Deliverable D3.1
5G-PPP security enablers technical roadmap (early vision)

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	11.03.2016	
Dissemination Level:	Public	
Lead beneficiary	Thales Services (TS)	Pascal Bisson, pascal.bisson@thalesgroup.com
Authors	VTT : Jouni Hiltunen, Olli Mämmelä, Jani Suomalainen TS: Pascal Bisson, Olivier Bettan ALBLF[1]: Linas Maknavicius EAB: Mats Näslund, Håkan Englund IT-Innov: Stephen C. Phillips, Bassem I. Nasser LMF: Bengt Sahlin NEC: Felix Klaedtke Nixu: Tommi Pernilä Orange: Jean-Philippe Wary, Ghada Arfaoui SICS: Martin Svensson, Rosario Giustolisi, Nicolae Paladi TASE: Ana JALÓN VALERO, Gorka Lendrino Vela TCS : Emmanuel Dotaro, Sébastien Keller, Jean-Marc Lacroix, Ermis Papastefanakis TIIT: Luciana Costa, Madalina Baltatu UOXF: Piers O'Hanlon	

[1] Nokia Bell Labs since Jan 14, 2016

Executive summary

This document provides an early vision (at M4) of the 5G security and privacy enablers proposed by the 5G-ENSURE project, and that are planned to be developed through two major releases: v1.0 (R1) due at M11/Sep'16 and v2.0 (R2) due at M22/Aug'17. It details the Technical Roadmap for v1.0 (R1) in terms of enablers in scope and their features, while providing insights for v2.0 (R2) enablers that will be fully detailed in an update of this deliverable (D3.5 due at M13/Nov'16) taking account of the progress and achievements made by that time. Enablers envisioned are here presented organized in categories, which represent major security areas recognized as topmost priorities for 5G-PPP & 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 for first release vs. next release.

In the AAA category the main focus is on 5G users' authentication, authorization and accounting, but the contribution of the AAA enablers goes beyond the incremental improvements to security that one would expect in a next-generation network. The evolving 5G network will support an unpredictable number of devices due to the boom of Internet of Things (IoT), whose security these enablers will aim to address. Moreover, the enablers target to integrate authentication and authorization functions between satellite and terrestrial systems.

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. For each 5G 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 Trust category will provide trust models which will address the complex relationships between the many actors in 5G networks including the machine-to-machine interactions characterising the next generation networks. The trust model needs to address the different aspects of trust, between automated systems (M2Mt), between human stakeholders holding responsibilities for different parts of 5G networks, between user and network operators and between users of the network (U2Ut), trust that a human stakeholder has towards a system (U2Mt), that an automated system (machine) has in users that it interacts with.

5G-ENSURE project also aims at providing new innovative solutions ensuring the highest level of security and resilience in 5G network. Mobile networks will dramatically evolve with the fifth generation of networks compared to 3/4G, in particular with new concepts and technologies such Internet of Things, infrastructure virtualization (SDN, NFV), network resource sharing, new access interfaces, dynamic network topologies, slicing and so forth. These technologies introduce new security and resilience and provide new opportunities to implement extensive and accurate security solutions. Thus, new innovative approaches to predict and counter these challenges will be considered by the category devoted to Monitoring the 5G security.

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 change network management into a more 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. The aim of the security enablers provided in the Management category is secure the network's control plane and the virtualized networks on top of it, and to secure network services and provide new security services.

The present document gives an overview of the initial set of enablers and security features envisaged/proposed by each category, together with the rationale behind them and their scheduling. It also details, at features level, the ones carefully selected for their relevance (especially from the 5G Use Cases perspective although if not uniquely), and in scope of the first release (v1.0/R1), while giving insights for enablers/features planned for next release (v2.0/R2). Overall, this deliverable paves the way towards the first release of 5G-ENSURE security enablers whose open specifications are one of the next steps. It also contributes to further progress on 5G Security Vision in terms of both the Technical Roadmap requested and its implementation. Last but not least it is also source for further collaboration with 5G-PPP Projects mainly through 5G-PPP Security Working Group about to be launched, this considering specific interest some of these projects did already exhibit and without presuming of additional security enablers they may add and/or even contribute.

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 D3.1 follows deliverable D2.1 on use cases from WP2 "*Security requirements and architecture"* and is the first deliverable of *WP3 "Security enablers for 5G"*. It provides an early vision of security enablers the project is about to propose and details more specifically the enablers and features in scope of the first release (v1.0) due at M11. Those enablers will be specified in the next WP3 deliverable (D3.2 5G-PPP security enablers open specifications (v1.0)). As for enablers and/or features planned for the next release, full details will be provided in the context of the Technical Roadmap update planned (D3.5 5G-PPP security enablers technical roadmap (update) /M13).

Overall, D3.1 initiates the work on Technical Roadmap and makes clear what is in scope of the first release (i.e. v1.0). It takes advantage of deliverable D2.1 on Use Cases to materialize relevance of enablers proposed with respect to use cases and 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 D3.1 also targets to be a reference document to initiate exchange and cross-collaboration (also cross-fertilization) with other 5G-PPP Projects this within the context of the 5G-PPP Security WG about to be launched.

Disclaimer

The information in this document is provided 'as is', and no guarantee or warranty is given that the information is fit for any particular purpose.

The EC flag in this deliverable is owned by the European Commission and the 5G PPP logo is owned by the 5G PPP initiative. The use of the flag and the 5G PPP logo reflects that 5G-ENSURE receives funding from the European Commission, integrated in its 5G PPP initiative. Apart from this, the European Commission or the 5G PPP initiative have no responsibility for the content.

Copyright notice

Contents

1 Introduction

This document provides an early vision (vision at M4) of the 5G security enablers proposed by the 5G-ENSURE project and that are planned to be developed through two major releases: v1.0 (R1) due M11/Sep'16 and v2.0 (R2) due M22/Aug'17. It details the Technical Roadmap for v1.0 in terms of enablers in scope and attached features, while providing insights for v2.0 enablers that will be fully detailed in the context of an update planned for this deliverable (D3.5 due at M13/Nov'16) taking account the progress and achievements made by that time. Enablers envisioned are here presented as per categories recognized as topmost priorities for 5G-PPP & 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 for first release vs. next release. As such, this deliverable gives an overview of the initial set of enablers envisaged, together with the rationale behind their choice/proposal and their scheduling. It also details at features level the ones carefully selected for their relevance (especially from the 5G Use Cases perspective although if not uniquely from that perspective) and in scope of the first release (v1.0/R1), while giving insights for enablers/features planned for the next release (v2.0/R2). Overall, this deliverable paves the way towards the first release of 5G-ENSURE security enablers whose open specifications will be one of the next steps as far as WP3 activity is concerned. It also contributes to further progress on 5G Security Vision in terms of both providing the requested Technical Roadmap and its implementation. Last but not least it is also source for further collaboration with 5G-PPP Projects mainly through 5G-PPP Security Working Group about to be launched, this considering specific interest some of these projects did already exhibit and without presuming of additional security enablers they may add and/or even contribute.

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 for the first release and drafts the plans for the next release.
- Section 8 concludes the document, while References are provided at the end.

Each of the category descriptions of Sections 2-6 provides early description of the envisioned enablers. As for enablers planned to be developed in R1, the technical roadmap is given under the format of features planned.

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
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
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

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
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

2 AAA Security Enablers

This document specifies four classes of 5G enablers for handling authentication, authorization, and accounting (AAA) requirements. The contribution of the AAA enablers goes beyond the incremental improvements to security that one would expect in a next-generation network. The evolving 5G network will support an unpredictable number of devices due to the boom of Internet of Things (IoT), whose security these enablers will aim to address. Moreover, the enablers target to integrate authentication and authorization functions between satellite and terrestrial systems.

The proposed enablers not only meet the AAA-related needs, as deducible from the use-case document [1], but also advance secure functions in support of the novel set of 5G use cases.

In particular, the Basic AAA enabler aims to enhance the security aspects of the existing AAA infrastructure utilized in third and fourth generation of 3rd generation partnership project (3GPP) protocols; the IoT enabler aims to secure the communication with IoT devices; the fine-grained authorization enabler aims to enforce multiple authentication policies and multiple authorization policies to access system services and resources; finally, the federative authentication and identification enabler aims to securely propagate authentication mechanisms into production lines[2]. These four enablers cover: the basic security requirements for authentication in 5G; the specific authentication requirements introduced by the boom of IoT devices; authorization enhancements in both constrained devices and the integration of terrestrial and satellite communication; and last, how existing federation protocols and trust and liability levels can be woven into 5G AAA protocols.

The specific enablers are detailed in the sections below.

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

[2] *Production line is composed with a set of equipment, functions and services used to deliver a service or a content over a 5G infrastructure in some context (time and localization). A production line could be composed with radio access equipment or technologies, AAA servers, HSS, EPC, services gateways, slices, non-limitative list…*

Table 1: Mapping between Basic AAA 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 Universal Integrated Circuit Cards (UICCs) [2] [3]. 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 detailed in Section 6 focusing on Network Management & Virtualization enablers.

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 Universal Subscriber Identity Module (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 Technical Roadmap for First Release (R1)

No software planned for release 1 of the enabler.

2.1.6 Next release

- **Feature name**: Forward Secrecy
- **Goal**: Limit and/or recover from impact of compromised long-term keys, preferably with backward compatibility.
- **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 secured 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 detailed in Section 6.5 on Network Management & Virtualization.
- **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 Remarks

The feature "Forward secrecy" of this enabler is related to the feature "Enhanced ID protection" of the Privacy enabler since they will both need to be integrated together into the 5G access authentication protocol. Therefore, a dedicated coordination activity will be implemented under the responsibility of this enabler.

2.2 Security Enabler "Internet of Things - IoT"

2.2.1 Product Vision

The collection of connected devices (or "things"), commonly referred to as Internet of Things or IoT, is likely to increase substantially, and 5G is expected to fully support the connectivity of IoT devices. In the context of 5G, IoT devices are characterized by 1) low-energy, 2) low-cost, and 3) massive deployments, which have to be supported by the 5G network, both as an overall aggregate and within the same cell.

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.

The UICC form-factor is believed to remain important for many types of access to 5G systems. While providing strong key protection, UICCs are also known to impose hurdle for certain use cases such as massive machine to machine type communication (mMTC) deployments: devices need to add physical UICC interfaces which may be a non-negligible cost. More fundamentally, the cost and complexity in distribution and managing of physical UICCs could limit the attractiveness of 5G. In recent years, eUICC has shown up as offering greater simplicity and manageability, but we have also seen a number of initiatives e.g. from device HW manufacturers, to develop other interesting alternatives to securely support device identifiers, e.g. ARM mbed [39].

With the emergence of group-based communication in massive deployment scenarios, there are a large number of UEs with the same properties in a network, e.g., machine-to-machine communication (M2M). These kinds of devices can dynamically form groups according to their similarity, such as being in the same region, belonging to the same application or being the same type of device. If a large number of devices in a group need to access the network successively over a short period of time, existing authentication methods will suffer from high network access latency until completing authentication procedures of all devices in the same group. This is especially true when these devices roam into a visited domain, which is far from their home domain. The reason is that every device must perform a full AKA procedure with home authentication server, hence the authentication signalling in the network will increase. It may here be argued that current radio network protocols, as such, would not be able to cope with a massive number of simultaneously connecting devices either. However, this enabler naturally assumes that enhancements to the radio protocols will be addressed by the new 5G RAT standards and, therefore, we here seek to ensure that AAA will not be a remaining showstopper. Meanwhile, the capacity requirements of the authentication server will increase due to frequently generating authentication vectors. 5G should explicitly support new efficient authentication protocols to efficiently authenticate devices in a group, compared to the traditional AKA protocol. See Figure 1 for an overview of authentication of IoT/M2M devices in 5G.

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.

The 5G Security enabler for IoT should investigate the possibility to support:

- Specification of one or more device hardware and/or software technologies to handle device credentials with sufficient security levels as a complement to UICC, and a low-cost management of device identities/credentials for such UICC-less devices.
- The use of different kinds of cryptographic techniques, such as pre-shared keys, certificates etc. Additionally, the enabler should support authentication based on these UICC-less credentials.
- Authentication based on third party identities, i.e. bring-your-own-identity.

- Efficient authentication in massive deployment scenarios, with explicit support for group based authentication, either via direct communication from an IoT device or via an IoT gateway, with 5G credentials.

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

Enabler Security Feature	Relevant Use Case
Specification of one or more technologies to handle device credentials, as a complement to UICC	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)
Efficient authentication in massive deployment of IoT devices	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 device platform technologies, such as trusted computing and secure execution environments for 5G IoT devices, to support UICC-less devices. 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 enabler 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 UICC-less 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 UICC-less devices, the key security aspect is to provide secure storage and processing support that can provide a “sufficient” level of trustworthiness. 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 UICC-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.

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.

In group authentication, three main security aspects will be investigated.

- A man-in-the-middle attack taking part in the bootstrapping procedure for authentication.
- A malicious IoT device, being grouped with other devices and is therefore authenticated together with the other IoT devices, will get unauthorized access to the 5G network.
- The nature of IoT might make it easier to subvert the security of these devices as they are available for physical attacks, their power constraints require lightweight protocols or lack the proper security in the hardware implementation to prevent side-channel attacks.

Furthermore, the enabler will also investigate key protocols and algorithms which provide the necessary protective measures of the security aspects. For example, group members may join and leave the group dynamically, hence the group requires backward and forward secrecy. 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.

2.2.4 Security Challenges

The challenges for authenticating UICC-less IoT devices lie in finding an alternative that is more cost efficient and flexible than the well-proven UICC, yet providing a sufficient level of security. Indeed, defining “sufficient” may in itself prove to be a challenge. The overall reputation of 5G as a trustworthy system must not be put at risk.

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.

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.

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 ME authentication). Moving groups of devices introduce new challenges in authentication, as a long delay and large computational overhead may occur during handover or roaming. Therefore, research of group-based communication in the duration of handover or roaming is needed.

2.2.5 Technical Roadmap for First Release (R1)

- **Feature name**: Group authentication by extending the LTE-AKA protocol
- **Goal**: Enable 5G to support massive deployments of IoT devices by adding explicit support for group authentication of devices.
- **Description**: The first release will provide a state-of-the-art survey and a proposal of a suitable extension of the AKA protocol to support basic group authentication. A key point is to identify criteria for defining the group concept, its relation to "subscriber", and the authorization level assigned to groups. Additionally, a first prototype will be developed, which will support group authentication of a statically defined group of up to 5 IoT devices. The protocol will be based on the existing LTE-AKA protocol, but will include the necessary enhancements to support group authentication. An evaluation of CPU, memory and latency cost and comparison with existing LTE-AKA costs will be provided.
- **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.

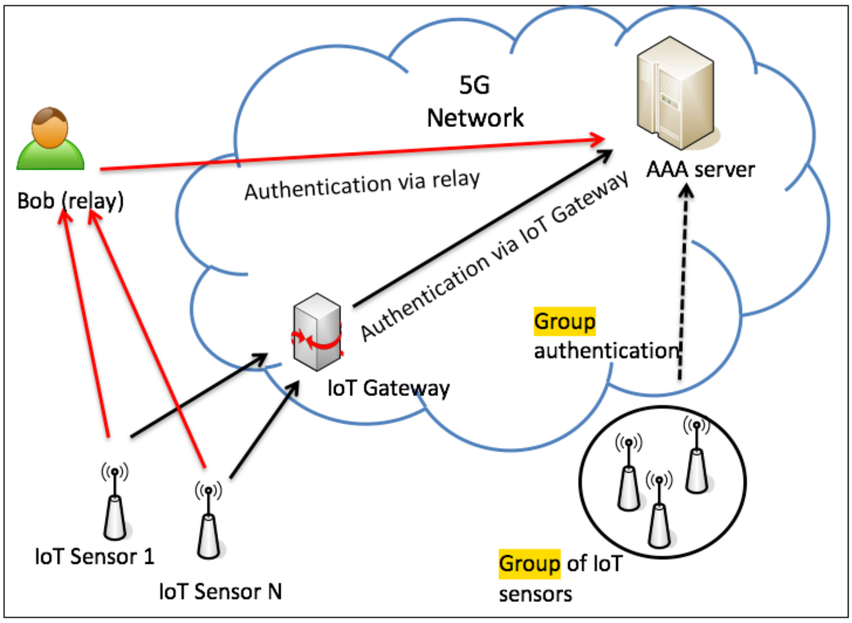

Figure 1: (From 5G-ENSURE D2.1 Use cases) Authentication of IoT/M2M devices in 5G

2.2.6 Next release

The next release is expected to further enhance the group authentication protocol. The research will focus on the possibilities to dynamically form groups and to enable IoT devices to join or leave an IoT group, including protocol properties that ensure forward and backward and secrecy.

Furthermore, the next release will include a state-of-the-art survey of alternatives to UICC and a proposal of one or more suitable technologies to be used in 5G devices, including suitable protocols for management/provisioning will be proposed.

2.3 Security Enabler "Fine-grained Authorization Enabler"

2.3.1 Product Vision

The role of interconnected resources, such as services and resource-constraint 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.

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.

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.

The security enabler should support:

- Multiple users with different rights.
- Decision per user, resource and action.
- Access based on dynamically changing parameters.
- Access based on a signed token containing Identity attributes of the user, and policy adapted for the user and the resource to be accessed.
- Access control directly embedded in the device (i.e. without connection to any external Authentication server).
- Integration of different Authentication 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
Integration of different Authentication servers (Satellite AAA & Terrestrial 5G AAA)	Satellite Identity Management for 5G Access (Use Case 1.3)
Access based on provided information (user/resource/action attributes)	MNO Identity Management Service (Use Case 1.4)
Integration of different Authentication servers (Terrestrial 5G AAA & IoT gateway)	Authentication of IoT Devices in 5G (Use Case 3.1)
Access based on provided information (user/resource/action attributes & Authorization token)	Authorization in Resource-Constrained Devices Supported by 5G Network (Use Case 4.1)
Access based on a central AAA	Authorization for End-to-End IP Connections (Use Case 4.2)
Device-to-Everything access with different security needs	Vehicle-to-Everything (Use Case 4.3)

2.3.2 Technology Area

The enabler operates in a technology area of interconnected resources. Some of these resources, especially 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.

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

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. These policies are re-evaluated according to the attribute values, 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) and a Policy Decision Point (PDP), which are directly embedded on the RCD, without a connection to an AAA server. The security policy can be defined with XACML.

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

2.3.4 Security Challenges

Different security challenges for the enabler can be envisaged. The main challenge to take into consideration is to find an appropriate format to formulate security policies and compute a policy restricted to the user requesting access and the resource requested by the user. The enabler should also deal with anonymous accesses, when 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 in 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 security 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, an integrity protection and a feature for the proof of origin of request to modify the stored security policy.

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 term of memory, CPU and power will be provided (in theory and in practice over the testbed).

2.3.5 Technical Roadmap for First Release (R1)

- **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 a prototype 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.

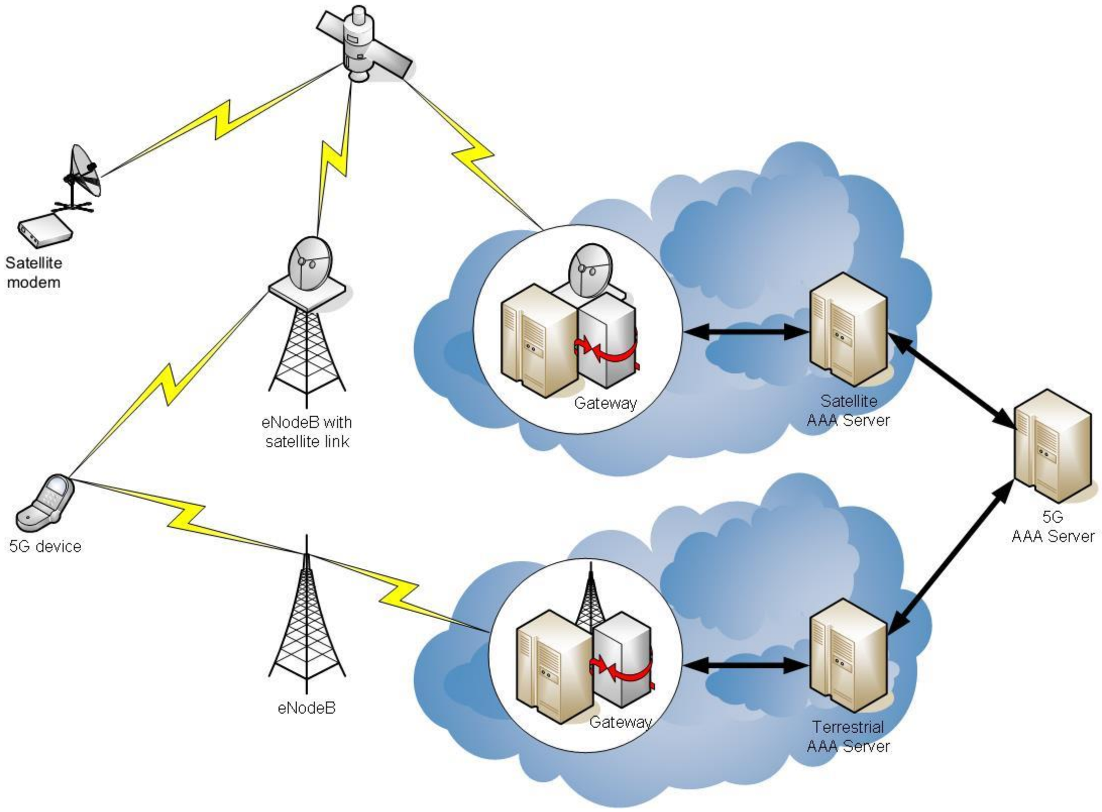

Figure 2: AAA system mechanism.

- **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:

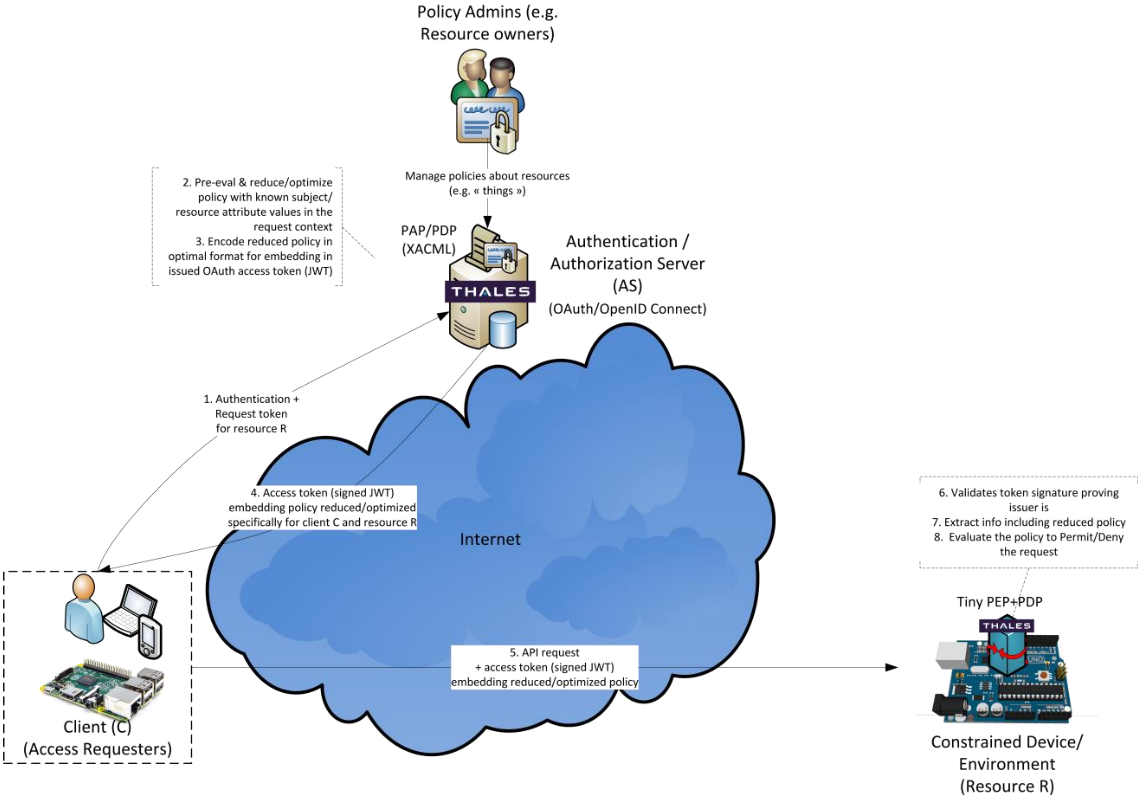
Policy Admins (e.g. Resource owners)
Manage policies about resources (e.g. « things »)
2. Pre-eval & reduce/optimize policy with known subject/ resource attribute values in the request context
3. Encode reduced policy in optimal format for embedding in issued OAuth access token (JWT)
PAP/PDP (XACML)
THALES
Authentication / Authorization Server (AS)
(OAuth/OpenID Connect)
1. Authentication + Request token for resource R
4. Access token (signed JWT) embedding policy reduced/optimized specifically for client C and resource R
Internet
6. Validates token signature proving issuer is
7. Extract info including reduced policy
8. Evaluate the policy to Permit/Deny the request
Tiny PEP+PDP
THALES
5. API request + access token (signed JWT) embedding reduced/optimized policy
Client (C) (Access Requesters)
Constrained Device/ Environment (Resource R)

Figure 3: Distributed Authorization Architecture for RCDs.

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

The solution is envisioned to rely on:

  - Central OAuth-compliant Authentication and Authorization service capable of:
    - On-the-fly XACML policy decapitation/pre-eval/optimization for specific client and resource,
    - Issuing signed XACML-policy-embedding OAuth tokens (e.g. based on JWT),
  - Minimal XACML PEP/PDP for enforcement on constrained resource and supporting such token.

- **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.

2.3.6 Next release

The next release is expected to support policies for decision per user, resource and action, access control for dynamically changing parameters.

Also, the next release is expected to integrate the authentication and authorization mechanism with the satellite system.

Finally, this release is expected to provide the final 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.

2.3.7 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 and identification enabler”

The aim of the proposed enabler is to propagate, inside production lines, (i) some level of commitment & liability and (ii) trust evaluation of a specific functional block used to deliver a service or a content. In order to have an end-to-end trust evaluation, the information consolidated for the different functional blocks are combined and used by different nodes (e.g. end user, a core network node). For the nodes requiring authentication, this evaluation is used as contextual information by the authentication server. A successful authentication can be also considered as a metric in the trust level computation.

2.4.1 Product Vision

The vision is that the enabler offers a way to evaluate the trust and liability for incoming requests in different nodes of the production line.

These nodes need to collect data provided by parties involved, e.g. telecom operators and network operators. Trust level (e.g., a certified value or tag) is based on several metrics such as collected data from the network, type of authentication.

If these nodes require an authentication, this trust level is provided to authentication mechanisms which use this contextual information to adapt, if necessary, its security policy.

If the authentication succeeds, this information is provided as trust information through KPI and added to the data already collected.

This information should be inserted in the running flow. This enabler will allow 5G nodes to adapt dynamically their security policy and / or manage their risks evaluation before delivering content or a service.

Table 4: Mapping between Federative authentication and identification enabler security features and relevant use cases

Enabler Security Feature	Relevant Use Case
Identity federation in 5G	Factory Device Identity Management for 5G Access (Use Case 1.1) Using Enterprise Identity Management for Bootstrapping 5G Access (Use Case 1.2) Authorization for End-to-End IP Connections (Use Case 4.2)
Trust and liability computation	Satellite Identity Management for 5G Access (Use Case 1.3) MNO Identity Management Service (Use Case 1.4) Authorization for End-to-End IP Connections (Use Case 4.2) Adding a 5G Node to a Virtualized Core Network (Use Case 5.2) Privacy in Context-Aware Services (Use Case 9.2) Authentication of New Network Elements (Use Case 9.3)

2.4.2 Technology Area

The technology areas of interest focus on AAA implementation and design, AAA safety and trust level of technologies used, AAA security maturity level of production organization, and others customers' contextual information. This contextual information will be used to enhance classical authentication and identification methods in order to evolve into federative methods.

2.4.3 Security Aspects

The aim of the trust and liability propagation through network is to allow nodes, operated by third parties, to distribute or receive information about the nature, the quality and the trust level of incoming requests. This security enabler will interact with the different 5G actors.

Authentication mechanisms, based on identity federation will use this information to adapt its security policy and will contribute by adding new elements (for example if the authentication is strong, if multi-factors, …).

One key security aspect is to guarantee the integrity of the provided information.

2.4.4 Security Challenges

The security challenges are related to:

- Establish metrics, KPIs and common evaluation schemes that commit (liability) every involved partner in an end-to-end delivery of service or content.
- Improve existing security protocols and cryptographic schemes in order to propagate the level of trust over a 5G Network.
- Define authentication mechanisms taking into account this kind of context and providing information to establish trust based on the authentication performed.

2.4.5 Technical Roadmap for First Release (R1)

No software planned for release 1 of the enabler.

2.4.6 Next release

Hereafter are the features planned for the next release:

- **Feature name**: Trust and liability computation
- **Goal**: To compute Trust and Liability level regarding an incoming request.
- **Description**: This feature will provide, and be in charge of, the Trust and Liability evaluation.
- **Rationale**: Different components of production lines should be able to associate a level of trust and liability for the different incoming request.

- **Feature name**: Identity federation in 5G
- **Goal**: To design and to implement identity federation in 5G including Internet and telco network providing trust and liability levels.
- **Description**: This feature will provide an identity federation for users or devices connected through Internet or directly through telco operators.
- **Rationale**: identity federation is important in 5G to allow the interconnectivity between an increasing numbers of actors. This identity federation should provide different attributes allowing a service, receiving an incoming request, to evaluate an associated trust level.

2.4.7 Remarks

This enabler has some similarities with enabler “Trust Metric”. Indeed, in both cases, a trust level is computed based on some metrics. However, the aim of this computation is different. “Trust Metric” enabler is designed to use the trust level in order to disable redundant security features. Regarding this enabler, it should use it to enhance the authentication and identification of nodes in a 5G network.

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 [1] 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, authentication and anonymization mechanisms to protect the privacy of the subscriber's identity (i.e., IMSI, but also temporal identities) in all the situations where it is currently send 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/EAP-SIM.

The second enabler proposes a 5G end to end encryption service able to guarantee the privacy of all user's communications from their source to their destination 5G device. The service also defines a fair and collusion free key escrow mechanism needed in order to guarantee the respect of user privacy under the constraints of LI.

The third 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 fourth and fifth 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 stored on the SIM by employing SIM-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 first release (R1) is detailed together with their features. As for others they are briefly introduced as part of the 5G Privacy Vision and next steps to come.

3.1 Privacy Enabler "Privacy Enhanced Identity Protection"

3.1.1 Product Vision

This enabler aims to provide protection against 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 leak 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 with the network's public key and, possibly, a request for identity transfer should only be received from authenticated network elements.

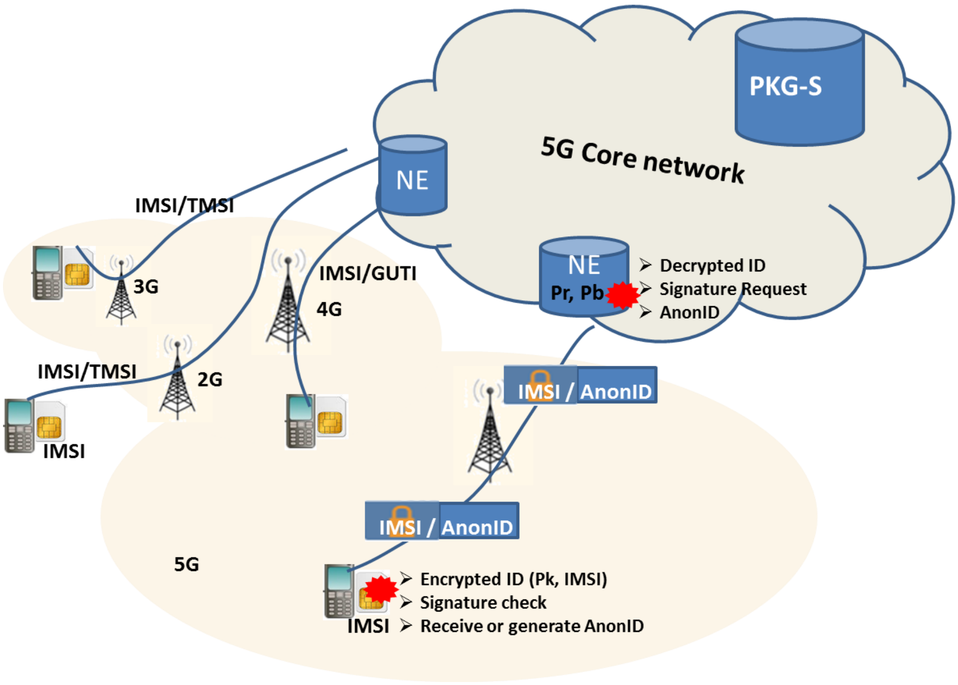

Figure 4: High level Privacy Enhanced ID Protection architecture.

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 [4]. Mobile devices engage in a number of AAA protocol interactions dependent upon their access to the network. In the case of mobile radio connection, the User Equipment (UE) will utilize the 5G AKA protocol when obtaining its temporary identity (e.g. S-TMSI, GUTI). If the UE attempts to attach to WiFi then it may utilize the EAP-SIM or EAP-AKA protocol to authorize connection to the local network, or to the evolved packet core (EPC). There are also new protocols being developed for constrained devices. One of the goals of this enabler is to utilize various techniques, such as protocol analysis and verification, to provide a solution that offers enhanced privacy in such interactions. The security enabler should therefore support:

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

The mapping between enablers' features and use cases defined in D2.1 [1] is illustrated in the table below.

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	Use Case 2.2: Subscriber Identity Privacy, Use Case 2.3: Enhanced Communication Privacy
Authentication of Identity Requests	Use Case 2.2: Subscriber Identity Privacy Use Case 2.3: Enhanced Communication Privacy
Pseudorandom dynamic pseudonyms	Use Case 2.2: Subscriber Identity Privacy
Random dynamic pseudonyms	Use Case 2.2: Subscriber Identity Privacy
Privacy Enhanced AAA	Use Case 2.2: Subscriber Identity Privacy, Use Case 2.3: Enhanced Communication Privacy

3.1.2 Technology Area

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

3.1.3 Security and Privacy 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 IMSI is transmitted in clear text in the first Attach Request.
- Identity Requests are not authenticated and the user's Identity response contains the 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 [4], [5], [6].

3.1.4 **Security and Privacy 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. A reliable key escrow mechanism might also be necessary for lawful interception.

The enabler aims to protect subscribers' 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 **Features of the enabler**

3.1.5.1 Encryption of Long Term Identifiers

The feature “Encryption of Long Term Identifiers” provides an encryption scheme for the user identifiers (IMSIs) in messages unprotected by symmetric cryptography due to lack of security context. In such cases, since no common secrets are yet shared, asymmetric encryption are necessary. 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 [4] 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 to all messages that contain the subscriber identifier: messages towards the network could be encrypted using the public key of the network; therefore, UE would not need to send the subscriber's identity in clear text in order to initiate the network attach procedure.

In a simple scenario where the UE connect only 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.

The private keys can be distributed to different MNOs as well as to Legal Authorities for lawful interception with possible key escrow. 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:

1. **Attach Request** – contains the IMSI in clear text: the IMSI (and maybe other sensitive information like, for example, the network and security capability) should be encrypted with the public key of the home network.
2. **Identity Response** – contains IMSI in clear text: the IMSI should be encrypted with the public key of the home network.

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 request, but it always protects the long term identifier against unauthorized access. An advantage is that it appears possible to never expose the long term identifier even to the serving network. In addition, this solution could probably be implemented using only public keys of the home network, thus reducing the “scope” of PKI (Public Key Infrastructure). This could however mean problems for the serving network to locate the home network. To that end, part of the identifier, e.g., the MNC (Mobile Network Code) and the MCC (Mobile Country Code) in the IMSI case, would need to be unprotected to be read by the serving network and respectively the home network. Operators which have roaming agreements can also agree on the use of an attribute encryption scheme in order to permit the UE to only have one public key instead of a number of public keys equal to the number of roaming networks the UE can visit.

Note that this approach seems possible to integrate also into authentication methods based on EAP (Extensible Authentication Protocol) such as EAP-AKA (EAP-Authentication Key Agreement). An issue to study is where to place the decryption function in the home network. One possibility is the use of a cluster of HSS (Home Subscriber Server) servers, and therefore the full identifier must be accessible to decide which HSS to use.

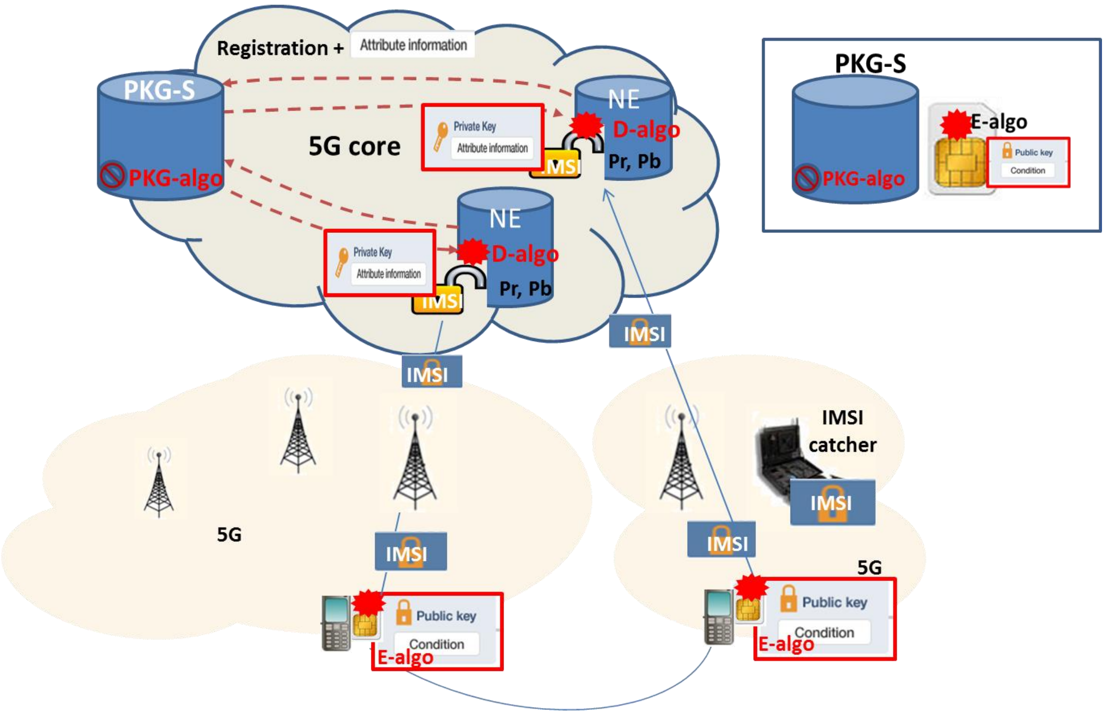

Figure 5: High level components of the feature "Encryption of Long Term Identifiers"

Considering the use of a key-policy ABE (KP-ABE) scheme, attributes (conditions to be satisfied for decryption) are labelled in the encrypted user identity (IMSI). Access structure is embedded in the private key. The private key is issued by a trusted private key generator (PKG). Figure 5 shows the high level components of this feature.

- **Private Key Generator Server (PKG-S)**: responsible for the generation of private keys to trusted entities (e.g., network elements, roaming partners) based on the user access policy. The server holds a public parameter (PK) and a master key (MSK), which is known only to the server.
- **Private Key Generator algorithm (PKG-algo):** runs on the server PKG-S. An entity entitled to perform decryption (e.g., a network element) requests the provisioning of the decryption key (D) by presenting an attribute "x". The key generation algorithm takes as input the public parameters (PK), the master key (MSK) and the provided attribute x. It outputs the private key D.
- **Encryption Algorithm (E-algo)**: runs on the client components, e.g., on the UE devices. The encryption algorithm takes as input the user identity (e.g., the IMSI), an access policy (condition), and the public parameter (PK). It outputs the ciphertext, i.e., the encrypted IMSI. In this way only the entities which have the decrypted key generated from the attribute that satisfies the condition will be able to decrypt the ciphertext.
- **Decryption algorithm (D-algo):** the decryption algorithm takes as input the ciphertext, which was encrypted under the set of attributes, the public key parameter (PK) and the private key (D) for access control. The output is the clear text, e.g., the IMSI.

The first release of the current feature will provide system definitions and a prototype software implementation of the main functions of the system (i.e., a library with the main cryptographic functions: key generation, encryption, decryption).

For demonstration and testbed integration purposes, we will evaluate the possibility to extend the identity protection mechanisms proposed by this feature to a non-3GPP access to the 5G network, for example WiFi access with EAP-SIM or EAP-AKA authentication.

3.1.5.2 *Authentication of Identity Requests*

The network ensures the UE will be able to verify the authenticity of Identity Requests messages sent to the UE. In order for this to work in cases where security context is not available, digital signatures and PKI seem the only viable solution. In the case the Encryption of Long Term Identifiers is implemented on the network, this feature would not be required. On the other hand, if the encryption is not available, the authentication mechanism can protect at least against fake BTS-like attacks, since a 5G UEs will accept only signed authorized messages. Since a fake network node does not possess the network private key, it is not able to produce valid signatures, so it will not be authorized to send sensitive messages to UEs, like, for example, identity requests and tracking area update reject messages.

Messages from the network could be signed by using a public key digital signature mechanism; UEs would then be able to verify the authenticity of such messages. This would prevent rogue network elements from sending false information.

Examples of where public key authentication is needed:

1. **Identity Requests** should be accepted by the UE if they arrive from authorized network entities only, therefore should be signed with the network private key. The UE should be able to validate the signature (because it has the public key of the network) and send IMSI encrypted only if the signature verification is successful. IMSI catchers cannot send valid Identity Requests.
2. **Tracking Area Update Reject** messages should be accepted by UE if they arrive from authorized network entities only, therefore should be signed with the network private key.

Figure 6 describes the high level components of the feature "*Authentication of Identity Requests*":

- **Signature algorithm**: runs on the network element and is also present on the UE device. It is used to compute a digital signature, by creating a one-way hash of the request that need to be signed. The private key is used to encrypt the hash of the message. The encrypted hash along with the message is sent to the users.
- **Signature check**: this function runs on the device and checks the received hash with the one computed locally.

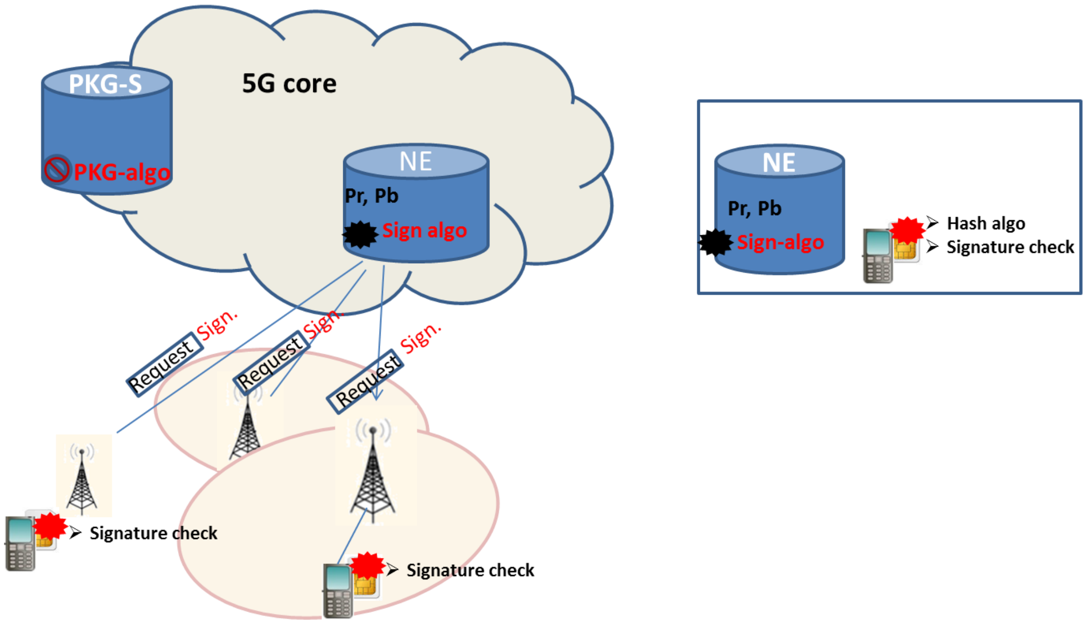

Figure 6: High level components for "Authentication of Identity Requests" feature

This type of mechanism, as such, still leaves transmitted identifiers in clear text, available to eavesdroppers. Therefore, either a "*Pseudo random dynamic pseudonyms*" or a "*Random dynamic pseudonyms*" scheme can be jointly (additionally) used. Moreover, since the signatures have to be performed by the serving network, a PKI covering all roaming partners of the home network seems required. In addition, in order to protect all signalling messages originated from the network it is required to ensure global availability and verifiability of private keys to all network components (such as eNodeB).

3.1.5.3 IMSI Pseudonymization

The goal of this feature is to totally avoid exposing user identities on (at least) the air interface (i.e., in Attach Requests, Identity Responses, Paging Responses). Some of the possible solution ideas identified at this stage are presented below, although the final choice could not be limited to the present ones.

Pseudorandom dynamic pseudonyms

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

These RIMSI/dGUTIs are always used by UEs instead of real IMSIs in response to an Identity Request, Paging Request, etc., and are consumed by usage (they follow a "one-time" scheme like in accesses based on RSA banking keys).

Figure 7 describes the high level components of the "Pseudo random dynamic pseudonyms" feature:

- **Pseudonym algorithm (pseudo-algo)**: runs on the device UE (or directly on the SIM) and on the network element. The RIMSI are generated independently by the device UE and by the network.

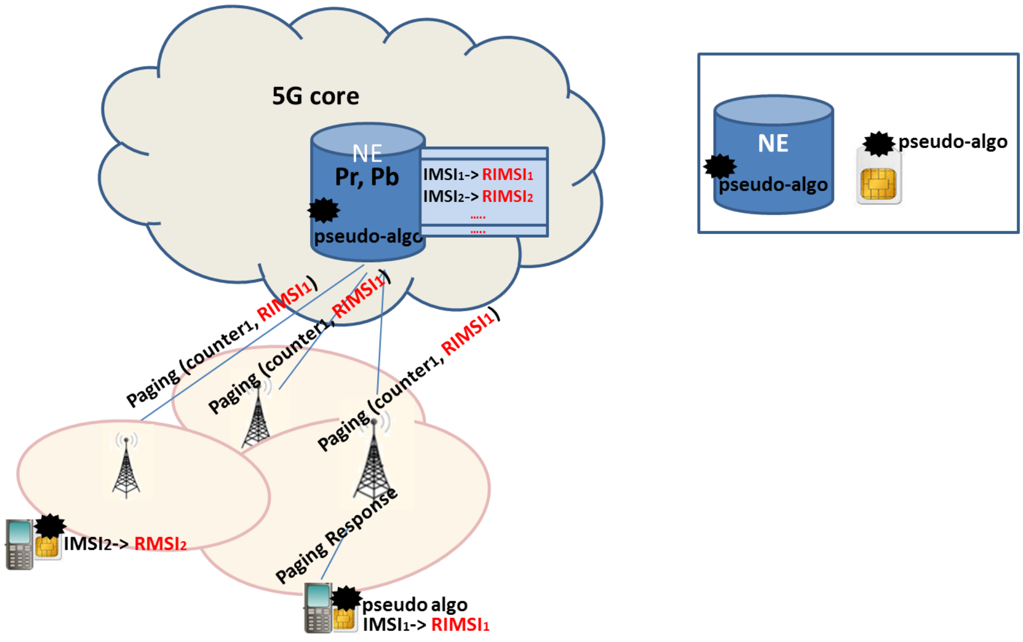

Figure 7: High level components of the "Pseudo random dynamic pseudonyms" feature

The RIMSI/dGUTI generation mechanisms must guarantee collisions avoidance over the entire subscription base or over a Tracking Area. At the moment there are some evidences that GUTIs are not random [4], therefore the proposed scheme can also apply to GUTI generation.

Random dynamic pseudonyms

This feature may be an alternative to the previous one in devices which are not able to host a pseudonym generation algorithm. The network generates the RIMSIs for all the subscriber's base and maintains the state for each UE (the UE active RIMSI or RMSI window). The real IMSI is communicated only once to the network in the first Attach Request through the first feature of this enabler (3.1.5.1). The RIMSI can also substitute GUTI. The one-time pseudonym is updated after each usage (i.e., after being used in each message for UE identification).

The RIMSIs are univocal random numbers over the entire subscribers' base, they change periodically (short periods) and are always used where IMSI is now used (and maybe also GUTI). The RIMSI is communicated by the network to the UE. The RIMSI generation mechanisms must guarantee collisions avoidance.

These RIMSI/RGUTIs are always used by UEs instead of real IMSIs in response to an Identity Request and a Paging Request.

Figure 8 describes the high level components of the "random dynamic pseudonyms" scheme:

- **Random pseudonym algorithm (rpseudo-algo)**: runs only on the network element and generates new RIMSI for each IMSI. The RIMSI is transmitted by the network element to the UE device encrypted. The UE stores the RIMSI and uses it in the next procedure.

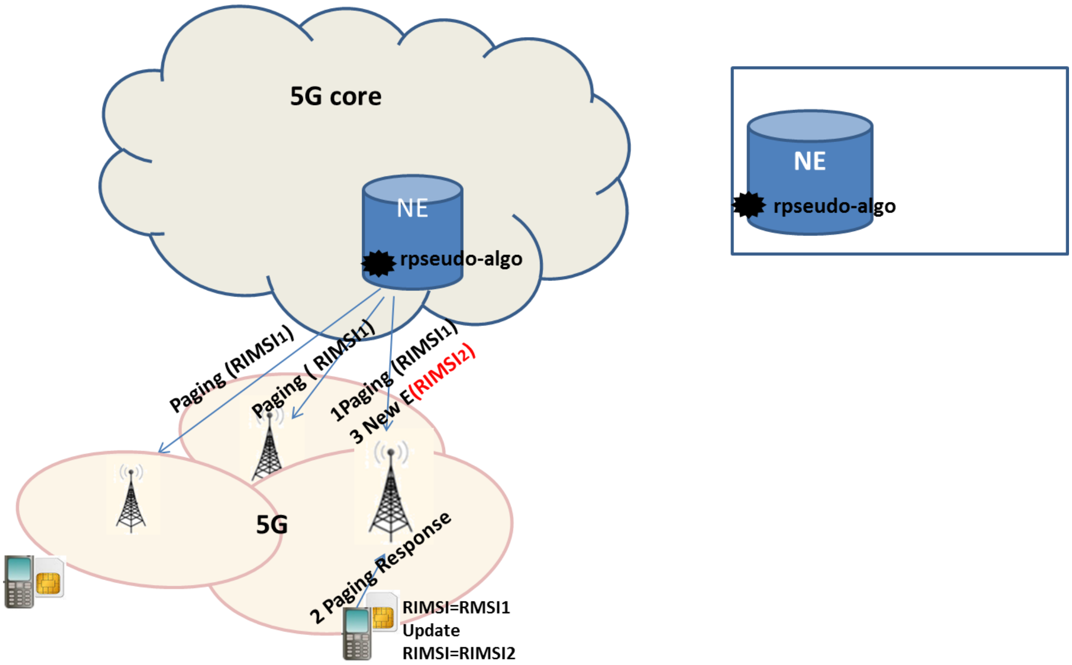

Figure 8: high level components of the "random dynamic pseudonyms" feature.

The RIMSI/RGUTI generation mechanisms must guarantee collisions avoidance over the entire subscription base or over a Tracking Area.

3.1.5.4 Privacy Enhanced AAA (for non-3GPP access)

This feature will analyse privacy issues related to additional types of access protocols used by UEs to connect to the 5G network. This in order to cover all aspects of privacy, also for any non-3GPP access, such as WiFi, which may use the EAP-SIM or EAP-AKA protocols to authorize connection to the local network, or to the evolved packet core (EPC). There are also new protocols being developed for constrained devices.

The goal of this feature is to utilize various techniques, such as protocol analysis and verification, to provide a solution that offers enhanced privacy in such interactions. The security enabler should therefore support:

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

3.1.6 Technical Roadmap for First Release (R1)

- **Feature name**: Encryption of Long Term Identifiers **(**IMSI public-key based encryption**)**
- **Goal**: Limit (preferably totally avoid) exposing user identities on (at least) the air interface (i.e., in Attach requests, Identity responses).
- **Description**: The release will provide system definitions and a prototype software implementation of the main functions of the system (i.e., a library with the main cryptographic functions: key generation, encryption, decryption). The release does not foresee the integration of the provided functionality in any UEs or network elements.
- **Rationale**: Preserving the confidentiality of the mobile subscriber's identity in 5G network, thus preventing privacy violations, such as user tracking.

3.1.7 Next release

The features planned for next release are:

- **Feature name**: IMSI Pseudonymization
- **Goal**: Totally avoid exposing user identities on (at least) the air interface (i.e., in Attach Requests, Identity Responses, Paging Responses).
- **Description**: The release will provide system definition 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 the temporal identities in 5G network (the GUTIs in LTE), thus preventing privacy violations, such as user tracking.

- **Feature name**: Privacy enhanced AAA
- **Goal**: To provide enhanced privacy for AAA protocols
- **Description**: The release will provide prototype privacy-enhanced protocols, and privacy policies for deployment. The software release will implement/demonstrate the privacy enhanced protocols.
- **Rationale**: It is essential that privacy is considered when devices connect to the network, especially as the range connection methods and RAN expands.

The plans for next release for the optional feature Authentication of Identity Requests is to mature it and come up with details regarding its planning.

3.1.8 Remarks

There are anticipated dependencies with the Basic AAA Enabler, since the privacy enhanced identity protection mechanism would probably be integrated in the basic authentication procedure. The issue is already addressed jointly.

There are also strong limitations as far as the testbed integration is concerned. For the cryptographic primitives to be integrated in real UEs and network elements, programmable open stack UEs are needed and also, at least a programmable MME. Note that such cryptographic functions are implemented by vendors themselves in their firmware optimized for the specific devices and network equipment hardware that they sell.

In order for the integration work to start, it is crucial to find a suitable open source (or similar) implementation of the basic core network infrastructure part. This means that we need working “ready-made” implementations of network functions such as MME, eNodeB, HSS, etc., since it is infeasible to build these functions from scratch. Moreover, in order to build a realistic proof of concept, we also need an open source implementations of the mobile device network stack.

A possible feasible option is to extend the IMSI protection enabler to other types of 5G access networks, and to evaluate the feasibility of its integration in security protocols such as EAP-SIM and/or EAP-AKA in order to demonstrate its validity.

The availability of the crypto library is useful for at least two reasons: the cryptographic functions can be tested with different security parameters in order to be able to answer the question how much public key ABE encryption will cost at the client and network side, and, further on, they can be readily optimized and integrated by vendors in their equipment.

3.2 Privacy Enabler “End-to-end encryption”

3.2.1 Product Vision

This enabler aims to provide end-to-end encryption support in 5G networks for protecting confidential user data/information, and preventing eavesdropping attacks on all possible paths the user data traffic flows through the mobile network. The main goal is to offer stronger protection of user data and user related information also in cases where a visited user does not trust the network to which he/she is connecting to since he/she does not have knowledge of the applied security mechanism.

Missing end-to-end security leaves communication vulnerable for compromised or malicious network components, while end-to-end security, where keys are managed by the services/devices themselves, on one hand prevents lawful interception and on the other may waste network resources as operators’ may still secure core network communication with their own mechanisms.

Key management solutions provided by the 5G operator are suitable for cases where the end-points trust the operator and operators’ capabilities (e.g., to provide truly random keys which do not leak to adversaries). In highly critical applications such trust assumptions may not always be justified. Availability of end-to-end connections may in these cases be achieved by replacing the key management that is provided by the 5G operator alone with a more trusted alternative.

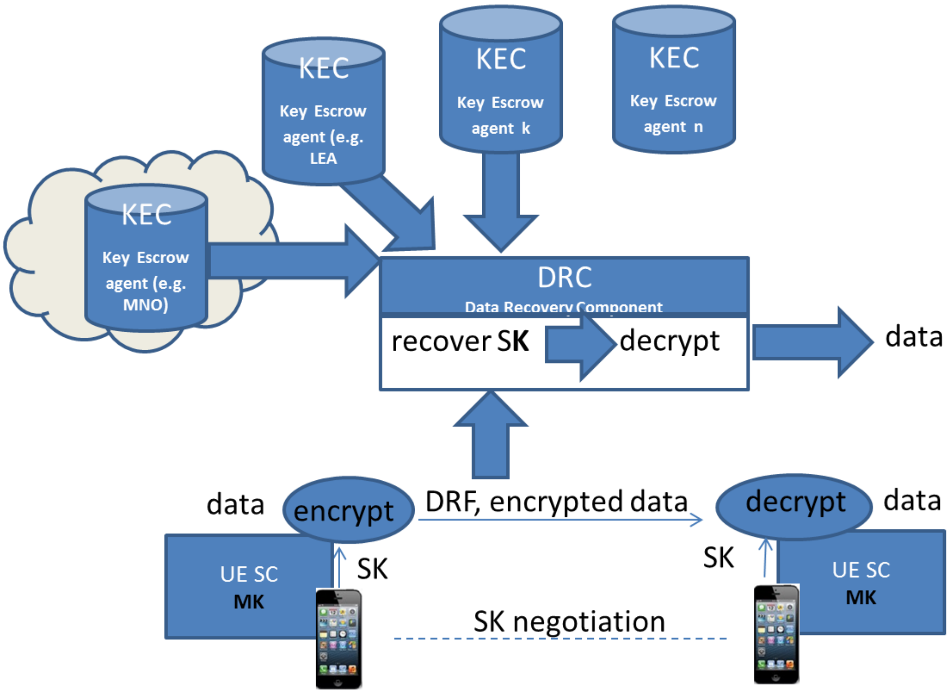

Figure 9: High level architecture for end to end encryption with key escrow.

The use case to which this enabler corresponds is Use Case: End-to-end encryption for device to device communications from the Cluster: LI.

Table 6: Mapping between End-to-end encryption enabler security features and relevant use cases.

Enabler security feature	Relevant Use Case
End to end encryption	Use Case 11.2: End-to-end Encryption in LI-aware network

3.2.2 Technology Area

Current mobile networks do not offer end-to-end encryption neither for device to device communications nor for device to server communications. Recently, many privacy violations occurred in current mobile networks. For instance, in 2013, it was reported that the national security authorities monitored phone calls of 35 world leaders [11]. This shows the interest of providing an end-to-end encryption solution that prevents illegal intercept while ensuring lawful intercept requests.

Since in most countries mobile communications have to support LI, the end-to-end encryption scheme has to take this requirement into consideration as well [12].

3.2.3 Security and Privacy Aspects

A main security problem in current networks is that user data is not protected in an end-to-end manner, i.e., all the way from the source to the destination device. In addition, since the current cryptographic model implies the use of symmetric key material, which may be exposed in various situations (e.g., during roaming the keys are transferred to the visited network), and which is all derived from a long term secret key, the user data might get vulnerable to key exposure attacks. Therefore, the encryption mechanism should limit the risk arisen from such exposures and offer fresh session key generation for each new end-to-end communication with forward and backward secrecy properties.

The enabler shall primarily take into consideration device to device mobile communications (like calls and SMS/MMS messages), since most of device to server communications are already protected at the application level (e.g., by means of TLS/SSL encryption). Nevertheless, even in the device to server communication the proposed end-to-end encryption scheme could be used if it guarantees stronger security than the existing protocols and practices.

3.2.4 Security and Privacy Challenges

There are inevitably situations where data (or at least parts thereof) need to be exposed, like lawful interception. Therefore, a solution that provides high degree of privacy even under these side conditions is challenging. This can be achieved by the so-called key escrow systems, where the short-term session keys are generated locally and shared only between the endpoints communicating to each other, but are encrypted by long-term master keys specific to endpoint users. In order to avoid single points of trust, which frequently become single points of failure, the master keys are shared among a number of independent escrow agents (government branches, jurisdiction, mobile operators, etc.). A threshold (k, n) secret sharing scheme will enable both privacy and robustness, in a sense that less than k agents do not get any information about the master key and that any k or more agents (possibly smaller than all n agents) can recover the master key.

However, this classical key escrow scheme does not satisfy the forward and backward secrecy, because if a master key is recovered, then it can be used to recover all the session keys and thus decrypt all encrypted traffic in the past or in the future. A practical solution for this exists and is known as threshold cryptography.

Probably the enabler will need to address backward compatibility requirements as well, in the sense that the end to end encryption service can be switched off by the network for compatibility reasons.

3.2.5 Features of the enabler

The enabler should satisfy the following properties:

- Under the assumption that the 5G network supports the necessary signalling protocols, etc., the end-to-end encryption service should be activated and deactivated by the user in a secured way. This may imply the use of Trusted User Interface (TUI) provided by some Trusted Execution Environments (TEEs).
- The credential used to perform the encryption must be provisioned and stored in a secure way, for instance in a tamper-resistant secure element like the SIM card.
- It should be impossible for any entity, except designated authorities (e.g., the designated authorities may include network operators, LEA, judges), to decrypt an encrypted communication of a given user.
- If we have n designated authorities, the decryption of a communication must involve at least k designated authorities. In other words, k-1 designated authorities cannot decrypt an encrypted communication.
- The decryption of a communication must involve all designated authorities. In other words, if only one designated authority is honest, the remaining compromised authorities cannot decrypt an encrypted communication.

A possible solution is represented by a threshold cryptography-based scheme for end-to-end encryption with key escrow.

A key escrow encryption system is an encryption system that allows authorized entities, (government officials, the police, a committee of the parliament for LI, etc.) to decrypt, under certain prescribed conditions, cipher text with the help of information supplied by one or more trusted parties, here called key escrow agents, holding special data recovery keys. The data recovery keys are not used to encrypt and decrypt the data, but rather provide a means of determining the data encryption key.

The components of key escrow encryption system are:

- UE Security Component (UE SC). The UE SC can be a hardware device or software program on the UE that provides:
  - Keys storage (it stores user keys, normally, these would be public private-key pairs used to establish data encryption key (session key SK) and global system keys used by the Key Escrow Component (KEC) in each key escrow agent.
  - Data encryption and decryption capabilities
  - Key escrow function support that include attaching a data recovery field (DRF) to encrypted data to permit the data recovery process.
- Key Escrow Agent: The escrow agents, also called trusted parties, (e.g. an operator and LEA) are responsible for:
  - Operating the key Escrow Component (KEC) used to store all *data recovery keys*.
  - Providing services, including release of information, to the DRC (data recovery component)
- Data Recovery Component (DRC): it supports recovery of plaintext from encrypted data using information supplied by the Key escrow agent and in the DRF.

The scheme proposed is based on threshold cryptography or, more precisely, shared decryption of encrypted session keys. In practice, this is a public-key encryption, where the user master key for encryption is public and the corresponding master key for decryption is private. This private master key (MK) is shared among the key escrow agents according to a secret sharing scheme such as a threshold scheme. The key escrow agents never combine their shares to recover the private master key. Instead, they each perform a partial decryption function to the encrypted session key (SK) with the corresponding share of the private master key. This is possible if the decryption function is homomorphic in the decryption key and if the secret sharing scheme is linear with respect to the operation over the key. Then, in a combiner (DRC), the results of these partial decryptions are combined to obtain the session key (SK). The same operation needs to be performed for each session key to be recovered. In fact, this is desirable as it enables lawful interceptions focused in time, satisfying forward and backward secrecy. There are several practical encryption schemes satisfying the homomorphic property, e.g., [13].

3.2.6 Technical Roadmap for First Release (R1)

The enabler has no feature planned in R1

3.2.7 Next release

The plans for next release are to mature this enabler and come up with details regarding the features and their planning.

3.3 Privacy Enabler “Device identifier(s) privacy”

3.3.1 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.

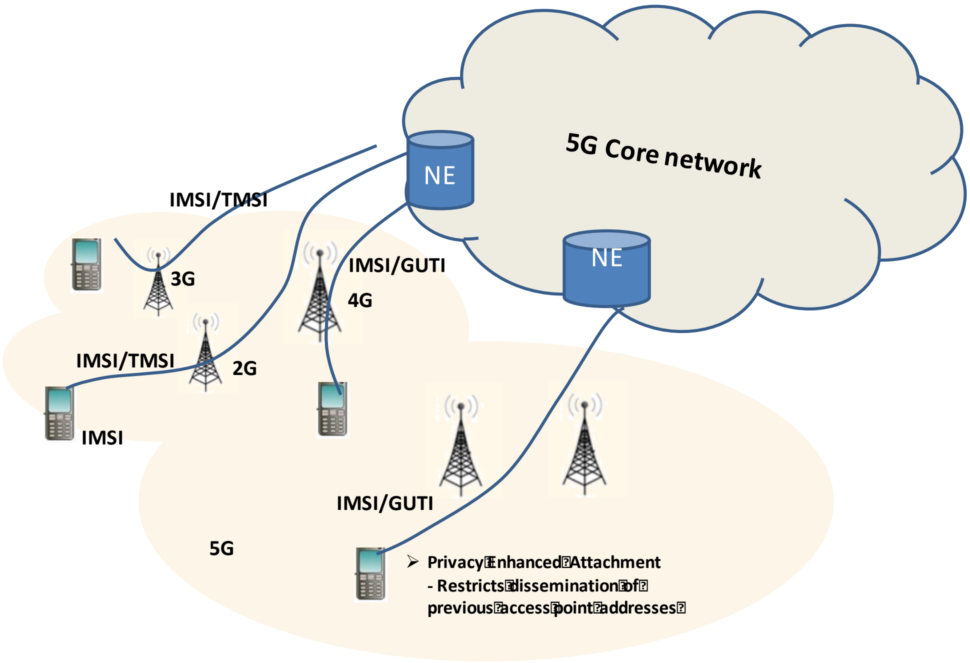
5G Core network
NE
NE
IMSI/TMSI
3G
IMSI/GUTI
4G
IMSI/TMSI
2G
IMSI
IMSI/GUTI
5G
➢ Privacy Enhanced Attachment
- Restricts dissemination of
previous access point addresses

Figure 10: 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 7: Mapping between Device identifier(s) privacy enabler security features and relevant use cases.

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

3.3.2 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 [14]. Relevant technologies include ways to securely anonymize identifiable device/user data in all or selected communications between the device and the network [15]. 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 [16]) directly on the device and at the network/server side.

3.3.3 Security and Privacy 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.

3.3.4 Security and Privacy 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.

3.3.5 Technical Roadmap for First Release (R1)

- **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) [17].
- **Rationale**: To ensure that users consider 5G as a privacy preserving technology for all types of network attachment.

The demonstrator for this enabler can be achieved considering a specific 5G use case (e.g., remote patient monitoring or an IoT scenario such as smart home).

3.3.6 Next release

The next release of the enabler will consider and address privacy challenges in additional protocols.

3.4 Privacy Enabler "SIM-based anonymization"

3.4.1 Product Vision

This enabler aims to provide anonymization techniques on the user's UICC (SIM), 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 SIM. The user's SIM will host a privacy agent application, therefore, independently on the user's device that uses the SIM, the agent will help to protect the user's privacy, according to the configured privacy profile.

The SIM implements the anonymization algorithms and offers access to their implementations through an API (Application Protocol Interface). The privacy agent can be configured to turn on and off the anonymization and to apply different algorithms on the stored sensitive data like IMSI, IMPI (IP Multimedia Private Identity), MSISDN, etc. When a user space application requires access to SIM data protected by an active privacy profile/configuration, the privacy agent is called in order to anonymize the protected data with the configured anonymization algorithm. Therefore, the requesting application will obtain the anonymized piece of data instead of the original one.

Table 8: Mapping between SIM-based anonymization enabler security features and relevant use cases.

Enabler security features	Relevant Use Case
Privacy Agent for SIM-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

Figure 11 illustrates a generic architecture containing the high level components of the enabler together with their indicative location.

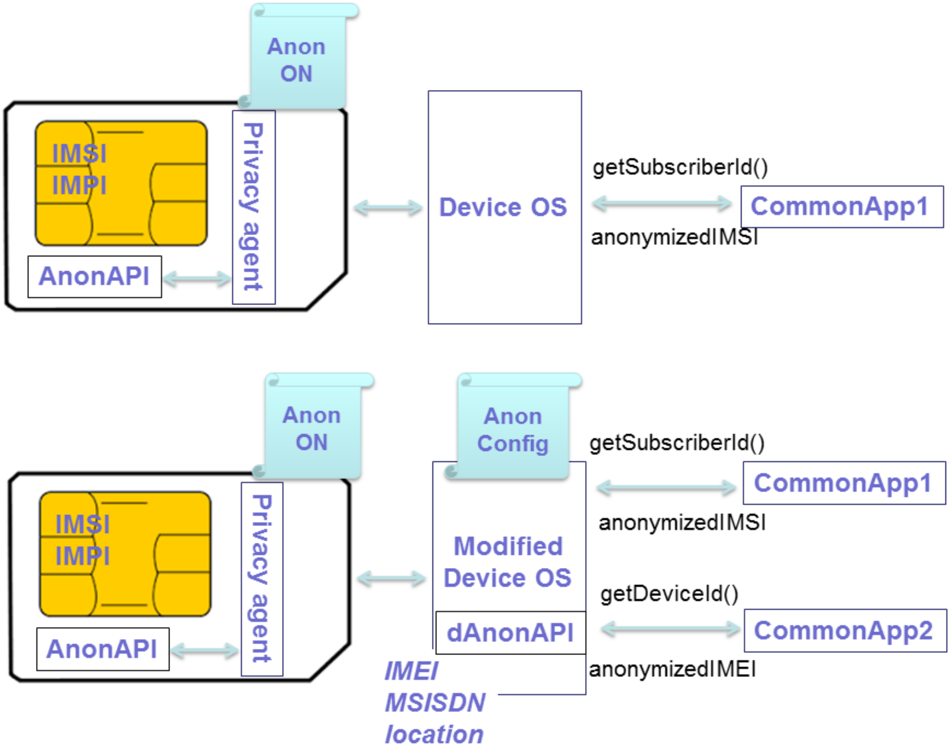

Figure 11: High level architecture for the SIM-based anonymization

- **Privacy Agent:** the mediator between the device and the anonymizing SIM. It receives calls from the OS, checks the configuration, applies the appropriate anonymization algorithms to the data and returns the anonymized data to the caller. It has a configuration mechanism through which the user can turn on and off the anonymization. This mechanism might also allow the users to configure the sensitive data to be anonymized and the algorithm to be applied (in Anon Config).
- **AnonAPI:** provides the implementation of the anonymization algorithms and offers a programming interface to the privacy agent. One algorithm may be a format preserving anonymization algorithm SIM used to provide data anonymization by preserving data syntax.

If a fine grained privacy profile configuration is needed (e.g., different anonymization algorithms applied to requests from different applications), the OS of the host device must be modified in order to handle application differentiation and communicate it to the privacy agent. Modification of the host OS is also needed if the same anonymization techniques are to be applied to other sensitive data stored on the device instead of SIM (e.g., IMEI, location information).

The SIM-based anonymization APIs can also be made accessible through the OS to common applications which desire to protect the data they handle.

The use case to which this enabler corresponds is Enhanced Services: SIM-based and device-based anonymization from the Cluster: 5G Enhanced Security Services.

3.4.2 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 anonymization algorithms and different categories of data to be anonymized.

3.4.3 Security and Privacy 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, as specified by the user's anonymization profile/configuration.

3.4.4 Security and Privacy 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.

3.4.5 Technical Roadmap for First Release (R1)

No feature is planned for R1.

3.4.6 Next release

- **Feature name**: AnonAPI - Format preserving anonymization algorithm
- **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.
- **Rationale**: Avoid disclosure of sensitive information.
- **General description**: this algorithm should preserve the format of the input data (e.g., IMSI, phone number, etc.).

- **Feature name**: Privacy agent
- **Goal**: the mediator between the caller and the anonymizing SIM.
- **Description**: The release will provide the prototype implementation of the agent.
- **Rationale**: Make active use of the anonymization APIs to protect sensitive data in order to avoid its disclosure if user desires so.
- **General description**: 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.

3.5 Privacy Enabler "Privacy policy analysis"

3.5.1 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 12 describes the high level architecture of "*Privacy Policy Analysis"* enabler.

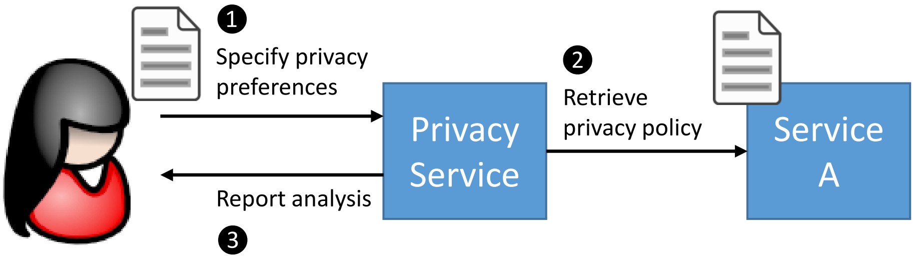

Figure 12: High level architecture of Privacy Policy Analysis Enabler

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 9: 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

3.5.2 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 [18] 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.

3.5.3 Security and Privacy 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.

3.5.4 Security and Privacy 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.

3.5.5 Technical Roadmap for First Release (R1)

No feature is planned for R1

3.5.6 Next Release

For next release 3 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 selected.
- **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.

4 Trust Security Enablers

5G-ENSURE will provide a new trust model which will address the complex relationships between the many actors in 5G networks including the machine-to-machine interactions characterising the next generation networks. The trust model needs to address the different aspects of:

- trust between automated systems (e.g. through advanced certificate and token based methods): that is M2Mt;
- trust between human stakeholders holding responsibilities for different parts of 5G networks, between user and network operators and between users of the network (U2Ut);
- trust that a human stakeholder has towards a system (U2Mt);
- trust that an automated system (machine) has in users that it interacts with, such as whether it believes the user is who they claim to be (M2Ut).

For the purpose of the rest of this introductory section we will define "trust" and "trustworthiness" terms as:

- Trust: a **quantifiable** but **subjective** measure of a *trustor's* belief that a *system* will produce acceptable outcomes.
- Trustworthiness (of a socio-technical system): its ability to produce outcomes acceptable to all trustors.

Where a socio-technical *system* is made up of technical assets as well as the involved stakeholders and a *trustor* is a stakeholder who is making a trust decision.

The trust security enablers constitute the family of technologies needed to enable and support the above trust relation in terms of the following categories:

- Trustworthy development process: this includes support for the development of 5G applications and services.
- Trust evaluation: supporting end-user to make trust related decisions based on objective evidence incorporating the behaviour and disposition aspects. By providing a trust model linked to trustworthiness features, 5G-ENSURE will map the user perceived quality and trust to the current system trustworthiness level.
- Trustworthy design: providing means to identify threats to the 5G system design and guidance on the controls to mitigate them. The focus is on providing an automated and user friendly mechanism for managing risk assessment at design-time.
- Evidence collection and certification: this category constitutes the set of enablers allowing the collection of evidences regarding a 5G system and the certification (or auditing) of its properties to support trust establishment.
- Trust maintenance: enablers for managing trust and trustworthiness during the operation of the system to support trust-based decisions in advanced, multi-stakeholder 5G-based systems and applications.

4.1 Security Enabler "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 and sub-slices 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 virtual MNOs. 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 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 with threats to enable a repeatable, systematic threat 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 10: 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	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

[3] www.optet.eu

systems using the knowledgebase	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.

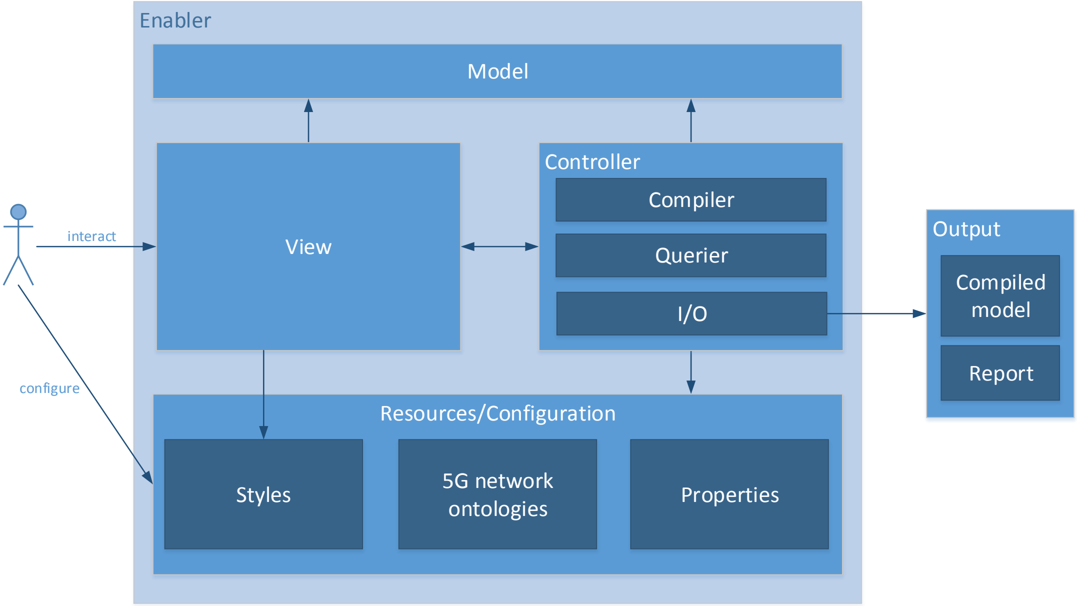

Figure 13: High level architecture of the Enabler

The trust model will be realised as an ontology which will encode the identified assets, threats and controls in a knowledgebase. The enabler will also provide a GUI for designing system models which specify the relationships between socio-technical assets in the system. 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.

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.

4.1.5 Technical Roadmap for First Release (R1)

For first release the following features are planned:

- **Feature name**: 5G Asset model
- **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.
- **Rationale**: an asset model is the basis for modelling a system and then identifying the threats and required controls.

- **Feature name**: 5G Threat knowledgebase v1
- **Goal**: allow the mapping of a limited subset of threats to the designed 5G system.
- **Description**: a second part of the ontology, the threat knowledgebase, includes a first pass at the description of the threats and how they would apply onto a 5G system. Moreover, the threats will be mapped to some of the controls that can be used to manage them.
- **Rationale**: a threat knowledge base supports the automated identification of threats in designed or existing 5G systems.

4.1.6 Next release

Features planned for next release are:

- **Feature name**: 5G Threat knowledgebase v2
- **Goal**: Allow the mapping of the threats to the designed 5G system
- **Description**: this includes an enriched base of 5G assets, threats and controls.
- **Rationale**: more threats will be added as the project matures.

- **Feature name**: A graphical editor for describing systems using the knowledgebase
- **Goal**: Allow the mapping of the threats to the designed 5G system
- **Description**: the editor will allow system designer to model their system and analyze the potential threats and their mitigation controls.
- **Rationale**: an editor will provide an easy to use interface for system threats and controls analysis.

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. 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 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.

The enabler is applicable in a wide variety of use cases as indicated in the table below. To take some specific examples from the use cases found in D2.1:

- in the case where a MNO is relying on a third party to authenticate devices attached to the MNO’s network, an SLA with the third party could be simplified by including a term based on the trust metric of the third party’s infrastructure (use case 1.1: Factory Device Identity Management for 5G Access);
- a service provider such as a bank may adjust its security policies based on the trust metric of a user (use case 1.4: MNO Identity Management Service);
- a user may make decisions about what networks and services to use based on their trust metrics (use case cluster 2: Enhanced Identity Protection and Authentication);
- an application in a vehicle can decide whether to trust information received from other vehicles based on their trust metrics (use case 4.3: Vehicle-to-Everything).

Table 11: 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	Use Case 1.1: Factory Device Identity Management for 5G Access Use Case 1.2: Using Enterprise Identity Management for Bootstrapping 5G Access Use Case 1.3: Satellite Identity Management for 5G Access Use Case 1.4: MNO Identity Management Service Use Case 2.1: Device Identity Privacy Use Case 2.2: Subscriber Identity Privacy Use Case 2.3: Enhanced Communication Privacy Use Case 3.1: Authentication of IoT Devices in 5G Use Case 3.2: Network-Based Key Management for End-to-End Security Use Case 4.1: Authorization in Resource-Constrained Devices Supported by 5G Network Use Case 4.2: Authorization for End-to-End IP Connections Use Case 4.3: Vehicle-to-Everything (V2X) 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 Use Case 7.1: Unprotected Mobility Management Exposes Network for Denial of Service Use Case 9.1: Alternative Roaming in 5G

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 due 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

There are some 5G-ENSURE enablers that can be utilized by the Trust Metric enabler. The security enabler "Bootstrapping Trust" provides the necessary measurements related to communication trust by attesting the integrity of SDN platforms and by providing positive trust metric evidence if the enabler is used for securing communication channels between network components. The security enabler "PulSAR: Proactive Security Analysis and Remediation" facilitates another kind of evidence related to communication and application trust by providing information regarding the existing vulnerabilities. Privacy enabler "end-to-end encryption" provides evidence related to the application trust level through applied end-to-end protection settings. Clearly, the more generic security monitoring enablers such as "Security Monitor for 5G Micro-segments" and "Satellite Network Monitoring" provide readily crucial information for trust metric aggregation such as anomaly detection, intrusion detection, networks status and credential status.

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 for First Release (R1)

- **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.
    - Some missing but required basic trust related measurements may be developed and implemented.
- **Rationale**: To enable UEs to offload security mechanisms to the network and to help 5G architecture to meet industrial Internet delay requirements by eliminating overlapping security features.

4.2.6 Next release

The next release will be more focused on enabling network segmentation based on different trust levels.

4.3 Security Enabler "VNF Certification"

4.3.1 Product Vision

The shift of network functions into a data center ("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 faultresilient 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 enables to instantiate several of them on commodity servers, thus sharing physical resources (CPU, RAM, memory and network) with other hosted virtual machines. Nowadays, the infrastructure provider manages its own VNF on its own infrastructure.

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

In the case of the VMNO wants to use a proprietary VNF (developed by itself for example), how could a VMNO actor provide trustworthiness assurances for 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 about:

- 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 trustworthiness model defined in 5G-Ensure (only the part concerning the VNF).

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, 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 12: 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 9.3: Authentication of New Network Elements

[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 12 above gives some indicative examples taken from Use cases deliverable [1].

4.3.3 Security Aspects

The enabler should deliver a Certification process and tools to provide the Digital Trustworthiness Certificate (DTwC). The following schema gives the proposed scenario. This scenario describes the different mandatory roles and could be instantiated in a more efficient way. 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 and NESAG process will be analysed.

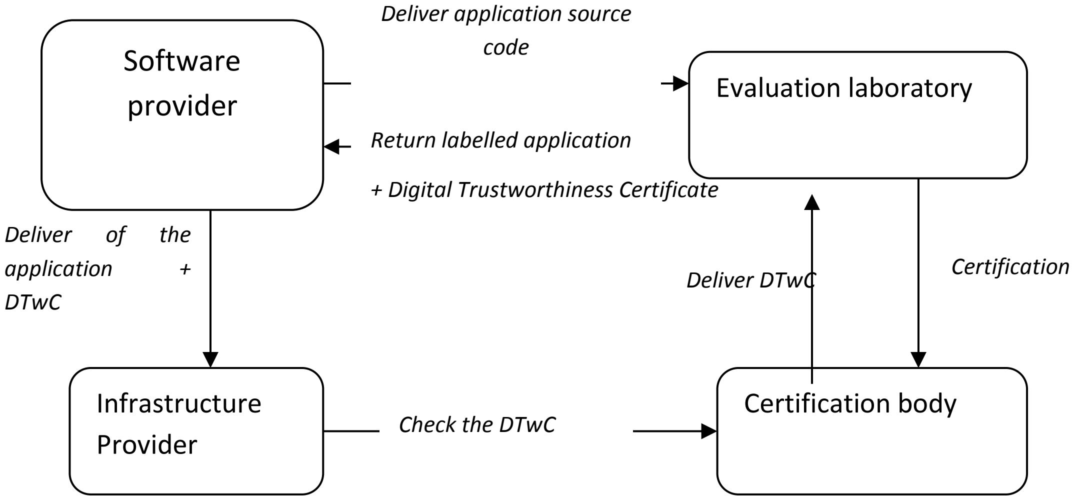
Software provider
Deliver application source code
Evaluation laboratory
Return labelled application
+ Digital Trustworthiness Certificate
Deliver of the application + DTwC
Deliver DTwC
Certification
Infrastructure Provider
Check the DTwC
Certification body

Figure 14 : 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.

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).
- To define a list of controls answering the main threats and a way to allow a monitoring tool to use them.

4.3.5 Technical Roadmap for First Release (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,

4.3.6 Next release

The next release is expected to provide a complete prototype for the VNF certification and for the Digital Trustworthiness Certificate.

5 Security Monitoring Security Enablers

5G-ENSURE project aims at providing new innovative solutions ensuring the highest level of security and resilience in 5G network. Mobile networks will dramatically evolve with the fifth generation of networks compared to 3/4G, in particular with new concepts and technologies such Internet of Things, infrastructure virtualization (SDN, NFV), network resource sharing, new access interfaces, dynamic network topologies, slicing and so forth. These technologies introduce new security and resilience challenges not taken into account so far in 3/4G. On the other hand, these new concepts provide also new opportunities to implement extensive and accurate security solutions.

Indeed, in a virtualized infrastructure, an isolation flaw may cause critical data leakage or performance impact between different virtualized network functions instances embedded in the same hardware. In dynamic topologies, the addition or removal of a network element (software or hardware) may introduce new attack vectors causing the violation of network integrity. Thus, new innovative approaches to predict and counter these challenges must be considered. We distinguish two axes that must be investigated: security by design and *security by operation* (e.g. Monitoring the 5G security). In this section, we focus on the 5G Security Monitoring aspects.

In the Release (R1) of 5G-ENSURE project, we propose five separate security monitoring enablers. They will be combined in Release (R2) of the project to benefit of their individual efficiency.

For the first release, the enablers considered are:

- Enabler "System Security State Repository": captures the system state in a model that later on can be visualized, shared, queried and analysed.
- Enabler "Security Monitor for 5G Micro-Segments": provides a Complex Event Monitoring framework enabling development of use case and threat specific monitoring applications / inference logic.
- Enabler "Satellite Network Monitoring "main goal is to provide pseudo real-time monitoring and threat detection in these Satellite and 5G networks systems.
- Enabler "Generic Collector Interface" allows efficient implementation of FastData inside 5G Networks.
- Enabler "PulSAR: Proactive Security Analysis and Remediation" relies on topological data and vulnerability data to compute predictions on on-going attacks' future steps and effective remediation proposals.

These specific enablers are detailed in the sections below.

5.1 Security Enabler "System Security State Repository"

5.1.1 Product Vision

Organizations deploy different tools in order to monitor their system (a system is composed of several servers, network equipments and softwares that constitute a coherent sub part of an infrastructure). It could be a complete slice or just an end to end abstraction of a service), 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 addresses the need to enrich the system view with information about threats, incidents, data aggregations, analysis results in order to capture 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 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 13: Mapping between System Security State Repository enabler security features and relevant use cases.

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

5.1.2 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 visualized, shared, queried and analyzed. 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.

5.1.3 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 and allowing other enablers (e.g. monitoring enabler, attack detection enabler) to update and query the model and hence keep the picture of the system state up to date. The same interface will also allow the building of more sophisticated analysis and visualization tools on top of it.

5.1.4 Technical Roadmap for First Release (R1)

- **Feature name**: Deployment model ontology
- **Goal**: Enable modeling 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.

5.1.5 Next release

The next release will include methods and approaches to update and query the model.

This enabler should be the first step towards threat runtime monitoring (and computation of threat likelihood) based on the design from Trust Builder. It will cover the modelling of basic system information (asset, controls). The interaction with the generic monitoring API enabler will be defined to make sure that the API allows in the future the capture of information regarding possible asset misbehaviours. These features, misbehaviours monitoring and threat likelihood computation, will be planned but not be addressed by this enabler within 5G-ENSURE project.

5.2 Security Enabler “Security Monitor for 5G Micro-Segments”

5.2.1 Product Vision

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. Micro-segments are created using software networking and virtualization concepts. 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 ‘micro-segment monitor’ is a security monitoring solution that can be customized for different micro-segment deployments and micro-segmented applications. It enables quick detection and reaction to security incidents by monitoring threats against 5G networks, against applications available in specific micro-segments, or against micro-segmentation mechanisms.

Security monitoring could be offered as a service by micro-segment providers (i.e. mobile and virtual mobile network operators) for different organizations needing high-security level. Potential customers include e.g. companies needing higher security assurance for industrial IoT, automotive, or e-health related services.

The enabler adopts the following technology paradigms:

- Publish-and-subscribe based information sharing provides extensibility as new data sources (probes, which publish monitored information) and security inference components (reasoning software, which subscribes monitored information) can be dynamically added.

- Complex event processor (CEP) provides efficient and extensible mechanism for handling and analyzing heterogeneous and real-time streams of monitored events.

These paradigms can be achieved using an event distribution and processing framework, which consists of existing software components. A prominent candidate is Distributed Decision Engine (DDE) framework [19]. Also, other open source components, including Apache Kafka, Apache Storm, and Esper, may be utilized.

The selected framework will be adapted during the project (release 2) to support 5G security monitoring. The framework will also be integrated with testbed and different security inference components in order to support risk management related to different use cases and threats. The development and prototyping of the monitoring systems requires some amount of implementation and integration work:

1. Probes providing compatible event information must be implemented or existing data sources adapted. Testing of anomaly-based security monitor requires traces of normal and malicious behaviour (output from probes). Hence, the security attacks must be implemented / simulated.
2. Security inference logic must be designed (based on the security metrics and threat work in WP2), implemented and integrated to existing inference engines.

Probes and inference components must be integrated using an event distribution framework.

Table 14: Mapping between Security Monitor for 5G Micro-Segments enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case
Complex Event Processing Framework for Security Monitoring and Inferencing	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
	Use Case 8.2: Standalone EPC
	Use Case 10.1: Botnet Mitigation

5.2.2 Technology Area for the Enabler

The enabler can be utilized to capture different security threats. The enabler may be customized for different micro-segments or network slices with particular applications. The enabler will implement inference algorithms that may be used in to detect and react to security incidents in virtualized networks. A particular focus in the enabler implementation is also given for industrial 5G Internet of Things network [20], [21].

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 example use cases that could benefit from the monitor are given in the table below.

5.2.3 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.

5.2.4 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 (unsegmented) 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:

- *Cross-segment attacks* - monitoring micro-segment alone is not enough as attackers may circumvent defenses 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.

5.2.5 Technical Roadmap for First Release (R1)

- **Feature name**: Complex Event Processing Framework for Security Monitoring and Inferencing
- **Goal**: Enable distributed security monitoring and reactions to security incidents.
- **Description**: The first release provides a more detailed design and a prototype that supports collection and sharing of monitored information. The first release 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.

5.2.6 Next Release

The next release is expected to provide more algorithms for inferring security incidents including monitoring of various 5G and micro-segment specific security threats. Particularly, the next release will integrate to micro-segment enabler (see section 6.5) and will provide on micro-segment/SDN specific monitoring and inferencing functionality. It will be able to adapt into dynamic changes in micro-segments – both within topologies and risk-levels – and to cover cross-segment issues. The release will also cover various 5G specific threats.

5.3 Security Enabler "Satellite Network Monitoring"

5.3.1 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.
- Hybrid EnodeB: traditional EnodeB improved with a satellite link.
- 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 15: 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
	Use Case 8.1: Satellite-Capable eNB

5.3.2 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.

5.3.3 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.

5.3.4 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 analyzed 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.

5.3.5 Technical Roadmap for First Release (R1)

Features for the security enabler:

- **Feature name**: Pseudo real-time monitoring
- **Goal**: Provide pseudo real-time monitoring of the satellite network
- **Description**: The first release will 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**: The first release will 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 signaling in heterogeneous 5G system.

5.3.6 Next Release

The next release is expected to provide the complete solution including the active security analysis to detect, investigate and response to the threats identified.

5.3.7 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.

5.4 Security Enabler “Generic Collector Interface”

5.4.1 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 will be developed 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.

Table 16: Mapping between Generic Collector Interface enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case
Log and Event Processing	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
	Use Case 5.6: Integrated Satellite and Terrestrial Systems Monitor
	Use Case 7.1: Unprotected Mobility Management Exposes Network for Denial of Service
	Use Case 8.1: Satellite-Capable eNB
	Use Case 8.2: Standalone EPC
	Use Case 9.3: Authentication of New Network Elements
	Use Case 10.1: Botnet Mitigation
	Use Case 10.2: Privacy Violation Mitigation
	Use Case 11.1: Lawful Interception in a Dynamic 5G Network

5.4.2 Technology Area for the Enabler

This enabler leverages the implementation of efficient FastData inside 5G Networks, in order to detect as soon as possible 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.

5.4.3 Security Aspects

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

5.4.4 Security Challenges

There are two major security challenges, first to define an efficient event structure (fix and dynamic parts) that suits and complies with 5G Networks' layers and nodes, second to manage the authorization to access to each flow of information in a multi-tenant infrastructure.

5.4.5 Technical Roadmap for First Release (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.

5.4.6 Next Release

The next release is expected to generalize the usage of this enabler to several 5G-ENSURE Enablers such as Trust enablers or AAA enablers, in order to efficiently monitor the 5G Networks and infrastructures.

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

5.5.1 Product Vision

The Proactive Security Analysis and Remediation (PulSAR) enabler aims at providing means to protect against cyber-attacks. Its main features can be summarized as follows:

1. Collect the vulnerabilities and evaluate the potential threats,
2. Identify most probable and impacting on-going attacks based on third parties' aggregated SIEM's and monitoring sensors' events and alerts about compromised nodes,
3. Assess risk and propose remediation solutions,
4. Deliver a visualization service centered on risk/attrition level.

The Security analysis and remediation enabler will be built upon the CyberCAPTOR (https://github.com/fiware-cybercaptor/) Generic Enabler that has been developed within the FI-PPP and 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 remediations.

CyberCAPTOR goes beyond today's offers typically used by SMEs and/or citizens (e.g. Firewall, Anti-virus) as it does enable complex attack detection, provides a clear view on an attack's progression by giving means to understand on-going attacks when a node is known as compromised, and also automatically compute possible remediations depending on the company assets (sensitive data and resources), and the IT system vulnerabilities. The possible means of remediation are sorted by a cost function based on the cost of deployment of the different remediation means such as network reconfiguration, patch deployment, etc.

Within 5G-Ensure, CyberCAPTOR features will have to be extended in the PulSAR version to allow reactive provisioning of remediation capabilities and dynamic security analysis taking into consideration the numerous topology and usage modifications taking place in a 5G infrastructure.

This PulSAR enabler relies on topological data and vulnerability data to compute predictions on ongoing attacks' future steps and effective remediation proposals. For release 1, new vulnerability patterns will be added to correspond to 5G environment using SDN and NFV technologies specific vulnerabilities. For release 2, it will rely on the Generic Collector Interface (R1) feature to gather all relevant inputs at a given time, necessary to compute risk predictions on on-going attacks and related remediation proposals.

Table 17: Mapping between Proactive Security Analysis and Remediation enabler security features and relevant use cases.

Enabler Security Feature	Relevant Use Case
Extension of the Cyber Attack modeling	Use Case 5.1: Virtualized Core Networks, and Network Slicing
	Use case 5.5: Control and Monitoring of Slice by Service Provider
	Use Case 10.1: Botnet Mitigation
	Use Case 10.2: Privacy Violation Mitigation
	Use Case 11.1: Lawful Interception in a Dynamic 5G Network

5.5.2 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.

5.5.3 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.

5.5.4 Security Challenges

As the CyberCAPTOR has not been created for analyzing 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 a such a 5G environment using SDN and NFV technologies.

5.5.5 Technical Roadmap for First Release (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 that will combine vulnerabilities of its different management components and systems. This Enabler will combine new vulnerability patterns, related to 5G environment using SDN and NFV technologies specific vulnerabilities, with existing CyberCaptor's models in order to deliver dynamic security analysis taking into consideration the numerous topology and usage modifications taking place in a 5G infrastructure.

5.5.6 Next Release

Features planned for next release are:

- **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.
- **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.

- **Feature name**: first study of a scenario based threat management
- **Goal**: Adaptive incident management
- **Description**: Deploy and maintain a detection and prevention policy based on attack scenario models specific to 5G. Maintenance includes the selection of remediations and their deployment as security VNF.
- **Rationale**: Leverage on 5G new adaptative remediation capabilities through dynamically configurable VNF.

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 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. However, centralized control represents a valuable target for attacks and a single point of failure.

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.

1. Anti-fingerprinting interactions between switches and network controller.
2. Access control mechanisms for the network's control plane.
3. Auditing the interactions between network components.
4. Bootstrapping trust in virtualized network environments between network endpoints and also between (SDN) network components.
5. Network management enabler (utilizing the SDN architecture) that facilitates micro-segmentation. Create secure network segments for fine-granular network flow policies.

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.

The relevant uses cases from [1] of this enabler's feature are listed in the following table.

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

Enabler Security Feature	Relevant Use Case
Controller-Switch-Interaction Imitator	Use Case 4.2: Authorization for end-to-end IP connections 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) [22]. 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 more costly 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 for First Release (R1)

The anti-fingerprinting enabler comprises one feature, which we describe in the following.

- **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) [23] [24] would be rather straightforward to realizable, 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. Our recent experiments 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%.

6.1.6 Next Release

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

6.1.7 Remarks

- The above described enabler is already sketched in the paper [25]. The security enabler and its evaluation are described in detail in the extended version of this paper [26].
- 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 is expected than in current mobile networks. It is also expected that various network applications will run at the network's control plane on top of the 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.

Related to untrusted network applications because of software bugs is the following. First, note that even if a network application runs in a virtualized network, the 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 [27]) might expose vulnerabilities to the network's control plane, which can be exploited by malicious network 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 network 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 SDN controllers do not provide any means to restrict the access of network applications to network resources. For example, a network application can send any OFPT_FLOW_MOD OpenFlow message to any switch (i.e., write any flow rule to a switch's flow table). This is analogous to a database user that can arbitrarily modify the tables of the database, or the root user of a computer that can write to any file. Another example concerns OpenFlow messages that request information about the current network configuration. If the controller maintains a network information base (NIB), not every application should have full read permissions to this database. For instance, not every application should be allowed to see all the currently installed flow rules at the switches.

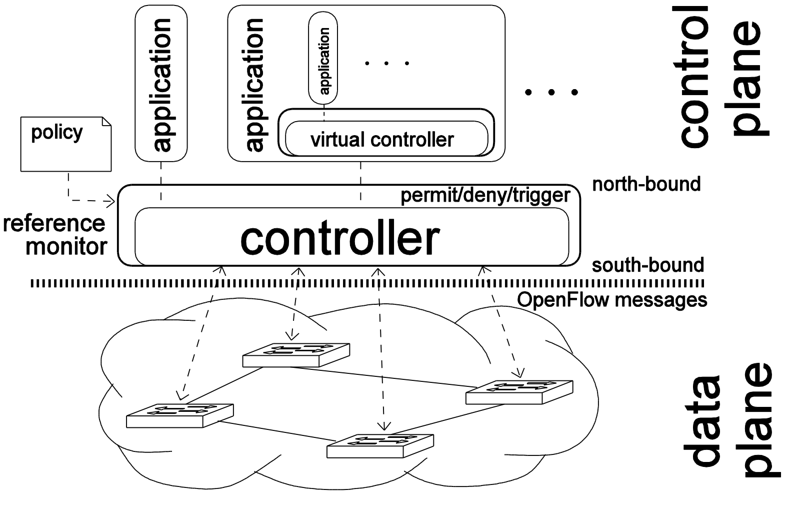

Figure 15 SDN controller extension with a reference monitor.

The security enabler described in this section **applies the *principle of least privilege* to the network applications**, that is, the enabler enforces that each network application must be able to only access the information and resources that are necessary for performing its tasks. To this end, the security enabler adds *reference monitors* to the network's control plane. See Figure 15 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.

The relevant uses cases from [1]of this enabler's feature are listed in table below.

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

Enabler Security Feature	Relevant Use Case
Southbound Reference Monitor	Use Case 4.2: Authorization for end-to-end IP connections Use Case 5.2: Adding a 5G node to a virtualized core network Use Case 9.3: Authentication of new network elements Use Case 11.1: Lawful interception in a dynamic 5G network

6.2.2 Technology Area

The enabler operates at the control plane of SDN networks in general. 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.

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, current SDN controllers 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 behaviour, 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 to SDN. 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 the SDN area.

Note that in general there is a trade-off 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 [28], and some expect a market size of $35B in 2018 with a significant growth in software, see [29] .

6.2.5 Technical Roadmap for First Release (R1)

The first release of the enabler will comprise the following feature.

- **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. The access control policy that the reference monitor enforces will be based on the (discretionary) access control schemes described in [30] and [31]. It assigns ownership to network entities like flow rules and flow tables. The owner of an entity can grant other network applications access to this entity.
- **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.
- ***Remarks*:** A first running prototype of the reference monitor for the ONOS controller [27] [32] should be ready in summer 2016 (around August). Additional features will then be added to this prototype, e.g., a policy specification language and the support for APIs at higher levels. It is planned that the policy specification language will be added in the first part of the project. The support for higher-level APIs will be on-going work for the second part of the project.

6.2.6 Next Release

The next release of this security enabler will support network abstractions at higher levels. More concretely, the developed access control mechanisms will target the northbound APIs of the SDN controllers. Furthermore, it is also planned that the next release of this security enabler will include mechanisms for multitenant networks, where 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 plan to focus on providing a trustworthy reference monitor. 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 Trust and is under investigation.

6.2.7 Remarks

- Our choice of extending the SDN controller ONOS [27] [32] 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 [33] should be similar to our ONOS extension.

- In the first release of our enabler (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 [34]. 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 topics of other topics, i.e., Trust and Privacy. 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. Furthermore, policies can be stated at different levels of abstractions.

The proposed security enabler checks compliance of the interactions concerning the network management between components in an SDN network with respect to a given policy. 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. The enabler checks policy 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. In this case, the compliance checker can be understood as a monitor that checks compliance of security policies about the exchanged OpenFlow messages between network components in an SDN network. 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.

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 [35]. In general, policy compliance checking is an "easier" problem than policy enforcement. Hence, the enabler in this section targets a wider range of security 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, 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 [1] of this enabler's feature are listed in following table.

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

Enabler Security Feature	Relevant Use Case
Basic OpenFlow Compliance Checker	Use Case 5.2: Adding a 5G node to a virtualized core network Use Case 5.4: Verification of the virtualized node and the virtualization platform Use Case 9.3: Authentication of new network elements Use Case 11.1: Lawful interception in a dynamic 5G network

6.3.2 Technology Area

This enabler is used for SDN networks. Since SDN concepts, in particular, separated network planes that interact with each other, will be adopted in 5G networks, this enabler will also apply to 5G networks. Note that a 5G network will provide multiple (virtualized) network services that directly or indirectly interact with each other, the network controller, and the network's data plane.

The enabler aims at verifying the interaction between network components, both at the control plane and the data plane. 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. Detecting noncompliant behaviour of components with respect to a given policy 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 behaviour 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 for First Release (R1)

The first release of this security enabler will comprise one feature, which we describe below.

- **Feature name:** Basic OpenFlow Compliance Checker.
- **Goal:** Verification of the interaction between multiple network components with respect to simple 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 behaviour about the components' interactions across different network layers makes a network less vulnerable to intended or unintended misconfigurations. Furthermore, additional checks on the interacting components make the network more trusted.
- ***Remarks*****:** A first running prototype of the Basic OpenFlow Compliance Checker should be ready in spring 2016 (around April 2016). It will be evaluated in a Mininet [36] [37] environment. The focus of this first evaluation will be to identify potential performance bottlenecks of the enabler's scalability to large physical networks. As a next step, the enabler will be evaluated within a 5G setting. This evaluation will include adjustments for the specifics of a 5G network and 5G use cases. It is planned that the project's 5G testbed network is used for this evaluation.

6.3.6 Next Release

Additional features will be added to the enabler's prototype, e.g., a more expressive policy specification language. The extension will also account for different network abstractions. Furthermore, it is planned that subsequent releases are optimized, and deployed and evaluated in the physical 5G testbed.

6.3.7 Remarks

- We point out that the compliance checker is trusted here. The input that the compliance checker receives is also trusted here. Enhancing the trustworthiness of the compliance checkers output falls topic wise into Trust. The enabler's trustworthiness might be considered in collaboration with Trust enablers in next releases of the enabler.
- We also remark that when checking online (i.e., during runtime) whether the interactions between different network components comply with a given security policy, overlaps topic wise with Security Monitoring. However, the enabler here does not account for network traffic but instead focuses on how the components are managed.

6.4 Security Enabler "Bootstrapping Trust"

6.4.1 Product Vision

The SDN architectural approach challenges many of the network infrastructure rules and best practices that have evolved over the decades since packet-switched digital network communication gained popularity and all but replaced circuit-switched networks. Likewise, many security best practices accumulated over the years are becoming increasingly obsolete and must be adapted to the new architectural model in order to adjust to the emerging risk factors and threat vectors. A potential risk factor is the proliferation of virtualized network components (such as *virtual switches*) running 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, reroute traffic to a malicious destination or hijack other network edge components through lateral attacks.

This enabler addresses impersonation attacks on network components by attesting the integrity of network edge 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 aims to protect the authenticity, confidentiality and integrity of internal management SDN communication by deploying secure communication channels among the virtualized network components and SDN controllers. 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 the enabler described in Section 6.3. 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 21, while a high-level architecture is presented in Figure 16.

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

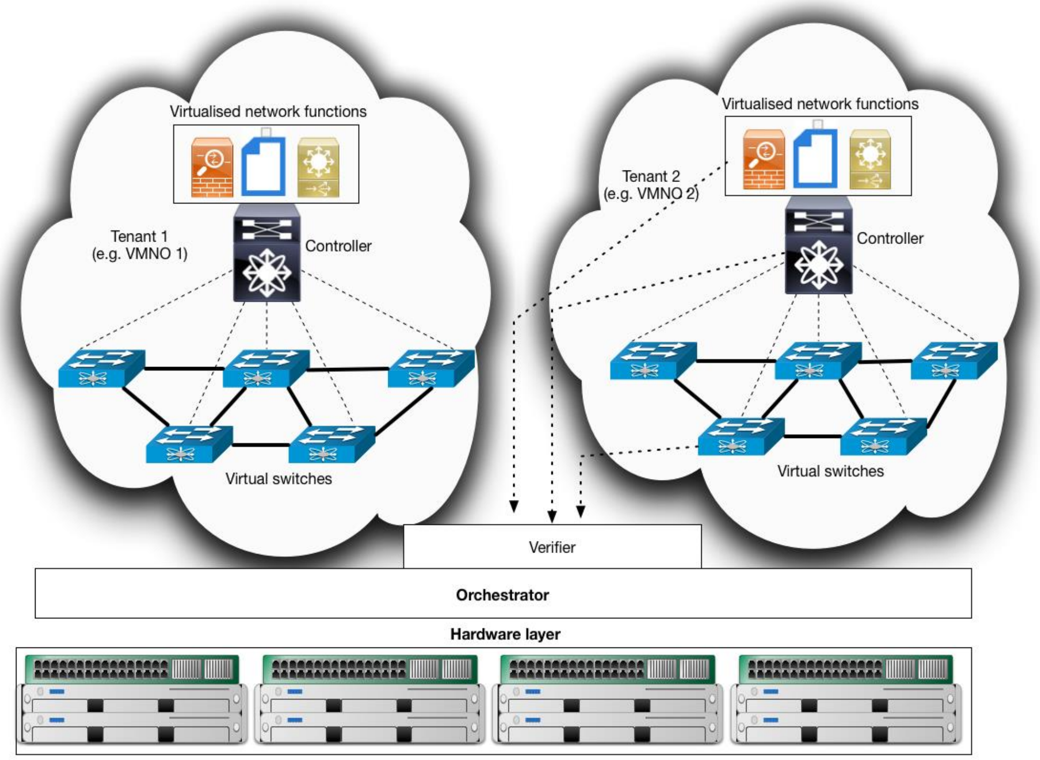

Figure 16: Integrity verification of virtual network components.

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

Enabler Security Feature	**Relevant Use Case**
Integrity Attestation of Virtual Network Components	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 5.4: Verification of the virtualized node and the virtualization platform Use Case 9.3: Authentication of new network elements

6.4.2 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. It produces integrity measurements of the software switches deployed on the data plane. The network controller then evaluates the measurements, prior to enrolling the respective data plane component into the deployment. This may require an extension to the OpenFlow protocol; alternatively, communication of the integrity measurements to the network controller can be done through an out-of-band channel.

6.4.3 Security Aspects

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

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

6.4.4 Security Challenges

The security challenge this enabler addresses the ability of the adversary to negatively affect the SDN deployment by either enrolling compromised software switches in the data plane, or impersonating enrolled switches. Likewise, this enabler aims to thwart the adversary's ability to attack the confidentiality or integrity of the communication within the deployment.

6.4.5 Technical Roadmap for First Release (R1)

- **Feature name:** Integrity Attestation of Virtual Network Components
- **Goal:** Implement the strictly minimal functionality of software components and protocols necessary to validate the concept of deploying SDN components in isolated execution environments with a hardware root of trust.
- **Description:** An SDN deployment orchestrator instantiates a network controller and verifies its integrity, reported by a hardware root of trust; similarly, the orchestrator verifies the integrity of the data plane components in the tenant's domain before they are enrolled into the SDN deployment by the network controller. The functionality of the network infrastructure components must be expanded in order to support the protocols required by this enabler; furthermore, additional software components – such as a remote integrity attestation component, as well as an orchestrator for trusted deployment of SDN components may have to be developed or extended from existing software.

  Linux *Integrity Measurement Architecture* is the more likely candidate software for attestation, while popular configuration management tools – such as *Chef* or *Ansible* – will be used for orchestration. The first release will focus on implementing integrity measurement of software switches as well as reporting the integrity measurements. Integrity measurement will be implemented using an open-source tool – such as the *Advanced Intrusion Detection Environment* utility or similar – and will be reduced to detecting *modifications* of the software switch binaries compared to an initially known state, recorded at deployment time.

  To add another layer of security, the integrity measurement utility could be modified to run in a secure execution environment, such as the ones enabled by Intel SGX. The first release will make use of hardware emulation in order to avoid complications arising from dependencies on specialized hardware components. This enabler aims to detect alteration attacks on both the software switch binaries and well as their related configuration files, ensuring that the binary and configuration files have not been modified since deployment time.
- **Rationale:** SDN deployments may be vulnerable in case of a malicious network controller; conversely, a benign network controller may be induced to misbehave if it is presented with a distorted view of the network topology, if fake data plane components are enrolled into the deployment, or if network management commands are spoofed.

6.4.6 Next Release

The next release R2 will build upon the obtained experience in order to construct a mature enabler that can be integrated into one of the popular SDN controllers, such as ONOS [32] or OpenDaylight [33]. The exact choice of the target network controller will depend on the progress of other enablers and will aim towards best possible interoperability with other enablers and the 5G testbed under definition at project level.

R2 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 a certain integrity configuration of the software switch.

6.4.7 Remarks

There is a certain overlap between this enabler and the VNF Certification enabler concerning the integrity verification of the switches. This overlap will be addressed in the following release.

6.5 Security Enabler “Micro Segmentation”

6.5.1 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, merging, and splitting 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. Micro-segments are in general isolated parts of the 5G network dedicated for particular application services or users. Compared to network slices, micro-segments can provide more specific access controls and stricter security policies. The mobile network is generally divided into smaller parts, each unique segment can have its own security controls defined, and services delivered. Only authenticated devices and network services can join the segment and traffic inside the segment should also be monitored.

It is yet to be defined what specific components are included in a network slice or micro-segment. One possible solution could be to include the PDN gateway (PGW) and the policy control resource function (PCRF) in one slice or micro-segment [38]. For machine type communication (MTC) and machine-to-machine (M2M) solutions, the slice or micro-segment should, however, include also the Mobile Management Entity (MME) and the Serving Gateway (SGW). Each slice or micro-segment could also have its own AAA entity. All these entities would be virtualized resources or functions.

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.

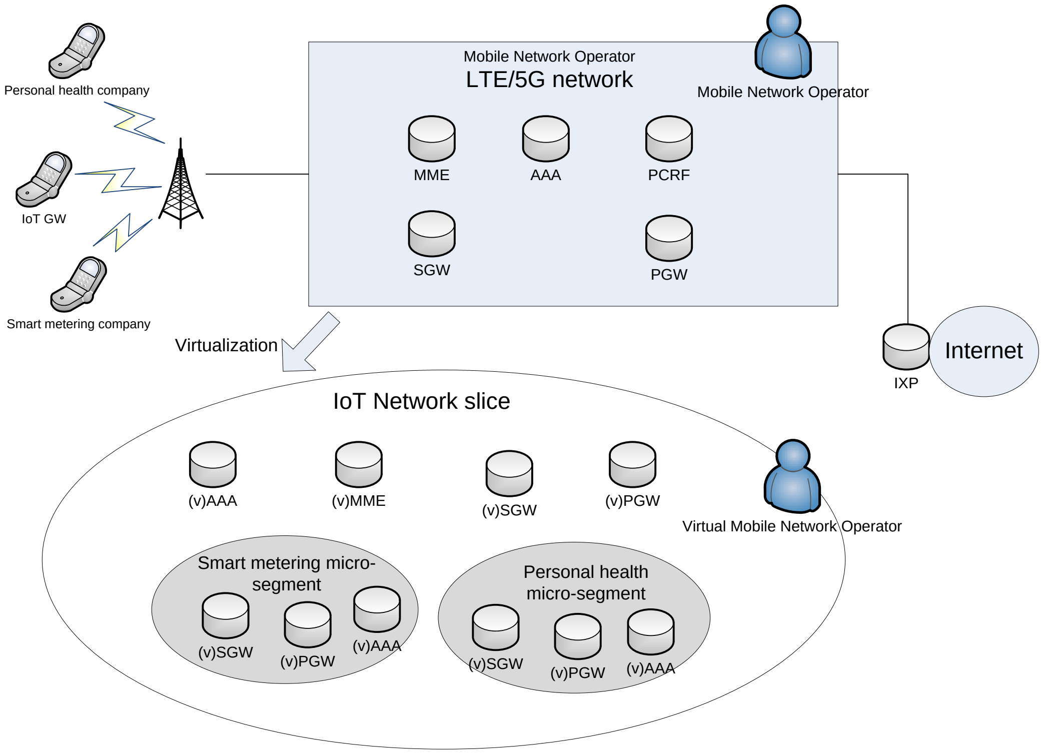

Figure 17 Micro-segmentation in a single domain network

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.

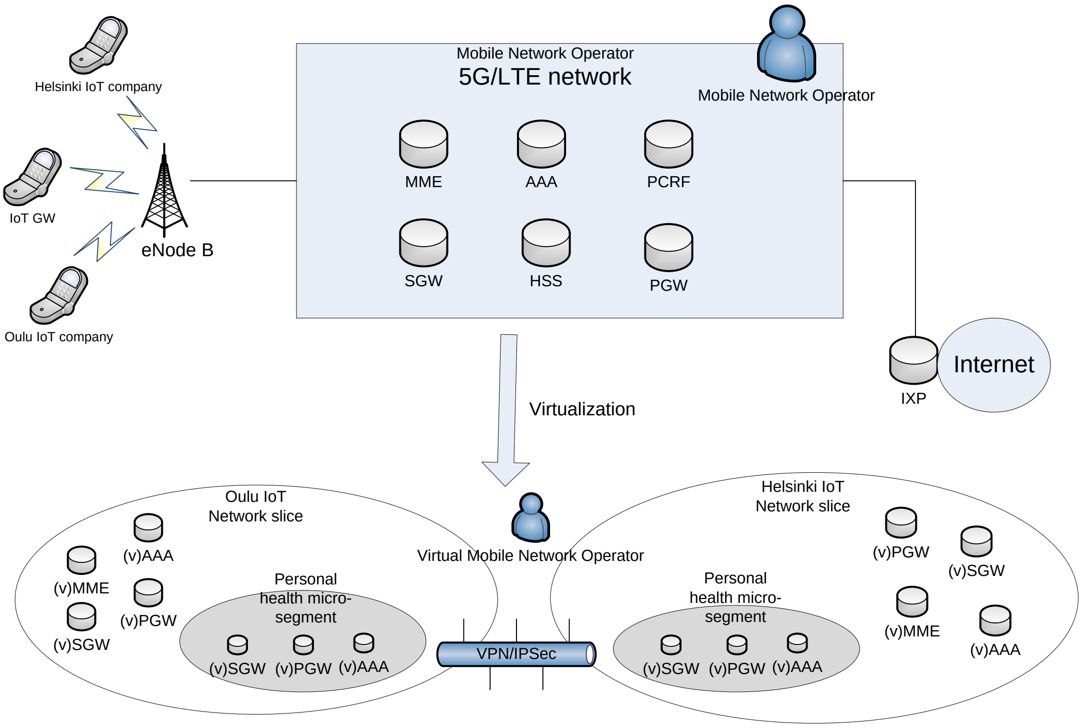

Figure 18 Micro-segmentation in a multi-domain network

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 unknown and unauthenticated devices are needed to join and exit the micro-segment on-the-fly. 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.

Table 22 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). As the main business value of the enabler is security of IoT based communications, Authentication of IoT Devices in 5G (Use Case 3.1) and Network-Based Key Management for End-to-End Security (Use Case 3.2) are also relevant to the enabler. Furthermore, micro-segmentation could be beneficial in satellite communications. For instance, the satellite network operator could isolate the more expensive satellite resources from other 5G traffic. Therefore, the enabler is related to the Satellite Identity Management for 5G Access (Use Case 1.3).

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

Enabler Security Feature	Relevant Use Case
Dynamic arrangement of Micro-Segments	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 3.1: Authentication of IoT devices in 5G Use Case 3.2: Network-based key management for end-to-end security Use Case 1.3: Satellite identity management for 5G access

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.

6.5.2 Technology Area

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

6.5.3 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.

6.5.4 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 and determine the AAA aspects of micro-segmentation. The enabler is thus reliant on the work done on AAA, Trust, and Security Monitoring.

6.5.5 Technical Roadmap for First Release (R1)

- **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.

6.5.6 Next Release

In the R2 release, the micro-segmentation enabler is planned to be extended by combining features from other security enablers, namely Security Monitoring, Trust, and AAA. Security Monitoring features will include specific methods for monitoring micro-segments and responding to threats and anomalous behaviour. A suitable trust model and the AAA aspects of micro-segmentation shall be investigated and incorporated into the enabler. Also, features related specifically to micro-segmentation are further developed, such as merging and splitting of micro-segments.

6.5.7 Remarks

- As mentioned earlier, this enabler is related to other enablers (AAA, Trust Security Monitoring) and coordination has been planned.
- The first release of the enabler is implemented in an SDN environment. First tests shall be carried out in an initial development environment consisting of Mininet [37], using OpenVirteX [39] software based virtualization and an SDN controller such as ONOS [32] or OpenDaylight [33]. In the second release, the aim is to implement micro-segmentation in a 5G testbed network environment and find what mobile network entities are included in a micro-segment. The definition of such a testbed is still under way at project level. The enabler will need to be adapted to the specification of the testbed (i.e. specific controller).

7 Summary

The table below summarizes the 5G-ENSURE technical roadmap for R1 (or v1.0). It shows the 5G security enablers in scope providing their (code) name, category to which they belong to (i.e. AAA, Privacy, Trust, Security Monitoring, Network management & virtualization isolation), as well as the features planned for their 1st software release.

Table 23: 5G-ENSURE Technical Roadmap for R1

5G-ENSURE security enablers	**Category**	**Features planned for 1st sw release (R1)**
Basic AAA enabler	*AAA*	
		A pre-study is required in the time frame of R1, however, due to lack of resources, an implementation is not feasible for the same release. Prototyping can potentially be done for R2.
Internet of things (IoT)	AAA	Group authentication
Fine-grained Authorization	AAA	Basic Authorization in Satellite systems
		Basic distributed authorization Enforcement for RCDs
Federative authentication and identification enabler	AAA	none
Privacy Enhanced Identity Protection	Privacy	Encryption of Long Term Identifiers **(**IMSI public-key based encryption**)**
End-to-end encryption	Privacy	none
Device identifier(s) privacy	Privacy	Enhanced privacy for network attachment protocols
SIM-based anonymization	Privacy	none
Privacy policy analysis	Privacy	none
Trust Builder	Trust	5G Asset model
		5G Threat knowledgebase v1
Trust Metric Enabler	Trust	Trust metric based network domain security policy management
VNF Certification	Trust	VNF Trustworthiness Evaluation
System Security State Repository	Security Monitoring	Deployment model ontology

5G-ENSURE security enablers	Category	Features planned for 1st sw release (R1)
Security Monitor for 5G Micro-Segments	Security Monitoring	Complex Event Processing Framework for Security Monitoring and Inferencing
Satellite Network Monitoring	Security Monitoring	Pseudo real-time monitoring
		Threat detection
Generic Collector Interface	Security Monitoring	Log and Event Processing
Proactive Security Analysis and Remediation	Security Monitoring	5G specific vulnerability schema
		5G specific vulnerability schema implementation
		PulSAR interface with Generic Collector
		first study of a scenario based threat management
Anti-Fingerprinting	Network management & virtualization isolation	Controller-Switch-Interaction Imitator
Access Control Mechanisms	Network management & virtualization isolation	Southbound Reference Monitor
Component-Interaction Audits	Network management & virtualization isolation	Basic OpenFlow Compliance Checker
Bootstrapping Trust	Network management & virtualization isolation	Integrity Attestation of Virtual Network Components
Micro Segmentation	Network management & virtualization isolation	Dynamic Arrangement of Micro-Segments

As for next release the table below summarizes early elements given highlighting some of the features planned for enabler in continuation and or enabler to come and/or (R&T/R&D) topics under investigation to derive them. This without presuming of final content for R2 since depending on R1 outcomes and also object of update of this deliverable (i.e. D3.5 5G-PPP security enablers technical roadmap (update) /M13).

Table 24: 5G-ENSURE plans for next release

5G-ENSURE security enablers	Category	Under analysis for next release and update of TR	
		Features under consideration	R&T/R&D Topics under discussion
Basic AAA enabler	*AAA*	*Forward Secrecy*	*Three areas will be analysed. The possibility to add forward secrecy to the AKA protocol, to limit and/or recover from compromised long term keys Analyse the possibility to find a suitable AAA solution in trusted micro segmentation of 5G Analyse the authentication and authorization protocols between networks, to add necessary security functionality of interconnecting parties*
		AAA aspects of trusted micro-segmentation	
		trusted interconnect and authorization	

5G-ENSURE security enablers	**Category**	**Under analysis for next release and update of TR**	
Internet of things (IoT)	AAA	Further development of the necessary features of group authentication. State-of-the-art survey of alternatives to UICC, including suitable protocols for management	To scale up group authentication, the enabler will analyse the possibility to dynamically form groups and to enable IoT devices to join or leave an IoT group. This will include protocol properties that ensure forward and backward and secrecy.
Fine-grained Authorization	AAA		The enabler will investigate how to support policies for decision per user, resource and action, access control for dynamically changing parameters. Additionally, it is expected to bring an integrated authentication and authorization mechanism with the satellite systems. Finally, it is expected to provide the final version of PEP and PDP embedded on the RCD and the Authentication server delivering the security token
		Provide final version of PEP and PDP embedded on an RCD, with the authentication server delivering the security token	
Federative authentication and identification enabler	AAA	Trust and liability computation	The enabler will investigate two topics It will analyse how different components can assess the level of trust and liability for incoming requests Furthermore, it will analyse how existing identity federations can expand into 5G, while providing trust and liability levels
Privacy Enhanced Identity Protection	Privacy	IMSI Pseudonymization	possibility to avoid using IMSIs and replace them with (random) pseudonyms
		Privacy enhanced AAA	possibility to extend IMSI encryption or pseudonymization to other non-3GPP access modalities
End-to-end encryption	Privacy	none	key escrow for end-to-end encryption
Device identifier(s) privacy	Privacy		address privacy challenges in additional protocols
SIM-based anonymization	Privacy	Format preserving anonymization algorithm	
		Privacy agent	
Privacy policy analysis	Privacy	privacy policy specification	
		privacy preferences specification	
		comparison of policies and preferences	
Trust Builder	Trust	5G Threat knowledgebase v2	
		A graphical editor for describing systems using the knowledgebase	
Trust Metric Enabler	Trust		enable network segmentation based on different trust levels.
VNF Certification	Trust		complete prototype for the VNF certification and for the Digital Trustworthiness Certificate

5G-ENSURE security enablers	**Category**	**Under analysis for next release and update of TR**	
System Security State Repository	Security Monitoring		methods and approaches to update and query the model
Security Monitor for 5G Micro-Segments	Security Monitoring		more algorithms for inferring security incidents including monitoring of various 5G and micro-segment specific security threats
Satellite Network Monitoring	Security Monitoring		active security analysis to detect, investigate and response to the threats identified.
Generic Collector Interface	Security Monitoring		generalization of this enabler to others
Proactive Security Analysis and Remediation	Security Monitoring		
Anti-Fingerprinting	Network management & virtualization isolation	*already evaluated; no further release planned*	
Access Control Mechanisms	Network management & virtualization isolation		support of network abstractions at higher levels. More concretely, the developed access control mechanisms will target northbound and westbound/eastbound APIs of SDN controllers
Component-Interaction Audits	Network management & virtualization isolation		extensions (e.g. more expressive policy specification languages and accounting for different network abstractions) and optimizations
Bootstrapping Trust	Network management & virtualization isolation		mature enabler to be in a position to integrate into one of the popular SDN controllers (e.g. ONOS or Floodlight)
Micro Segmentation	Network management & virtualization isolation		extensions by incorporating additional features related to AAA, Trust & Security Monitoring to enhance the security of micro-segments

8 Conclusions

This document provides an early vision and rough descriptions of the 5G Security enablers in scope of the project together with the rationale behind their choice/proposal. The presentation is structured on a per category (thematic area covered) basis, i.e., AAA, Privacy, Trust, Security Monitoring, Network management & virtualization isolation, and with a clear scheduling of the enablers to be developed over R1 vs. next release (v2.0 or R2). Technical Roadmap for R1 enablers is given, detailing each of the features planned to be released. As for the next release and although this is in scope of an update of this deliverable (i.e. D3.5), some insights are already given in order to figure the new features anticipated for enablers initiated in R1 and/or enablers specifically planned for R2.

Furthermore, this deliverable takes advantage of the Use Case deliverable recently submitted [1] to early state the relevance of the planned security enablers and features to the corresponding 5G use cases, showing an overall good coverage/fit.

Overall, this deliverable paves the way towards the first release of 5G-ENSURE security enablers whose open specifications will be one of the next steps. It also contributes to further progress on 5G Security Vision in terms of both the Technical Roadmap requested and its implementation. Last but not least it is also a source for further cross-collaboration (also cross-fertilization) with other 5G-PPP Projects interested through 5G-PPP Security WG about to be launched.

References

[1] 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.

[2] "The Guardian," [Online]. Available: http://www.theguardian.com/us-news/2015/feb/19/nsa-gchq-sim-card-billions-cellphones-hacking.

[3] "Gemalto," [Online]. Available: http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx.

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

[5] N. Foo Kune, J. Koelndorfer and Y. Kim, "Location Leaks on the GSM Air Interface," 8 August 2013. [Online]. Available: http://www-users.cs.umn.edu/~foo/research/docs/fookune_ndss_gsm.pdf.

[6] F. Van den Broek, R. Verdult and J. de Ruiter, "Defeating IMSI Catchers," in *ACM CCS 2015*, 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 and Sahai, "Attribute-based encryption for fine-grained access control of encrypted data," in *ACM CCS'06*, 2006.

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

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

[11] Huffington Post, [Online]. Available: http://www.huffingtonpost.com/2013/10/24/nsa-world-leaders_n_4158922.html.

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

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

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

[15] J. Wright, "Characterising Anonymity Systems," in *York University*, 2009.

[16] “Privacy Level Agreements,” [Online]. Available: https://cloudsecurityalliance.org/group/privacy-level-agreement/.

[17] B. Aboba, J. Carlson and S. Cheshire, “Detecting Network Attachment in IPv4 (DNAv4),” in *RFC4436, IETF*, 2006.

[18] “COWL,” [Online]. Available: http://w3c.github.io/webappsec-cowl/.

[19] 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.

[20] 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.

[21] 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.

[22] Open Networking Foundation, “OpenFlow switch specification - version 1.3.0 (wire protocol 0x04),” 2012.

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

[24] “Open vSwitch - a production quality, multilayer virtual switch,” [Online]. Available: http://openvswitch.org/.

[25] R. Bifulco, H. Cui, G. O. Karame and F. Klaedtke, “Fingerprinting software defined networks,” in *Proceedings of the 23rd International Conference on Network Protocols (ICNP)*, 2015.

[26] H. Cui, G. O. Karame, F. Klaedtke and R. Bifulco, “Fingerprinting of software-defined networks,” 2015. [Online]. Available: http://arxiv.org/abs/1512.06585.

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

[28] Hewlett Packard, “SDN App Store,” [Online]. Available: https://saas.hpe.com/marketplace/sdn.

[29] “SDN Market Sizing,” 2013. [Online]. Available: https://www.sdxcentral.com/wp-content/uploads/2015/02/sdn-market-sizing-report-0413-4.pdf.

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

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

[32] “ONOS - a new carrier-grade SDN network operating system designed for high availability,

performance, scale-out," [Online]. Available: http://onosproject.org/.

[33] "The OpenDaylight Platform," [Online]. Available: https://www.opendaylight.org/.

[34] J. Anderson, "Computer security technology planning study," 1973.

[35] F. B. Schneider, "Enforceable security policies," *ACM Transactions on Information and System Security,* vol. 3, no. 1, 2000.

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

[37] "Mininet: an instant virtual network on your laptop," [Online]. Available: http://mininet.org/.

[38] Ericsson, "Network functions virtualization and software management," 2014. [Online]. Available: http://www.ericsson.com/res/docs/whitepapers/network-functions-virtualization-and-software-management.pdf.

[39] "OpenVirteX Network Virtualization Platform," [Online]. Available: http://ovx.onlab.us/.