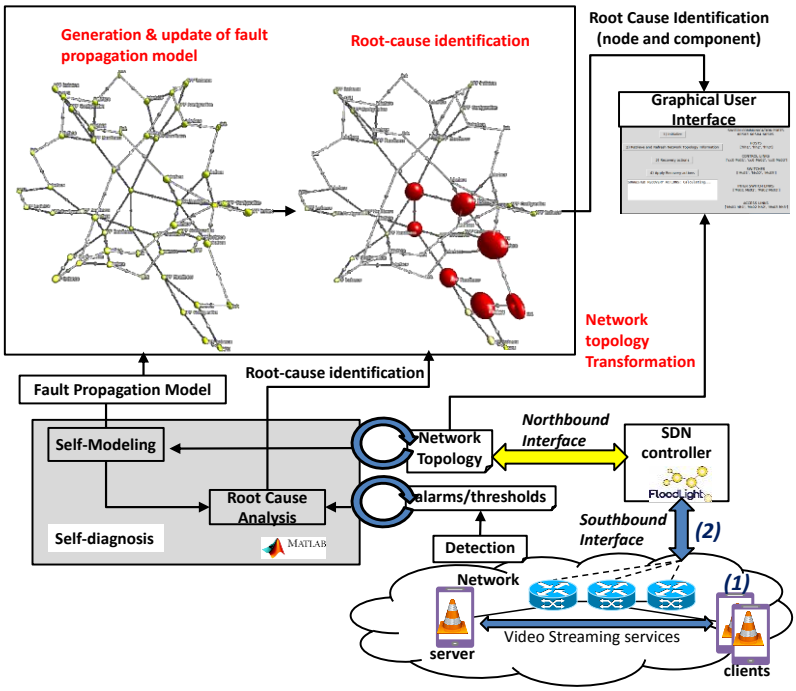

Figure 11: High-level view on the RCA for one single domain

The results of the RCA will be information on which network component n in the domain d is responsible for the service failure. The reputation calculation block domain d receives 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 is calculated for every network component within the domain d. The timestamps values are necessary because the reputation calculation block needs to calculate the availability of that network component, defined here as the amount of time the resource is not operating correctly (m) in a given time window W.

The reputation values from the network components r_n in each network domain d are 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 is 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 12.

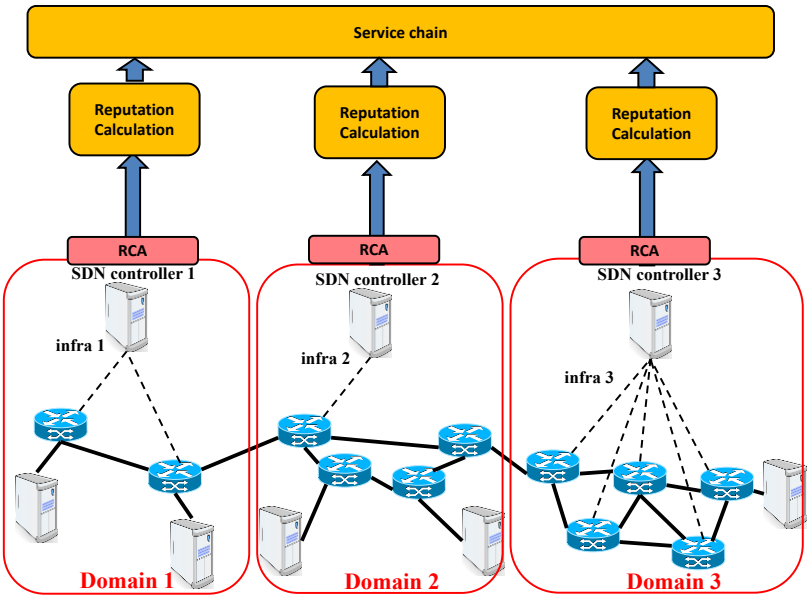

Figure 12. Hierarchical reputation propagation mechanism.

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 Technology Area

This reputation calculation mechanism is based on a RCA mechanism already implemented that takes 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.

4.5.3 Security Aspects

The centralization of the intelligence inside certain nodes in SDN/NFV enabled infrastructures makes paramount ensuring the resilience and security of those infrastructures. In addition, where some network service is delivered across several domains, it is very important to determine the domain responsible for service outages.

4.5.4 Security Challenges

The high dynamicity of SDN/NFV infrastructures such as the changes on the infrastructures, the rapid changing flows sent by the SDN controller, and the instantiation at run-time of the vNFs, are really challenging to establish an updated and accurate network model from which reputation can be computed in an accurate manner. This reputation calculation block is based on a RCA that takes into account all these changes at physical and virtual resource level.

4.5.5 Technical Roadmap

4.5.5.1 Features achieved in R1

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

4.5.5.2 Features in R2

This enabler is expected to be 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 [24].

We are going to consider two domains and a video streaming application traversing both domains as a proof of concept.

- **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 are planned to be released in R2 for that enabler.

4.5.6 Early 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

5.5 System Security State Repository

5.5.1 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 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 a knowledgebase 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 will also allow querying and analysis for a higher-level view of security incidents and trends.

Such a model of the system will document 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 can be 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

5.5.2 Technology Area for the Enabler

This enabler is the foundation for security practice governance and evaluation. It allows the system state to be captured in a model that later on can be compared with the design-time model from the Trust Builder enabler, visualized, shared, queried and analysed. The same semantic modelling technologies as the Trust Builder enabler can be used here in order to express the relations between the system entities and the security information regarding threats and controls.

5.5.3 Security Aspects

Security governance and compliance require a consistent overview of the system. This in turns requires a knowledge representation that allows the system state, security practice, incidents, remediation plans and results to be captured.

An ontology will be developed for the Trust Builder enabler to model systems at design-time. The same modelling approach can represent a system at runtime. This enabler will provide a service wrapping the deployment model of the system using data from other monitoring enablers to update the model and hence keep the picture of the system state up to date. A query interface will be provided which ultimately will allow the building of more sophisticated analysis and visualization tools on top of it.

5.5.4 Technical roadmap

5.5.4.1 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 can be 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.

5.5.4.2 Features in R2

- **Feature name**: System Security State Repository service
- **Goal**: software to create, update and query the runtime model
- **Description**: the software will ingest monitoring data from other monitoring enablers such as the Generic Collector and PulSAR (topology scanner component) and use the data and the 5G asset model (from R1 and to be updated in R2 of Trust Builder) to build a model of the assets and controls present in the system which can be compared with the design-time model from the Trust Builder. The 5G threat knowledgebase from Trust Builder R2 will be used to discover possible uncontrolled threats. The software will provide a query interface to allow other enablers' access to the data and for visualisation interfaces to be devised.

5.5.5 Early Recommendations

This enabler will be the first step towards runtime threat monitoring and will 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 will involve the monitoring of possible asset misbehaviours which can be used to determine the likelihood that a threat is on-going. Misbehaviour monitoring and threat likelihood computation will be planned but not be addressed by this enabler within the 5G-ENSURE project.

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

5.6.1 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[7] can be used to increase the accuracy of monitoring as monitoring can be focused 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 was defined for the first release (**R1**) of the enabler. The framework enables distributed monitoring, inferencing, and reactions to security incidents. It

[7] 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.

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 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 for the second release (**R2**), will extend the monitoring framework by

- Integrating it with different 5G network specific information sources (e.g. KPIs, counters, measurements and logs from eNodeB and core services available in the 5G-ENSURE testbed)
- Adding inferencing and control logic for adapting micro-segments by utilizing analysed risk-information.
- Integrating it with the Generic collector interface (CGI) enabler, PulSAR enabler and Trust metric enabler.

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 will be integrated with micro-segments and will thus enable 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	Use case 5.5: Control and Monitoring of

Security Monitoring and Inferencing (Release 1)	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 (Release 2)	Use case 5.5: Control and Monitoring of Slice by Service Provider
Cross-domain information exchange (Release 2)	Use case 5.5: Control and Monitoring of Slice by Service Provider

5.6.2 Technology Area

The enabler adopts the following technology paradigms:

- Machine learning technologies are leveraged for gaining security awareness.
- To increase scalability of monitoring, big-data paradigms and technologies (distributed computing, cluster computing, complex event processing, and publish-and-subscribe pattern) are utilized. State of the art software implementations, particularly Apache Kafka and Spark are utilized in the framework, which is illustrated in Figure 13.

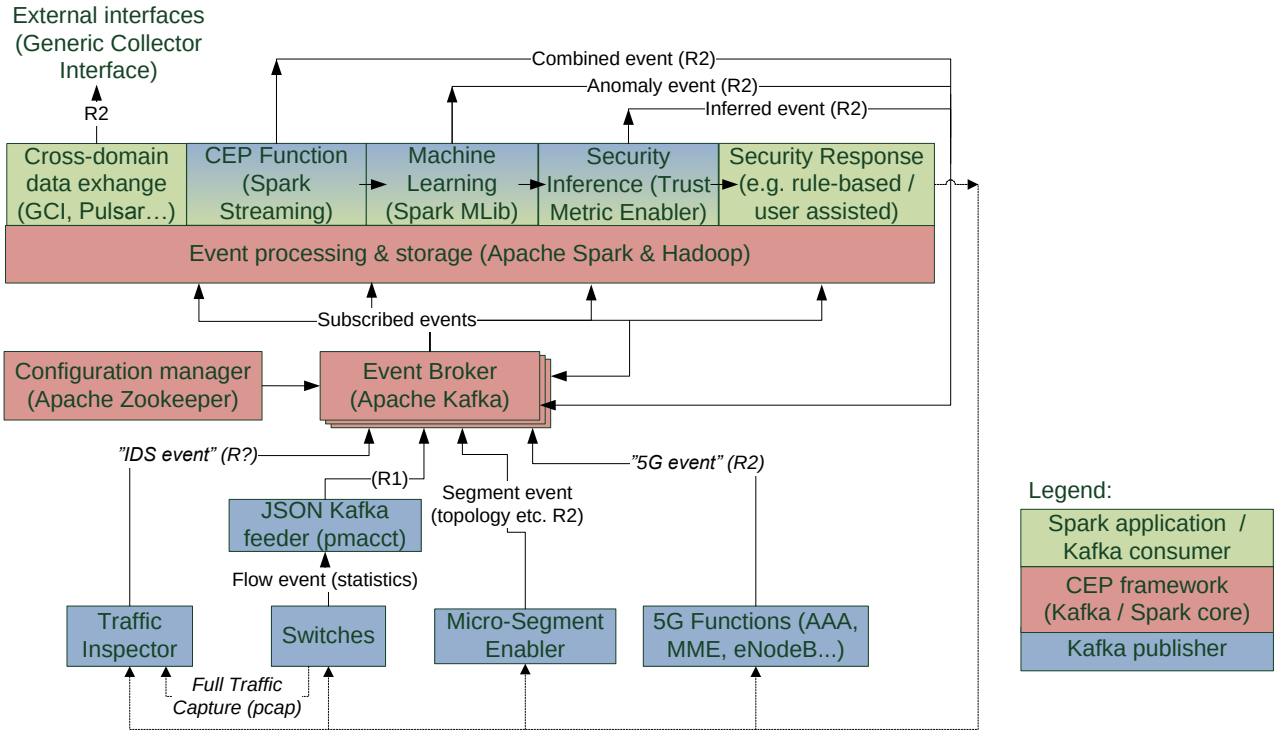

Figure 13. Framework for distributing monitoring information

The enabler is targeted for monitoring of 5G micro-segments. During Release 2 it will be integrated with the micro-segmentation enabler as well as with the trust metric enabler, the generic collector interface (CGI) enabler and PulSAR enabler. An initial architecture for integration has been illustrated in Figure 14.

Essentially, the monitoring enabler will collect information from the micro-segmentation enabler and from 5G testbed components in the micro-segment. This information will also be forwarded for the CGI enabler which will transmit it to the designated service such as the PulSAR for further analysis. The monitoring enabler will also itself analyse the collected data and based on this it will control micro-segment.

The objective is also to address multi-domain issues and enable orchestrating / building of end-to-end slices from several micro-segments. The monitoring enabler may support risk management of multi-domain scenarios by delivering information that is related to cross-domain attacks. For instance, after detecting excessive traffic (Denial-of-Service attack) originating from one micro-segment, the cross-segment risk manager may request the cross-segment orchestrator to select an alternative micro-segment to provide required end-to-end services.

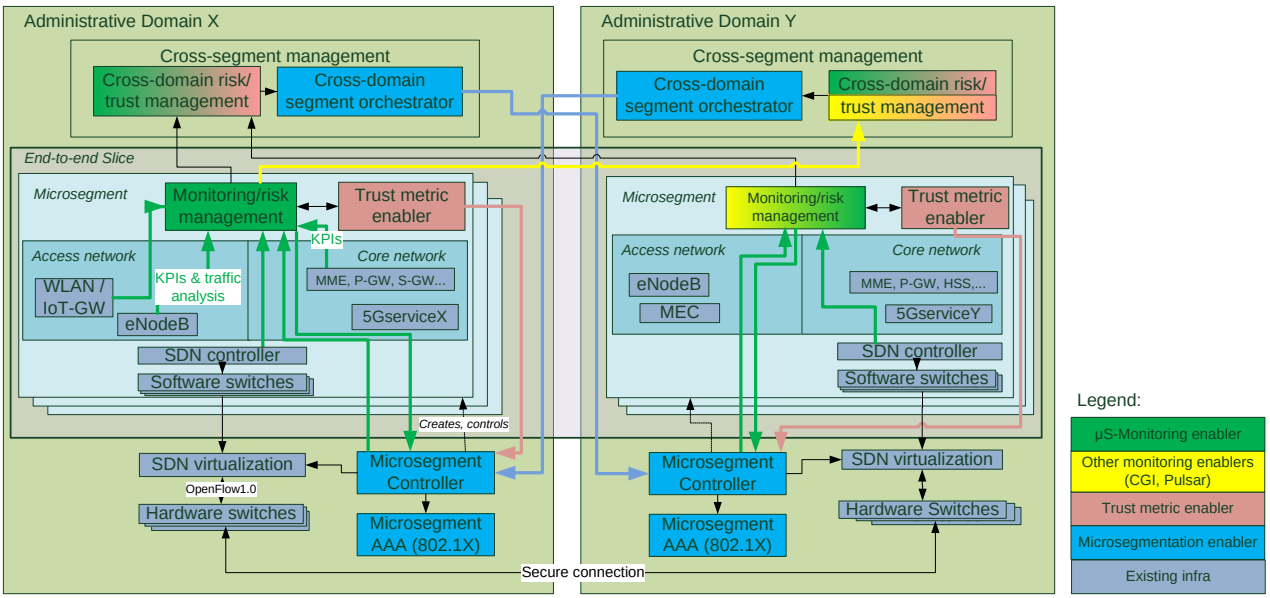

Figure 14 Architecture for integrating micro-segmentation related enablers

5.6.3 Security Aspects

Micro-segmentation based monitoring provides scalability and accuracy as monitoring can be focused to fewer devices and coherent traffic patterns. The approach enables fine-grained mean to control what security services are provided for which devices or type of communication. Essentially, micro-segmentation should enable monitoring system to be:

- *Adaptive* - Security monitoring for different micro-segments can be provided at different security levels. For instance, some micro-segments can be deeply monitored by inspecting communication in the different levels (cross-layer monitoring), by inspecting encrypted traffic (decrypting payload for monitoring) and from various aspects (searching different known threat patterns and anomalies with known effects); whereas some micro-segments can be monitored only in lightweight-manner.
- *Dynamic* - The intensity or focus of monitoring may change dynamically. For instance, detected suspicious traffic may trigger more intensified monitoring.

5.6.4 Security Challenges

The enabler addresses the following generic monitoring challenges (which are present when monitoring mobile networks):

- *Scalability* - the amount of heterogeneous data that needs to be analyzed at near real-time may be large. In (un-segmented) 5G networks, the 'attack surface' that must be monitored is large. With micro-segmentation the goal is to monitor each segment separately with solutions tailored for segment' needs.
- *Stealthiness of incidents* - many attacks do not have clear signs (indicators of compromise such as anomalies) that can be easily detected.
    - Micro-segmentation eases detection of some security incidents. For instance, as information within segments is more homogenous, anomalies are easier to detect. Also, in segments where endpoints are known and controlled, it is easier to detect attacker's control channels where the other endpoint is outside the segment.
    - Correlation (combining information from different sources) provides one approach to gain more accurate situation awareness.

The micro-segmentation concept introduces also some new challenges:

- *Multi-domain / cross-segment attacks* - monitoring micro-segment alone is not enough as attackers may circumvent defences in segment's borders. Therefore, the enabler must provide means to address attacks originating outside the segment (outside segment's authenticated and authorized users).
    - Detection of cross-segment incidents requires exchange of actionable information between different actors. Efficient and secure information brokering solutions are needed to enable this information sharing.
- *Dynamicity of micro-segments* - when micro-segments are constantly changing (e.g. nodes are added or removed) it is more difficult to learn 'normal behaviour' and detect anomalies.

5.6.5 Technical Roadmap

5.6.5.1 Features Achieved in R1 (Reminder)

- **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 will provide a CEP framework enabling development of use case and threat specific monitoring applications / inference logic. However, the monitoring and inference capabilities, in release 1, will be limited to few example cases. Existing event distribution framework exists (e.g. DDE) but integration requires adaptation work.
- **Rationale**: Enable scalable and extensible security monitoring in 5G networks.

5.6.5.2 Technical Roadmap for Release 2 (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 will provide algorithms for determining risk-levels related to selected threats. Machine learning techniques (anomaly detection, correlation analysis) will be utilized in the process. The algorithms will also be 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 and from eNodeB.
- **Description**: The feature will enable colleting of information from different data sources, particularly from 5G eNodeB as well as from micro-segment. Interface to Key Performance Indicators (KPIs) provided eNodeB within 5G-ENSURE testbed accouring data from the eNodeB which is hosted in VTT's testbed node) will be provided. Capabilities to collect topology and configuration information as well as traffic statistics from micro-segmentation enabler will be provided.
- **Rationale**: Enable extensive awareness over security state of 5G application

- **Feature name**: Cross-domain information exchange
- **Goal**: Exchanging monitoring data (with respect to the format described in D3.2) between the GCI enabler and micro-segmentation enabler
- **Description**: The micro-segmentation enabler collects data about a given micro-segment. The GCI enabler needs this information to feed other enablers such as PulSAR enabler.
- **Rationale**: Enable interconnection between heterogeneous administrative domains that support different monitoring enablers

5.6.6 Early recommendations for further research

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.

To increase accuracy of monitoring and security awareness in distributed, multi-domain scenarios information must be shared. However, such information sharing introduces new challenges. Hence, solutions are needed e.g. to enable sharing of monitoring information between different parties without revealing party specific secrets and at the same time addressing risks related to bogus information coming from untrustworthy (hostile or compromised) parties. These solutions can be based on privacy (e.g. anonymization) and access control mechanisms that enable sharing of sensitive information across administrative domains. Also, new mechanisms are needed for verifying trustworthiness of monitoring information that is coming from potentially hostile or compromised sources.

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

5.7.1 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 (For ex. CVEs).
3. Dynamic risk analysis: Context-awareness triggered by Security Information and Event Management (SIEM) reports
4. Remediation and countermeasure propositions at both design-time and run-time.

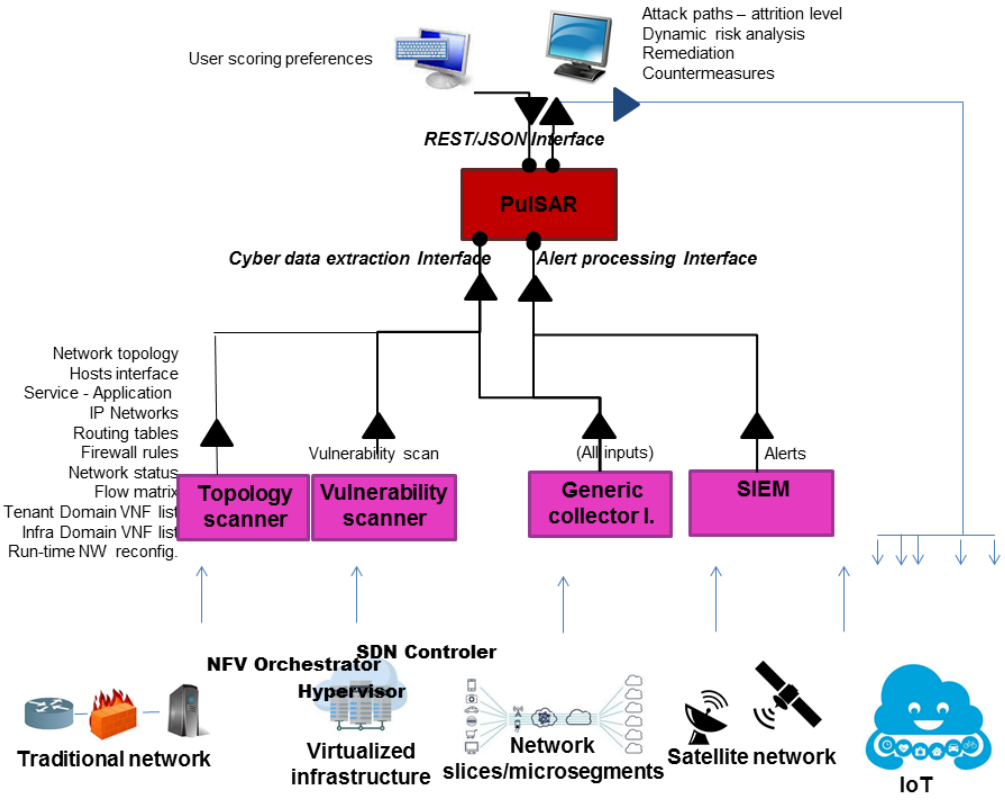

Figure 15. PulSAR overview

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 at the end of the Achievements of First Release (R1) section:

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

- Dynamic Risk Analysis: Using a Security information and event management (SIEM) report as input, the feature dynamically computes an up-to-date risk picture.
- Countermeasure: To cut an on-going attack
- 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

5.7.2 Technology Area for the Enabler

This enabler leverages on:

- Cyber-attack modelling technologies to capture and maintain attacker modus operandi through a scenario-oriented approach

- Graph theory (Bayesian attack graph modelling) to predict the evolution of a risk situation fed by security events and information collected within the networks, sensors, devices that make the Internet of Thing a vast and heterogeneous environment.

5.7.3 Security Aspects

The way this enabler is used will drastically change according to the role and business positioning of its owner, but confidentiality and integrity of the data and information collected will remain an essential security requirement.

5.7.4 Security Challenges

As the CyberCAPTOR has not been created for analysing vulnerabilities in a virtualized environment, this PulSAR enabler will thus have to be adapted (in particular by adding new attack rules for the Bayesian attack graph engine) to take into account the particularities of such a 5G environment using SDN and NFV technologies.

5.7.5 Technical roadmap

5.7.5.1 Features achieved in R1

- **Feature name**: 5G specific vulnerability schema
- **Goal:** Extension of the Cyber-attack modelling.
- **Description:** This feature will benefit 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 who 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.

In fact, together with the 5G specific vulnerability schema, software has been delivered in Release 1 with a first implementation of the schema. Here below is illustrated the coverage of this implementation towards the initial CyberCAPTOR perimeter.

Table 17: PulSAR roadmap summary

CyberCAPTOR	PulSAR R1 as announced in D3.1 roadmap	PulSAR R1 delivery	PulSAR R2 delivery target
	5G specific vulnerability schema	5G specific vulnerability schema	5G specific vulnerability schema
Cyber inputs integration		Cyber data extraction	Cyber data extraction
Scored Attack Paths – Fusion		Attack graphs	Attack graphs
Scored Attack Paths – User preferences		Scored attack paths	Scored attack paths
Risk Visualization – Attrition level		Visualization	Visualization
Dynamic Risk Analysis			Dynamic Risk Analysis
Remediation catalog - Virtual patching			Remediation
Remediation catalog – Network configuration			Countermeasures
Remediation automation		5G specific vulnerability schema implementation	5G specific vulnerability schema implem.
			PulSAR interface with Generic Collector

NB: Features inherited from CyberCAPTOR are put in black. Features developed in PulSAR are put in blue.

5.7.5.2 Features in R2

Feature name: 5G specific vulnerability schema implementation

- **Goal**: Implementation of an extended Cyber-attack modelling for 5G.
- **Description**: This feature implements the 5G specific vulnerability schema. This release is expected to provide an enhanced version of the 5G vulnerability schema, according to the new attacks methodology discovered during the project lifetime. PulSAR should work on the whole initial perimeter of CyberCAPTOR.
- **Rationale**: 5G networks will face novels complex cyber-attacks who 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.

5.7.6 Early Recommendations

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.

5.7.7 Remarks

For further insight with the early recommendations presented here, please refer also to D2.4 Security Architecture (draft) available on project web site (see there Recommendation section).

5.8 Security Enabler "Satellite Network Monitoring"

5.8.1 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 will be identified. Security metrics, counter measures and the mitigation level they provide should be determined.

The main goal of this security enabler is to provide pseudo real-time monitoring and threat detection in these systems. Several indicators (including security metrics) will be collected from the listed 5G integrated satellite and terrestrial systems and will be periodically delivered to the monitoring system using a Generic Interface in a secure way.

Later, an active security analysis will be 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 18: 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

5.8.2 Technology Area for the Enabler

The enabler operates in a technology area of 5G integrated satellite and terrestrial systems. Such systems ensure high availability and service reliability with a 100% geographic coverage.

Such as a security enabler is important because there are several 5G use cases that can only be served by satellites or for which satellites provide a more efficient solution.

5.8.3 Security Aspects

The main goal of this security enabler is to provide pseudo real-time monitoring of indicators collected from the system in a secure way (e.g. using AAA protocols). The aim of these indicators is to protect against internal and external threats coming from the heterogeneous 5G satellite networks.

These indicators can be classified in three categories:

- Health status:
  - Intrusion detection.
  - Alarms scanned by satellite network devices.
  - Excessive load.
- Configuration state:
  - Network status.
  - Credential status.
- Counters:
  - Volume counters.
  - Efficiency counters.

For each component, the security enabler should allow to periodically deliver the collected indicators to the monitoring using a Generic Interface in a secure way.

The enabler will use active security analysis to detect, investigate and respond to the threats identified.

5.8.4 Security Challenges

Components are distributed in a heterogeneous 5G wide-area network. The area to be monitored is “wide” in the sense that it is remote and/or large enough that other wired or wireless network connectivity for the number of nodes deployed is impractical.

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

The amount of data that needs to be analysed at near real-time may be large and heterogeneous. The Satellite Network Monitoring needs to handle large amount of metrics, graphs and indicators and needs to visualize them to the operator in a quick, effective and intuitive format. Partitioning the satellite network into virtual private network might be an efficient solution, so that each segment is managed separately and appropriate solutions are tailored to each partition.

This security enabler should improve the security of operators/users, while maintaining or increasing the level of productivity. The challenge is the definition of the KPI that demonstrate such improvements.

5.8.5 Technical Roadmap

During R1 was achieved both features described in R1, pseudo real-time monitoring and threat detection. During the first release, it was done both of them separately, achieving in the first feature a prototype to monitor the indicators and with the second feature a threat generation and detection correlating different incidents to detect them. This threat detection is also the feature which know why this threat appears and a gives an advice to the operator about which will be the prefer procedure. The R2 will join both features in order to do an active security analysis, where the indicators can be monitored and used to detect or to give a better advice with the threats.

5.8.5.1 Features achieved in R1 (Reminder)

- **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 will be collected in a heterogeneous 5G satellite system and will be periodically delivered to the monitoring system using a Generic Interface 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.

The features achieved in R1, for the different features were:

- **Feature name**: Pseudo real-time monitoring:
  - Indicators generator was developed, including the credentials management.
  - Those indicators are collected and joined together.
  - The same indicators list can be delivered to the monitoring system using a generic interface.

- **Feature name**: Threat detection:
  - Creation of the different rules to detect threats.
  - Threats generation to simulate the scenario.
  - Those threats have been linked to the probable cause.
  - A relation between the previous threats and a possible advice for the operation have been created.

5.8.5.2 Features 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 will be 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 will be 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, will be possible to 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 will be enable to define 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 will suggest 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. The next step to improve the security capabilities is the possibility to determine and prepare 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.

5.8.6 Early 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 splitted 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.

5.8.7 Remarks

The advantages of incorporating satellite network monitoring as a 5G Security Monitoring enabler will benefit other 5G enablers:

- Regarding AAA enablers, even though network members (devices, nodes, etc.) might be securely authenticated when they join the satellite network, Satellite Network Monitoring enabler is expected to detect changes in network member's configuration.
- In the case of BotNet attacks, Satellite Network Monitoring enabler is expected to identify abnormal activity occurring at mobile devices and report this activity, by:
    a) Providing the end user with visually represented historical data of the activity of terminals connecting through Satellite Network, as well as with representation of which Satellite Network Operator controls the terminal connecting to.
    b) Configuring 5G satellite terminals, hubs and hybrid EnodeB's with specific restrictions and privileges

Finally, in the case of "Verification of the Virtualized Node and the Virtualization Platform" use case, this enabler is expected to add monitoring policies upon request of the testers of Virtualized Nodes, so that the tester receives a notification if the location of the node is changed in the satellite network.

5.9 Generic Collector Interface

5.9.1 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 in Release R1 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.

5.9.2 Technology Area for the Enabler

This enabler implementation and integration in some 5G Nodes and other 5G-Ensure enablers ease the detection of fraud schemes, first signal of security incident or divergence in the availability of network. The capacity to react in near real-time is linked to the capacity to deliver events that are not accessible today and in particular to propose a fixed header format, that suits all 5G network's layers.

5.9.3 Security Aspects

The way this enabler is used will drastically change the capacity of the network to be monitored in real-time.

5.9.4 Security Challenges

The major challenge was to define an efficient event structure (fix and dynamic parts) that suits and complies with 5G Networks' layers and nodes.

5.9.5 Technical Roadmap

5.9.5.1 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 will be 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.

5.9.5.2 Feature in R2

There is no release R2, we will support 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 already planned as feature release in the following enablers R2.

- System Security State Repository enabler R2: System Security State Repository service
- Security Monitor for 5G Micro-Segments enabler R2: Cross-domain information exchange
- PulSAR: Proactive Security Analysis and Remediation enabler R2: PulSAR interface with Generic Collector

5.9.6 Early 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.

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 [25] 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
Controller-Switch-Interaction Imitator	Use Case 5.3: Reactive traffic routing in a virtualized core network

6.1.2 Technology Area

The enabler operates at the data plane of SDN networks in general. Since SDN concepts, in particular, a (logically) centralized and software-based control plane, will be adopted in 5G networks, this enabler will also apply to 5G networks.

The enabler delays the forwarding of packets of a network flow. Note that delaying all network packets is prohibitive in terms of network performance. Hence, the components at the data plane (e.g., the switches) select the packets that are delayed. This means that the use of the enabler does not produce any additional overhead to the network's control plane of forwarding packets. However, the control plane configures the selection process and the delay time.

The enabler's implementation requires minor modifications of an OpenFlow switch. Most of these modifications are already supported by the OpenFlow protocol (version 1.3) [26]. Note that OpenFlow is the most deployed protocol in today's SDN networks. It defines how data-plane components (e.g., switches) interact with the network controller at the network's control plane.

6.1.3 Security Aspects

The enabler prevents information leakage about how network packets are processed in an SDN network. In particular, it prevents the leakage of the information about which packets trigger a controller-switch interaction. Having such information at hand makes an SDN network vulnerable to different kinds of attacks.

Rule Scanning. By fingerprinting the SDN network, an adversary can infer whether a flow rule has been already installed by the controller to handle a specific type of traffic or route towards a given destination. For example, the adversary can craft probe packets whose headers match the traffic type and/or destination address and infer by measuring the timing of the packets whether these packets triggered the installation of a rule. This provides a strong evidence for the adversary that communication with the given destination address has recently occurred. Depending on the underlying rule, the adversary might also be able to infer the used network protocol, and the destination port address. By doing so, the adversary obtains additional information about the occurrence of a particular communication event. For example, the adversary can infer whether the destination address has recently established an SSL session to perform an e-banking transaction. Note that this leakage is only particular to SDN networks, and does not apply to traditional networks. Also note that the adversary can send the probe packets from a remote destination. However, additional knowledge about the network or the network slices reduces the adversary's space of crafted probe packets.

The fingerprinting of rules enables the adversary to better understand the logic adopted by the controller in managing the SDN network. This includes inferring the timeouts set for the expiry of specific rules, whether the controller aims at fine-grained or coarse-grained control in the network, etc. Similar to existing port and traffic scanners, this knowledge can empower the adversary with the necessary means to compromise the SDN network. Even worse, the adversary can leverage this knowledge to attack other networks which implement a similar rule installation logic. For instance, in a geographically dispersed datacenter, different subdomains typically implement the same policies. The adversary can train using one subdomain and leverage the acquired knowledge in order to compromise another subdomain.

Denial of Service. The rule space is a scarce resource in existing hardware switches. Namely, state-of-the-art OpenFlow hardware switches can only accommodate few tens of thousands rules, and only support a limited number of flow-table updates per second. While these limitations can be circumvented by means of a careful design of the rule installation logic, an adversary that knows which packets cause an interaction with the controller can abuse this knowledge to launch tailored DoS attacks. For instance, an adversary might simply try to overload the controller with processing OFPT_PACKET_IN OpenFlow messages. Instead of blindly guessing for which packets a switch sends an OFPT_PACKET_IN OpenFlow message, the adversary first fingerprints the SDN network, i.e., it gains knowledge for which packets a switch interacts with the controller. This can be done passively by observing the network traffic. The adversary then exploits this knowledge by sending dedicated packets, where each of them most likely triggers a controller-switch interaction.

Another kind of DoS attack is to fill up the switches' flow tables. An analogy to this is when a computer runs out of memory and starts swapping. Usually, the computer becomes unusable. Similarly, the network performance is severely harmed when the flow tables are full (or even almost full). First, installing flow rules in an almost full table is costlier than in an almost empty flow table. Second, in case the flow table is full, either new network flows cannot be established, which would already be a denial of service, or some installed flow rules need to be deleted. However, in general, it is not obvious which rules should be deleted to make room for new rules; this needs to be coordinated by the controller and is a complex operation, which can quickly overload the controller and the switches. For example, the deletion of a rule of an ongoing network flow might entail the rule's immediate reinstallation. This can escalate and the controller will have to constantly delete and reinstall rules.

6.1.4 Security Challenges

The challenge this security enabler faces is the prevention of an adversary to gain knowledge about the forwarding logic of an SDN network without significantly decreasing network performance. In particular, the speed of forwarding packets at the network’s data plane must not be significantly decreased. To this end, the enabler has to select a few packets that need to be delayed. It might be necessary to dynamically adapt the selection criteria and the delaying times when network conditions change. A general security challenge is to prevent DoS attacks to networks.

6.1.5 Technical Roadmap

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 [27]), 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 [28] 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) [29] [30] 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 [31].

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

6.1.6 Remarks

Note that the above described enabler enhances the privacy of an SDN network as it makes rule scanning as described in Section 6.1.3 harder. From this point of view, the enabler overlaps topic wise with Privacy enablers that target the protection of the privacy of network users and their data. In contrast, this enabler focuses more on privacy issues of network operators or service providers.

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 [32]) 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.

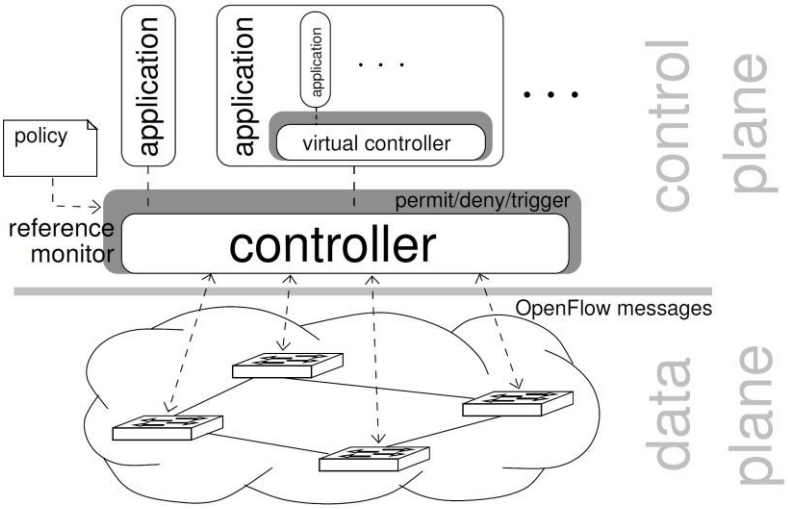

Figure 16: SDN controller extension with a reference monitor.

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 [25] of this enabler's feature (see Section 6.2.5) are listed in the following table.

Table 20: 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 Technology Area

The enabler operates at the control plane of networks that are managed and operated through software components. Since SDN concepts, in particular, a software-based control plane, will be adopted in 5G networks, this enabler will also apply to 5G networks.

This enabler adds access control mechanisms to state-of-the-art SDN controllers. These mechanisms are crucial to secure the control plane of an SDN network. The network's data plane is only indirectly affected

in the sense that any access to a component at the data plane that is initiated by a component of the control plane must be policy compliant. Furthermore, this enabler also adds mechanisms to containers that host VNFs for the permissions of these containers.

Access control mechanisms are fundamental in information systems. They are standard in computer systems like operating systems, database systems, and web services, where multiple users share computing resources. However, softwarized networks, e.g., SDN network, currently lack such mechanisms, even the most basic ones. Note that network resources will be shared in 5G networks. Multiple network services will be running at the control plane of a 5G network, possibly by different service providers with competing objectives. Even when these (virtualized) network services run in different (virtualized) network slices, they will access and configure physical resources shared at the network's control plane.

6.2.3 Security Aspects

A fundamental principle in information systems is the *principle of least privilege*, that is, any subject must only access the information and resources that are necessary for its legitimate purpose. Adherence to this principle is beneficial for data protection, the prevention of malicious behavior, and system stability.

6.2.4 Security Challenges

Although various access control solutions already exist for a wide range of systems, it is not obvious that these solutions are applicable in the context of softwarized networks in general and SDN and NFV in particular. One main challenge will be the development of access control mechanisms that do not harm network performance and still cover a wide range of access control policies. This means, one must balance well between expressivity and performance. Another challenge is to provide access control mechanisms that account for different network views and network abstractions. Consistency between access control policies is another challenge. However, this is a general challenge and not specific to access control mechanisms for SDN and NFV.

Note that in general there is a tradeoff between performance (and usability) and security guarantees. In particular, the enabler faces the challenge to be compliant on the one hand with the 5G's performance KPIs. On the other hand, the enabler protects the network's control plane from vulnerable or even malicious network applications. This allows a network provider to use third-party software tools to manage the network. Note that there are already various startups that offer such software products for SDN networks. This market is expected to grow significantly in the future. For example, Hewlett Packard has opened an SDN app store in 2013 [33], and some expect a market size of $35B in 2018 with a significant growth in software, see [34].

6.2.5 Technical Roadmap

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 [32] [35] was developed and evaluated in a Mininet environment [36]. 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 [37] 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.

6.2.6 Early 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 Task 3.3.

6.2.7 Remarks

- Our choice of extending the SDN controller ONOS [32] [35] with a reference monitor is as follows. ONOS is a high-performance, state-of-the-art, actively developed SDN controller. Furthermore, it is widely used—both in academia and industry—and it is open source with a fairly small code base in JAVA. It also maintains a NIB, possibly between multiple controllers, and it provides higher level APIs (e.g., the intend framework for network flows), for which we plan to extend our access control model and the reference monitor. However, adding the feature of a reference monitor to other state-of-the-art SDN controllers like OpenDaylight [38] should be similar to our ONOS extension.
- In the releases of the first feature of the enabler (i.e., the Southbound Reference Monitor), we opt for an access control scheme that is simple and close to the southbound API of the controller, which interfaces directly with the switches using OpenFlow. Furthermore, it focuses on the network flows. The rationale behind this design decision is as follows. First, it supports one to build a tamperproof and verifiable reference monitor. This is rooted in the scheme's simplicity and its particular focus, namely, the access to flow rules and flow tables. Furthermore, since the controller only communicates via OpenFlow messages with the switches, we obtain complete mediation by permitting or denying OpenFlow messages by the reference monitor before they are sent. These are essential principles for a reference monitor; see [39]. Second, the switches' flow tables are one of the most sensitive resources in a multi-tenant network. Their entries determine how the network handles the traffic. Moreover, they are shared between the tenants and their capacities are scarce. Controlling the access to them protects the network flows. Finally, we expect that future northbound APIs in SDN will support multiple different abstractions of the network at the control plane. Any such interface will be built on top of the interface provided by OpenFlow, which directly interacts with the network components. Access control at higher layers will utilize access control scheme for the southbound interface of the network's control plane and complement it.
- Finally, we want to remark that this enabler is related to other tasks. For example, as already pointed out in Section 6.2.1 network applications might not be trusted. Furthermore, restricting the access of network tenants to the NIB of a network is a privacy-enhancing mechanism for an SDN controller.

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 6.2 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. 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 grants or prevents a request of a network component of accessing network resources. It *enforces* a given access control policy [40]. 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. 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 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 [25] of this enabler's feature (see Section 6.3.5) are listed in the following table.

Table 21: 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 Technology Area

This enabler targets softwarized networks, e.g., SDN networks and networks in which some of their functions are virtualized. Since SDN and NFV concepts will play a major role in 5G networks, this enabler will apply to 5G networks. As in SDN, it is expected that separated network planes will interact with each other via standardized protocols. For instance, a 5G network will provide multiple (virtualized) network

services (possibly running on different network planes) that directly or indirectly interact with each other, similar to an SDN network, where the network controller interacts with the switches at the network's data plane.

The enabler aims at verifying the interaction between network components, e.g., controller and switches, and NFVs. In case a virtualized network is running on top of the physical network, the enabler can check that the two networks interact correctly with each other, i.e., commands from one network are correctly translated to commands of the other network. Analogously, the policy compliance of the interaction between network services can be checked.

6.3.3 Security Aspects

Networks comprise multiple components. Security policies specify both how these components should behave and how they must not behave. Similar, workflows specify how an entity should react to certain events. Detecting noncompliant behavior of components with respect to a given policy or workflow is an important task to ensure the correct and save operation of a network. In particular, in a network in which (physical and virtual) components are managed by different tenants and directly or indirectly interact with each other, the detection of noncompliant behavior of a component is a major concern for the network operator. It helps the operator to protect the network, e.g., against misbehaving components and misconfigurations.

6.3.4 Security Challenges

One challenge for this security enabler is to cope with a wide range of security policies. However, the policy specification language must be carefully designed since policies must be handled efficiently by the enabler, this means, the enabler must efficiently check policy compliance of the interaction of the network components. Furthermore, the enabler must scale to networks that comprise many components that frequently interact with each other.

Another challenge is to account for interactions that comprise different network layers. The system components must generate meaningful messages about their performed actions. For simple SDN networks that comprise a single data plane and one controller, this is rather straightforward. However, for more complex networks with virtualized networks or virtualized network functions, this is less obvious.

Another challenge is to relate the output produced by the compliance checker to audit standards (e.g., CSA CCM). Tool support for automation such a conversion would be a huge benefit. Such audits are often required in regulated areas and must be performed by external entities.

6.3.5 Technical Roadmap

This security enabler will comprise 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 will be continued 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 nonpolicy 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 [41] [24] environment, identifying performance bottlenecks. In the second year of the project, we will focus 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 will be 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 will comprise a proof-of-concept of the compliance checker of the basic NFV reconfiguration that will be able to check the compliance of simple workflows for reconfiguring VNFs. To this end, we will instrument Docker [42] to send messages to the compliance checker about the performed actions that are relevant for containers that host VNFs. Furthermore, we will provide a simple NFV orchestrator that also sends messages about its performed actions to the compliance checker.

6.3.6 Early Recommendations for Further Research

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

6.3.7 Remarks

We remark that when checking online (i.e., during runtime) whether the interactions between different network components comply with a given security policy, overlaps topicwise with Task 3.4 (Security Monitoring). However, the enabler here does not account for network traffic but instead focuses on how the components are managed and how they interact with each other.

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 [43]. 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 17 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.

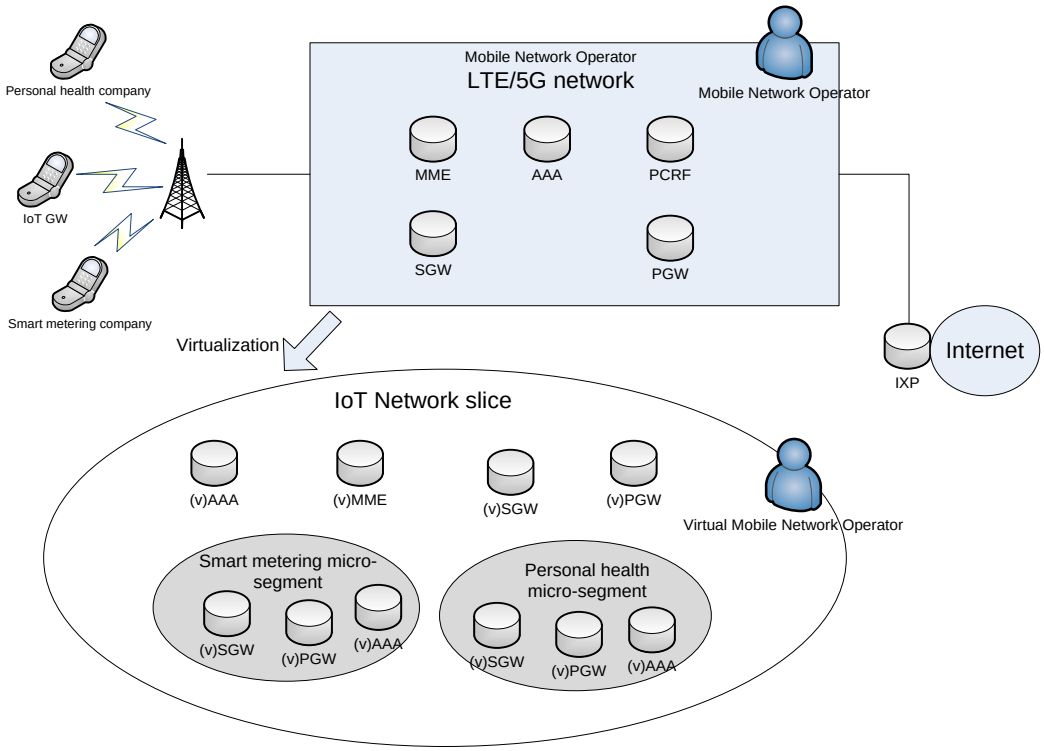

Figure 17 Micro-segmentation in a single domain network

In a multi-domain/multi-operator setting, end-to-end security could be achieved by chaining micro-segments from multiple network slices. Figure 18 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.

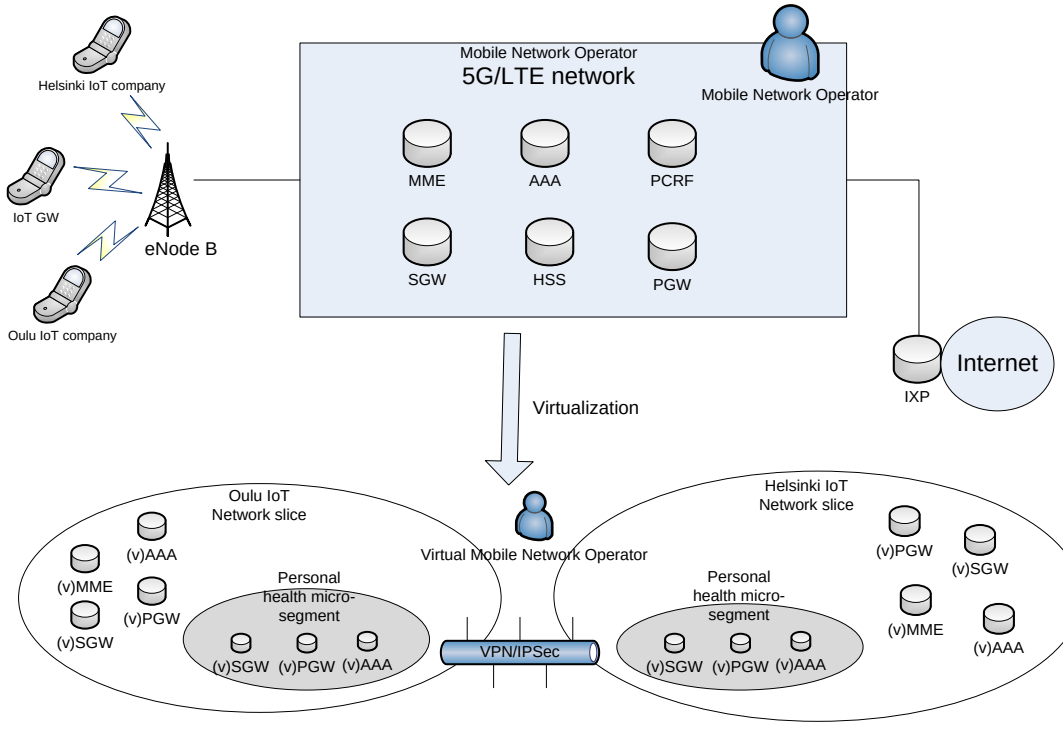

Figure 18 Micro-segmentation in a multi-domain network

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 22 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 Technology Area

The main technology areas of the enabler are single domain and multi-domain software networks.

6.4.3 Security Aspects

The upcoming 5G networks are envisioned to consist of a large number of heterogeneous devices, services, and amount of network traffic. This brings scalability challenges for the security of the mobile network.

Having large segmented security zones can create significant attack surfaces and enable threats to move throughout large portions of the 5G network unrestricted. The aim of the enabler is to divide the network into smaller parts, i.e., micro-segments so that monitoring of anomalous behavior or threats and responding to them would be easier, thereby significantly reducing the surface for attacks and threats. The security functions within a micro-segment can target both 5G specific generic threats and threats related to micro-segments [19].

6.4.4 Security Challenges

This enabler has several different security challenges. First, the enabler should guarantee a high level of security for devices that belong to the micro-segment. More specifically, the enabler has to prevent attacks from outside the domain directed towards the micro-segment. Other attacks coming from adjacent micro-segments can also be considered. It is also important to enable dynamic restructuring within a micro-segment by utilizing dynamic security monitoring and combining it with micro-segmentation. Another challenge is to find a suitable trust model for micro-segmentation [18] and determine the AAA aspects of micro-segmentation.

6.4.5 Technical Roadmap

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 will be continued 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 [41] [24] environment and used IEEE 802.1X access control. The prototype used OpenVirtex [44] software based virtualization and Ryu SDN controller [45].

The second release (R2) of this security enabler will include 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.

6.4.6 Early Recommendations for Further Research

Possible future research includes flexible cooperation and connection mechanisms between micro-segments residing in different domains and different operators.

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 will consist 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 23 while a high-level architecture is presented in Figure 19.

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.

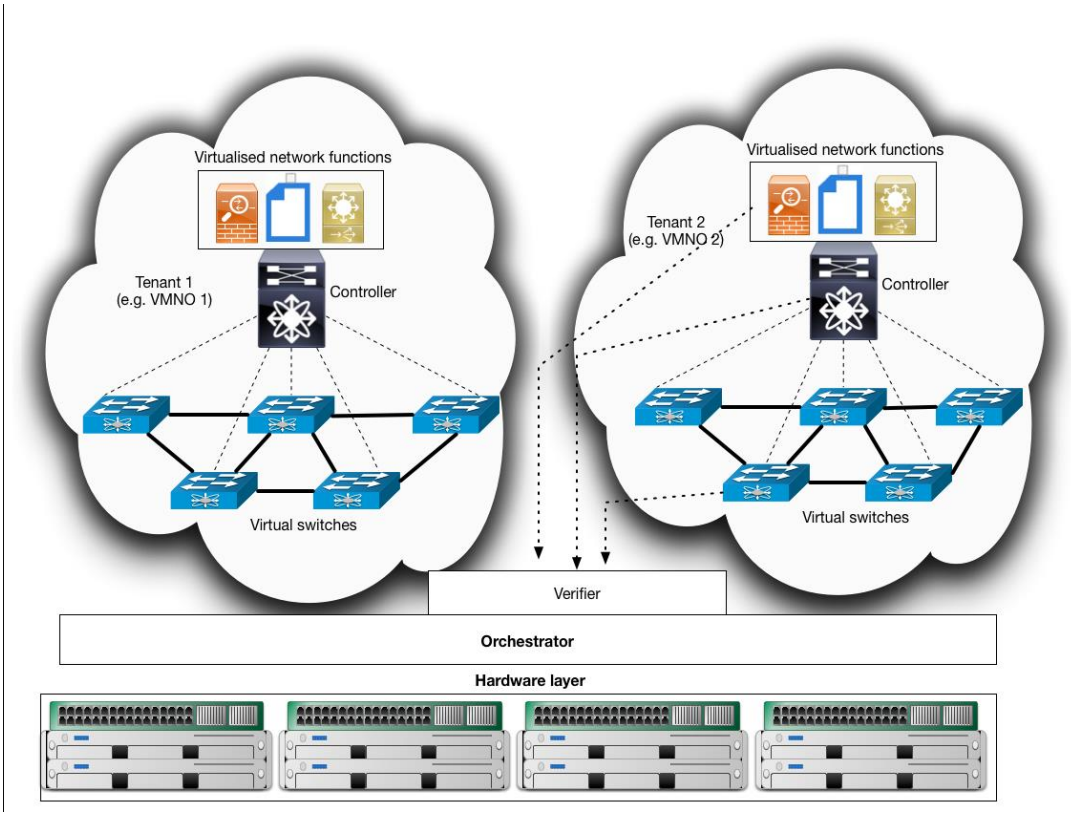

Figure 19: Integrity verification of virtual network components.

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 23 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 Technology Area

This enabler is used in SDN networks. It operates in both the control plane and data plane of an SDN network deployment, addressing exclusively software switch implementations and VNFs. Its features produce integrity measurements of the software switches deployed on the data plane and of the VNFs deployed on the control plane. The network controller evaluates the measurements prior to enrolling the respective virtual switches and VNFs into the deployment. Communication of the integrity measurements to the network controller is done through an out-of-band channel.

6.5.3 Security Aspects

This enabler addresses several security aspects of constructing the SDN topology:

(1) Including network components that have a *known* and *expected* configuration; integrity of the virtual switches and VNFs must be verified prior to enrollment. Cryptographic material required for component authentication access must be protected with a hardware root of trust.
(2) Preventing impersonation of network components; the network controller must be protected from network components that attempt to distort the global network view. This applies both to centralized and distributed network controllers.
(3) Preserving confidentiality and integrity of communication between virtual network endpoints in the presence of an untrusted cloud infrastructure provider.

6.5.4 Security Challenges

This enabler addresses the ability of the adversary to negatively affect the SDN deployment by either enrolling compromised network components in the data or control plane, or impersonating and changing the configuration and integrity of enrolled network components. Likewise, this enabler helps thwart the adversary's ability to attack the assets critical to protecting the confidentiality or integrity of the communication within the deployment.

6.5.5 Technical Roadmap

- **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 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 [46]. 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 [47].
- **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. In the second year of the project, we plan to improve the stability of the enabler and use the Intel SDK for SGX [23] in order to implement components that require an isolated execution environment.

The second feature of this security enabler is described below. It will be developed 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 [46] – 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 proof-of-concept of the *Integrity Attestation of VNFs* will be able to verify the integrity of a limited set of assets and reliably report the verification results to the security orchestrator. To this end, we will measure security-critical Docker assets using Linux IMA, verify them using a trust

agent running in an SGX isolated execution environment, and report the verification results to a security orchestrator.

6.5.6 Early Recommendations for Further Research

Improved versions of the enabler will be developed, in order to be integrated with one of the popular SDN controllers, namely, Floodlight. Furthermore, subsequent releases will 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 [46] 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 [46] 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.

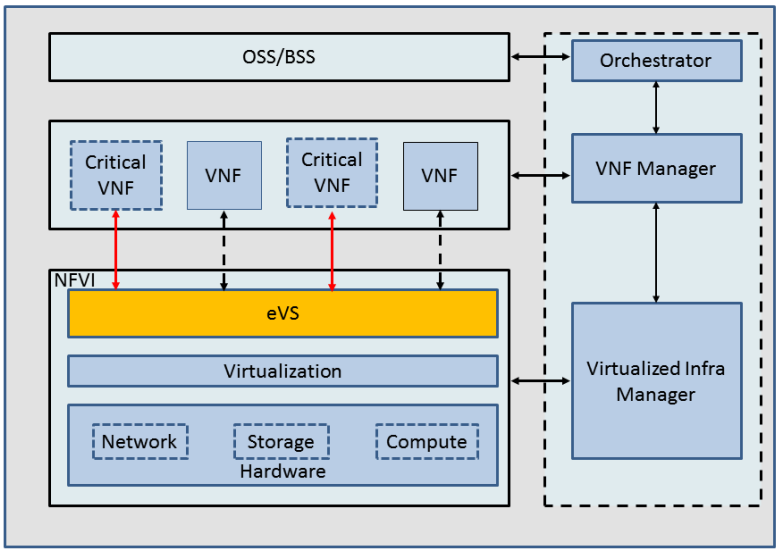

Figure 20: ETSI NFV Architectural framework comprising an eVS protecting critical VNFs from network-based threats.

Table 24 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 Technology Area

The enabler provides security and resiliency at the data plane of the 5G networks. The flow control, threats detection and mitigation rules offered by the *eVS* are provisioned through the control plane using the programmability of the *eVS* and reusing concepts from SDN. The SDN controller resides inside the *Virtualized Infrastructure Manager* block (MANO part of the architecture defined by ETSI NFV) in Figure 20 and provides the basic security rules to be enforced by the *eVS*.

As of today, flow control, detection of security threats and mitigation in virtual networks is delegated to the virtualized manager (controller) which becomes easily congested and represents a single point of failure. To

avoid this, state-of-the-art solutions propose to adopt packet sampling or flow aggregation strategies, losing thus the granularity of information that can be exploited during the phases of detection and mitigation. The enabler proposes to protect critical VNFs behind an eVS which is a programmable switch that has the possibility to enforce detection and mitigation rules directly on the eVS.

6.6.3 Security Aspects

In order to protect network functioning from protocol and applicative attacks critical services offered by VNFs, it is of paramount importance to rapidly detect and mitigate network-based attacks. For instance, in 2014, 21% of DDoS attacks were targeting Firewall applications, 10% IPS/IDS, and 3% load balancers.

6.6.4 Security Challenges

Although threat detection and mitigation solutions already exist for virtual networks, they repose solely on the ability of the network controller to supervise the overall network. This poses scaling issues whenever the amount of traffic to analyse becomes huge, concurring also in congesting the links between the controller and switches and thus facilitating the achievement of attacks.

The main challenge consists in offering the possibility to the *eVS* to automatically detect and mitigate possibly threats targeting certain critical VNFs. The programmability of *eVS* makes it possible to update and adapt the behaviour at runtime and protect them directly on the virtual network interfaces.

6.6.5 Technical Roadmap

- **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 will be implemented, in order to be integrated with one of the most popular SDN controllers (Ryu).

6.6.6 **Early 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.

7 Summary

The table below summarizes the update of the 5G-ENSURE Technical Roadmap. 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, Network management & virtualization isolation) the features in scope distinguishing between the ones in scope of release 1 and the ones (either continued or fully new) in scope of the second release of 5G-ENSURE. Whereas features of enablers in R1 have been already worked out and software released through v1.0 in September 2016, the ones in R2 would be delivered as part of the next release (i.e. v2.0) due by end of the project. Overall this table also shows each of the 5G-ENSURE security enablers with the features it would have specified and for most be developed by the end of the 5G-ENSURE Project.

Table 25: 5G-ENSURE Technical Roadmap update (reminding R1 features and highlighting features for R2)

Category	Security enabler Name	Security features	
		R1 features (achieved)	R2 features (planned)
AAA	Basic AAA enabler	Forward Secrecy (early specification) AAA aspects of trusted micro-segmentation (early specification)	Forward Secrecy AAA aspects of trusted micro-segmentation Trusted interconnect and authorization
	IoT	*Group authentication by extending the LTE-AKA protocol* *«GBA*	Group-based AKA continued (focus on PFS, OAI impl.) Non-USIM based AKA Bring Your Own Identity (BYOI)
	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 ongoing IETF standardization
	Federative authentication context usage	*none*	Storage of authentication level Usage of authentication level
Privacy	Privacy Enhanced Identity Protection	*Encryption of Long Term Identifiers (IMSI KPABE-based)*	Home Network centric IMSI protection IMSI Pseudonymization
	Device Identifiers Privacy	*Enhanced privacy for network attachment protocols*	Anonymous and optimised address selection for network attachment
	Device-based Anonymization	*none*	Format preserving anonymization algorithm Privacy configuration
	Privacy Policy Analysis	*none*	privacy policy specification privacy preferences specification comparison of policies and preferences
Trust	Trust Builder	*5G asset model v1* *Graphical modelling tool v1*	5G asset model v2 Graphical modelling tool v2 5G threat and trust knowledgebase
	Trust Metric Enabler	Trust metric based network domain security policy management	Improved trust metric based on extended data
	VNF Certification	VNF Trustworthiness Evaluation	VNF Trustworthiness Certification
	Security Indicator	none	Security indicator subscriber display
	Reputation based on Root Cause Analysis for SDN	none	Root Cause Analysis for SDN
Security monitoring	System Security State Repository	Deployment model ontology (also known as 5G asset model)	System Security State Repository service
	Security Monitor for 5G Micro-Segments	Complex Event Processing Framework for Security Monitoring and Inferencing	Risk-based adaptation of micro-segments Extended data gathering Cross-domain information exchange
	PulSAR: Proactive Security Analysis and Remediation	5G specific vulnerability schema	5G specific vulnerability schema implementation PulSAR interface with Generic Collector
	Satellite Network Monitoring	Pseudo real-time monitoring v1 Threat detection	Pseudo real-time monitoring v2 Active security analysis Pre-emptive mitigation security actions
	Generic Collector Interface (GCI)		integration within others monitoring enablers
Network Management and Virtualization Isolation	Anti-Fingerprinting	Controller-Switch-Interaction Imitator	no further release
	Access Control Mechanisms	Southbound Reference Monitor v1	Southbound Reference Monitor v2 Access Requirements for VNF Container Resources
	Component-Interaction Audits	Basic OpenFlow Compliance Checker v1	Basic OpenFlow Compliance Checker v2 Basic NFV Reconfiguration Compliance Checker
	Micro-segmentation	Dynamic arrangement of Micro-Segments	Extended Northbound API Support for multi-domain micro-segments
	Bootstrapping Trust	Integrity Attestation of virtual switches v1	Integrity Attestation of virtual switches v2 Integrity Attestation of VNFs running in Docker containers
	Flow Control		Detection of malicious behaviours in virtual networks In-network threat mitigation for critical functions in virtual networks.

As for table below it provides early insights regarding research and innovation work which could be think of at the time this deliverable is produced. This goes into the direction of the final Technical Roadmap that would be delivered at the end of the project. Of course, final content would here also dependent on the work achieved in R2 but at least the table below gives already some insights regarding possible directions for future work.

Table 26: Recommended for future work

Category	Security enabler Name	*Recommendation for future research & innovation work (beyond end of the project)*
AAA	Basic AAA enabler	performance and security aspects of quantum immune algorithms for Perfect Forward Secrecy.
	IoT	secure handover among different MME, and dynamic groups with key forward/backward secrecy
	Fine-grained Authorization Enabler	synchronization of all elements in the network (time mangement) Dynamic client and RCD registration protocols at the Authorization Server
	Federative authentication context usage	evolve communication protocols to integrate authentication characterization and so usage/exploitation
Privacy	Privacy Enhanced Identity Protection	Authentication of Identity Requests and Paging requests
	Device Identifiers Privacy	
	Device-based Anonymization	Format preserving anonymization algorithm on the SIM or on the device's proprietary binary blob Privacy agent (mediator between the caller and the anonymizing SIM/proprietary code)
	Privacy Policy Analysis	Multiple layers of privacy policy specification
Trust	Trust Builder	Combined it with the System Security State Repository to support the design lifecycle in 5G systems
	Trust Metric Enabler	Enable network segmentation based on different trust levels
	VNF Certification	Enable NFV infrastructure to make use of VNF certifcation info (e.g. at orchestrator level)
	Security Indicator	
	Reputation based on Root Cause Analysis for	NA
Security monitoring	System Security State Repository	runtime misbehaviour monitoring (and computation of threat likelihood) and comparison with system design from Trust Builder.
	Security Monitor for 5G Micro-Segments	Extended security inferencing, Trust, access control and privacy management for monitoring information that is shared over multiple-domains
	PulSAR: Proactive Security Analysis and Remediation	cyber-attacks at run-time requesting dynamic reconfiguration of the VNFs
	Satellite Network Monitoring	features performance improvements
	Generic Collector Interface (GCI)	NA
Network Management and Virtualization Isolation	Anti-Fingerprinting	NA
	Access Control Mechanisms	Differernt APIs and network abstractions, multitenant networks
	Component-Interaction Audits	Different network abstractions, algorithmic improvements
	Micro-segmentation	Flexible cooperation and connection mechanisms between micro-segments
	Bootstrapping Trust	Combination of component authentication with integrity measurements Key distribution to protect confidentiality and integrity of information
	Flow Control	

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 will have in R2 through

features developed. Indeed, most of the clusters and use cases are covered with some being covered by enablers from various categories addressed.

Table 27: 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
	UC1.2	Using Enterprise Identity Management for Bootstrapping 5G Access	IoT Federative authentication context usage enabler
	UC1.3	Satellite Identity Management for 5G Access	Fine-grained Authorization Enabler Federative authentication context usage enabler
	UC1.4	MNO Identity Management Service	Federative authentication context usage enabler
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 Netw	Fine-grained Authorization Enabler
	UC4.2	Authorization for End-to-End IP Connections	Fine-grained Authorization Enabler
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
	UC5.2	Adding a 5G Node to a Virtualized Core Network	VNF Certification Access Control Mechanisms Component-Interaction Audits Micro-segmentation Bootstrapping Trust
	UC5.3	Reactive traffic routing in a virtualized core network	Anti-Fingerprinting
	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
	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
	UC5.6	Integrated Satellite and Terrestrial Systems Monitor	Satellite Network Monitoring
C8	UC8.1	Satellite-Capable eNB	Satellite Network Monitoring
C9	UC9.3	Authentication of New Network Elements	Basic AAA enablers Trust Builder Security Indicator
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 Conclusions

This document provides update of Technical Roadmap previously delivered to encompass detailed descriptions of 5G security enablers in scope of the second release (i.e. R2) as well as their rationale.

The presentation is structured on a per category (thematic area covered) basis, i.e., AAA, Privacy, Trust, Security Monitoring, Network management & virtualization isolation where enablers of each category are presented according to the same template ranging from product vision through features detailed description and scheduling (reminded for R1/v1.0 and stated for R2/v2.0) as well as early recommendations for future research work beyond R2 and so end of the project (considering here sustainability of the Technical Roadmap on 5G Security this for the benefits of 5G Community at large).

Furthermore, this deliverable takes advantage of the Use Case deliverable [5] to further state the relevance of the planned security enablers and accompanying features to the corresponding 5G use cases, showing an overall good coverage/fit.

Overall, this deliverable paves the way towards the second (also last) release of 5G-ENSURE security enablers. It also enters the second iteration during which a number of steps already conducted for release one would be re-conducted starting first with the open specifications of security enablers for Release 2 till their software release in v2.0 going through their documentation. But this deliverable also contributes to further materialize the 5G Security Vision through security enablers product vision depicted as well as features they encompass and which are key for 5G to make its promises. It also shows the benefits of having 5G Security Technical Roadmap be exposed to engage with 5G-PPP community and beyond to communicate and cross-fertilize on the 5G Security Vision and its implementation. With this respect, Technical Roadmap on 5G Security through security enabler products vision it conveys remains among other documents central to number of discussions and especially the ones within the 5G-PPP Security WG.

9 Bibliographie

[1] The Register, «Did NSA, GCHQ steal the secret key in YOUR phone SIM? It's LIKELY,» 2015.

[2] R. Giustolisi, G. Christian, M. Åhlstrom et S. Holmberg, «A Secure Group-Based AKA Protocol for Machine-Type Communications,» chez *19th Annual International Conference on Information Security and Cryptology*, Seoul, 2016.

[3] B. Podgursky, «GitHub - bpodgursky/jbool_expressions: jbool_expressions is a simple open-source library for creating and manipulating propositional logic expressions in java,» [En ligne]. Available: https://github.com/bpodgursky/jbool_expressions.

[4] OASIS, «JSON Profile of XACML 3.0 Version 1.0,» [En ligne]. Available: http://docs.oasis-open.org/xacml/xacml-json-http/v1.0/xacml-json-http-v1.0.html.

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

[6] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi et J. Seifert, «Practical attacks against privacy and availability in 4G/LTE mobile communication systems,» chez *Cryptography and Security, arXiv:1510.07563*, Cornell University Library, 2015.

[7] 3GPP, «Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE),» 3GPP TR 33.82, 2008.

[8] Goyal, Pandey, Waters et Sahai, «Attribute-based encryption for fine-grained access control of encrypted data,» chez *ACM CCS'06*, 2006.

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

[10] P. Paillier, «Public-key cryptosystems based on composite degree residuosity classes,» chez *Eurocrypt'99, LNCS 1592, pp.223-238*, 1999.

[11] N. Foo Kune, J. Koelndorfer et Y. Kim, «Location Leaks on the GSM Air Interface,» 8 August 2013. [En ligne]. Available: http://www-users.cs.umn.edu/~foo/research/docs/fookune_ndss_gsm.pdf.

[12] F. Van den Broek, R. Verdult et J. de Ruiter, «Defeating IMSI Catchers,» chez *ACM CCS 2015*, 2015.

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

[14] J. Wright, «Characterising Anonymity Systems,» chez *York University*, 2009.

[15] «Privacy Level Agreements,» [En ligne]. Available: https://cloudsecurityalliance.org/group/privacy-level-agreement/.

[16] B. Aboba, J. Carlson et S. Cheshire, «Detecting Network Attachment in IPv4 (DNAv4),» chez *RFC4436, IETF*, 2006.

[17] «COWL,» [En ligne]. Available: http://w3c.github.io/webappsec-cowl/.

[18] 5G-ENSURE, «Deliverable D2.2 Trust Model (draft),» 2016. [En ligne]. Available: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.2-TrustModel.pdf.

[19] 5G-ENSURE, «Deliverable D2.3 Risk Assessment, Mitigation and Requirements (draft),» 2016. [En ligne]. Available: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.3-RiskAssessmentMitigationRequirements.pdf.

[20] I. G. B. Y. N. C. J. Sanchez, «THESARD: on The road to resiliencE in SoftwAre-defined network-ing thRough self-Diagnosis,» chez *2nd IEEE Conference on Network Softwarization*, Seoul, Korea, 2016.

[21] I. G. B. Y. N. C. J. Sanchez, «"Self-Modeling Based Diagnosis of Software-Defined Networks,» chez *1st IEEE Conference on Network Softwarization*, London, 2015.

[22] I. G. B. Y. e. a. J. Sanchez, «"Softwarized 5G networks resiliency with self-healing,» chez *1st International Conference on 5G for Ubiquitous Connectivity (5GU)*, 2014.

[23] I. G. B. Y. N. C. J. Sanchez, «"Self-Modeling based Diagnosis of Services over Programmable Networks,» chez *2nd IEEE Conference on Network Softwarization*, Seoul, Korea, 2016.

[24] «Mininet: an instant virtual network on your laptop,» [En ligne]. Available: http://mininet.org/.

[25] 5G-ENSURE Consortium, *Deliverable 2.1: Use Cases,* [Online] Available: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.1-UseCases.pdf, 2016.

[26] Open Networking Foundation, «OpenFlow switch specification - version 1.3.0 (wire protocol 0x04),» 2012.

[27] 5G-ENSURE Consortium, *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, 2016.

[28] 5G-ENSURE Consortium, *Deliverable 3.3: 5G-PPP security enabler software release (v1.0),* 2016.

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

[30] «Open vSwitch - a production quality, multilayer virtual switch,» [En ligne]. Available: http://openvswitch.org/.

[31] H. Cui, G. O. Karame, F. Klaedtke et R. Bifulco, «On the fingerprinting of software-defined networks,» *IEEE Transactions on Information Forensics and Security,* vol. 11, n° %110, pp. 2160-2173, 2016.

[32] P. Berde, M. Geralo, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Conner, P. Radoslavov, W. Snow et G. M. Parulkar, «ONOS: Towards an open, distributed SDN OS,» chez *Proceedings of the 3rd SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN)*, 2014.

[33] Hewlett Packard, «SDN App Store,» [En ligne]. Available: https://saas.hpe.com/marketplace/sdn.

[34] «SDN Market Sizing,» 2013. [En ligne]. Available: https://www.sdxcentral.com/wp-content/uploads/2015/02/sdn-market-sizing-report-0413-4.pdf.

[35] «ONOS - a new carrier-grade SDN network operating system designed for high availability, performance, scale-out,» [En ligne]. Available: http://onosproject.org/.

[36] D. Gkounis, F. Klaedtke, R. Bifulco et G. O. Karame, «Cases for including a reference monitor to SDN,» chez *Proceedings of the 2016 ACM SIGCOMM Conference*, 2016.

[37] «Docker,» [En ligne]. Available: http://www.docker.com.

[38] «The OpenDaylight Platform,» [En ligne]. Available: https://www.opendaylight.org/.

[39] J. Anderson, «Computer security technology planning study,» 1973.

[40] F. B. Schneider, «Enforceable security policies,» *ACM Transactions on Information and System Security,* vol. 3, n° %11, 2000.

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

[42] «Docker - Build, Ship, and Run Any App, Anywhere,» [En ligne]. Available: https://www.docker.com/.

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

[44] «OpenVirteX Network Virtualization Platform,» [En ligne]. Available: http://ovx.onlab.us/.

[45] «Ryu SDN Framework,» [En ligne]. Available: https://osrg.github.io/ryu/.

[46] K. Thimmaraju, B. Shastry, T. Fiebig, F. Hetzelt, J.-P. Seifert, A. Feldmann et S. Schmid, «Reigns to the Cloud: Compromising Cloud Systems via the Data Plane,» arXiv, 2016.

[47] N. Paladi et C. Gehrmann, «TruSDN: Bootstrapping Trust in Cloud Network Infrastructure,» chez *12th EAI International Conference on Security and Privacy in Communication Networks*, 2016.

[48] «The Guardian,» [En ligne]. Available: http://www.theguardian.com/us-news/2015/feb/19/nsa-gchq-sim-card-billions-cellphones-hacking.

[49] «Gemalto,» [En ligne]. Available: http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx.

[50] Huffingtonb Post, [En ligne]. Available: http://www.huffingtonpost.com/2013/10/24/nsa-world-leaders_n_4158922.html.

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

[52] R. Bifulco, H. Cui, G. O. Karame et F. Klaedtke, «Fingerprinting software defined networks,» chez *Proceedings of the 23rd International Conference on Network Protocols (ICNP)*, 2015.

[53] H. Cui, G. O. Karame, F. Klaedtke et R. Bifulco, «Fingerprinting of software-defined networks,» 2015. [En ligne]. Available: http://arxiv.org/abs/1512.06585.

[54] F. Klaedtke, G. O. Karame, R. Bifulco et H. Cui, «Access control for SDN controllers,» chez *Proceedings of the 3rd SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN)*, 2014.

[55] F. Klaedtke, G. O. Karame, R. Bifulco et H. Cui, «Towards an access control scheme for accessing flows in SDN,» chez *Proceedings of the 1st IEEE Confernce on Network Softwarization (NetSoft)*, 2015.

[56] ELISS, «Regulatory Status of Lawful Interception in Italy,» [En ligne]. Available: http://www.eliss.org/index.php/sicurezza-e-giustizia-regulatory-status-of-lawful-interception-in-italy-g-nazzaro/.

[57] M. Luoto, T. Rautio, T. Ojanpera and J. Makela, "Distribueted decision engine - An information management architecture for autonomic wireless wetworking," in *IFIP/IEEE International Symposium on Integrated Network Management*, 2015.

[58] M. Mantere, I. Uusitalo, M. Sailio and S. Noponen, "Challenges of Machine Learning Based Monitoring for Industrial Control System Networks," in *26th International Conference on Advanced Information Networking and Applications Workshops*, 2012.

[59] M. Mantere, M. Sailio and S. Noponen, "A module for anomaly detection in ICS networks," in *the 3rd international conference on High confidence networked systems - HiCoNS '14*, New York, 2014.

[60] 5G-ENSURE, «Deliverable D2.1 - Use Cases,» 2016. [En ligne]. Available: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.1-UseCases.pdf.

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 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 a vulnerability on the VM which enables privilege escalation, then malicious code can be executed on the VM.