Deliverable D4.4

Evaluation of the security enablers: Results of the testbed runs

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	16/11/2017	
Dissemination Level:	Public	
Lead beneficiary	PARTNER	Jose Sanchez jose2.sanchez@orange.com Jean-Philippe Wary jeanphilippe.wary@orange.com
Authors	Orange: José Sanchez, Jean-Philippe Wary	

Executive summary

5G-ENSURE aims at providing security proven enablers. In order to achieve this goal, a 5G Security testbed has been designed within the scope of the project to host the enablers issued from the project. The enabler's security claims have been tested against the security threats previously identified within the project. This will prove efficiency of the features developed.

This document version provides with the results of analysis of the test plan execution of those enablers over the 5G Security testbed.

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.

This document provides with the execution results of the evaluated enablers over the 5G Testbed.

Disclaimer

Copyright notice

Contents

Abbreviations

5G-PPP	5G Infrastructure Public Private Partnership
AAA	Authentication Authorisation Accounting
Dx.y	Deliverable x.y
E.O	Enabler Owner
ETSI	European Telecommunications Standards Institute
ID	Identifier
NDA	Non Disclosure Agreement
NFV	Network Function Virtualisation
SDN	Software-Defined Networking
UC	Use Case
VNF	Virtualised Network Function
VPN	Virtual Private Network
TFE	Testbed Feasilibty Evaluation, WP4 evaluation as defined in D4.3
TCE	Theoretical Coverage Evaluation, WP2 evaluation as defined in D4.3
TestBed	The **5G-Ensure testbed**, composed of 3 nodes operated by B.Com, VTT and Nokia.

1 5G Security TestBed achievements

One of the 5G-ENSURE project targets is to be able to evaluate in a real or a simulated environment the proposed enablers delivered by work package WP3. It means that the role of WP4 is to provide a suitable testing environment for partners, providing with the hardware and software resources, including tools for the proper Quality Assurance, reusability of already integrated resources over the TestBed, as well as an easy showcase and collection of evidences for the evaluation of the enablers.

In the testbed architecture design shown in the deliverable D4.1, we identified the need to establish and define specific NDA and Charter to improve the content of the existing 5G-ENSURE Project Consortium Agreement. Those two additional documents have been defined and delivered inside the document D4.2 "Test plan". They cover the following need to describe and establish rules for:

- the interconnection between remote systems / platforms and the testbed,
- the delivery and allocation of resources (HW and SW) between partners and users, and relative access right management,
- the usage of the testbed and partners respective Intellectual Property Rights protection,
- Data and Confidential Information management, Privacy and result's ownership,
- Prevention of abnormal behaviours and process to handle potential conflict.

During the project, we have designed a TestBed tailored to the project requirements on which to integrate all the different enablers. Those requirements collected have driven the design and the further improvement of the proposed testbed architecture. Moreover, this design has been made in parallel with the delivery of the R1 and R2 enablers as well as the evaluation procedures.

One of major TestBed's constraints is the diverse nature of enablers and features to be integrated, tested and evaluated over the TestBed. Since the beginning of 5G Ensure project, we have decided that the role of the WP4 is to deliver a TestBed with industrial processes and proper tooling to make it possible. Note that this is not common in Research activities at TRL3 or TRL4.

This industrialization allows to:

- Replicate, trace, replay, chain or connect together whatever components, enablers or specific features integrated inside the TestBed.
- Monitor different activities of partners and deliver maintenance and user supports.
- Deliver workflow materializing the responsibilities between parties; meaning WP2 for theoretical claims qualification and WP4 for Technical TestBed operations.
- Interconnect nodes and partners and demonstrate the flexibility and efficiency of the TestBed as natural candidate for Phase 2 and 3 of 5G PPP.

At WP4 level there is a core team composed with 4 partners involved in the following duties:

- Orange as a leader of the Testbed activities (WP4), providing its view on Telco operations and security expertise,
- B<>com as the main contributor and providing a Core Testbed node, as well as all the necessary tooling towards a DevOps environment,
- VTT as key player in testbed activities, providing and operating an external Testbed node
- Nokia, providing and operating an external Testbed node with the strategic vision of a Telco manufacturer

The main driver of the TestBed has been to separate scientific expertise that Partners could share in different work packages from the technical need and operation of a real testbed (WP4). This approach has driven all actions during the project and we have clearly dedicated to work packages WP3 and WP2 the security expertise around 5G enablers, risks and 5G security architecture.

The TestBed team is focusing on **operations**, but was able to integrate it with the technical expertise deliveries of other work packages (WP2 and WP3) as well as to chain those individual deliveries in the shape of enablers together in order to build more added value systems.

The TestBed aimed to integrate WP3 deliveries and operate the already defined Tests (WP2 and WP3). Therefore, the responsibility of Test description and coverage was outside the TestBed team responsibility.

The Testbed capacity has been demonstrated with several enablers already integrated in the TestBed which have been instantiated during the last EuCNC 2017 (see Annex7.2). In this demonstration, several enablers were connected or chained, operated together and deployed over several Nodes. And end-to-end delivery of service between headquarters of B.com (Rennes, France) and VTT (Oulu, Finland) was successfully shown at this event. It was also shown the fact that, thanks to the 5G testbed, several external nodes such as the node from VTT in Finland can be connected and a video service can be flexibly launched on top of a microsegment by means of the micro-segmentation enabler provided by VTT.

The initial target of 5G-Ensure TestBed was to deliver a fully operational TestBed for the 5G-PPP Phase 2. That is why WP4 focused on industrializing all processes, workflows, tooling and interconnection procedures.

The choice of diverse tools has imposed a significant effort to partners for the first release R1 due to the fact that it was a new process with new tools and workflow to be implemented, which implied to be understood by every partner in the consortium. Nevertheless, this process was adopted by the partners and it was followed also in Release R2 with the inherent enhancement in the evaluation and integration processes (see chapter 2 to analyse the improvement between releases R1 and R2). The automatization and definition of TestBed workflows was one of the major achievements and it has been deemed to be one of the most important results of the Testbed, which could be assimilated today as a pre-industrial TestBed for the future phases of 5G-PPP.

The 5G-Ensure TestBed aims to go beyond usual testbeds, that usually try to simulate an environment adhoc in order to test some project results or proof of concepts (in simulated or pseudo real environment). The aim of the 5G-Ensure TestBed is to demonstrate an almost industrial capacity to deliver or chain or connect on demand secure enablers/features coexisting with real traffic. One of the major topics is to demonstrate how the TestBed is dynamically able to chain, add, reroute, reconfigure or remove enablers over network infrastructures in a flexible way. Regarding the 5G Network future, this capacity will be crucial in order to track dynamic network topology evolution, react and adapt against moving threats landscape. One of the potential TestBed evolution will be to compute and deliver, in an optimized way, the right level of countermeasures per 5G slices, in order to maintain the security and availability level requested by Vertical services [35].

2 Enabler integration and evaluation process overview

One of the major activities inside WP4 was the integration of Enablers delivered by WP3 on the TestBed in order to be used standalone or to be chained (combined) with other enablers, whether those are embedded in different Nodes in a different TestBed from any partner.

This integration process consists of integrating and evaluating the WP3 enablers belonging to the two releases defined in the project, namely Release R1 and R2. This process demands strictness as a fundamental requirement to ensure the repeatability and reproducibility of the integration and evaluation of those WP3 enablers. This notion of strictness as understood inside the project can only be warranted by conceiving a concrete workflow and a minimal set of tools to be shared, to be disseminated and eventually to be utilized by the different partners of the consortium during the project duration.

The roadmaps to integrate 5G security enablers had to cope with project duration (aka 2 Years) which was somehow challenging for the Testbed team. . Even more that those enablers treat 5 different functional areas (e.g. AAA, privacy, trust, security monitoring and network management and virtualization) over 31 different use cases with very different technologies in use and security requirements. In conclusion, the integration and evaluation of the WP3 enablers has been a real challenge to be achieved, during this 2 years period.

Another major challenge was the effort made by partners to understand and clearly adopt the proposed workflow and tools of the TestBed. It has to be taken into account the different nature of the partners in the project, composed of academics, operators, vendors, among others, which inherently have different background in development and DevOps related areas.

Nevertheless, we have successfully achieved this task as witnessed by some key figures in the integration phase, for instance, the average integration time between releases R1 and R2 decreased by 30% (9 weeks to 6 weeks), even if the enablers from R2 were delivered simultaneously by the end of August 2017, which supposed an overwhelming workload just 2 months before end of the project.

Regarding the evaluation process between WP2 and WP4, a.k.a. WP2/WP4 workflow, where all the integrated enablers were evaluated based on their claimed threats on the different reference scenarios (enabler threat coverage), we clearly separated the theoretical (paper based) assessment of the enabler threats coverage (done by WP2 taskforce, named TCE process) and the Technical evaluation of the enabler threats coverage over the TestBed (done by WP4 taskforce, named TFE process). The theoretical evaluation was performed through a test description and when it was reviewed by WP2 taskforce it was technically evaluated (implementation and run) by the WP4 TestBed team.

For instance, the average duration of the technical review made by WP4 taskforce (TFE) was 4.2 weeks per enabler tested in R1 and it was reduced until 2.5 weeks for R2 enablers, almost divided by half. This result clearly indicates the improvement achieved between both releases, despite the fact that R2 evaluation was made during the last two months of the project, as shown in the evaluation roadmap (Figure 2). In addition, R2 integration phase was made in the same period as the R2 evaluation, which can be seen in the evaluation and integration roadmaps of Figure 1 and Figure 2.

As it can be noticed, the massive concentration of WP4 activities due to late WP3 enabler delivery, which fell very close to the end of project, imposed WP4 to take urgent steps. The first one consisted in prioritizing the R2 integration and evaluation w.R.t to the R1 evaluation. The idea was to evaluate the R1 enablers by following a best effort policy, but focusing the WP4 effort and manpower on Release R2 integration and evaluation at all cost.

Regarding the last months of the project, we were not able to finalize and run all evaluation of tests validated by TCE/TFE process. Some of them are categorized as blocked, which means that additional information on the scenario description are needed in order to perform the described test. In the same way, there was no time to manage those tests assessed as failed. As it will be seen later, an evaluation test is declared as failed when the result obtained does not match with the results planned in the Test description. Just to remind that test describes threat claimed to be covered under a given scenario as this description is made by each enabler Owner. The TestBed role is to execute that scenario over the Testbed once validated by the TCE/TFE workflow, in a blind way where there is neither any interpretation of the underlying strategy to cover the threat nor evaluation of the appropriateness of that strategy to cover that threat. This is assessed by the TCE process as clearly stating if the scenario is valid to cover the identified threat by that enabler.

In TestBed taskforce, the input taken from the Enabler Owner on the succession of steps to be performed over the testbed and the result to be obtained in order to assess the test as ‘passed’.

2.1 Enablers integration roadmap

This section aims at providing information on the actual and final integration roadmap for both releases R1 and R2. Those roadmaps have already been planned in D4.2 and D4.3 and we present hereafter the real integration roadmaps done over the 5G Security testbed for WP3 Enablers (releases R1 and R2).

Figure 1 shows the final integration roadmap. In this R1 roadmap we should note that two enablers have been postponed to R2 Release (see table 1 and table 2 of reference between technical ID and 5G Ensure enablers and features delivered), due to technical issues at enablers owner level.

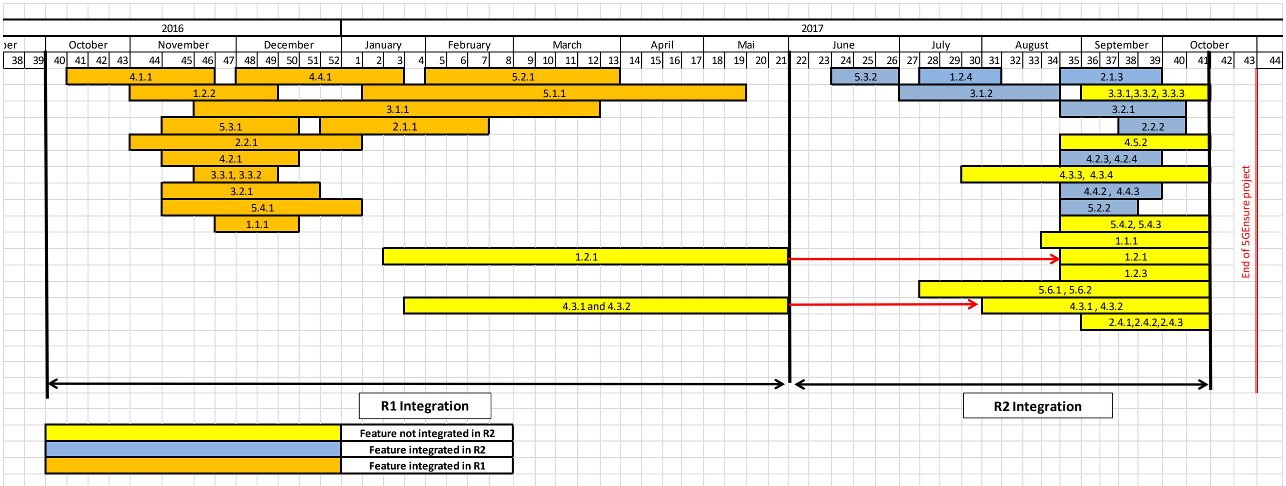


Figure 1. Final R1 & R2 enabler integration roadmap

Those enablers which have not been integrated (due to high concentration of workload on the last 2 months of the project, see section 2 above) on the 5G Security testbed are marked as yellow whilst the enablers integrated on the 5G Security testbed are colored in orange for release R1 and in blue for release R2.

Hereafter the Table 1 shows the time needed in weeks to integrate each helpdesk request in release R1. In the release R1, 15 enablers have been integrated, where each is composed of one feature. The average integration time has been around 9 weeks for R1.

Table 1. Integration time of helpdesk deployment requests for R1

Enabler	Feature	Integration time
1.1 IoT	1.1.1 Group authentication by extending the LTE-AKA protocol	4
1.2 Fine-grained Authorization	1.2.1 Basic distributed authorization Enforcement for RCDs	2
2.1 Privacy Enhanced Identity Protection	2.1.1 Encryption of Long Term Identifiers (IMSI public-key based encryption)	9
2.2 Device identifier(s) privacy	2.2.1 Enhanced privacy for network attachment protocols	11
3.1 VNF certification	3.1.1 VNF Trustworthiness Evaluation	20
3.2 Trust metric	3.2.1 Trust metric based network domain security policy management	7
3.3 Trust builder	3.3.1 5G Asset Model & 3.3.2 Graphical editor v1	4
4.1 Generic Collector Interface	4.1.1 Log and Event Processing	6
4.2 Security monitor for 5G microsegments	4.2.1 Complex Event Processing Framework for Security Monitoring and Inferencing	6
4.4 Pulsar: Proactive security analysis and remediation	4.4.1 5G specific vulnerability schema	9
5.1 Access control mechanism	5.1.1 Southbound Reference Monitor	19
5.2 Component-Interaction audits	5.2.1 Basic OpenFlow Compliance Checker	13
5.3 Bootstrapping trust	5.3.1 Integrity Attestation of virtual network components	6
5.4 Microsegmentation	5.4.1 Dynamic Arrangement of Micro-Segments	10
	average	9

Hereafter the Table 2 shows the time to integrate each helpdesk request for R2. 9 enablers have been integrated for release R2, where each is composed of one or more features as shown in the Table 2.

The average integration time has been around 6 weeks for R2, which means an improvement in efficiency of the integration workflow of 3 weeks (66%). This improvement is essentially explained by the awareness acquired during the release 1 over 5G Security testbed tooling.

Table 2. Integration time of helpdesk deployment requests for R2

Enabler	Feature	Integration time
1.2 Fine-grained authorization	1.2.4 Authorization and authentication for RCD based on ongoing IETF standardization (R2)	4
2.1 Privacy Enhanced Identity Protection	2.1.3 IMSI Pseudonymization (R2)	4
2.2 Device identifier(s) privacy	2.2.2Anonymous and optimised address selection for network attachment protocols (R2)	3
3.1 VNF Certification	3.1.2 VNF Trustworthiness Certification (R2)	4
3.2 Trust Metric Enabler	3.2.1 Improved trust metric based on extended data (R2)	10
4.2 Microsegment monitor	4.2.3 Extended data gathering (R2) 4.2.4 Cross-domain information exchange (R2)	9
4.4 PulSAR: Proactive Security Analysis and Remediation	4.4.3 5G specific vulnerability schema implementation (R2)	9
5.2 Component-Interaction Audits	5.2.2 Basic NFV Reconfiguration Compliance Checker (R2)	9
5.3 Bootstrapping Trust	5.3.2 Integrity Attestation of VNFs running in Docker containers (R2)	2
	average	6

An important point is the effective delivery date of R2 enablers, it was planned to open the integration phase the 1rst of June 2017 until 31st of August 2017. We received 12 R2 enablers over the 17 planned or 18 R2 features over the 28 R2 features planed. We decided to manage in Best Effort mode enablers integration requests received after the deadline (see Figure 6).

2.2 Enabler evaluation roadmap

This section aims at providing the actual and final roadmaps for releases R1 and R2 of the evaluation workflow defined in D4.3.

Figure 2 shows the final evaluation roadmap achieved for both releases R1 and R2. Those enablers that have not been evaluated neither in WP2 or WP4 for the release R1 have not been included in the roadmap. Nevertheless, those are listed in the Annex of the Management Tables for R1 and for R2.

Release R1:

- Microsegmentation (Dynamic Arrangement of Micro-Segments)
- GCI (Log and Event Processing)
- Microsegment monitor (Complex Event Processing Framework for Security Monitoring and Inferencing)
- Fine-grained Authorization (Fine-Grained Authorization – RCD)
- Access control mechanism (Southbound Reference Monitor)
- Trust metric enabler (Trust Metrics)
- Component-Interaction audits (Basic OpenFlow Compliance Checker)
- Internet Of Things (vGBA)

Release R2: all the enablers and features were evaluated

The reason why those Enablers (and features) could not be evaluated in the TCE/TFE process for R1 is essentially due to the fact that their features were an extension for the Release R2, which was planned to be evaluated.

The enablers evaluated at TCE process in R1 were coloured in orange. For traceability and efficiency reasons we have disconnected the TCE process from TFE process on R2 enablers in order to parallelize the processes. You will then show R2 enablers TCE in blue and R2 enablers TFE in green here after.

In terms of effort, 30 different features were evaluated for two aspects: on one hand, the theoretical aspects (TCE) and on the other hand, the technical feasibility aspects over the TestBed (TFE) during September and mid-October, as it can be seen in figure 3.

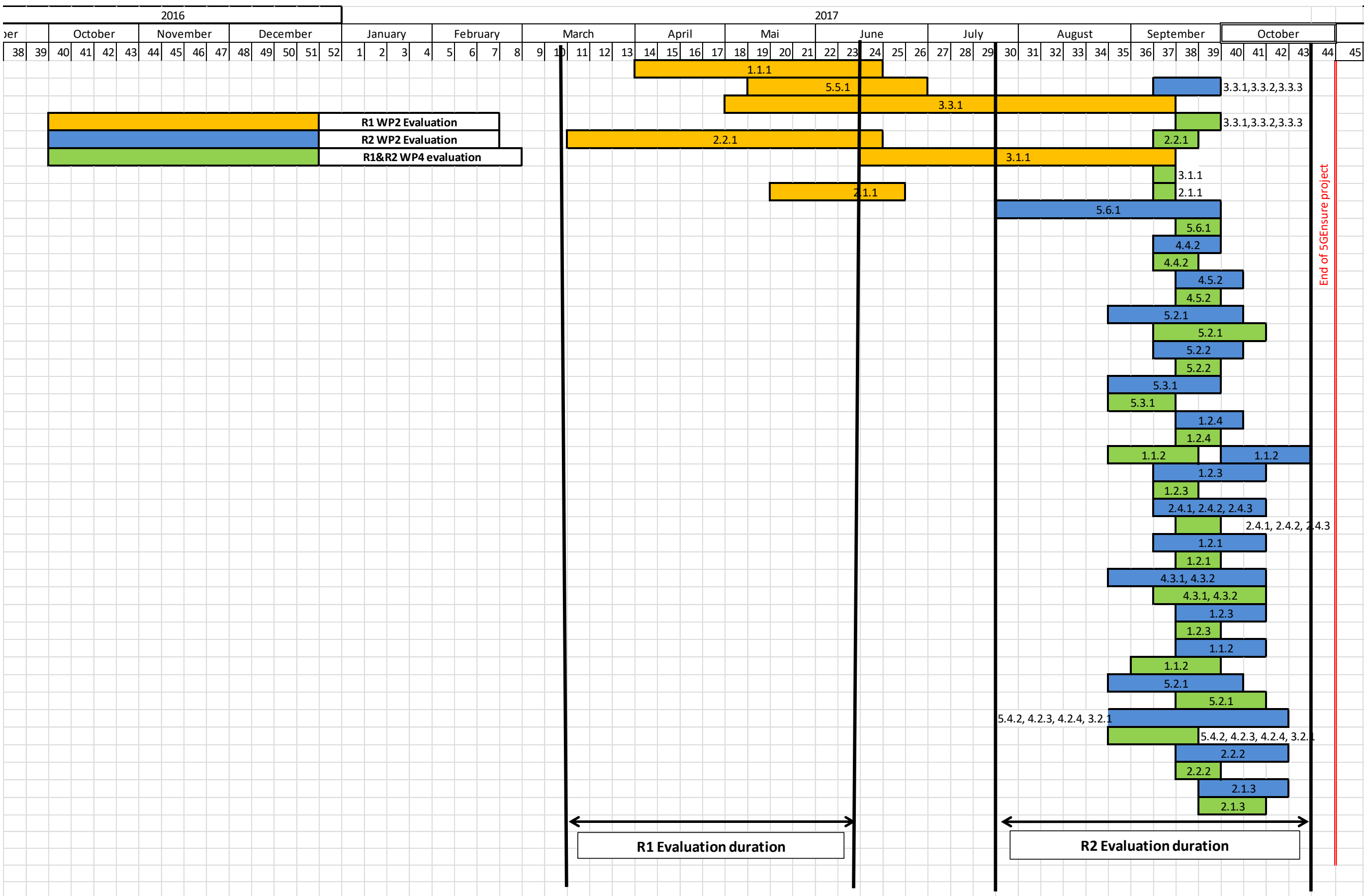


Figure 2. Final R1 & R2 enabler evaluation roadmap (finished the 24th of October)

The Figure 3 illustrates a high concentration of workload despite an identified mitigation plan to get early deliveries for enablers already available, but their number was not enough and the summer time period didn't help.

Several corrective actions were foreseen such as getting the deliveries earlier in advance for those already available enablers, but there were not enough enablers available at the beginning of the summer period and those deliveries accumulated over the beginning of September.

Nevertheless, despite the corrective actions made it was not possible to achieve a complete evaluation for all the delivered enablers in R2.

Based on the R1 figures for the TCE/TFE process, we decided during the plenary meeting held in Heidelberg in September to increase the frequency of the TCE/TFE coordination meeting to speed up the evaluation process.

In addition, TestBed taskforce had to take the necessary steps in order to accommodate the overwhelming integration workload for R2 as it was overlapping with the exiting evaluation workload from R1. In this case, TestBed taskforce had to set different priorities for the enabler deployment requests for R2. Those priorities were based on the available information on each request and its quality, the availability of the corresponding unitary test, as well as evaluation scenarios. This mitigation plan has been applied to achieve the dates shown in the roadmap.

The average evaluation time for R1 was around 12.6 weeks for TCE and around 1.8 weeks for TFE, which makes in total 14.4 weeks of evaluation in R1.

The average evaluation time for R2 decreased then to 4.2 weeks for TCE and around 2.5 weeks for TFE (due to technical workload at Testbed level during last months of project). This makes in total 6.7 weeks of evaluation in R2.

It can be seen that TCE process is improved by a 66% w.r.t to R1 whilst the TFE almost remains the same. These figures do not imply full-time weeks, as the treatment of each helpdesk ticket is based on a dialog between the testbed operator, the enabler owner (E.O.), and the evaluator, whose response delay may differ to a great extent.

In total there is a decrease from 14.4 to 6.7 weeks in the total evaluation process along the project which makes 53 % of improvement.

2.2.1 TCE/TFE procedure

The TCE/TFE workflow, described throughout the document D4.3, firstly relies on TCE phase, where the WP2 taskforce assigns the different test scenarios described by each E.O. in the testlink tool to a given partner. Two conditions were met in this assignment in order to guarantee a blind review:

- no partner can review its own test scenarios, and
- each partner is assigned with a number of test scenarios to review according to its workload in WP2.

This procedure has been followed for both releases R1 and R2.

2.2.2 R1 and R2 high level summary

The following tables contain a high level summary on the status of each enabler as well as the corresponding features. The technical ID of the features is the same as in the document D4.3. Those enablers and features integrated and evaluated throughout the TCE/TFE process are classed as P=Performed.

num	Enabler R1	Feature	Technical ID	Integration on TestBed	WP2WP4 eval N / Y / P	WP2WP4 Score
1	IoT	Group authentication by extending the LTE-AKA protocol	1.1.1.	P	P	3
2	Fine-grained Authorization	Fine-Grained Authorization - RCD	1.2.2	P	N	-
3	PulSAR: Proactive Security Analysis and Remediation	5G specific vulnerability schema	4.4.2	P	N	-
4	Component-Interaction Audits	Basic OpenFlow Compliance Checker	5.2.1	P	N	-
5	Microsegment monitor	Complex Event Processing Framework for Security Monitoring and Inferencing	4.2.1	P	N	-
6	Micro Segmentation	Dynamic Arrangement of Micro-Segments	5.4.1	P	N	-
7	Trust Builder	5G Asset model	3.3.1	P	P	3
		Graphical editor	3.3.2	P	P	3
		5G Threat knowledgebase	3.3.3	P	P	3
8	Trust Metric	Trust metrics	3.2.1	P	N	-
9	Device identifier(s) privacy	Enhanced privacy for network attachment protocols	2.2.1	P	P	3
10	Privacy Enhanced Identity Protection	Encryption of long term identifiers	2.1.1	P	P	4
11	VNF Certification	VNF Trustworthiness Evaluation	3.1.1	P	P	2
12	Antifingerprinting	Controller-Switch-Interaction Imitator	5.5.1	P	P	1
13	Access Control Mechanisms	Southbound Reference Monitor	5.1.1	P	N	-
14	Generic Collector Interface	Log and Event Processing	4.1.1	P	N	-
	integration request done after evalaution deadline	enabler to be technically evaluated over TestBed	N : Not integrated, P : Integration Performed			

Figure 3. R1 enabler integration and evaluation high level summary

num	Enabler R2	Feature	Technical ID	Integration on TestBed	WP2WP4 eval N / Y / P	WP2WP4 Score
1	IoT	Group based AKA	1.1.2	N	P	1
2	Fine-grained Authorization	Basic Authorization in Satellite systems	1.2.1	N	N	3
		AAA integration with satellite systems	1.2.3	N	P	-
		Authorization and authentication for RCD based on ongoing IETF standardization	1.2.4	P	P	4
3	System Security State Repository	System Security State Repository service	4.5.2	N	P	3
4	PulSAR: Proactive Security Analysis and Remediation	Pulsar Interface with Generic Collector	4.4.3	N	N	-
		5G specific vulnerability schema implementation	4.4.2	P	P	3
5	Component-Interaction Audits	Basic NFV Reconfiguration Compliance Checker	5.2.2	P	P	3
		Basic OpenFlow Compliance Checker	5.2.1	P	P	3
6	Bootstrapping Trust	Integrity Attestation of VNFs running in Docker containers	5.3.2	P	P	3
7	Flow Control: in-network Threat Detection and Mitigation for Critical Functions in Virtual Networks	Detection of malicious behaviours in virtual networks	5.6.1	N	P	4
		Mitigation of detected network threats	5.6.2	N	N	-
8	Satellite Network Monitoring	Pseudo real-time monitoring	4.3.1	N	P	3
		Threat detection	4.3.2	N	P	3
9	Microsegment monitor	Extended data gathering	4.2.3	N	P	4
		Cross-domain information exchange	4.2.4	N	P	4
10	Micro Segmentation	Extended Northbound API	5.4.2	N	P	4
11	Trust Builder	5G Asset model	3.3.1	N	P	3
		Graphical editor	3.3.2	N	P	3
		5G Threat knowledgebase	3.3.3	N	P	3
12	Trust Metric	Improved trust metric based on extended data	3.2.1	P	P	4
13	Privacy policy analysis	Privacy policy specification	2.4.1	N	P	3
		Privacy preferences specification	2.4.2	N	P	3
		Comparison of policies and preferences	2.4.3	N	P	3
14	Device identifier(s) privacy	Anonymous and optimised address selection for network attachment protocols	2.2.2	P	P	3
15	Privacy Enhanced Identity Protection	IMSI Pseudonymization	2.1.3	P	P	3
16	VNF Certification	VNF Trustworthiness Certification	3.1.2	P	N	3
17	Nixu Network Sensor	Nixu Network Sensor		P		-
	integration request done after deadline (31/08/17)	enabler to be technically evaluated over TestBed	N : Not integrated, P : Integration Performed			

Figure 4. R2 enabler integration and evaluation High level summary

Despite the effort made by the 5G Ensure testbed team to integrate those enablers following a best effort policy, they could not be integrated by the end of the project.

In total, 12 features were not evaluated in the TCE/TFE process for R1 and R2, whereas 4 enablers were evaluated from a theoretical point of view in total along both releases R1 and R2. Those enablers evaluated as theoretical are the following:

- Anti-fingerprinting: 5.5.1 Controller-Switch-Interaction Imitator (R1)
- VNF certification: 3.1.1 VNF Trustworthiness Evaluation (R1)
- Internet Of Things: 1.1.2 Group-based AKA (R2)
- Fine-grained Authorization: 1.2.4 Authorization and authentication for RCD based on ongoing IETF standardization (R2)

In R1, 9 out of 14 evaluation scenarios were reviewed by TCE (64.3%), whilst 8 out of 9 evaluation scenarios were reviewed by TFE (88.9%).

In R2, 16 out of 16 evaluation scenarios were reviewed by TCE and TFE, which makes 100% of evaluation rate. The overall addition makes 49 evaluation scenarios evaluated along the project, corresponding to 22 enablers (6 enablers for R1 and 16 enablers for R2) and corresponding to 26 features (6 features for R1 and to 20 features for R2).

Only those integrated and evaluated enablers in TCE/TFE process could go under technical evaluation and execution on the 5G Security testbed, which are to be presented in the section below.

2.3 Enablers Evaluation Results

The TestPlan after the integration phase and the WP2-WP4 evaluation phase has been provided as annex of D4.3. We present in this section the results on the execution of the aforementioned TestPlan.

TestBed taskforce has adopted the following grading to score the execution of each enabler:

- Blocked: the enabler cannot be run on the 5G Security testbed. This is mainly due to the fact that is not integrated or its evaluation scenario is not compatible with the 5G Security testbed itself.
- Failed: the enabler has not passed the test suite, due to incoherence on its result or unexpected results.
- Passed: the enabler has successfully passed the test suite. All the theoretical scenarios which do not need to be executed on the 5G Security testbed are considered in this state on the condition that have followed the evaluation workflow mentioned in D4.3 for the TCE/TFE process.

The results of the execution of the TestPlan for R1 shows that 6 out of 22 were run and passed their corresponding test suites on the 5G Security testbed, which makes 21 % in total. The reason for not running these 22 enablers is due to the fact that did not complete the TCE/TFE process and prefer to focus their effort on R2 releases deliveries..

In the meantime that WP2-WP4 process came late and was difficult to acquire and to master by all parties (would it be WP2 stakeholders and/or EOs themselves) which caused discussion on it and also triggering of a Webinar on it (triggered by TM) to address and solve the issues. What was key here was to fine-tuned the process and get it acquired/master for R2 (being most of R1 enablers where continued in R2 – as such evaluation not performed in R1 would be performed in R2))

The results of the execution of the TestPlan for R2 are the following : 27 out of 28 enablers/features (96.4%) were run, 4 enablers did not passed their corresponding test suites 'Failed' (ie 14% of tests executions), whilst 11 enablers did pass their corresponding test suites, a total of 41%.

In the following table 3, the execution tests are grouped per use case. Those use cases were mentioned in the document D2.1 and the enablers covering threats in each use case for R1 and R2 were mentioned in the document D4.3. We can see that the score evaluation for TCE/TFE process is also shown for each scenario. This

Table 3 shows the results of the execution of the testplan over the Testbed. Those results were collected from TestLink the 31/10/2017.

Table 3. R2 enabler integration evaluation per use case (run execution 31/10/2017)

			Scenario evaluation score	Execution Result	Notes
Test Suite : Use Cases cluster 1 - Identity Management					
1	T_UC1.3_1 Unauthorised activities related to satellite devices or network				
	1	Test Case 5ge-130: Unauthorised user verification	3	blocked	Scenario approved but not executed because the Enabler could not be integrated on the testbed.
	2	Test Case 5ge-136: Authorised user verification	3	blocked	Scenario approved but not executed because the Enabler could not be integrated on the testbed.
2	Test Suite : T_UC1.3_2 Fake roaming from terrestrial network into satellite network				
	3	Test Case 5ge-131: Registered user from unknown location	3	blocked	Scenario approved but not executed because the Enabler could not be integrated on the testbed.
	4	Test Case 5ge-135: Registered user from known location	3	blocked	Scenario approved but not executed because the Enabler could not be integrated on the testbed.
3	Test Suite : T_UC1.4_1 Compromised data				
	5	Test Case 5ge-87: ProVerif security analysis of the group-based AKA protocol	1	Passed	1- Theoretical evidence
	6	Test Case 5ge-146: STRIDE analysis of the ACE framework	1	Passed	1- Theoretical evidence
Test Suite : Use Cases cluster 2 - Enhanced Identity Protection and Authentication					
4	Test Suite : T_UC2.2_1 Tracking of device's (user's) location				
	7	Test Case 5ge-149: IMSI Pseudonymization test - check RTMSI pseudonyms	4	Passed	attach cell done and no more details
5	Test Suite : T_UC2.2_2 Mobile user interception and information interception				
	8	Test Case 5ge-86: ProVerif privacy analysis of the group-based AKA protocol	1	Passed	1- Theoretical evidence
	9	Test Case 5ge-151: IMSI Pseudonymization test - check RTMSI pseudonyms	4	Passed	see 5ge-149: IMSI Pseudonymization test case execution
6	Test Suite : T_UC2.1_2 Tracking of device's (user's) location				
	10	Test Case 5ge-144: Device Identity Privacy Evaluation R2	3	Passed	ok
Test Suite : Use Cases cluster 3 - IoT Device Authentication and Key Management					
7	Test Suite : T_UC3.1_1 Authentication traffic spikes				
	11	Test Case 5ge-85: ProVerif security and privacy analysis of the group-based AKA protocol	1	Passed	1- Theoretical evidence
8	Test Suite : T_UC3.1_2 Compromised authentication gateway				
	12	Test Case 5ge-147: STRIDE analysis of the ACE framework	1	Passed	1- Theoretical evidence
9	Test Suite : T_UC3.2_1 Leaking keys				
	13	Test Case 5ge-94: No key in plain-text	3	Failed	* The port 8081 is not open as there is no precondition on having Floodlight running on any of the VMs, and particularly on VM1 (see 5ge-41 integration test) * The main issue (even once restarted floodlight) is that the sgx calls fail. The integration tests do not seem to cover that sgx framework operates properly.
Test Suite : Use Cases cluster 5 - Software-Defined Networks, Virtualization and Monitor					
10	Test Suite : T_UC5.1_1 Misbehaving control plane				
	14	Test Case 5ge-99: Detection and mitigation of malicius traffic directed to critical network function	4	Blocked	Scenario approved but not executed because the Enabler could not be integrated on the testbed.
	15	Test Case 5ge-110: Removal check of misbehaving node in micro-segment	3	Passed	
	16	Test Case 5ge-120: Capture attack against VNFM	3	Passed	
	17	Test Case 5ge-138: Reactive adding of flow rules in SDN networks	3	Passed	
	18	Test Case 5ge-139: Deactiviation of SDN network applicatons	3	Failed	So far, There is no traffic generated towards port 50010. This has been double checked by performing a wireshark capture.
11	Test Suite : T_UC5.2_1 Add malicious nodes into core network				
	19	Test Case 5ge-25: Authentication to a micro-segment	3	Passed	Test performed with testbed 2 nodes micro segmentation setup
	20	Test Case 5ge-93: Malicious enclave don't get key	3	Failed	The verification manager report an error but it is not the one expected (step 3). So we can't conclude that it has attested the trustiness of the enclave
	Test Suite : T_UC5.2_2 Forwarding logic leakage				
	21	Test Case 5ge-95: TLS connection to controller	3	Failed	This tests uses the same SGX frame work as 5ge-93 and 5ge-94, and thus it is not possible to successfully execute it
12	Test Suite : T_UC5.5_1 Misuse of open control and monitoring interfaces				
	22	Test Case 5ge-128: Monitoring access control misuse in a mobile network	3	Blocked	Scenario approved but not executed because the Enabler could not be integrated on the testbed.
13	Test Suite : T_UC5.5_4 No control of Cyber-attacks by the Service providers				
	23	Test Case 5ge-108: Two types of security control for service provider	4	Passed	ok
14	Test Suite : T_UC5.6_1 Security threats in a satellite network				
	24	Test Case 5ge-133: Unauthorised user athentication	3	Blocked	Scenario approved but not executed because the Enabler could not be integrated on the testbed.
	25	Test Case 5ge-137: Authorised user authentication	3	Blocked	Scenario approved but not executed because the Enabler could not be integrated on the testbed.
Test Suite : Use Cases cluster 8 - Ultra-Reliable and Standalone Operations					
15	Test Suite : T_UC8.1_1 Service failure over satellite capable eNB				
	26	Test Case 5ge-132: Reconfigure the network topology	3	Blocked	Scenario approved but not executed because the Enabler could not be integrated on the testbed.
Test Suite : Use Cases cluster 9 - Trusted Core Network and Interconnect					
16	Test Suite : T_UC9.3_1 Hardening or patching of systems is not done				
	27	Test Case 5ge-127: T_UC9.3_1 - "Hardening or patching of systems is not done" R2	3	Blocked	Scenario approved but not executed because the Enabler could not be integrated on the testbed.
Test Suite : Use Cases cluster 10 - 5G Enhanced Security Services					
17	Test Suite : T_UC10.2_1 Nefarious activities: privacy violations				
	28	Test Case 5ge-142: Modelling T_UC10.2_1 Nefarious activities: "privacy violations"	3	Blocked	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

2.4 Aspects to be improved

Hereafter we highlight several aspects to be improved from the perspective of TestBed operation:

Tool diversity: On one hand, the choice of diverse tools (cf D4.1 and D4.2) has imposed a significant effort to partners for the first release R1 due to the fact that it was a new process with new tools and workflow to be implemented, which implied to be understood by every partner in the consortium.

On other hand, the management of the integration and evaluation process made by TestBed team consisted in collecting the information from three different tools and two different processes the integration and evaluation.

TestBed team created a series of management tables for tracking the integration and the evaluation processes by collecting the information of every ticket in a manual manner, which is prone to errors and asynchronization between workflow.

Integration process:

1) Following the evolution of the different integration tickets available at the helpdesk tool,
2) verifying that the corresponding enabler packages were correctly uploaded in the Artifact tool.

Evaluation process:

1) TCE process
   1. Evolution of the different TCE tickets available at the helpdesk tool,
   2. Description of the corresponding tests in the Testlink tool to identify the threat to be covered
   3. Assignment of the ticket and test description to partner by TCE team

2) TFE process
   1. Evolution of the different TFE tickets available at the helpdesk tool,
   2. Description of the corresponding tests in the Testlink tool to identify the threat to be covered
   3. Assignment of the ticket and test description to partner by TFE team to check the feasilibity on the testbed

The management tables are available in Annex WP4 detailed tracking activities. Those tables are structured in releases R1 and R2:

- R1 enabler integration management table

- R2 enabler integration management table
- R1 enabler evaluation management table
- R2 enabler evaluation management table

However, we need more automation on the heldpesk and testlink tools in order to reduce the errors in the collection of information that required additional meetings with partners to come to an understanding on the information missing in each ticket. The main issue is that there is no synchronization between both tools.

3 Analysis of the coverage of the 5G Ensure threats

In the following section we detail the analysis of the different threats identified along the 5G ENSURE project. As it can be seen in

Table **4**, a total of 48 threats were identified belonging to 29 different use cases, which in turn belong to 11 different clusters. Those use cases and their corresponding clusters are further detailed in the document D2.1.

At the end of the project, 11 out of 48 threats were proved to be covered in the 5G testbed, which makes 23% of the initially identified threats. This means that the enablers and features claiming to cover those threats underwent successfully the integration and evaluation processes already defined in the project.

We can also say that 13 threats were covered by integrated enablers. However, those enablers could not be evaluated nor executed on the testbed.

Table 4. Identified threats in the project

5G Ensure Threats	at least an enabler claims to mitigate the threat	at least an integrated enabler claims to mitigate the threat	at least a theorical mitigation by an enabler validation	at least a tecnhical evaluation done over the Testbed	nb of enablers.features per threat before integration	nb of integrated enablers.features per threat	nb of evaluated enablers.features per threat
	14	11	10	6			
T_UC1.1_1 : Attacker tries to freeride devices authenticated by					0	0	
T_UC1.2_1 : Leaked AAA credentials					0	0	
T_UC1.3_1 : Unauthorised activities related to satellite devices or (satellite) network resources					1	0	
T_UC1.3_2 : Fake roaming from terrestrial network into satellite network (and vice versa)					3	0	
T_UC1.4_1 : Compromised data	1	1	1	1	4	2	2
T_UC1.4_2 : User's privacy attack					0	0	
T_UC2.1_1 : Tracking of device's (user's) location					1	0	
T_UC2.1_2 : Mobile user interception and information	1	1	1	1	2	2	2
T_UC2.2_1 : Tracking of device's (user's) location	1	1	1	1	5	2	1
T_UC2.2_2 : Mobile user interception and information	1	1	1	1	9	2	2
T_UC2.3_1 : Passive communication interception					0	0	
T_UC3.1_1 : Authentication traffic spikes	1	1	1		**14**	4	1
T_UC3.1_2 : Compromised authentication gateway	1				10	2	
T_UC3.2_1 : Leaking keys					3	1	
T_UC4.1_1 : Unauthorized data access	1				1	2	
T_UC5.1_1 : Misbehaving control plane	1	1	1		13	6	3
T_UC5.2_1 Add malicious nodes into core network	1	1	1	1	13	4	1
T_UC5.2_2 : Forwarding logic leakage					3	0	
T_UC5.2_3 : Manipulation of forwarding logic					3	0	
T_UC5.3_1 : Fingerprinting attack on a virtualised network	1	1	1		2	1	1
T_UC5.4_1 : Generic Location hacking					0	0	
T_UC5.4_2 : Manipulation of data stored in repository					0	0	
T_UC5.4_3 : Compromised software signing key					0	0	
T_UC5.4_4 : Integrity of the testing machine is compromised					0	0	
T_UC5.5_1 : Misuse of open control and monitoring interfaces	1	1	1		13	3	1
T_UC5.5_2 : Unauthorized access to a network slice	1				2	1	
T_UC5.5_3 : Bogus monitoring data					4	0	
T_UC5.5_4 : No control of Cyber-attacks by the Service	1	1			13	2	1
T_UC5.6_1 : Security threats in a satellite network					7	1	
T_UC6.1_1 : Unable to attach when Overloaded					0	0	
T_UC6.2_1 : Unprotected User Plane on Radio Interface					0	0	
T_UC7.1_1 : Denial of service due to Unprotected Mobility Management Exposes Network					1	0	
T_UC8.1_1 : Service failure over satellite capable eNB					3	0	
T_UC8.2_1 : Standalone EPC loses connection to the Home					0	0	
T_UC9.1_1 : Spoofed signalling messages					0	0	
T_UC9.1_2 : Disputes in charging					0	0	
T_UC9.1_3 : Disclose of sensitive data					0	0	
T_UC9.2_1 : User privacy policies are not respected					0	0	
T_UC9.3_1 : Hardening or patching of systems is not done	1	1	1	1	8	2	2
T_UC9.3_2 : Unauthentic device installed into the system					12	0	
T_UC10.1_1 : Subverted user equipment					0	0	
T_UC10.2_1 : Nefarious activities (malicious software, unauthorized activities, interception of information): privacy					5	0	
T_UC10.3_1 : Nefarious activities (manipulation of information, interception of information): personal information disclosure					2	0	
T_UC11.1_1 : Compromised / malicious LI (Lawful Interception)					4	0	
T_UC11.2_1 : Nefarious activities (manipulation of information, interception of information) over LI-aware network					4	0	

3.1 Top ten of most claimed threats to be covered in the project

The following table shows the top ten of threats ranked based on the number of enablers treating those threats. However, not all the enablers and features treating the threats underwent the TCE/TFE process and the test execution over the testbed at this step.

We can see that the most covered threat (before the integration process and the TCE/TFE process) was the threat T_UC3.1_1 with 14 enablers claiming to cover it. The threat T_UC9.3_2 was claimed to be covered in the project but its enabler could not be integrated in the end in the 5G TestBed.

Table 5. Top ten of threats claimed to be covered in the project

5G Ensure Threats	at least an enabler claims to mitigate the threat	at least an integrated enabler claims to mitigate the threat	at least a theorical mitigation by an enabler validation	at least a tecnhical evaluation done over the Testbed	nb of enablers.features per threat before integration	nb of integrated enablers.features per threat	nb of evaluated enablers.features per threat
T_UC3.1_1 : Authentication traffic spikes	1	1	1		**14**	4	1
T_UC5.1_1 : Misbehaving control plane	1	1	1		**13**	6	3
T_UC5.2_1 : Add malicious nodes into core network	1	1	1	1	**13**	4	1
T_UC5.5_1 : Misuse of open control and monitoring interfaces	1	1	1		**13**	3	1
T_UC5.5_4 : No control of Cyber-attacks by the Service providers	1	1			**13**	2	1
T_UC9.3_2 : Unauthentic device installed into the system					**12**	0	
T_UC3.1_2 : Compromised authentication gateway	1				**10**	2	
T_UC2.2_2 : Mobile user interception and information interception	1	1	1	1	**9**	2	2
T_UC9.3_1 : Hardening or patching of systems is not done	1	1	1	1	**8**	2	2
T_UC5.6_1 : Security threats in a satellite network					**7**	1	

3.2 Top ten of threats actually covered over the 5G Testbed

The following table shows the top ten of threats ranked based on the number of enablers actually covering those threats. The difference with respect to the previous section is that the enablers and features claiming to cover these threats all underwent the TCE/TFE process and the test execution over the 5G TestBed, therefore we can confirm that these threats have been really mitigated in the 5G testbed proposed in the project.

The threats are ranked based on two phases, the integration of the corresponding enabler and the evaluation of the enabler. In some threats the evaluation was done over all the integrated enablers such is the case of T_UC1.4_1, T_UC2.1_2, T_UC2.2_2, and T_UC9.3_1, but in other cases, the evaluation was not done over all the enablers such is the case of threat T_UC5.5_1 where only three enablers were evaluated out of 6 enablers integrated covering that threat.

Table 6. Top ten of threats mitigated with the corresponding enablers after integration, evaluation and test execution in the testbed

5G Ensure Threats	at least an enabler claims to mitigate the threat	at least an integrated enabler claims to mitigate the threat	at least a theorical mitigation by an enabler validation	at least a tecnhical evaluation done over the Testbed	nb of enablers.features per threat before integration	nb of integrated enablers.features per threat	nb of evaluated enablers.features per threat
T_UC5.1_1 : Misbehaving control plane	1	1	1		13	**6**	3
T_UC3.1_1 : Authentication traffic spikes	1	1	1		14	**4**	1
T_UC5.2_1 : Add malicious nodes into core network	1	1	1	1	13	**4**	1
T_UC5.5_1 : Misuse of open control and monitoring interfaces	1	1	1		13	**3**	1
T_UC1.4_1 : Compromised data	1	1	1	1	4	**2**	2
T_UC2.1_2 : Mobile user interception and information interception	1	1	1	1	2	**2**	2
T_UC2.2_1 : Tracking of device's (user's) location	1	1	1	1	5	**2**	1
T_UC2.2_2 : Mobile user interception and information interception	1	1	1	1	9	**2**	2
T_UC5.5_4 : No control of Cyber-attacks by the Service providers	1	1			13	**2**	1
T_UC9.3_1 : Hardening or patching of systems is not done	1	1	1	1	8	**2**	2

3.3 List of non-treated threats in the project

The following table shows the list of threats identified during the 5G Ensure project for which there was no enabler covering them. This means that at the beginning of the project no enabler was conceived to cover any of those threats. Nevertheless, these threats were identified by WP2 in order to provide with a consistent and coherent threat map where all the possible threats per use case were identified, but not all of them were possible to be mitigated.

This aspect shows that there is large room for improvement for conceiving new enablers and features for these new threats.

Table 7. Threats identified but not treated in the project

T_UC1.1_1 : Attacker tries to freeride devices authenticated by factory owner
T_UC1.2_1 : Leaked AAA credentials
T_UC1.3_1 : Unauthorised activities related to satellite devices or (satellite) network resources
T_UC1.3_2 : Fake roaming from terrestrial network into satellite network (and vice versa)
T_UC1.4_1 : Compromised data
T_UC1.4_2 : User's privacy attack
T_UC2.1_1 : Tracking of device's (user's) location
T_UC2.1_2 : Mobile user interception and information interception
T_UC2.2_1 : Tracking of device's (user's) location
T_UC2.2_2 : Mobile user interception and information interception
T_UC2.3_1 : Passive communication interception
T_UC3.1_1 : Authentication traffic spikes
T_UC3.1_2 : Compromised authentication gateway
T_UC3.2_1 : Leaking keys
T_UC4.1_1 : Unauthorized data access
T_UC5.1_1 : Misbehaving control plane

4 Conclusion

In the evaluation process there is large room for improvement, for instance, we could imagine to close tests assessed as ‘failed’ on the condition that each enabler owner is reactive enough, by changing the test description accordingly and submitting again to the TCE/TFE process to validate the new proposed test and then to be executed over the 5G Security testbed. However, the execution of the TestPlan was firstly performed and achieved the Friday 27 of October where several executions were already performed by Wednesday 25 of October. Being that close to the end of the project, it was not possible for certain Enablers Owners to troubleshoot some of their issues.

As conclusion, many aspects can be improved in general. For instance to allow sufficient time for integration and evaluation in future project for different releases, taking into account that the first release is where all the different workflows and tools are presented to the consortium, whereas those are taken in by the consortium and already in use in the following releases. An important point for future projects could be to systematically allocate time and resources to challenge initial uses cases and risks analysis visions with testbed results and reality in order to reconciliate and mature 5G project outcomes(this dimension is outside natural TestBed team and task responsibility).

5 As final aspect, we performed and assess the final demonstrations (listed in the Annex : TestBed Evaluation Results

TestLink Community [configure $tlCfg->document_generator->company_name]

Test Plan Execution Report

Test Project: 5G-ENSURE
Test Plan: Enablers Security Evaluation (R2)

Printed by TestLink on 31/10/2017

Test Project: 5G-ENSURE

This project aims to provide the testbook allowing to evalutate the 5G-ENSURE enablers agains their security claims with regard to the identified security Use Cases and their associated security threats

Test Suite: Threats

5.1 Test Suite : Use Cases cluster 1 - Identity Management

5.1.1 Test Suite : T_UC1.3_1 Unauthorised activities related to satellite devices or network

Test Case 5ge-130: Unauthorised user verification	
Summary: An authorized user tries to make a rest petition on a non-authorized resource. The response of the test, should be that the user is not allowed to perform the operation because the conditions of the petition does not match with the rules applied in the policy (i.e. $FGA_SAT_PATH/test/UT01/input/TestPolicy_UT01a.xml). Conditions: - The user is registered in the LDAP server. - The user is authorized to perform this action. - The user is non-authorized to perform this action on this resource.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	depends on - 5ge-54:Installing and configure environment related to - 5ge-136:Authorised user verification
Requirements	Feature-1.2.1: Basic Authorization in Satellite systems Use Case 1.3: Satellite Identity Management for 5G Access
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

Test Case 5ge-136: Authorised user verification	
Summary: An authorized user tries to make a rest petition using an user declared inside the policy. The response of the test, should be that the user is allowed to perform the operation because the conditions of the petition does not match with the rules applied in the policy. Conditions: - The user is registered in the LDAP server. - The time when the user is trying to make the petition is in the range 08:00-18:00. - The location from where the user is trying the connection is in Spain. To simulate the above conditions, the policy file in the server can be modified, just for environment verification.	
Execution type:	Manual

Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	related to - 5ge-130:Unauthorised user verification depends on - 5ge-54:Installing and configure environment
Requirements	Feature-1.2.1: Basic Authorization in Satellite systems Use Case 1.3: Satellite Identity Management for 5G Access
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

5.1.2 Test Suite : T_UC1.3_2 Fake roaming from terrestrial network into satellite network

Test Case 5ge-131: Registered user from unknown location	
Summary: An authorised user registered in LDAP server tries to make a REST petition. This is done from an unknown or not registered location (country) in the policy. The only one authorized country is Spain, so to make the right petition should be done from an user registered and from an specified country. The response of the test, should be that the user is not allowed to perform the operation because the conditions of the petition does not match with the rules applied in the policy. Conditions: - The user is registered in the LDAP server, and it is using the same user role that the declared in the policy. - The time when the user is trying to make the petition is in the range 08:00-18:00 - The location from where the user is trying the connection is outside Spain. To simulate the above conditions, the policy file in the server can be modified, just for environment verification.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	High
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	related to - 5ge-135:Registered user from known location depends on - 5ge-54:Installing and configure environment
Requirements	Use Case 1.3: Satellite Identity Management for 5G Access Feature-1.2.3: AAA integration with satellite systems
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

Test Case 5ge-135: Registered user from known location	
Summary: An authorised user registered in LDAP server tries to make a REST petition. This is done from an registered country in the policy. The only one authorized country is Spain, so to make the right petition should be done from this specified country or modify the policy to make it match. The response of the test, should be that the user is allowed to perform the operation because the conditions of the petition does match with the rules applied in the policy. Conditions: - The user is registered in the LDAP server, and it is using the same user role that the declared in the policy. - The time when the user is trying to make the petition is in the range 08:00-18:00. - The location from where the user is trying the connection is in Spain. To simulate the above conditions, the policy file in the server can be modified, just for environment verification.	
Execution type:	Manual
Estimated exec. duration (min):	

Priority:	High
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	related to - 5ge-131:Registered user from unknown location depends on - 5ge-54:Installing and configure environment
Requirements	Use Case 1.3: Satellite Identity Management for 5G Access Feature-1.2.3: AAA integration with satellite systems
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

5.1.3 Test Suite : T_UC1.4_1 Compromised data

Test Case 5ge-87: ProVerif security analysis of the group-based AKA protocol	
Summary: Feature 1.1.1 is a group-based Authentication and Key Agreement (AKA) protocol in which group authentication parameters are stored on the device outside of the UICC. However, the symmetric long-term key K, which is stored on the UICC, is also used in the protocol. Since parameters stored outside of the UICC could easily be leaked, the fundamental security properties of the protocol must not depend on whether the group authentication parameters are compromised or not. Specifically, an adversary having access to the group authentication parameters must be unable to authenticate to the network or derive a session master key by eavesdropping on communication. If the adversary could manage to derive the session master key, the confidentiality of all the data sent between the machine-type communications (MTC) device and the network would be compromised. Also, the adversary should not be able to break authentication or confidentiality even if, additionally, members of the same group share all its authentication parameters (including the long-term secret) with the adversary. It is proven with ProVerif that the protocol meets confidentiality and mutual authentication when the adversary has access to all the authentication parameters of members in the same group in addition to all group authentication parameters of the MTC device. See the following paper for a presentation of the proof. Giustolisi, R., Gehrmann, C., Ahlström, M. and Holmberg, S., 2017. A secure group-based AKA protocol for machine-type communications. In *International Conference on Information Security and Cryptology ICISC 2016: Information Security and Cryptology–ICISC 2016. 30 November 2016 through 2 December 2016* (pp. 3-27).	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	1- Theoretical evidence
Requirements	Feature-1.1.1: Group authentication by extending the LTE-AKA protocol Use Case 1.4: MNO Identity Management Service
Attached files	• A secure group-based AKA protocol for machine-type communications : icisc_cameraready.pdf • icisc_cameraready.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	Theoretical evidence provided. No execution required

Test Case 5ge-146: STRIDE analysis of the ACE framework
Summary: For Feature 1.2.4. We have analyzed the ACE framework with Microsoft's Threat Modeling Tool to be able to evaluate the security of the ACE-framework. The attached document contains the analysis.

Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	1- Theoretical evidence
Requirements	Use Case 1.4: MNO Identity Management Service Feature-1.2.4: Authorization and authentication for RCD based on ongoing IETF standard
Attached files	• ACE_threat_report : ACE_threat_report.pdf • ACE_threat_report.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	Theoretical evidence provided. No execution required

5.2 Test Suite : Use Cases cluster 2 - Enhanced Identity Protection and Authentication

5.2.1 Test Suite : T_UC2.2_1 Tracking of device's (user's) location

Test Case 5ge-149: IMSI Pseudonymization test - check RTMSI pseudonyms	
Summary: **Description**: Verify that the feature IMSI Pseudonymization provides different pseudonyms for the same input IMSI value in different attach procedures using EAP-AKA full authentication **Strategy**: Configure the public key on the client (wpa_supplicant) and the private key on the server (hostapd). Insert a SIM card (with a known IMSI value) in the smart card reader and connect to the SSID1 WiFi network with EAP-AKA full authentication method. Check that the EAP-AKA authentication is successsful and observe the IMSI value that is transiting in Identity Response messages. Detach (stop the wpa_supplicant process) and connect again to the SSID1 WiFi network with EAP-AKA full authentication. Observe the IMSI value that is transiting in Identity Response messages. Repeat the procedure a desired number of times to test that different identities are used each time.	
Execution type:	Manual
Estimated exec. duration (min):	15.00
Priority:	Medium
Scenario evaluation score:	4 - Testbed evaluation (real flows)
Relations	related to - 5ge-125:Supplementary Test: Check the RTMSI pseudonyms with Wireshark related to - 5ge-151:IMSI Pseudonymization test - check RTMSI pseudonyms
Requirements	Use Case 2.2: Subscriber Identity Privacy Feature-2.1.3: IMSI Pseudonymization
Attached files	• IMSI_Pseudonymization_test_description.txt • IMSI_Pseudonymization_test_description.txt
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**20.00**
Execution notes	Wireshark trace is attached to step 1

5.2.2 Test Suite : T_UC2.2_2 Mobile user interception and information interception

Test Case 5ge-86: ProVerif privacy analysis of the group-based AKA protocol
Summary: Feature 1.1.1 is a group-based Authentication and Key Agreement (AKA) protocol. A machine-type communications (MTC) device using the protocol identifies itself by the combination of a group identifier, called GID, and a value that identifies the device within the group, called PATH. Since the long-term key K (stored in the UICC) is needed for a device to authenticate using the protocol, the device identifier (GID, PATH) is associated with an International Mobile Subscriber Identity (IMSI). However, in order to achieve MTC identity privacy, it is important that an adversary cannot identify the IMSI by observing a run of the group-based AKA protocol, even though the group-based AKA device

identifier is sent in the clear. The following paper presents a ProVerif verification proving that the protocol meets this MTC identity privacy property. Giustolisi, R., Gehrmann, C., Ahlström, M. and Holmberg, S., 2017. A secure group-based AKA protocol for machine-type communications. In *International Conference on Information Security and Cryptology ICISC 2016: Information Security and Cryptology–ICISC 2016. 30 November 2016 through 2 December 2016* (pp. 3-27).	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	1- Theoretical evidence
Requirements	Feature-1.1.1: Group authentication by extending the LTE-AKA protocol Use Case 2.2: Subscriber Identity Privacy
Attached files	• A secure group-based AKA protocol for machine-type communications : icisc_cameraready.pdf • icisc_cameraready.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	Theoretical evidence provided. No execution required

Test Case 5ge-151: IMSI Pseudonymization test - check RTMSI pseudonyms	
Summary: The same test as 5ge-149 also proves the coverage of this threat.	
Execution type:	Manual
Estimated exec. duration (min):	0.00
Priority:	Medium
Scenario evaluation score:	4 - Testbed evaluation (real flows)
Relations	related to - 5ge-149:IMSI Pseudonymization test - check RTMSI pseudonyms
Requirements	Use Case 2.2: Subscriber Identity Privacy Feature-2.1.3: IMSI Pseudonymization
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant

Execution Result:	Passed
Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	See 5ge-149 test case execution

5.2.3 Test Suite : T_UC2.1_2 Tracking of device's (user's) location

Test Case 5ge-144: Device Identity Privacy Evaluation R2	
Summary: This evaluation test should demonstrate that the DIP enabler R2 DNA privacy enhancement features for both retest for R1 features (Dummy address injection and Random ordering) and R2 features (Dummy address injection automatic mode and Geolocation prefiltering) provide for improvement of path location privacy.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 2.1: Device Identity Privacy Feature-2.2.1: Enhanced privacy for network attachment protocols Feature-2.2.2: Anonymous and optimised address selection for network attachment protocols
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	Passed
Execution Mode:	**Manual**
Execution duration (min):	**20.00**

5.3 Test Suite : Use Cases cluster 3 - IoT Device Authentication and Key Management

5.3.1 Test Suite : T_UC3.1_1 Authentication traffic spikes

Test Case 5ge-85: ProVerif security and privacy analysis of the group-based AKA protocol	
Summary: An authentication scheme for IoT devices that aims to mitigate the authentication traffic spikes threat must still provide adequate security and privacy, otherwise the effect could be that an adversary can break authentication, derive a session master key or compromise the privacy. In the paper referenced below a ProVerif analysis of the group-based AKA protocol (feature 1.1.1) is presented. It is proven that the protocol meets mutual authentication, key confidentiality and device identity privacy. Giustolisi, R., Gehrmann, C., Ahlström, M. and Holmberg, S., 2017. A secure group-based AKA protocol for machine-type communications. In *International Conference on Information Security and Cryptology ICISC 2016: Information Security and Cryptology–ICISC 2016. 30 November 2016 through 2 December 2016* (pp. 3-27).	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	1- Theoretical evidence
Requirements	Feature-1.1.1: Group authentication by extending the LTE-AKA protocol Use Case 3.1: Authentication of IoT Devices in 5G
Attached files	• A secure group-based AKA protocol for machine-type communications : icisc_cameraready.pdf • icisc_cameraready.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	Theoretical evidence provided. No execution required

5.3.2 Test Suite : T_UC3.1_2 Compromised authentication gateway

Test Case 5ge-147: STRIDE analysis of the ACE framework
Summary: For Feature 1.2.4. We have analyzed the ACE framework with Microsoft's Threat Modeling Tool to be able to evaluate the security of the ACE-framework. The attached document contains the analysis.

Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	1- Theoretical evidence
Requirements	Use Case 3.1: Authentication of IoT Devices in 5G Feature-1.2.4: Authorization and authentication for RCD based on ongoing IETF standard
Attached files	• WP2 Evaluation score : 5ge-147-WP2Evaluationscore.txt • 5ge-147-WP2Evaluationscore.txt • ACE_threat_report : ACE_threat_report.pdf • ACE_threat_report.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	Theoretical evidence provided. No execution required

5.3.3 Test Suite : T_UC3.2_1 Leaking keys

Test Case 5ge-94: No key in plain-text	
Summary: The private key required for accessing the controller should never be available in clear text on the system. This prevents the key from being leaked to an adversary.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 3.2: Network-Based Key Management for End-to-End Security Feature-5.3.1: Integrity Attestation of Virtual Network Components
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Failed**
Execution Mode:	**Manual**

Execution duration (min):	**30.00**
Execution notes	Two issues identified : * The port 8081 is not open as there is no precondition on having Floodlight running on any of the VMs, and particularly on VM1 (see 5ge-41 integration test) * The main issue (even once restarted floodlight) is that the sgx calls fail. The integration tests do not seem to cover that sgx framework operates properly.

5.4 Test Suite: Use Cases cluster 5 - Software-Defined Networks, Virtualization and Monitor

5.4.1 Test Suite : T_UC5.1_1 Misbehaving control plane

Test Case 5ge-99: Detection and mitigation of malicius traffic directed to critical network function	
Summary: This test aims at detecting and mitigating malicious traffic pattern targeting vital VNFs deployed in vEPC. The Flow Control enabler is deployed as a gateway for the VNF to protect, providing filtering and shaping for incoming traffic. In the test case, a DoS attack is performed against the vMME, a key node of the EPC that performs Mobility management A DDoS attack against the MME (e.g., overloading through a botnet of infected devices) would prevent the network from operating. To be successful the test should be able to identify and block the malicious traffic while not blocking the legitimate traffic.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	4 - Testbed evaluation (real flows)
Relations	related to - 5ge-98:Setup check
Requirements	Use Case 5.1: Virtualized Core Networks, and Network Slicing Feature-5.5.1: Detection of malicious behaviors Feature-5.5.2: Mitigation of detected malicious behaviors
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

Test Case 5ge-110: Removal check of misbehaving node in micro-segment	
Summary: This scenario comprises three enablers, namely, the compliance checker (CC), the micro-segmentation enabler (MSE), and the micro-segmentation monitoring enabler (MSME). CC checks—based on the information it receives from the two other enablers—that malicious nodes identified by the MSME are eventually deleted within a specified deadline by the MSE from the micro-segment. Other policies are possible, e.g., that the MSE only removes nodes from the micro-segment that the MSME has previously identified as malicious. In this scenario, the CC acts here as a control mechansim that checks that the MSE and the MSME interact with each other as intended. Note that this scenario was part of the EuCNC demo by VTT and others showing the use of micro-segments. See the EuCNC video. The theoretical underpinnings, the algorithms used by the CC are described in the following conference paper together with an experimental evaluation of the tool's performance. D. Basin, F. Klaedtke, and E. Zalinescu. Runtime Verification of Temporal Properties over Out-of-Order Data Streams. In Proceedings of the 29th International Conference on Computer Aided Verification (CAV). Lecture Nodes in Computer Science, volume 10426, Springer 2017.	
Execution type:	Manual

Estimated exec. duration (min):	30.00
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 5.1: Virtualized Core Networks, and Network Slicing Use Case 5.4: Verification of the Virtualized Node and the Virtualization Platform Feature-5.2.2: Basic NFV Reconfiguration Compliance Checker
Attached files	• malnodedeletion.log • malnodedeletion.log • malnodedeletion.spec • malnodedeletion.spec • malnodedeletion.msgs • malnodedeletion.msgs • malnodedeletion.comp • malnodedeletion.comp
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**20.00**
Execution notes	Attention the Keep Alives messages are logged on the console ([V]:true) in opposition what is described on the execution steps Notice that the last step (7) doesn't explicitly request an action so it was ignored in the execution.

Test Case 5ge-120: Capture attack against VNFM	
Summary: This test aims at checking that an attack leveraging a compromised control plane (VNF Manager) is detected by CyberCAPTOR. It uses en example topology where a VNF is present with vulnerabilities that permits to take control of its VNF manager.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	depends on - 5ge-126:Cyber-data-extract running depends on - 5ge-37:API running depends on - 5ge-38:Attack graph generation depends on - 5ge-39:Custom attack graph generation depends on - 5ge-40:Web UI running

Requirements	Use Case 5.1: Virtualized Core Networks, and Network Slicing Use Case 5.5: Control and Monitoring of Slice by Service Provider Feature-4.1.2: 5G specific vulnerability schema implementation
Attached files	• configuration de cyber-data-extract : auto-fetcher-config-10.102.8.68.yaml • auto-fetcher-config-10.102.8.68.yaml • GCI report : gci-report2.xml • gci-report2.xml
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**40.00**
Execution notes	For the record, the right way to launch the cyber-data-extract container from the artifact repository is: sudo docker run -it -v ${PWD}/auto-fetcher-config-10.102.8.68.yaml:/root/cyber-data-extract/auto-fetcher-config.yaml fivegensure-docker-virtual.artifact.b-com.com/cyber-data-extract:1.8.1 Another think is that the final step does not clearly state whether there is an action to be performed to check the threat mitigation.

Test Case 5ge-138: Reactive adding of flow rules in SDN networks	
Summary: In this scenario, the compliance checker is used to check a simple policy about the interactions between the SDN controller and SDN switches. Namely, whenever a switch receives a network packet with no matching flow rule, the controller must reconfigure the switch accordingly, within a time bound. In other words, the compliance checker checks that the controller timely reacts to packet-in OpenFlow messages by corresponding flow-mod OpenFlow messages. For the moment, we restrict ourselves to this simple policy. Other, more complex, policies about the interactions via OpenFlow messages between the control plane and the data plane can be checked accordingly. An example is that barrier requests are handled appropriately. However, the setup will be more involved and we want to keep things simple here. In the following, we describe how to configure, setup, and run the different involved components, namely, runverif, OVS, ONOS, and Mininet.	
Execution type:	Manual
Estimated exec. duration (min):	45.00
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Feature-5.2.1: Basic OpenFlow Compliance Checker Use Case 5.3: Reactive Traffic Routing in a Virtualized Core Network Use Case 5.4: Verification of the Virtualized Node and the Virtualization Platform

Attached files	• flowmod-prop.spec • flowmod-prop.spec • README-flowmod • README-flowmod • flowmod-prop.msgs • flowmod-prop.msgs • flowmod-prop.comp • flowmod-prop.comp • flowmod.spec • flowmod.spec • flowmod.msgs • flowmod.msgs • flowmod.comp • flowmod.comp
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**60.00**
Execution notes	The runverif connection log from OVS is wrong. In fact, it always returns "connection established" but in fact it is not a really tested. My guess is that communication is not bi-directional between OVS <> runverif so it is not really possible to get a correct status.

Test Case 5ge-139: Deactiviation of SDN network applicatons	
Summary: In this scenario, the compliance checker checks whether deactivating a network service is allowed. We restrict ourselves here to deactivating network applications of the controller ONOS. Concretely, we consider the policy that it is only allowed to deactivate the driver app when the OpenFlow app is not active. In a broader setting, the network services could be NFVs that for example run in Docker containers. More complex dependencies between services can also be expressed. Furthermore, we could also check that certain network services, when deactivated, must be reactivated within a specified time window. Another example is that certain network services should not be activated at the same time, e.g., because of conflicting use of network resources.	
Execution type:	Manual
Estimated exec. duration (min):	45.00
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 5.4: Verification of the Virtualized Node and the Virtualization Platform Feature-5.2.2: Basic NFV Reconfiguration Compliance Checker
Attached files	• README-deactivatingapps • README-deactivatingapps

	• deactivatingapps.spec • deactivatingapps.spec • deactivatingapps.proxy • deactivatingapps.proxy • deactivatingapps.msgs • deactivatingapps.msgs • deactivatingapps.comp • deactivatingapps.comp
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Failed**
Execution Mode:	**Manual**
Execution duration (min):	**60.00**
Execution notes	So far, There is no traffic generated towards port 50010. This has been double checked by performing a wireshark capture.

5.4.2 Test Suite : T_UC5.2_1 Add malicious nodes into core network

Test Case 5ge-25: Authentication to a micro-segment	
Summary: The objective of this test is to check how the micro-segmentation enabler is able to respond to the threat T_UC5.2_1 Add malicious nodes into core network. In this threat malicious nodes may e.g. eavesdrop, tamper, and prevent data flows. The enabler applies security verification procedures, namely IEEE 802.1X based authentication for assuring that the added nodes are trustworthy. This test presumes that the single node version of the enabler has been installed.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 5.2: Adding a 5G Node to a Virtualized Core Network Feature-5.4.1: Dynamic Arrangement of Micro-Segments
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**30.00**
Execution notes	Test performed with testbed 2 nodes microsegmentation setup.

Test Case 5ge-93: Malicious enclave don't get key	
Summary: A malicious or compromised enclave should not be added to the network. This means that if the actual measurement of the application is not in the list of expected hashes, the application should not be provisioned with a key and the network can thus not connect to the SDN controller.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 5.2: Adding a 5G Node to a Virtualized Core Network Feature-5.3.1: Integrity Attestation of Virtual Network Components
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Failed**
Execution Mode:	**Manual**
Execution duration (min):	**30.00**
Execution notes	The verification manager report an error but it is not the one expected (step 3). So we can't conclude that it has attested the trustiness of the enclave

5.4.3 Test Suite : T_UC5.2_2 Forwarding logic leakage

Test Case 5ge-95: TLS connection to controller	
Summary: Ensures that a TLS connection is setup between the Application and the Controller, after a successful provisioning of the Application. This makes the communication between the application and the controller both integrity and confidentiality protected.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 5.2: Adding a 5G Node to a Virtualized Core Network Feature-5.3.1: Integrity Attestation of Virtual Network Components
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Failed**

Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	This tests uses the same SGX frame work as 5ge-93 and 5ge-94, and thus it is not possible to successfully execute it

5.4.4 Test Suite : T_UC5.5_1 Misuse of open control and monitoring interfaces

Test Case 5ge-128: Monitoring access control misuse in a mobile network	
Summary: The System Security Threat Repository (SSSR) makes use of a knowledgebase encoding information about the assets, trust relationships, threats and controls in the 5G architecture. This knowledgebase is used to addresses the need to enrich the system view with information about the system's assets, the threats, incidents, and analysis results in order to understand the state of the whole system. The enabler allows querying and analysis for a higher-level view of security incidents and trends. See attached PDF for detailed description and screenshots. Sample mobile network model for trust builder provided as well	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 5.5: Control and Monitoring of Slice by Service Provider Feature-4.5.2: System Security State Repository service
Attached files	• T34 R2 SSSR : T34_SSSR_sml.pdf • T34_SSSR_sml.pdf • Trust Builder Mobile Network Model : Model_for_SSSR_validated.nq • Model_for_SSSR_validated.nq • T_UC5.5_1 - Misuse of open control and monitoring interfaces : T_UC5.5_1 Misuse of open control and monitoring interfaces sml.pdf • T_UC5.5_1 Misuse of open control and monitoring interfaces sml.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

5.4.5 Test Suite : T_UC5.5_4 No control of Cyber-attacks by the Service providers

Test Case 5ge-108: Two types of security control for service provider
Summary: This test scenario demonstrates how three enablers - micro-segmentation, security monitor for 5G microsegments, and trust metric enabler - provide more control over the cyber attacks for service providers that using are the 5G network.

The case demonstrates how service providers can be delivered coarse or fine-grained security and trust information from the 5G network (segment) that has been dedicated for the service provider. The case also illustrates that, when the control and monitoring APIs to 5G network are opened, service provider are able to get custom security functionality to 5G networks (to microsegments). In this test case, the service provider gets futher availability quarantees as a machine learning algorithm for anomaly detection is analysing network flows (and able to quarantine flows from suspected DoS attacks). Further, a status notifications on the real-time trust situation (based e.g. anomaly detection and availability of security services in the micro-segment) is delivered to the service provider. In this scenario, the service provider is given two types of alternative security controls: 1) Coarse-grained: Trust Metric enabler provides real time information to the service provider about the security level of the segmented network, i.e., a micro-segment. (Coarse grained information does not disclose information that is sensitive for the operator or other clients/service providers). The service provider may use this information during orchestration, when deciding whether the network offered by the operator can be trusted or not. 2) Fine-grained - Security Monitor for 5G Micro-Segments enabler provides observation/reaction algorithms to the network. (Fine-grained information is available, if the network operator wants to pass this information forward. The operator may also agree with the service provider on the customization of the monitoring algorithms.) The security control is enabled by the micro-segmentation enabler, which segments the network so that the service provider is able to retrieve information from it and control it (in cooperation with the operator without disturbing traffic flows of other services providers). (Microsegmentation removes also some legal / privacy obstacles from sharing of monitoring information as monitoring can focus to segmented flows originating to the service provider. Hhence information belonging to other customers of operator are not disclosed). The purpose of the test case is to show that A) enablers are starting and running B) one security monitoring instance is running focusing on the micro-segment (this enabler is running monitoring and control algorithms preferred by the service providers) C) Trust metric enabler shows to the service provider how secure / trusted the micro-segment is. For further information on the enablers, please see open specifications and user guides.

Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	4 - Testbed evaluation (real flows)
Requirements	Feature-3.2.1: Trust metric based network domain security policy management Feature-4.4.1: Complex Event Processing Framework for Security Monitoring and Inferencing Use Case 5.5: Control and Monitoring of Slice by Service Provider Feature-5.4.1: Dynamic Arrangement of Micro-Segments
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**30.00**

5.4.6 Test Suite : T_UC5.6_1 Security threats in a satellite network

Test Case 5ge-133: Unauthorised user athentication

Summary: In this test case, it is going to be tested all the policy rules setted in the policy file. For this an user registered but with other role, will try to access from a different country in a different time that the allowed. The response of the test, should be that the user is not allowed to perform the operation because the conditions of the petition does not match with the rules applied in the policy. Conditions: - The user is registered in the LDAP server and the role does not match with the role declared in the policy file. - The time when the user is trying to make the petition is out of the range 08:00-18:00 - The location from where the user is trying the connection is outside Spain.

To simulate the above conditions, the policy file in the server can be modified, just for a verification of the conditions.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	depends on - 5ge-54:Installing and configure environment related to - 5ge-137:Authorised user authentication
Requirements	Use Case 5.6: Integrated Satellite and Terrestrial Systems Monitor Feature-1.2.3: AAA integration with satellite systems
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

Test Case 5ge-137: Authorised user authentication

Summary:

In this test case, it is going to be tested all the policy rules setted in the policy file. For this an user registered, will try to access from a the country declared in the policy in a the time allowed.
The response of the test, should be that the user is allowed to perform the operation because the conditions of the petition does not match with the rules applied in the policy.
Conditions:
- The user is registered in the LDAP server and the role does match with the role declared in the policy file.
- The time when the user is trying to make the petition is in the range 08:00-18:00
- The location from where the user is trying the connection is in Spain.

To simulate the above conditions, the policy file in the server can be modified, just for a verification of the conditions.

Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	depends on - 5ge-54:Installing and configure environment related to - 5ge-133:Unauthorised user athentication
Requirements	Use Case 5.6: Integrated Satellite and Terrestrial Systems Monitor Feature-1.2.3: AAA integration with satellite systems
Execution Details	
Build	Enablers Security Evaluation (R2)

Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

5.5 Test Suite : Use Cases cluster 8 - Ultra-Reliable and Standalone Operations

5.5.1 Test Suite : T_UC8.1_1 Service failure over satellite capable eNB

Test Case 5ge-132: Reconfigure the network topology

Summary:

Checks that the user can configure the security/performance indicators to be collected.
Checks that the updated topology may be forwarded.

The initial topology is configured in step #8 and can be checked in steps #9, #10 and #11.
http://10.102.0.51/lib/attachments/attachmentdownload.php?id=111

The indicators to be collected are configured in step #12. Node 5g-enodeb3 is configured with $MON_SAT_PATH/test/UT01/input/indicators_UT01.5g-enodeb3.json:

- ifOperStatus from terrestrial terminal 1.
- ifOperStatus from terrestrial terminal 2.
- ifOperStatus from satellite terminal 1.

Each node sents the operational state of the interface (ifOperStatus) to the satellite-network-monitoring-server every 10 seconds (snmp_retry_timeout_msg property in $MON_SAT_PATH/client/SatelliteNetworkMonitoringClient.properties). If the operational state of the interface is set to down ("error_value": 2) the node sends an alarm message.

Link failure is emulated in step #13.

The incident/failure is detected in step #14. The satellite-network-monitoring-server is continuosly collecting messages from the message broker (i.e. ActiveMQ). When the SatelliteNetworkMonitoringServer detecs an alarm message (messageType field in the header set to "alarm") it launches the Topology Manager (see "apply" trace in $MON_SAT_PATH/logs/monitoring.log).

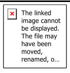
The Topology Manager calculates the best topology that fixes the issue based on two KPIs:

- Similarity (the final topology should be similar as the original one).
- TotalPowerConsumed (the lower the better).

Later, this topology is forwarded to all the nodes.

The final topology can be checked in steps #15, #16 and #17.
http://10.102.0.51/lib/attachments/attachmentdownload.php?id=112

Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Feature-4.2.1: Pseudo real-time monitoring Feature-4.2.2: Threat detection Use Case 8.1: Satellite-Capable eNB
Attached files	• output : output.png • • TopologyMatrix : TopologyMatrix.png

	• 
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

5.6 Test Suite : Use Cases cluster 9 - Trusted Core Network and Interconnect

5.6.1 Test Suite : T_UC9.3_1 Hardening or patching of systems is not done

Test Case 5ge-127: T_UC9.3_1 - "Hardening or patching of systems is not done" R2	
Summary: 5G networks allow more dynamism through virtualisation and new functions can be introduced to the network on the fly. As these environments are more virtualised, there is always a danger that someone manages to introduce a malicious function into the network. Similarly, unauthorized physical elements could be attached to the network, if their authenticity is only based on the location in the network. This test case describes the sequence of steps that correspond to Release 2 of Tust Builder. For the detailed description of individual steps please refer to the attached document "Modelling_T_UC9.3_1_TrustBuilder_Release2.pdf".	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 9.3: Authentication of New Network Elements Feature-3.3.1: 5G Asset Model Feature-3.3.2: 5G Threat knowledge base v1 Feature-3.3.3: Graphical editor
Attached files	• Modelling_T_UC9.3_1_TrustBuilder_Release2 : Modelling_T_UC9.3_1_TrustBuilder_Release2.pdf • Modelling_T_UC9.3_1_TrustBuilder_Release2.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	

Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

5.7 Test Suite : Use Cases cluster 10 - 5G Enhanced Security Services

5.7.1 Test Suite : T_UC10.2_1 Nefarious activities: privacy violations

Test Case 5ge-142: Modelling T_UC10.2_1 Nefarious activities: "privacy violations"	
Summary: 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. This issue is going to be even more pressing within 5G networks where a single service may be the result of a compositions of different layers managed by different parties with different views on privacy. For the detailed description of the test please refe to the attached document "Modelling T_UC10.2_1_PrivacyEnabler_R2.pdf".	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 10.2: Privacy Violation Mitigation Feature-2.3.1: Privacy policy specification Feature-2.3.2: Privacy preferences specification Feature-2.3.3: Comparison of policies and preferences
Attached files	• Modelling T_UC10.2_1_PrivacyEnabler_R2 : Modelling_T_UC9.3_1_TrustBuilder_Release2.pdf • Modelling_T_UC9.3_1_TrustBuilder_Release2.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

Annex : WP4 final demonstrations) in which we demonstrate how the proposed 5G Security testbed can support the combination of the major enablers delivered in the project. Note that we only integrate in the final demonstration enablers integrated and evaluated over the 5G Security testbed.

In terms of future improvement for the 5G Security testbed, we could identify:

- Integration of the B.Com Unifier Gateway for future 5G usages.
- Automatization of existing tooling in order to automatically monitor the 5G Security testbed activities related to all partners and on-going actions status. This includes automated monitoring of tickets.
- A possibility to automatically generate by email, on a periodic way, a recall of pending actions by each actor involved (TestBed Operator, Enabler Owner, etc.)

References

[1] W. Rudin, Functional Analysis, McGraw-Hill, 1973.

[2] 5G-ENSURE, “5G-ENSURE D3.2 5G-PPP security enablers open specifications (v1.0),” [Online]. Available: http://5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D3.2-5G-PPPSecurityEnablersOpenSpecifications_v1.0.pdf.

[3] 5G-ENSURE, “5G-ENSURE D3.1 5G-PPP Security Enablers Technical Roadmap early vision,” [Online]. Available: http://5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D3.1-5G-PPPSecurityEnablersTechnicalRoadmap_early_vision.pdf.

[4] 5G-ENSURE, “5G-ENSURE D2.1 Uses Cases,” [Online]. Available: http://5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.1-UseCases.pdf.

[5] 5G-ENSURE, “5G-ENSURE D2.2 Trust Model (draft),” [Online]. Available: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.2-TrustModel.pdf.

[6] 5G-ENSURE, “5G-ENSURE D2.3 Risk assessment, mitigation and requirements (draft),” [Online]. Available: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.3-RiskAssessmentMitigationRequirements.pdf.

[7] 5G-ENSURE, “5G-ENSURE D4.1 5G Security testbed architecture,” [Online]. Available: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D4.1-5G_Security_testbed_architecture_v1.0.pdf.

[8] “Testlink user manual,” [Online]. Available: https://wiki.openoffice.org/w/images/1/1b/Testlink_user_manual.pdf.

[9] “Artifactory home page,” [Online]. Available: https://www.jfrog.com/confluence/display/RTF/Welcome+to+Artifactory.

[10] “Artifactory as a Debian repository,” [Online]. Available: https://www.jfrog.com/video/setting-up-artifactory-4-as-a-debian-repository-in-minutes/.

[11] “Artifactory as a YUM repository,” [Online]. Available: https://www.jfrog.com/video/artifactory-yum-repository/.

[12] “Artifactory as a Docker registry,” [Online]. Available: https://www.jfrog.com/video/install-artifactory-docker-registry-one-minute-less/.

[13] “Artifactury user manual,” [Online]. Available: https://www.jfrog.com/confluence/display/RTF/Welcome+to+Artifactory.

[14] “TestLink Screencast,” [Online]. Available: https://www.youtube.com/watch?v=6s48WGuX2WE.

[15] “TestLink home page,” [Online]. Available: http://testlink.org/.

[16] Ansible, “Ansible home page,” [Online]. Available: https://www.ansible.com/.

[17] 5G-ENSURE, “5G-ENSURE D3.4 5G-PPP_Security_Enablers_Documentation,” [Online]. Available: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D3.4_5G-PPP_Security_Enablers_Documentation.pdf.

[18] 5G-ENSURE, “5G-ENSURE D3.1 5G-PPP Security Enablers Technical Roadmap early vision,” [Online]. Available: http://5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D3.1-5G-PPPSecurityEnablersTechnicalRoadmap_early_vision.pdf.

[19] 5G-ENSURE, “5G-ENSURE D2.1 Uses Cases,” [Online]. Available: http://5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.1-UseCases.pdf.

[20] 5G-ENSURE, “5G-ENSURE D3.2 5G-PPP Security Enablers Open Specifications,” [Online]. Available: http://5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D3.2-5G-PPPSecurityEnablersOpenSpecifications_v1.0.pdf.

[21] “KVM4FV,” [Online]. Available: http://artifacts.opnfv.org/kvmfornfv/docs/all/all.pdf.

[22] “IPSecS2S vpn template,” [Online]. Available: https://workspace.vtt.fi/sites/5g-ensure/Shared%20Documents/Workpackages/WP4/T4.1/Testbed/Nodes_interconnection/IPsecS2S-vpn-template.docx.

[23] “Open Air Interface,” [Online]. Available: http://www.openairinterface.org/.

[24] A. Diez, “Understanding NFV Management and Orchestration,” 2015.

[25] “ETSI NFV home page,” [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/nfv.

[26] “RHEL Virtualisation KVM timing management,” [Online]. Available: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Virtualization_Deployment_and_Administration_Guide/chap-KVM_guest_timing_management.html.

[27] “Cisco Anyconnect,” [Online]. Available: http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html.

[28] “IPerf home page,” [Online]. Available: https://iperf.fr/.

[29] “OpenEPC Home Page,” [Online]. Available: http://www.openepc.com.

[30] VTT, “QoSMet home page,” [Online]. Available: http://www.vttresearch.com/qosmet.

[31] Wikipedia, “Wikipedia - Orchestration,” [Online]. Available: https://en.wikipedia.org/wiki/Orchestration_(computing).

[32] Wikipedia, “Wikipedia - Blackbox definition,” [Online]. Available: https://en.wikipedia.org/wiki/Black_box.

[33] B. Dictionary, “Businees Dictionary - White box,” [Online]. Available: http://www.businessdictionary.com/definition/white-box.html.

[34] 5GNorma, “5G Norma D3.1 Functional network architecture and security requirements,” [Online]. Available: https://5gnorma.5g-ppp.eu/wp-content/uploads/2016/01/5G_NORMA_D3.1.pdf.

[35] 5G PPP White Paper on vertical Services : https://5g-ppp.eu/white-papers/

[36] 5G-PPP, “5G-PPP 5G Architecture White Paper,” [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-5G-Architecture-WP-For-public-consultation.pdf.

[37] 5G-ENSURE, “5G-ENSURE D3.5 5G-PPP security enablers technical roadmap (update),” [Online]. Available: http://www.5gensure.eu/sites/default/files/5G-ENSURE_D3.5%205G-PPP%20security%20enablers%20technical%20roadmap%20%28Update%29.pdf.

[38] 5G-ENSURE, “5G-ENSURE D4.2 Test plan (draft),” [Online]. Available: http://www.5gensure.eu/sites/default/files/5G-ENSURE_D4.2_TestPlan_v1.0.pdf.

[39] 5G-ENSURE, “5G-ENSURE D3.6 5G-PPP security enablers open specifications (v2.0),” [Online].

[40] 5G-ENSURE, “5G-ENSURE D3.5 5G-PPP security enablers technical roadmap (Update),” [Online]. Available: http://www.5gensure.eu/sites/default/files/5G-ENSURE_D3.5%205G-PPP%20security%20enablers%20technical%20roadmap%20%28Update%29.pdf.

[41] 5G-ENSURE, “5G-ENSURE D4.3 Test plan (final): Final description of how to evaluate the selected security enablers"

6 Annex WP4 detailed tracking activities

In the following annex we provide with the management tables used along the 5GPPP-ENSURE project. Those tables have allowed us to track both the integration and evaluation procedures defined in D4.3 for both releases R1 and R2.

6.1 R1 enabler integration management table

The R1 enabler integration management table indicating used at task T4.2 level. This table covers all the enablers and features for R1 and their integration

Enabler	Feature	Deploy ment Req.	Packaging	UT description	Status	Request date	Integration date	Integration duration	Nb Msg
GCI (Orange)	Log and Event Processing	Y	100%	Y	Integrated	07/10/2016 (S27)	10/09/2016 (S32)	6	15
IoT (SICS)	Group authentication by extending the LTE-AKA protocol	Y	100%	Y	Integrated	14/11/2016 (S46)	05/12/2016 (S49)	4	28
Fine-grained Authorization	Basic Authorization in Satellite systems (TASE)	Y		N	No delivered	19/01/2017	-	-	-
	Basic distributed authorization Enforcement for RCDs (TS)	Y	100%	Y	Integrated	27/10/2016 (S43)	01/12/2016 (S44)	2	27
Satellite Network Monitoring (TASE)	Pseudo real-time monitoring & threat detection	Y		N	No delivered	27/01/2017	-	-	-
Component-Interaction audits (NEC)	Basic OpenFlow Compliance Checker	Y	100%	Y	Integrated	01/02/2017 (S53)	29/03/2017 (S65)	13	19
Device identifier(s) privacy	Enhanced privacy for network attachment protocols (OXFORD)	Y	100%	Y	Integrated	25/10/2016 (S43)	05/01/2017 (s53)	11	20
Bootstrapping trust (SICS)	Integrity Attestation of virtual network components	Y	100%	Y	Integrated	02/11/2016 (S44)	05/12/2016 (S49)	6	11
Access control mechanism (NEC)	Southbound Reference Monitor	Y	100%	Y	Integrated	10/01/2017 (S53)	09/05/2017 (S72)	**19**	**50**
Microsegmentation (VTT)	Dynamic Arrangement of Micro-Segments	Y	100%	Y	Integrated	02/11/2016 (S44)	05/01/2017 (S53)	10	23
Security monitor for 5G microsegments (VTT)	Complex Event Processing Framework for Security Monitoring and Inferencing	Y	100%	Y	Integrated	03/11/2016 (S44)	9/12/2016 (S49)	6	8
Pulsar: Proactive security analysis and remediation (TS)	5G specific vulnerability schema	Y	100%	Y	Integrated	23/11/2016 (S47)	20/01/2017 (S55)	9	9
Trust builder (IT-INNOV)	5G Asset Model & Graphical editor v1	Y	100%	Y	Integrated	09/11/2016 (S45)	01/12/2016 (S48)	4	16
Trust metric enabler (VTT)	Trust metric based network domain security policy management	Y	100%	Y	Integrated	04/11/2016 (S44)	14/12/2016 (S50)	7	10
VNF certification (TCS)	VNF Trustworthiness Evaluation	Y	100%	Y	Integrated	11/11/2016 (S45)	21/03/2017 (S64)	**20**	**36**
Privacy Enhanced Identity Protection (TIIT)	Encryption of Long Term Identifiers (IMSI public-key based encryption)	Y	100%	Y	Integrated	21/12/2016 (S51)	14/02/2017 (S59)	9	21

6.2 R2 enabler integration management table

The R2 enabler integration management table indicating used at task T4.2 level. This table covers all the enablers and features for R2 and their integration status.

Enabler	Feature	Deployment Req.	Packaging	UT description	Status	Request date	Integration date	Integ. duration	nb msg
(IoT)	Group based AKA (R1/R2)**	Y	1	5ge-102, 5ge-103, 5ge-104, 5ge-106	P	23/08/2017			
	Non-USIM based AKA (R2)								
	BYOI (Bring Your Own Identity) (R2)								
	vGBA (Vertical GBA) (R2)								
Fine-grained Authorization	Basic Authorization in Satellite systems (R1)**	Y	2	5ge-54, 5ge-55, 5ge-56, 5ge-57	P	31/08/2017			
	Basic distributed authorization Enforcement for RCDs (R1)								
	AAA integration with satellite systems (R2)**	Y	3	5ge-54, 5ge-55, 5ge-56, 5ge-57	P	31/08/2017			
	Authorization and authentication for RCD based on ongoing IETF standardization (R2)**	Y	1	5ge-100, 5ge-101	I	12/07/2017	02/08/2017	4	15
Basic AAA enabler	Forward Secrecy (R1/R2)								
	AAA aspects of trusted micro-segmentation (R1 /R2)								
	Trusted interconnect and authorization (R2)								
Federative authentication and identification enabler	Storage of authentication level (R2)								
	Usage of authentication level (R2)								
Privacy Enhanced Identity Protection	Encryption of Long Term Identifiers (IMSI public-key based encryption) (R1)								
	Home Network centric IMSI protection (R2)								
	IMSI Pseudonymization (R2)**	Y	2	5ge-122, 5ge-124, 5ge-125	I	31/08/2017	25/09/2017	4	9
Device identifier(s) privacy	Enhanced privacy for network attachment protocols (R1)								
	Anonymous and optimised address selection for network attachment protocols (R2) ?	Y	1	5ge-145	I	18/09/2017	03/10/2017	3	6
Device-based Anonymization (standalone)	Format preserving anonymization algorithm (R2)								
	Privacy configuration (R2)								
Privacy policy analysis	Privacy policy specification (R2)**	Y	1	5ge-116, 5ge-117, 5ge-118, 5ge-119	P	04/09/2017			
	Privacy preferences specification (R2)**								
	Comparison of policies and preferences (R2)**								
Trust Builder	5G Asset model (R1/R2)**	Y	1	5ge-111 5ge-112, 5ge-113	P	04/09/2017			
	Graphical editor (R1/R2)**								
	5G Threat knowledgebase (R2)**								
Trust Metric Enabler	Trust metric based network domain security policy management (R1)								
	Improved trust metric based on extended data (R2)**	Y	1	5ge-34, 5ge-35, 5ge-36	I	31/08/2017	03/10/2017	10	12
VNF Certification	VNF Trustworthiness Evaluation (R1)								
	VNF Trustworthiness Certification (R2)**	Y	2	5ge-7, 5ge-8, 5ge-9	I	06/07/2017	20/08/2017	4	22

Enabler	Feature	Deployment Req.	Packaging	UT description	Status	Request date	Integration date	Int dura
Security Indicator	Security indicator subscriber display (R2)							
Reputation based on Root Cause Analysis for SDN	Root Cause Analysis for SDN (R2)							
System Security State Repository	Deployment model ontology (also known as 5G asset model) (R1)							
	System Security State Repository service (R2)	Y	1	5ge-107, 5ge-109	P	31/08/2017		
Microsegment monitor	Complex Event Processing Framework for Security Monitoring and Inferencing (R1)							
	Risk-based adaptation of micro-segments (R2)**							
	Extended data gathering (R2)**	Y		5ge-32, 5ge-33	I	31/08/2017	29/09/2017	[illegible]
	Cross-domain information exchange (R2)**							
Satellite Network Monitoring	Pseudo real-time monitoring (R1)**	Y	2	5ge-58, 5ge-59, 5ge-60	P	31/07/2017		
	Threat detection (R1)**							
	Active security analysis (R2)							
	Pre-emptive mitigation security actions (R2)							
Generic Collector Interface	Log and Event Processing (R1)							
Malicious Traffic Generator	Traffic generator engine (R2)**							
	Malicious pattern library (R2)**							
	Fuzzing engine (R2)**							
PulSAR: Proactive Security Analysis and Remediation	5G specific vulnerability schema (R1)							
	5G specific vulnerability schema implementation (R2)	Y	1	5ge-37, 5ge-38, 5ge-39, 5ge-40, 5ge-126, 5ge-120	I	31/08/2017	29/09/2017	[illegible]
	PulSAR interface with Generic Collector (R2)							
Anti-Fingerprinting	Controller-Switch-Interaction Imitator (R1)							
Access Control Mechanisms	Southbound Reference Monitor (R1)							
	Access Requirements for VNF Container Resources (R2)							
Component-Interaction Audits	Basic OpenFlow Compliance Checker (R1)							
	Basic NFV Reconfiguration Compliance Checker (R2)**	Y	0	5ge-46, 5ge-47	I	31/08/2017	22/09/2017	[illegible]
Bootstrapping Trust	Integrity Attestation of Virtual Network Components (R1)							
	Integrity Attestation of VNFs running in Docker containers (R2)**	Y	4	5ge-41, 5ge-42	I	16/06/2017	29/06/2017	[illegible]
Micro Segmentation	Dynamic Arrangement of Micro-Segments (R1)							
	Extended Northbound API (R2)**	Y	1	5ge-21, 5ge-22, 5ge-23, 5ge-24	P	31/08/2017		
	Support for multi-domain micro-segments (R2)**							
Flow Control: in-network Threat Detection and Mitigation for Critical Functions in Virtual Networks	Detection of malicious behaviours in virtual networks (R1)**	Y	1	5ge-98	P	11/07/2017		
	Mitigation of detected network threats (R2)**							

6.3 R1 enabler evaluation management table

The R1 enabler evaluation management table indicating used at task T4.2 level. This table covers all the enablers and features for R1 and their evaluation status.

Enabler	Feature	Feature Integrated on TestBed	Threats claimed	Testlink Scenarios	WP2 review request date	Date of of WP2 approval	WP2 Approval / Close	WP4 review request date	Date of of WP4 approval	WP4 evaluation result	WP4 Approval / Close	WP2WP4 assigned score	Global status (EO / WP2 / WP4 pending action)
IoT	1.1.1 Group authentication by extending the LTE-AKA protocol	Y	T_UC1.4_1	5ge-66, 5ge-84	06/04/2017	15/06/2017	Y	06/09/2017	18/09/2017	Y	Y	5ge-66:3 5ge-84:3	Evaluated in WP2 and WP4
IoT	1.1.4 vGBA	Y	T_UC3.1_1	5ge-88	05/07/2017		Y			N	N	?	Not avaluated
Microsegmentation	5.4.1 Dynamic Arrangement of Micro-Segments	Y	T_UC5.2_1	5ge-25	02/05/2017		N	28/08/2017	18/09/2017	Y	Y	5ge-25: 3	Not Evaluated in WP2
GCI	4.1.1 Log and Event Processing	Y	T_UC5.5_1	5ge-74	02/05/2017	29/09/2017	Y		-	N	N	?	Not evaluated
Antifingerprinting	5.5.1 Controller-Switch-Interaction Imitator	Y	T_UC5.3_1	5ge-71, 5ge-72	08/05/2017	28/06/2017	Y	07/09/2017	12/09/2017	Y	Y	5ge-71:1 5ge-72:1	Evaluated in WP2 and WP4
Trust Builder	3.3.1 5G Asset model 3.3.2 Graphical editor 3.3.3 threat knowledge base	Y	T_UC9.3_1	5ge-73	03/05/2017	11/09/2017	Y	07/09/2017	13/09/2017	Y	Y	5ge-73: 3	Evaluated in WP2 and WP4
Microsegment monitor	4.2.1 Complex Event Processing Framework for Security Monitoring and Inferencing	Y	T_UC5.1_1 T_UC5.5_1 T_UC5.5_2	5ge-76 5ge-77 5ge-78	03/05/2017	07/09/2017	N		-	Y	Y	5ge-76:3 5ge-77:3 5ge-78:3	Evaluated in WP2 and WP4
Fine-grained Authorization	1.2.2 Fine-Grained Authorization - RCD	Y	T_UC4.1_1 T_UC3.1_1 T_UC3.1_2	5ge-68	19/05/2017		N	28/04/2017	18/09/2017	N	N	?	Not Evaluated
Access control mechanism	5.1.1 Southbound Reference Monitor	Y	T_UC5.1_1	5ge-81	11/05/2017		N		-	N	N	?	Not evaluated
Trust metric enabler	3.2.1 Trust Metrics	Y	T_UC3.1_1 T_UC5.5_4	5ge-82 5ge-83	09/05/2017	11/09/207	Y	07/09/2017	-	N	N	5ge-82 :3 5ge-83:3	Not evaluated
Device identifier privacy	2.2.1 Enhanced privacy for network attachment protocols	Y	T_UC2.1_2	5ge-75	15/03/2017	15/06/2017	Y	07/09/2017	12/09/2017	Y	Y	5ge-75:3	Evaluated in WP2 and WP4
VNF certification	3.1.1 VNF Trustworthiness Evaluation	Y	T_UC5.2_1	5ge-65	12/06/2017	11/09/2017	Y	11/09/2017	12/09/2017	Y	Y	5ge-65:2	Evaluated in WP2 and WP4
Privacy Enhanced Identity Protection	2.1.1 Encryption of long term identifiers	Y	T_UC2.2_1 T_UC2.2._2	5ge-2 5ge-62 5ge-63 5ge-64	18/05/2017	19/06/2017	Y	07/09/2017	07/09/2017	Y	Y	5ge-2:4 5ge-62:3 5ge-63:4 5ge-64:3	Evaluated in WP2 and WP4
Component-Interaction audits	5.2.1 Basic OpenFlow Compliance Checker	Y	T_UC5.1_1	5ge-110	31/08/2017		N			N	N	?	Not avaluated

Real workflows
theoretical

6.4 R2 enabler evaluation management table

The R2 enabler evaluation management table indicating used at task T4.2 level. This table covers all the enablers and features for R2 and their evaluation status.

Enabler	Feature	Feature Integ. on TestBed	Threats claimed	TestlinkTest Case	WP2 review request date	Date of WP2 approval	WP4 review request date	WP2WP4 assigned score	Date of WP4 approval
Fine-grained Authorization	1.2.1 Basic Authorization in Satellite systems	N	T_UC5.6_1	5ge-130	30/08/2017	12/10/2017	14/09/2017	5ge-130:3	18/09/2017
Flow Control: in-network Threat Detection and Mitigation for Critical Functions in Virtual	5.6.1 Detection of malicious behaviours in virtual networks	N	T_UC5.1_1	5ge-99	24/07/2017	26/09/2017	21/09/2017	5ge-99:4	25/09/2017
Microsegmentation	5.4.2 Extended Northbound API								
Security Monitoring	4.2.3 Extended data gathering & 4.2.4 Cross-domain information exchange	Y	T_UC5.5_4	5ge-108	31/08/2017	17/10/2017	31/08/2017	5ge-108:4	18/09/2017
Trust metrics	3.2.1 Improved trust metric based on extended data								
Satellite Network Monitoring	4.3.1 Pseudo real-time monitoring & 4.3.2 threat detection	N	T_UC5.6_1 T_UC8.1_1	5ge-132	30/08/2017	12/10/2017	14/09/2017	5ge-132:3	11/10/2017
Pulsar	4.4.2 5G specific vulnerability schema	Y	T_UC5.1_1 T_UC5.5_1	5ge-120	12/09/2017	28/09/2017	12/09/2017	5ge-120: 3	18/09/2017
Trust Builder	3.3.1 5G Asset model & 3.3.2 Graphical editor & 3.3.3 threat knowledge base	Y	T_UC9.3_1	5ge-127	14/09/2017	27/09/2017	19/09/2017	5ge-127:3	25/09/2017
Fine grained authorization	1.2.3 AAA integration with satellite systems	N	T_UC1.3_2 T_UC5.6_1	5ge-131	14/09/2017	10/10/2017	14/09/2017	5ge-131,135,133,137: 3	18/09/2017
Internet Of Things	1.1.2 Group-based AKA	Y	T_UC3.1_1 T_UC2.2._2 T_UC1.4_1	5ge-87, 5ge-86, 5ge-85	20/09/2017	12/10/2017	02/09/2017	5ge-87:1, 5ge-86:1, 5ge-85:1	25/09/2017
Device identifier(s) privacy	2.2.2 Anonymous and optimised address selection for network attachment protocols	Y	T_UC2.1_2	5ge-144	21/09/2017	17/10/2017	18/09/2017	5ge-144:3	25/09/2017
System Security State Repository	4.5.2 System Security State Repository service	N	T_UC5.5_1	5ge-128	19/09/2017	02/10/2017	19/09/2017	5ge-128:3	25/09/2017
Component-Interaction Audits	5.2.1 Basic OpenFlow Compliance Checker	Y	T_UC5.1_1	5ge-138,	31/08/2017	03/10/2017	15/09/2017	5ge-138:3	11/10/2017
	5.2.2 Basic NFV Reconfiguration Compliance Checker	Y	T_UC5.1_1	5ge-110, 5ge-139	15/09/2017	01/10/2017	20/09/2017	5ge-110:3 5ge-139:3	25/09/2017
Bootstrapping trust	5.3.1 Integrity Attestation of virtual network components	Y	T_UC5.2_1 T_UC3.2_1 T_UC5.2_2	5ge-93 5ge-94 5ge-95	31/08/2017	26/09/2017	31/08/2017	5ge-93: 3, 5ge-94:3, 5ge-95:3:	18/09/2017
Fine-grained Authorization	1.2.4 Authorization and authentication for RCD based on ongoing IETF standardization	Y	T_UC3.1_2 T_UC4.1_1 : 5	5ge-146 5ge-147	21/09/2017	02/10/2017	20/09/2017	5ge-146:1 5ge-147:1	25/09/2017
Privacy Policy Analisis	2.4.1 Privacy policy specification 2.4.2 Privacy preferences specification 2.4.3 Comparison of policies and preferences	N	T_UC10.2_1	5ge-142	15/09/2017	12/10/2017	19/09/2017	5ge-142:3	25/09/2017
Privacy Enhanced Identity Protection	IMSI Pseudonymization	Y	T_UC2.2.1 T_UC2.2_2	5ge-149, 5ge-151	25/09/2017	20/10/2017	25/09/2017	5ge-149:4, 5ge-151:4	09/10/2017

Real workflows
theoretical
Simulation
Implementation

6.5 TCE/TFE processes helpdesk evaluation requests

(a)

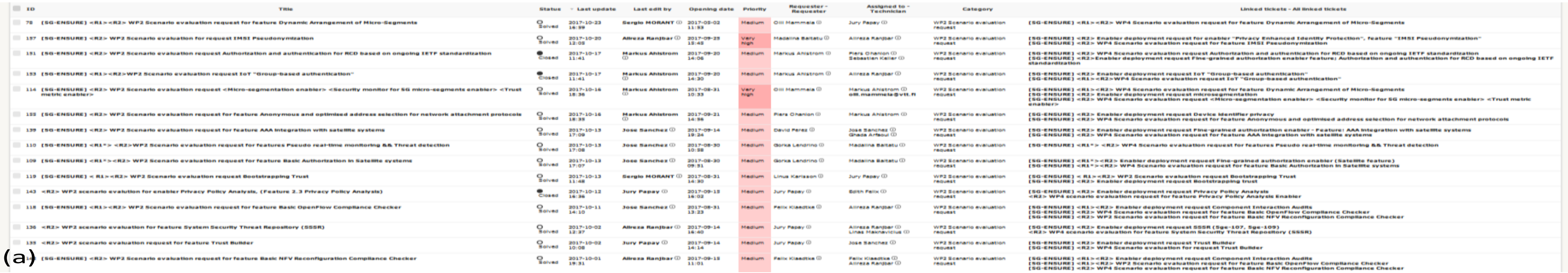
ID	Title	Status	Last update	Last edit by	Opening date	Priority	Requester - Requester	Assigned to - Technician	Category	Linked tickets - All linked tickets
89	[5G-ENSURE] <R1> WP2 Scenario evaluation request for feature Group authentication by extending the LTE-AKA protocol	Solved	2017-10-23 17:21	Sergio MORANT	2017-05-24 13:08	Medium	Simon Holmberg	Edith Felix Gorka Lendrino Linas Maknavicius Ravi Borgaonkar	WP2 Scenario evaluation request	
88	[5G-ENSURE] <R1> WP2 Scenario evaluation request Fine-Grained Authorization - RCD	Solved	2017-10-23 17:17	Sergio MORANT	2017-05-19 16:49	Medium	Cyrille Martins	Tommi Pernila	WP2 Scenario evaluation request	[5G-ENSURE] <R1> WP4 Scenario evaluation request for feature Fine-Grained Authorization - RCD
83	[5G-ENSURE] <R1> WP2 Scenario evaluation request for feature Controller-Switch-Interaction Imitator	Processing (assigned)	2017-10-23 17:11	Sergio MORANT	2017-05-08 10:21	Medium	Felix Klaedtke	Alireza Ranjbar	WP2 Scenario evaluation request	[5G-ENSURE] <R1> WP4 Scenario evaluation request for feature Controller-Switch-Interaction Imitator
78	[5G-ENSURE] <R1><R2> WP2 Scenario evaluation request for feature Dynamic Arrangement of Micro-Segments	Solved	2017-10-23 16:59	Sergio MORANT	2017-05-02 11:53	Medium	Olli Mammela	Jury Papay	WP2 Scenario evaluation request	[5G-ENSURE] <R1><R2> WP4 Scenario evaluation request for feature Dynamic Arrangement of Micro-Segments
153	[5G-ENSURE] <R1><R2>WP2 Scenario evaluation request IoT "Group-based authentication"	Closed	2017-10-17 11:41	Markus Ahlstrom	2017-09-20 14:30	Medium	Markus Ahlstrom	Alireza Ranjbar	WP2 Scenario evaluation request	[5G-ENSURE] <R2> Enabler deployment request IoT "Group-based authentication" [5G-ENSURE] <R1><R2>WP4 Scenario evaluation request IoT "Group-based authentication"
110	[5G-ENSURE] <R1*> <R2>WP2 Scenario evaluation request for features Pseudo real-time monitoring && Threat detection	Solved	2017-10-13 17:08	Jose Sanchez	2017-08-30 10:58	Medium	Gorka Lendrino	Madalina Baltatu	WP2 Scenario evaluation request	[5G-ENSURE] <R1*> <R2> WP4 Scenario evaluation request for features Pseudo real-time monitoring && Threat detection
109	[5G-ENSURE] <R1*><R2> WP2 Scenario evaluation request for feature Basic Authorization in Satellite systems	Solved	2017-10-13 17:07	Jose Sanchez	2017-08-30 09:51	Medium	Gorka Lendrino	Madalina Baltatu	WP2 Scenario evaluation request	[5G-ENSURE] <R1*><R2> Enabler deployment request Fine-grained authorization enabler (Satellite feature) [5G-ENSURE] <R1*><R2> WP4 Scenario evaluation request for feature Basic Authorization in Satellite systems
119	[5G-ENSURE] < R1><R2> WP2 Scenario evaluation request Bootstrapping Trust	Solved	2017-10-13 11:48	Sergio MORANT	2017-08-31 14:30	Medium	Linus Karlsson	Jury Papay	WP2 Scenario evaluation request	[5G-ENSURE] < R1><R2> WP2 Scenario evaluation request Bootstrapping Trust [5G-ENSURE] <R2> Enabler deployment request Bootstrapping trust
118	[5G-ENSURE] <R1><R2> WP2 Scenario evaluation request for feature Basic OpenFlow Compliance Checker	Solved	2017-10-11 14:10	Jose Sanchez	2017-08-31 13:23	Medium	Felix Klaedtke	Alireza Ranjbar	WP2 Scenario evaluation request	[5G-ENSURE] <R1><R2> Enabler deployment request Component Interaction Audits [5G-ENSURE] <R2> WP4 Scenario evaluation request for feature Basic OpenFlow Compliance Checker [5G-ENSURE] <R2> WP2 Scenario evaluation request for feature Basic NFV Reconfiguration Compliance Checker
80	[5G-ENSURE] <R1> WP2 Scenario evaluation request GCI	Solved	2017-09-28 23:00	Jury Papay	2017-05-02 16:27	Medium	Ghada Arfaoui	Linas Maknavicius	WP2 Scenario evaluation request	
94	[5G-ENSURE] <R1> WP2 Scenario evaluation request for feature VNF trustworthiness evaluation	Solved	2017-09-15 11:56	Jose Sanchez	2017-06-12 11:00	Medium	Frederic Motte	Jose Sanchez	WP2 Scenario evaluation request	[5G-ENSURE] <R1> WP4 Scenario evaluation request for feature VNF trustworthiness evaluation
75	[5G-ENSURE] <R1> WP2 Scenario evaluation for request Group authentication by extending the LTE-AKA protocol	Solved	2017-09-11 17:18	Jose Sanchez	2017-04-06 13:20	Medium	Simon Holmberg	Jani Suomalainen	WP2 Scenario evaluation request	[5G-ENSURE] <R1/R2> WP4 Scenario evaluation request Group-based AKA
85	[5G-ENSURE] <R1> WP2 Scenario evaluation request for feature Southbound Reference Monitor	Solved	2017-09-11 17:16	Jose Sanchez	2017-05-11 14:18	Medium	Alessandro Sforzin	Alireza Ranjbar	WP2 Scenario evaluation request	
84	[5G-ENSURE] <R1> WP2 Scenario evaluation request for feature Trust Metics	Solved	2017-09-11 17:09	Madalina Baltatu	2017-05-09 15:47	Medium	Pekka Ruuska	Madalina Baltatu	WP2 Scenario evaluation request	[5G-ENSURE] WP4 Scenario evaluation request for feature Trust Metrics
81	[5G-ENSURE] <R1> WP2 Scenario evaluation request for feature Complex Event Processing Framework for Security Monitoring and Inferencing	Solved	2017-09-11 16:59	Jose Sanchez	2017-05-03 08:01	Medium	Jani Suomalainen	Jury Papay Linas Maknavicius	WP2 Scenario evaluation request	

(b)

ID	Title	Status	Last update	Last edit by	Opening date	Priority	Requester - Requester	Assigned to - Technician	Category	Linked tickets - All linked tickets
131	[5G-ENSURE] <R1> WP4 Scenario evaluation request for feature Encryption of Long Term Identifiers	Processing (planned)	2017-10-23 15:42	Sergio MORANT	2017-09-07 13:20	Medium	Madalina Baltatu	Sergio MORANT	WP4 Scenario evaluation request	[5G-ENSURE] <R2> Enabler deployment request for enabler "Privacy Enhanced Identity Protection", feature "IMSI Pseudonymization" [5G-ENSURE]<R1> Enabler deployment request for enabler "Privacy Enhanced Identity Protection", feature "Encryption of Long Term Identifiers" [5G-ENSURE] <R1> WP2 Scenario evaluation request for feature Encryption of Long Term Identifiers
138	[5G-ENSURE] <R1*><R2> WP4 Scenario evaluation request for feature Basic Authorization in Satellite systems	Solved	2017-10-19 17:38	Sergio MORANT	2017-09-14 19:17	Medium	David Perez	Sergio MORANT Gorka Lendrino	WP4 Scenario evaluation request	[5G-ENSURE] <R1*><R2> WP2 Scenario evaluation request for feature Basic Authorization in Satellite systems [5G-ENSURE] <R1*><R2> WP4 Scenario evaluation request for feature Basic Authorization in Satellite systems [5G-ENSURE] <R2> WP4 Scenario evaluation request for feature AAA integration with satellite systems
137	[5G-ENSURE] <R1*> <R2> WP4 Scenario evaluation request for features Pseudo real-time monitoring && Threat detection	Solved	2017-10-19 17:27	Sergio MORANT	2017-09-14 19:13	Medium	Gorka Lendrino	Sergio MORANT Gorka Lendrino	WP4 Scenario evaluation request	[5G-ENSURE] <R1*><R2> Enabler deployment request Satellite network monitoring [5G-ENSURE] <R1*> <R2>WP2 Scenario evaluation request for features Pseudo real-time monitoring && Threat detection
120	[5G-ENSURE] <R1><R2> WP4 Scenario evaluation request Bootstrapping Trust	Processing (assigned)	2017-10-19 10:34	Linus Karlsson	2017-08-31 14:42	Medium	Linus Karlsson	Sergio MORANT	WP4 Scenario evaluation request	[5G-ENSURE] < R1><R2> WP2 Scenario evaluation request Bootstrapping Trust [5G-ENSURE] <R2> Enabler deployment request Bootstrapping trust
154	[5G-ENSURE] <R1><R2>WP4 Scenario evaluation request IoT "Group-based authentication"	Solved	2017-10-18 10:38	Sergio MORANT	2017-09-20 14:46	Medium	Markus Ahlstrom	Sergio MORANT Markus Ahlstrom	WP4 Scenario evaluation request	[5G-ENSURE] <R2> Enabler deployment request IoT "Group-based authentication" [5G-ENSURE] <R1><R2>WP2 Scenario evaluation request IoT "Group-based authentication"
76	[5G-ENSURE] <R1> WP4 Scenario evaluation request for feature Fine-Grained Authorization - RCD	Closed	2017-10-11 12:14	Cyrille Martins	2017-04-28 17:11	Medium	Cyrille Martins		WP4 Scenario evaluation request	[5G-ENSURE] <R1> WP2 Scenario evaluation request Fine-Grained Authorization - RCD
108	[5G-ENSURE] <R1><R2> WP4 Scenario evaluation request for feature Dynamic Arrangement of Micro-Segments	Processing (planned)	2017-10-09 11:01	Olli Mammela	2017-08-28 13:03	Medium	Olli Mammela		WP4 Scenario evaluation request	[5G-ENSURE] <R2> WP2 Scenario evaluation request <Micro-segmentation enabler> <Security monitor for 5G micro-segments enabler> <Trust metric enabler> [5G-ENSURE] <R1> Enabler deployment request micro-segmentation [5G-ENSURE] <R1><R2> WP2 Scenario evaluation request for feature Dynamic Arrangement of Micro-Segments
126	[5G-ENSURE] <R1/R2> WP4 Scenario evaluation request Group-based AKA	Closed	2017-09-20 10:53	Markus Ahlstrom	2017-09-06 14:32	Medium	martin.gunnarson@ri.se thomas.carnehult@ri.se	Sergio MORANT	WP4 Scenario evaluation request	[5G-ENSURE] <R1> WP2 Scenario evaluation for request Group authentication by extending the LTE-AKA protocol
127	[5G-ENSURE] <R1> WP4 Scenario evaluation request for feature Controller-Switch-Interaction Imitator	Closed	2017-09-13 11:04	Felix Klaedtke	2017-09-07 13:03	Medium	Felix Klaedtke	Sergio MORANT	WP4 Scenario evaluation request	[5G-ENSURE] <R1> WP2 Scenario evaluation request for feature Controller-Switch-Interaction Imitator
129	[5G-ENSURE] <R1> WP4 Scenario evaluation request for feature Trust Builder	Solved	2017-09-13 10:39	Sergio MORANT	2017-09-07 13:16	Medium	Jury Papay	Sergio MORANT	WP4 Scenario evaluation request	[5G-ENSURE] <R1> WP2 Scenario evaluation for feature Trust Builder
130	[5G-ENSURE] <R1> WP4 Scenario evaluation request for feature Enhanced privacy for network attachment protocols	Closed	2017-09-12 15:56	Piers Ohanlon	2017-09-07 13:18	Medium	Piers Ohanlon	Sergio MORANT	WP4 Scenario evaluation request	[5G-ENSURE] <R1> WP2 Scenario evaluation request for feature Enhanced privacy for network attachment protocols
132	[5G-ENSURE] <R1> WP4 Scenario evaluation request for feature VNF trustworthiness evaluation	Closed	2017-09-12 15:45	Frederic Motte	2017-09-11 13:30	Medium	Frederic Motte	Sergio MORANT	WP4 Scenario evaluation request	[5G-ENSURE] <R1> WP2 Scenario evaluation request for feature VNF trustworthiness evaluation

Figure 5. R1 received evaluation requests in heldpesk: (a) TCE requests, (b) TFE requests

Hereafter, all the TCE/TFE requests found in the helpdesk tool as of 20th of October 2017 for R2. There are 16 evaluation requests registered in helpdesk for WP2 and WP4 at release R2.



(a)

(b)

Figure 6. R2 received evaluation requests in heldpesk: (a) TCE requests, (b) TFE requests

7 Annex : TestBed Evaluation Results

TestLink Community [configure $tlCfg->document_generator->company_name]

Test Plan Execution Report

Test Project: 5G-ENSURE
Test Plan: Enablers Security Evaluation (R2)

Printed by TestLink on 31/10/2017

Test Project: 5G-ENSURE

This project aims to provide the testbook allowing to evalutate the 5G-ENSURE enablers agains their security claims with regard to the identified security Use Cases and their associated security threats

Test Suite: Threats

7.1 Test Suite : Use Cases cluster 1 - Identity Management

7.1.1 Test Suite : T_UC1.3_1 Unauthorised activities related to satellite devices or network

Test Case 5ge-130: Unauthorised user verification	
Summary: An authorized user tries to make a rest petition on a non-authorized resource. The response of the test, should be that the user is not allowed to perform the operation because the conditions of the petition does not match with the rules applied in the policy (i.e. $FGA_SAT_PATH/test/UT01/input/TestPolicy_UT01a.xml). Conditions: - The user is registered in the LDAP server. - The user is authorized to perform this action. - The user is non-authorized to perform this action on this resource.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	depends on - 5ge-54:Installing and configure environment related to - 5ge-136:Authorised user verification
Requirements	Feature-1.2.1: Basic Authorization in Satellite systems Use Case 1.3: Satellite Identity Management for 5G Access
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

Test Case 5ge-136: Authorised user verification	
Summary: An authorized user tries to make a rest petition using an user declared inside the policy. The response of the test, should be that the user is allowed to perform the operation because the conditions of the petition does not match with the rules applied in the policy. Conditions: - The user is registered in the LDAP server. - The time when the user is trying to make the petition is in the range 08:00-18:00. - The location from where the user is trying the connection is in Spain. To simulate the above conditions, the policy file in the server can be modified, just for environment verification.	
Execution type:	Manual

Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	related to - 5ge-130:Unauthorised user verification depends on - 5ge-54:Installing and configure environment
Requirements	Feature-1.2.1: Basic Authorization in Satellite systems Use Case 1.3: Satellite Identity Management for 5G Access
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

7.1.2 Test Suite : T_UC1.3_2 Fake roaming from terrestrial network into satellite network

Test Case 5ge-131: Registered user from unknown location

Summary:

An authorised user registered in LDAP server tries to make a REST petition. This is done from an unknown or not registered location (country) in the policy. The only one authorized country is Spain, so to make the right petition should be done from an user registered and from an specified country.
The response of the test, should be that the user is not allowed to perform the operation because the conditions of the petition does not match with the rules applied in the policy.
Conditions:
- The user is registered in the LDAP server, and it is using the same user role that the declared in the policy.
- The time when the user is trying to make the petition is in the range 08:00-18:00
- The location from where the user is trying the connection is outside Spain.

To simulate the above conditions, the policy file in the server can be modified, just for environment verification.

Execution type:	Manual
Estimated exec. duration (min):	
Priority:	High
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	related to - 5ge-135:Registered user from known location depends on - 5ge-54:Installing and configure environment
Requirements	Use Case 1.3: Satellite Identity Management for 5G Access Feature-1.2.3: AAA integration with satellite systems
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

Test Case 5ge-135: Registered user from known location

Summary:

An authorised user registered in LDAP server tries to make a REST petition. This is done from an registered country in the policy. The only one authorized country is Spain, so to make the right petition should be done from this specified country or modify the policy to make it match.
The response of the test, should be that the user is allowed to perform the operation because the conditions of the petition does match with the rules applied in the policy.
Conditions:
- The user is registered in the LDAP server, and it is using the same user role that the declared in the policy.
- The time when the user is trying to make the petition is in the range 08:00-18:00.
- The location from where the user is trying the connection is in Spain.

To simulate the above conditions, the policy file in the server can be modified, just for environment verification.

Execution type:	Manual
Estimated exec. duration (min):	

Priority:	High
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	related to - 5ge-131:Registered user from unknown location depends on - 5ge-54:Installing and configure environment
Requirements	Use Case 1.3: Satellite Identity Management for 5G Access Feature-1.2.3: AAA integration with satellite systems
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

7.1.3 Test Suite : T_UC1.4_1 Compromised data

Test Case 5ge-87: ProVerif security analysis of the group-based AKA protocol	
Summary: Feature 1.1.1 is a group-based Authentication and Key Agreement (AKA) protocol in which group authentication parameters are stored on the device outside of the UICC. However, the symmetric long-term key K, which is stored on the UICC, is also used in the protocol. Since parameters stored outside of the UICC could easily be leaked, the fundamental security properties of the protocol must not depend on whether the group authentication parameters are compromised or not. Specifically, an adversary having access to the group authentication parameters must be unable to authenticate to the network or derive a session master key by eavesdropping on communication. If the adversary could manage to derive the session master key, the confidentiality of all the data sent between the machine-type communications (MTC) device and the network would be compromised. Also, the adversary should not be able to break authentication or confidentiality even if, additionally, members of the same group share all its authentication parameters (including the long-term secret) with the adversary. It is proven with ProVerif that the protocol meets confidentiality and mutual authentication when the adversary has access to all the authentication parameters of members in the same group in addition to all group authentication parameters of the MTC device. See the following paper for a presentation of the proof. Giustolisi, R., Gehrmann, C., Ahlström, M. and Holmberg, S., 2017. A secure group-based AKA protocol for machine-type communications. In *International Conference on Information Security and Cryptology ICISC 2016: Information Security and Cryptology–ICISC 2016. 30 November 2016 through 2 December 2016* (pp. 3-27).	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	1- Theoretical evidence
Requirements	Feature-1.1.1: Group authentication by extending the LTE-AKA protocol Use Case 1.4: MNO Identity Management Service
Attached files	• A secure group-based AKA protocol for machine-type communications : icisc_cameraready.pdf • icisc_cameraready.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	Theoretical evidence provided. No execution required

Test Case 5ge-146: STRIDE analysis of the ACE framework
Summary: For Feature 1.2.4. We have analyzed the ACE framework with Microsoft's Threat Modeling Tool to be able to evaluate the security of the ACE-framework. The attached document contains the analysis.

Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	1- Theoretical evidence
Requirements	Use Case 1.4: MNO Identity Management Service Feature-1.2.4: Authorization and authentication for RCD based on ongoing IETF standard
Attached files	• ACE_threat_report : ACE_threat_report.pdf • ACE_threat_report.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	Theoretical evidence provided. No execution required

7.2 Test Suite : Use Cases cluster 2 - Enhanced Identity Protection and Authentication

7.2.1 Test Suite : T_UC2.2_1 Tracking of device's (user's) location

Test Case 5ge-149: IMSI Pseudonymization test - check RTMSI pseudonyms	
Summary:	
Description: Verify that the feature IMSI Pseudonymization provides different pseudonyms for the same input IMSI value in different attach procedures using EAP-AKA full authentication **Strategy**: Configure the public key on the client (wpa_supplicant) and the private key on the server (hostapd). Insert a SIM card (with a known IMSI value) in the smart card reader and connect to the SSID1 WiFi network with EAP-AKA full authentication method. Check that the EAP-AKA authentication is successsful and observe the IMSI value that is transiting in Identity Response messages. Detach (stop the wpa_supplicant process) and connect again to the SSID1 WiFi network with EAP-AKA full authentication. Observe the IMSI value that is transiting in Identity Response messages. Repeat the procedure a desired number of times to test that different identities are used each time.	
Execution type:	Manual
Estimated exec. duration (min):	15.00
Priority:	Medium
Scenario evaluation score:	4 - Testbed evaluation (real flows)
Relations	related to - 5ge-125:Supplementary Test: Check the RTMSI pseudonyms with Wireshark related to - 5ge-151:IMSI Pseudonymization test - check RTMSI pseudonyms
Requirements	Use Case 2.2: Subscriber Identity Privacy Feature-2.1.3: IMSI Pseudonymization
Attached files	• IMSI_Pseudonymization_test_description.txt • IMSI_Pseudonymization_test_description.txt
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**20.00**
Execution notes	Wireshark trace is attached to step 1

7.2.2 Test Suite : T_UC2.2_2 Mobile user interception and information interception

Test Case 5ge-86: ProVerif privacy analysis of the group-based AKA protocol
Summary:
Feature 1.1.1 is a group-based Authentication and Key Agreement (AKA) protocol. A machine-type communications (MTC) device using the protocol identifies itself by the combination of a group identifier, called GID, and a value that identifies the device within the group, called PATH. Since the long-term key K (stored in the UICC) is needed for a device to authenticate using the protocol, the device identifier (GID, PATH) is associated with an International Mobile Subscriber Identity (IMSI). However, in order to achieve MTC identity privacy, it is important that an adversary cannot identify the IMSI by observing a run of the group-based AKA protocol, even though the group-based AKA device

identifier is sent in the clear. The following paper presents a ProVerif verification proving that the protocol meets this MTC identity privacy property. Giustolisi, R., Gehrmann, C., Ahlström, M. and Holmberg, S., 2017. A secure group-based AKA protocol for machine-type communications. In *International Conference on Information Security and Cryptology ICISC 2016: Information Security and Cryptology–ICISC 2016. 30 November 2016 through 2 December 2016* (pp. 3-27).	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	1- Theoretical evidence
Requirements	Feature-1.1.1: Group authentication by extending the LTE-AKA protocol Use Case 2.2: Subscriber Identity Privacy
Attached files	• A secure group-based AKA protocol for machine-type communications : icisc_cameraready.pdf • icisc_cameraready.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	Theoretical evidence provided. No execution required

Test Case 5ge-151: IMSI Pseudonymization test - check RTMSI pseudonyms	
Summary: The same test as 5ge-149 also proves the coverage of this threat.	
Execution type:	Manual
Estimated exec. duration (min):	0.00
Priority:	Medium
Scenario evaluation score:	4 - Testbed evaluation (real flows)
Relations	related to - 5ge-149:IMSI Pseudonymization test - check RTMSI pseudonyms
Requirements	Use Case 2.2: Subscriber Identity Privacy Feature-2.1.3: IMSI Pseudonymization
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant

Execution Result:	Passed
Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	See 5ge-149 test case execution

7.2.3 Test Suite : T_UC2.1_2 Tracking of device's (user's) location

Test Case 5ge-144: Device Identity Privacy Evaluation R2	
Summary: This evaluation test should demonstrate that the DIP enabler R2 DNA privacy enhancement features for both retest for R1 features (Dummy address injection and Random ordering) and R2 features (Dummy address injection automatic mode and Geolocation prefiltering) provide for improvement of path location privacy.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 2.1: Device Identity Privacy Feature-2.2.1: Enhanced privacy for network attachment protocols Feature-2.2.2: Anonymous and optimised address selection for network attachment protocols
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	Passed
Execution Mode:	**Manual**
Execution duration (min):	**20.00**

7.3 Test Suite : Use Cases cluster 3 - IoT Device Authentication and Key Management

7.3.1 Test Suite : T_UC3.1_1 Authentication traffic spikes

Test Case 5ge-85: ProVerif security and privacy analysis of the group-based AKA protocol	
Summary: An authentication scheme for IoT devices that aims to mitigate the authentication traffic spikes threat must still provide adequate security and privacy, otherwise the effect could be that an adversary can break authentication, derive a session master key or compromise the privacy. In the paper referenced below a ProVerif analysis of the group-based AKA protocol (feature 1.1.1) is presented. It is proven that the protocol meets mutual authentication, key confidentiality and device identity privacy. Giustolisi, R., Gehrmann, C., Ahlström, M. and Holmberg, S., 2017. A secure group-based AKA protocol for machine-type communications. In *International Conference on Information Security and Cryptology ICISC 2016: Information Security and Cryptology–ICISC 2016. 30 November 2016 through 2 December 2016* (pp. 3-27).	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	1- Theoretical evidence
Requirements	Feature-1.1.1: Group authentication by extending the LTE-AKA protocol Use Case 3.1: Authentication of IoT Devices in 5G
Attached files	• A secure group-based AKA protocol for machine-type communications : icisc_cameraready.pdf • icisc_cameraready.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	Theoretical evidence provided. No execution required

7.3.2 Test Suite : T_UC3.1_2 Compromised authentication gateway

Test Case 5ge-147: STRIDE analysis of the ACE framework
Summary: For Feature 1.2.4. We have analyzed the ACE framework with Microsoft's Threat Modeling Tool to be able to evaluate the security of the ACE-framework. The attached document contains the analysis.

Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	1- Theoretical evidence
Requirements	Use Case 3.1: Authentication of IoT Devices in 5G Feature-1.2.4: Authorization and authentication for RCD based on ongoing IETF standard
Attached files	• WP2 Evaluation score : 5ge-147-WP2Evaluationscore.txt • 5ge-147-WP2Evaluationscore.txt • ACE_threat_report : ACE_threat_report.pdf • ACE_threat_report.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	Theoretical evidence provided. No execution required

7.3.3 Test Suite : T_UC3.2_1 Leaking keys

Test Case 5ge-94: No key in plain-text	
Summary: The private key required for accessing the controller should never be available in clear text on the system. This prevents the key from being leaked to an adversary.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 3.2: Network-Based Key Management for End-to-End Security Feature-5.3.1: Integrity Attestation of Virtual Network Components
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Failed**
Execution Mode:	**Manual**

Execution duration (min):	**30.00**
Execution notes	Two issues identified : * The port 8081 is not open as there is no precondition on having Floodlight running on any of the VMs, and particularly on VM1 (see 5ge-41 integration test) * The main issue (even once restarted floodlight) is that the sgx calls fail. The integration tests do not seem to cover that sgx framework operates properly.

7.4 Test Suite: Use Cases cluster 5 - Software-Defined Networks, Virtualization and Monitor

7.4.1 Test Suite : T_UC5.1_1 Misbehaving control plane

Test Case 5ge-99: Detection and mitigation of malicius traffic directed to critical network function	
Summary: This test aims at detecting and mitigating malicious traffic pattern targeting vital VNFs deployed in vEPC. The Flow Control enabler is deployed as a gateway for the VNF to protect, providing filtering and shaping for incoming traffic. In the test case, a DoS attack is performed against the vMME, a key node of the EPC that performs Mobility management A DDoS attack against the MME (e.g., overloading through a botnet of infected devices) would prevent the network from operating. To be successful the test should be able to identify and block the malicious traffic while not blocking the legitimate traffic.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	4 - Testbed evaluation (real flows)
Relations	related to - 5ge-98:Setup check
Requirements	Use Case 5.1: Virtualized Core Networks, and Network Slicing Feature-5.5.1: Detection of malicious behaviors Feature-5.5.2: Mitigation of detected malicious behaviors
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

Test Case 5ge-110: Removal check of misbehaving node in micro-segment	
Summary: This scenario comprises three enablers, namely, the compliance checker (CC), the micro-segmentation enabler (MSE), and the micro-segmentation monitoring enabler (MSME). CC checks—based on the information it receives from the two other enablers—that malicious nodes identified by the MSME are eventually deleted within a specified deadline by the MSE from the micro-segment. Other policies are possible, e.g., that the MSE only removes nodes from the micro-segment that the MSME has previously identified as malicious. In this scenario, the CC acts here as a control mechansim that checks that the MSE and the MSME interact with each other as intended. Note that this scenario was part of the EuCNC demo by VTT and others showing the use of micro-segments. See the EuCNC video. The theoretical underpinnings, the algorithms used by the CC are described in the following conference paper together with an experimental evaluation of the tool's performance. D. Basin, F. Klaedtke, and E. Zalinescu. Runtime Verification of Temporal Properties over Out-of-Order Data Streams. In Proceedings of the 29th International Conference on Computer Aided Verification (CAV). Lecture Nodes in Computer Science, volume 10426, Springer 2017.	
Execution type:	Manual

Estimated exec. duration (min):	30.00
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 5.1: Virtualized Core Networks, and Network Slicing Use Case 5.4: Verification of the Virtualized Node and the Virtualization Platform Feature-5.2.2: Basic NFV Reconfiguration Compliance Checker
Attached files	• malnodedeletion.log • malnodedeletion.log • malnodedeletion.spec • malnodedeletion.spec • malnodedeletion.msgs • malnodedeletion.msgs • malnodedeletion.comp • malnodedeletion.comp
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**20.00**
Execution notes	Attention the Keep Alives messages are logged on the console ([V]:true) in opposition what is described on the execution steps Notice that the last step (7) doesn't explicitly request an action so it was ignored in the execution.

Test Case 5ge-120: Capture attack against VNFM	
Summary: This test aims at checking that an attack leveraging a compromised control plane (VNF Manager) is detected by CyberCAPTOR. It uses en example topology where a VNF is present with vulnerabilities that permits to take control of its VNF manager.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	depends on - 5ge-126:Cyber-data-extract running depends on - 5ge-37:API running depends on - 5ge-38:Attack graph generation depends on - 5ge-39:Custom attack graph generation depends on - 5ge-40:Web UI running

Requirements	Use Case 5.1: Virtualized Core Networks, and Network Slicing Use Case 5.5: Control and Monitoring of Slice by Service Provider Feature-4.1.2: 5G specific vulnerability schema implementation
Attached files	• configuration de cyber-data-extract : auto-fetcher-config-10.102.8.68.yaml • auto-fetcher-config-10.102.8.68.yaml • GCI report : gci-report2.xml • gci-report2.xml
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**40.00**
Execution notes	For the record, the right way to launch the cyber-data-extract container from the artifact repository is: sudo docker run -it -v ${PWD}/auto-fetcher-config-10.102.8.68.yaml:/root/cyber-data-extract/auto-fetcher-config.yaml fivegensure-docker-virtual.artifact.b-com.com/cyber-data-extract:1.8.1 Another think is that the final step does not clearly state whether there is an action to be performed to check the threat mitigation.

Test Case 5ge-138: Reactive adding of flow rules in SDN networks

Summary:

In this scenario, the compliance checker is used to check a simple policy about the interactions between the SDN controller and SDN switches. Namely, whenever a switch receives a network packet with no matching flow rule, the controller must reconfigure the switch accordingly, within a time bound. In other words, the compliance checker checks that the controller timely reacts to packet-in OpenFlow messages by corresponding flow-mod OpenFlow messages.

For the moment, we restrict ourselves to this simple policy. Other, more complex, policies about the interactions via OpenFlow messages between the control plane and the data plane can be checked accordingly. An example is that barrier requests are handled appropriately. However, the setup will be more involved and we want to keep things simple here.

In the following, we describe how to configure, setup, and run the different involved components, namely, runverif, OVS, ONOS, and Mininet.

Execution type:	Manual
Estimated exec. duration (min):	45.00
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Feature-5.2.1: Basic OpenFlow Compliance Checker Use Case 5.3: Reactive Traffic Routing in a Virtualized Core Network Use Case 5.4: Verification of the Virtualized Node and the Virtualization Platform

Attached files	• flowmod-prop.spec • flowmod-prop.spec • README-flowmod • README-flowmod • flowmod-prop.msgs • flowmod-prop.msgs • flowmod-prop.comp • flowmod-prop.comp • flowmod.spec • flowmod.spec • flowmod.msgs • flowmod.msgs • flowmod.comp • flowmod.comp
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**60.00**
Execution notes	The runverif connection log from OVS is wrong. In fact, it always returns "connection established" but in fact it is not a really tested. My guess is that communication is not bi-directional between OVS <> runverif so it is not really possible to get a correct status.

Test Case 5ge-139: Deactiviation of SDN network applicatons

Summary:

In this scenario, the compliance checker checks whether deactivating a network service is allowed. We restrict ourselves here to deactivating network applications of the controller ONOS. Concretely, we consider the policy that it is only allowed to deactivate the driver app when the OpenFlow app is not active.

In a broader setting, the network services could be NFVs that for example run in Docker containers. More complex dependencies between services can also be expressed. Furthermore, we could also check that certain network services, when deactivated, must be reactivated within a specified time window. Another example is that certain network services should not be activated at the same time, e.g., because of conflicting use of network resources.

Execution type:	Manual
Estimated exec. duration (min):	45.00
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 5.4: Verification of the Virtualized Node and the Virtualization Platform Feature-5.2.2: Basic NFV Reconfiguration Compliance Checker
Attached files	• README-deactivatingapps • README-deactivatingapps

	• deactivatingapps.spec • deactivatingapps.spec • deactivatingapps.proxy • deactivatingapps.proxy • deactivatingapps.msgs • deactivatingapps.msgs • deactivatingapps.comp • deactivatingapps.comp
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Failed**
Execution Mode:	**Manual**
Execution duration (min):	**60.00**
Execution notes	So far, There is no traffic generated towards port 50010. This has been double checked by performing a wireshark capture.

7.4.2 Test Suite : T_UC5.2_1 Add malicious nodes into core network

Test Case 5ge-25: Authentication to a micro-segment	
Summary: The objective of this test is to check how the micro-segmentation enabler is able to respond to the threat T_UC5.2_1 Add malicious nodes into core network. In this threat malicious nodes may e.g. eavesdrop, tamper, and prevent data flows. The enabler applies security verification procedures, namely IEEE 802.1X based authentication for assuring that the added nodes are trustworthy. This test presumes that the single node version of the enabler has been installed.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 5.2: Adding a 5G Node to a Virtualized Core Network Feature-5.4.1: Dynamic Arrangement of Micro-Segments
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**30.00**
Execution notes	Test performed with testbed 2 nodes microsegmentation setup.

Test Case 5ge-93: Malicious enclave don't get key	
Summary: A malicious or compromised enclave should not be added to the network. This means that if the actual measurement of the application is not in the list of expected hashes, the application should not be provisioned with a key and the network can thus not connect to the SDN controller.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 5.2: Adding a 5G Node to a Virtualized Core Network Feature-5.3.1: Integrity Attestation of Virtual Network Components
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Failed**
Execution Mode:	**Manual**
Execution duration (min):	**30.00**
Execution notes	The verification manager report an error but it is not the one expected (step 3). So we can't conclude that it has attested the trustiness of the enclave

7.4.3 Test Suite : T_UC5.2_2 Forwarding logic leakage

Test Case 5ge-95: TLS connection to controller	
Summary: Ensures that a TLS connection is setup between the Application and the Controller, after a successful provisioning of the Application. This makes the communication between the application and the controller both integrity and confidentiality protected.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 5.2: Adding a 5G Node to a Virtualized Core Network Feature-5.3.1: Integrity Attestation of Virtual Network Components
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Failed**

Execution Mode:	**Manual**
Execution duration (min):	**0.00**
Execution notes	This tests uses the same SGX frame work as 5ge-93 and 5ge-94, and thus it is not possible to successfully execute it

7.4.4 Test Suite : T_UC5.5_1 Misuse of open control and monitoring interfaces

Test Case 5ge-128: Monitoring access control misuse in a mobile network	
Summary: The System Security Threat Repository (SSSR) makes use of a knowledgebase encoding information about the assets, trust relationships, threats and controls in the 5G architecture. This knowledgebase is used to addresses the need to enrich the system view with information about the system's assets, the threats, incidents, and analysis results in order to understand the state of the whole system. The enabler allows querying and analysis for a higher-level view of security incidents and trends. See attached PDF for detailed description and screenshots. Sample mobile network model for trust builder provided as well	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 5.5: Control and Monitoring of Slice by Service Provider Feature-4.5.2: System Security State Repository service
Attached files	• T34 R2 SSSR : T34_SSSR_sml.pdf • T34_SSSR_sml.pdf • Trust Builder Mobile Network Model : Model_for_SSSR_validated.nq • Model_for_SSSR_validated.nq • T_UC5.5_1 - Misuse of open control and monitoring interfaces : T_UC5.5_1 Misuse of open control and monitoring interfaces sml.pdf • T_UC5.5_1 Misuse of open control and monitoring interfaces sml.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

7.4.5 Test Suite : T_UC5.5_4 No control of Cyber-attacks by the Service providers

Test Case 5ge-108: Two types of security control for service provider
Summary: This test scenario demonstrates how three enablers - micro-segmentation, security monitor for 5G microsegments, and trust metric enabler - provide more control over the cyber attacks for service providers that using are the 5G network.

The case demonstrates how service providers can be delivered coarse or fine-grained security and trust information from the 5G network (segment) that has been dedicated for the service provider. The case also illustrates that, when the control and monitoring APIs to 5G network are opened, service provider are able to get custom security functionality to 5G networks (to microsegments). In this test case, the service provider gets futher availability quarantees as a machine learning algorithm for anomaly detection is analysing network flows (and able to quarantine flows from suspected DoS attacks). Further, a status notifications on the real-time trust situation (based e.g. anomaly detection and availability of security services in the micro-segment) is delivered to the service provider. In this scenario, the service provider is given two types of alternative security controls: 1) Coarse-grained: Trust Metric enabler provides real time information to the service provider about the security level of the segmented network, i.e., a micro-segment. (Coarse grained information does not disclose information that is sensitive for the operator or other clients/service providers). The service provider may use this information during orchestration, when deciding whether the network offered by the operator can be trusted or not. 2) Fine-grained - Security Monitor for 5G Micro-Segments enabler provides observation/reaction algorithms to the network. (Fine-grained information is available, if the network operator wants to pass this information forward. The operator may also agree with the service provider on the customization of the monitoring algorithms.) The security control is enabled by the micro-segmentation enabler, which segments the network so that the service provider is able to retrieve information from it and control it (in cooperation with the operator without disturbing traffic flows of other services providers). (Microsegmentation removes also some legal / privacy obstacles from sharing of monitoring information as monitoring can focus to segmented flows originating to the service provider. Hhence information belonging to other customers of operator are not disclosed). The purpose of the test case is to show that A) enablers are starting and running B) one security monitoring instance is running focusing on the micro-segment (this enabler is running monitoring and control algorithms preferred by the service providers) C) Trust metric enabler shows to the service provider how secure / trusted the micro-segment is. For further information on the enablers, please see open specifications and user guides.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	4 - Testbed evaluation (real flows)
Requirements	Feature-3.2.1: Trust metric based network domain security policy management Feature-4.4.1: Complex Event Processing Framework for Security Monitoring and Inferencing Use Case 5.5: Control and Monitoring of Slice by Service Provider Feature-5.4.1: Dynamic Arrangement of Micro-Segments
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Passed**
Execution Mode:	**Manual**
Execution duration (min):	**30.00**

7.4.6 Test Suite : T_UC5.6_1 Security threats in a satellite network

Test Case 5ge-133: Unauthorised user athentication
Summary: In this test case, it is going to be tested all the policy rules setted in the policy file. For this an user registered but with other role, will try to access from a different country in a different time that the allowed. The response of the test, should be that the user is not allowed to perform the operation because the conditions of the petition does not match with the rules applied in the policy. Conditions: - The user is registered in the LDAP server and the role does not match with the role declared in the policy file. - The time when the user is trying to make the petition is out of the range 08:00-18:00 - The location from where the user is trying the connection is outside Spain.

To simulate the above conditions, the policy file in the server can be modified, just for a verification of the conditions.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	depends on - 5ge-54:Installing and configure environment related to - 5ge-137:Authorised user authentication
Requirements	Use Case 5.6: Integrated Satellite and Terrestrial Systems Monitor Feature-1.2.3: AAA integration with satellite systems
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

Test Case 5ge-137: Authorised user authentication	
Summary: In this test case, it is going to be tested all the policy rules setted in the policy file. For this an user registered, will try to access from a the country declared in the policy in a the time allowed. The response of the test, should be that the user is allowed to perform the operation because the conditions of the petition does not match with the rules applied in the policy. Conditions: - The user is registered in the LDAP server and the role does match with the role declared in the policy file. - The time when the user is trying to make the petition is in the range 08:00-18:00 - The location from where the user is trying the connection is in Spain. To simulate the above conditions, the policy file in the server can be modified, just for a verification of the conditions.	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Relations	depends on - 5ge-54:Installing and configure environment related to - 5ge-133:Unauthorised user athentication
Requirements	Use Case 5.6: Integrated Satellite and Terrestrial Systems Monitor Feature-1.2.3: AAA integration with satellite systems
Execution Details	
Build	Enablers Security Evaluation (R2)

Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

7.5 Test Suite : Use Cases cluster 8 - Ultra-Reliable and Standalone Operations

7.5.1 Test Suite : T_UC8.1_1 Service failure over satellite capable eNB

Test Case 5ge-132: Reconfigure the network topology

Summary:

Checks that the user can configure the security/performance indicators to be collected.
Checks that the updated topology may be forwarded.

The initial topology is configured in step #8 and can be checked in steps #9, #10 and #11.
http://10.102.0.51/lib/attachments/attachmentdownload.php?id=111

The indicators to be collected are configured in step #12. Node 5g-enodeb3 is configured with $MON_SAT_PATH/test/UT01/input/indicators_UT01.5g-enodeb3.json:

- ifOperStatus from terrestrial terminal 1.
- ifOperStatus from terrestrial terminal 2.
- ifOperStatus from satellite terminal 1.

Each node sents the operational state of the interface (ifOperStatus) to the satellite-network-monitoring-server every 10 seconds (snmp_retry_timeout_msg property in $MON_SAT_PATH/client/SatelliteNetworkMonitoringClient.properties). If the operational state of the interface is set to down ("error_value": 2) the node sends an alarm message.

Link failure is emulated in step #13.

The incident/failure is detected in step #14. The satellite-network-monitoring-server is continuosly collecting messages from the message broker (i.e. ActiveMQ). When the SatelliteNetworkMonitoringServer detecs an alarm message (messageType field in the header set to "alarm") it launches the Topology Manager (see "apply" trace in $MON_SAT_PATH/logs/monitoring.log).

The Topology Manager calculates the best topology that fixes the issue based on two KPIs:

- Similarity (the final topology should be similar as the original one).
- TotalPowerConsumed (the lower the better).

Later, this topology is forwarded to all the nodes.

The final topology can be checked in steps #15, #16 and #17.
http://10.102.0.51/lib/attachments/attachmentdownload.php?id=112

Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Feature-4.2.1: Pseudo real-time monitoring Feature-4.2.2: Threat detection Use Case 8.1: Satellite-Capable eNB
Attached files	• output : output.png The linked image cannot be displayed. The file may have been moved, renamed, o... • • TopologyMatrix : TopologyMatrix.png

Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

7.6 Test Suite : Use Cases cluster 9 - Trusted Core Network and Interconnect

7.6.1 Test Suite : T_UC9.3_1 Hardening or patching of systems is not done

Test Case 5ge-127: T_UC9.3_1 - "Hardening or patching of systems is not done" R2	
Summary: 5G networks allow more dynamism through virtualisation and new functions can be introduced to the network on the fly. As these environments are more virtualised, there is always a danger that someone manages to introduce a malicious function into the network. Similarly, unauthorized physical elements could be attached to the network, if their authenticity is only based on the location in the network. This test case describes the sequence of steps that correspond to Release 2 of Tust Builder. For the detailed description of individual steps please refer to the attached document "Modelling_T_UC9.3_1_TrustBuilder_Release2.pdf".	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 9.3: Authentication of New Network Elements Feature-3.3.1: 5G Asset Model Feature-3.3.2: 5G Threat knowledge base v1 Feature-3.3.3: Graphical editor
Attached files	• Modelling_T_UC9.3_1_TrustBuilder_Release2 : Modelling_T_UC9.3_1_TrustBuilder_Release2.pdf • Modelling_T_UC9.3_1_TrustBuilder_Release2.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	

Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

7.7 Test Suite : Use Cases cluster 10 - 5G Enhanced Security Services

7.7.1 Test Suite : T_UC10.2_1 Nefarious activities: privacy violations

Test Case 5ge-142: Modelling T_UC10.2_1 Nefarious activities: “privacy violations”	
Summary: 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. This issue is going to be even more pressing within 5G networks where a single service may be the result of a compositions of different layers managed by different parties with different views on privacy. For the detailed description of the test please refe to the attached document "Modelling T_UC10.2_1_PrivacyEnabler_R2.pdf".	
Execution type:	Manual
Estimated exec. duration (min):	
Priority:	Medium
Scenario evaluation score:	3 - Testbed evaluation (simulation)
Requirements	Use Case 10.2: Privacy Violation Mitigation Feature-2.3.1: Privacy policy specification Feature-2.3.2: Privacy preferences specification Feature-2.3.3: Comparison of policies and preferences
Attached files	• Modelling T_UC10.2_1_PrivacyEnabler_R2 : Modelling_T_UC9.3_1_TrustBuilder_Release2.pdf • Modelling_T_UC9.3_1_TrustBuilder_Release2.pdf
Execution Details	
Build	Enablers Security Evaluation (R2)
Tester	smorant
Execution Result:	**Blocked**
Execution Mode:	**Manual**
Execution duration (min):	
Execution notes	Scenario approved but not executed because the Enabler could not be integrated on the testbed.

8 Annex : WP4 final demonstrations

Testbed orchestration and service function chaining

EUCNC 2017 Demonstration

8.1 Demonstration 1: Service Function Chaining for new enabler deployment

8.1.1 Objective

The demo illustrates the 5G Testbed integration and orchestration capabilities to perform:

- Automatic testbed services provisioning for newly deployed host
  - Active Directory , IP Management, Host Monitoring
- Enabler integration tests (Unitary Tests)
- Automatic enabler deployment from Artifact repository
- Automatic enabler chaining

8.1.2 Scenario & Architecture

The demo will show a live deployment of the "component interaction audits" enabler and the chaining with Micro-segmentation Enablers (MSE) and MSME (Micro-Segmentation Monitoring Enablers). The following steps will be performed:

- Apply the testbed engineering rules to already deployed host
- Will add the host to the corresponding services
- Automatically deploy the « component Interaction Audits » Enabler and perform its integration tests
- Chain the deployed enabler to the microsegmentation environment
- Allows to audit the interaction between micro-segmentation Enablers

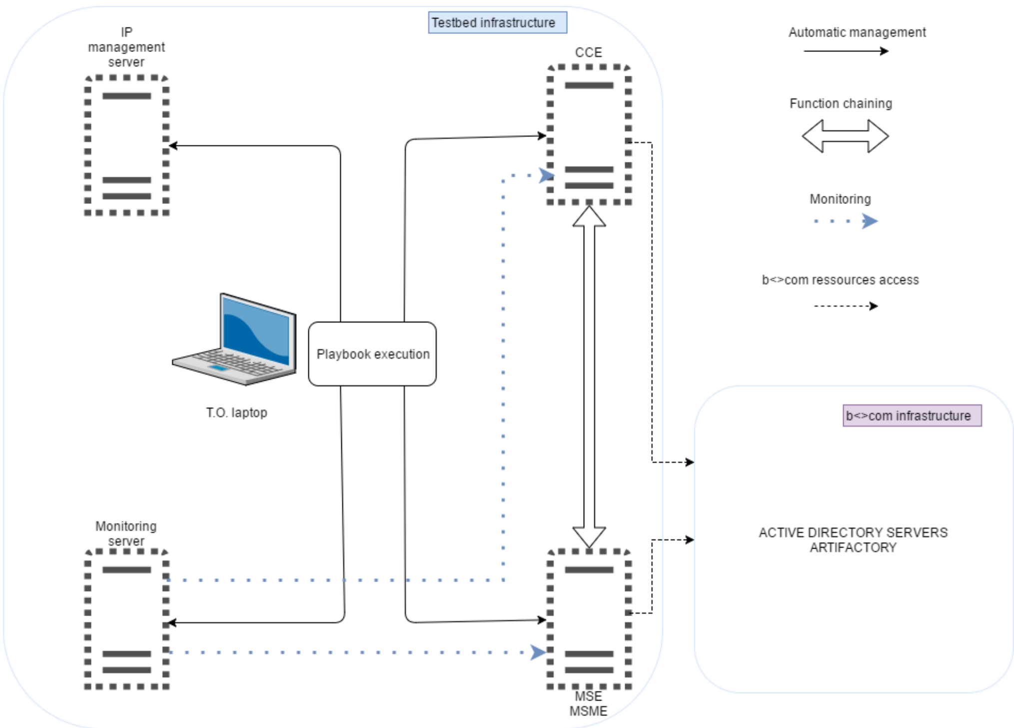


Figure 7. Service Function Chaining for new enabler deployment architecture

- The Testbed Operator (T.O) presents the dashboards of both monitoring and IP management tools, showing that none of the enabler servers is listed

- The T.O tries to log on one of the enablers host with a domain account and shows that it is not possible.
- The T.O runs an Ansible playbook and shows that all of the aforementioned services are provisioned, the enabler hosts show up on dashboards and domain login is working.
- The T.O. logs on the CCE host and shows that the enabler is not installed by showing the runverif command is not available
- The T.O. runs an Ansible playbook and shows that the enabler is now present and working by running (the integration?) tests defined in TestLink.
- The T.O starts both CCE and MSE and shows that CCE is not receiving any information from MSE.
- The T.O displays the contents of MSE and MSME configuration files showing no link to CCE
- The T.O runs an Ansible playbook and shows that the previously displayed configuration file now references the second enabler host.
- The T.O shows that CCE is receiving data from MSE

8.2 EuCNC demo

Objective of the EuCNC exhibition was to show some of the results coming from the 5G-ENSURE project, particularly several of the security enablers, which were developed. The aim was to demonstrate the security enhancements the enablers provide as standalones, through their capabilities/features, but also to show, in specific use cases, the added value provided by the enablers, working in cooperation, with regards to enhancements in access control, privacy, trust, as well as network management and virtualization security.

The exhibition also described how the demonstrated test-bed (with remote nodes in Rennes, France, and Oulu, Finland) enabled the development and testing of complex end-to-end, multi-domain, multi-operator security scenarios.

The demonstration showed 5G security solutions from several project partners (VTT, Telecom Italia, NEC, SICS and Thales -TCS) and a geographically distributed 5G test-bed.

The following technologies were demonstrated:

• Micro-segmentation - i.e. software defined networking based approach for network function virtualization. The technology enables isolation of different 5G applications and user organizations from each other. Consequently, security can be customized based on clients' specific needs.

• Internet of Things - the enabler provided a new definition of protocols for credential management and authentication of users and devices, such as sensors and IoT devices in general. 5G-ENSURE demonstrated the capability of the group-based AKA protocol to make the simultaneous authentication of groups of devices.

• Security monitoring and trust metrics - the demonstrated monitoring approaches included policy compliance checking and anomaly detection in 5G micro-segments. This combined with real-time trust metric evaluation demonstrated how 1) service providers and end-users can be made more aware of 5G connections trustworthiness and 2) how 5G network can be made more self-resilient.

• Privacy enhancements - the enabler prevents tracking of mobile users by hiding user identifiers. The demonstration showed the privacy enhancement in EAP-AKA through the user identifiers (IMSI) encryption and how its adoption provides evidence of identity trust that can be used to calculate a trust metric value for 5G systems.

• VNF Certification - the enabler certifies trustworthy implementation of the VNF and exposes their characteristics through a Digital Trustworthiness Certificate. The demonstration showed the certificate creation.

- Nixu Sensor - Visualization of the traffic flows.

As part of the demonstration two scenarios were also reproduced "factory's video monitoring" and "remote control of an IoT home heating system". It showed privacy and DoS attacks against these applications (in '3G/4G environments') with the objective to provide concrete cases where the adoption and integration of the described enablers allowed addressing these threats. Figure 8 shows the architecture of the demo.

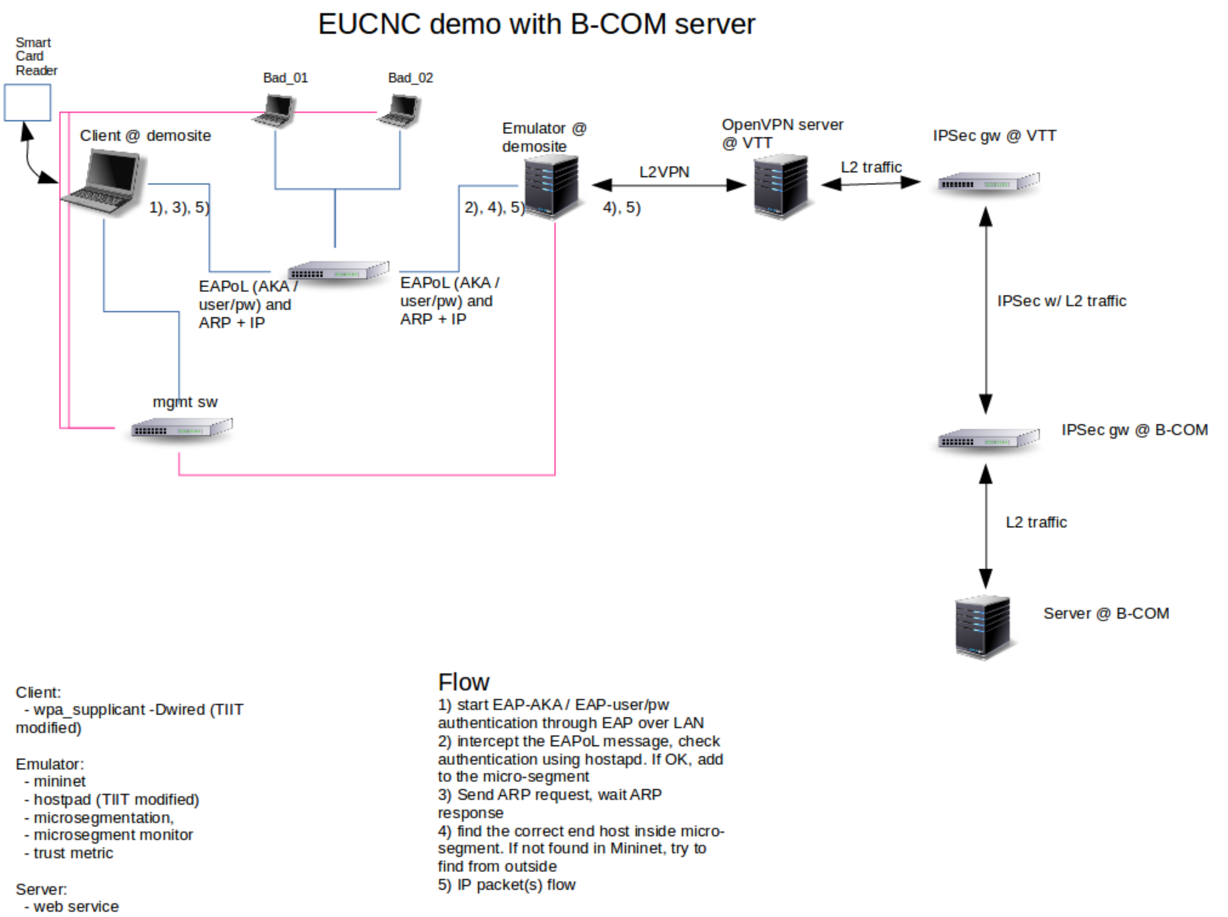


Figure 8: EuCNC demo architecture.

8.2.1 Factory's video monitoring

A company wants to provide a video monitoring service to its factory by using the 5G network. Carol, a company employee, uses her 5G mobile device to view the video service. This service should be highly secure and isolated from the rest of the network so that malicious nodes would not be able to access or disturb it. In addition, in the case of an attack or intrusion, security monitoring should be able to detect malicious nodes (IoT botnet operated by Mallory) and remove them. The trustworthiness of the service should also be monitored.

In this scenario, the micro-segmentation enabler was used for creating and deleting micro-segments, adding and deleting nodes from micro-segments, and providing strong access control to the micro-segment. The security monitoring enabler monitored behaviour inside the micro-segment and detected any anomalous behaviour. This was achieved by machine learning techniques and by monitoring the network traffic. An attack can be caused by the other IoT devices that have been connected to the same network and been turned into a botnet that is being used in denial of service (DoS) attacks. When an anomaly revealing such attack was detected, the micro-segmentation enabler was be automatically contacted to quarantine suspected flows. For the demo viewer, the attack became visible when the quality of service degrades. Similarly, advantages from micro-segmentation were evident by quick recovery of service quality. The attack was also visualized for the demo viewer: the Nixu sensor illustrated traffic flows and the tool emphasized those used in attack.

The trust metric enabler functioned in unison with the security monitoring enabler. The trust metric enabler provided information about the trustworthiness of a micro-segment for the service provider - for the company using the micro-segment. If a micro-segment becomes untrustworthy, the service provider was notified. The service provider visualized trustworthiness for the end-users, e.g., by displaying green or red icons or textual information stating that company’s trust requirements were either met or were not satisfactory.

The compliance checker verified whether the micro-segmentation enabler quarantines the flows detected by the monitoring enabler. In particular, it checks at runtime that maliciously behaving nodes are removed from the micro-segment and that the data plane is reconfigured. In case one of these steps are not performed (e.g., because of a misconfiguration or bug at the control plane), the compliance checker issues a warning, which is visualized by a red flag at the web service displaying the micro-segment.

VTT was a video service provider, i.e., micro-segmented service was hosted at the VTT's side of the test bed. The video service was Video-on-Demand (VoD). Carol and Mallory's devices were at the demo site and trying to access the micro-segment and the service operated by VTT.

The following steps summarize what the audience saw:

- Carol viewed video using her mobile device; the trust metrics from another window showed "green"
- Embedded devices (botnet) were added to the network / or botnet gets command -> attack starts
- The quality of video degraded for short time, trust metrics in another window turned to "red", and traffic flows that adversary uses were emphasized by visualization tool.
- The quality of video improved quickly as adversaries were removed from microsegment in verified manner.
- Trust metric changed to "yellow" and after verification to "green".

By the use of the four enablers, we were able to highlight the following points:

- Threats by IoT towards 5G infrastructure/services can be mitigated with by isolating the traffic flows (with SDN based virtualization),
- Access controlled and monitored micro-segments enable quick detection of threats and verified recovery, and
- Service providers and end-users can be made more aware of network's trustworthiness.

8.2.2 Remote IoT heating and alarm system with IMSI hiding mechanism

Alice has incorporated a remote heating and alarm system into her house. This system uses multiple sensors that track different parameters, such as outside and inside air temperature, movement patterns, humidity, etc. Eve - a possible adversary - could do a considerable amount of damage to Alice's house. To maximize the damage, Eve tracks Alice's movements to initiate attack when Alice is not at her home. Tracking is possible if Alice is using the 5G network with her smartphone and her phone is associated with an (unprotected, unencrypted) international mobile subscriber identity (IMSI). This is a unique number for identifying her as subscriber to the 5G network.

For achieving a secure and private service to operate her system, the micro-segmentation enabler created an isolated micro-segment for Alice's service. For access control, the EAP-AKA implementation of the Privacy Enhanced Identity Protection enabler was used. The enabler protected the long term identifier (IMSI) with

asymmetric encryption. In this way, the IMSI is hidden and it is not visible for tracking by possible adversaries. The security monitoring enabler monitored behaviour inside the micro-segment and detected any anomalous behaviour. The trust metric enabler provided information about the trustworthiness of a micro-segment for Alice. If a micro-segment became untrustworthy, Alice was be notified. Since the micro-segment is using EAP-AKA implementation for access control, the trust metric enabler stated that privacy is adequate and trustworthiness of the micro-segment was true.

The B-com side of the test bed was used to host a web service providing user interface to the heating system. The service was located inside a micro-segment.

By the use of the four enablers on a multi-domain testbed, it was possible to show that

1) We can provide services that are isolated and highly secure with strong access control,
2) Privacy can be enhanced with the IMSI hiding mechanism,
3) Service providers and end-users can be made aware of current trust and privacy level, and
4) We have a testbed that enables development of complex end-to-end multi-operator security scenarios.

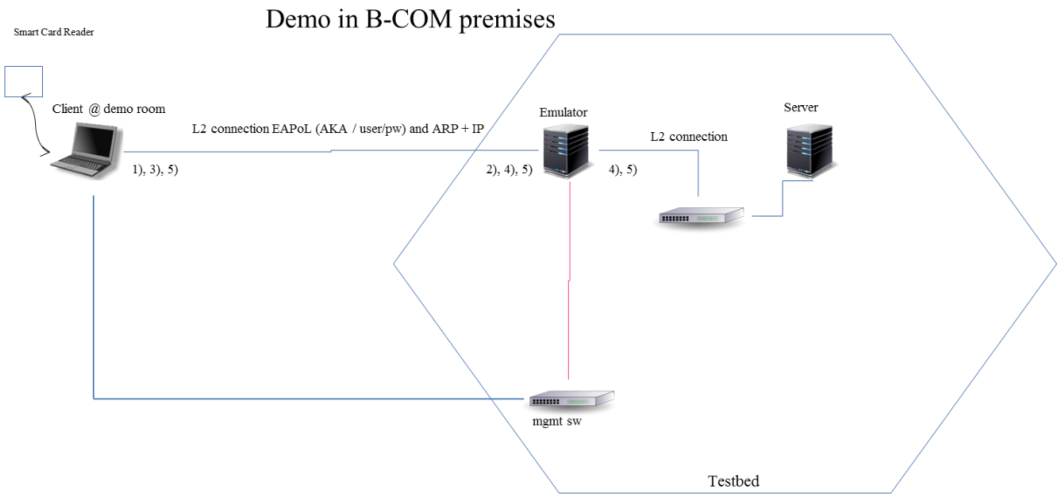
8.2.3 Scenario 3: Micro-segment access based on trust level

The purpose of this demo is to illustrate how micro-segments in a network can have different authentication methods for allowing nodes to access a micro-segment. The trustworthiness level of the micro-segment can also be checked.

The following steps summarize what the scenario will show:

- Unauthenticated UE X wants to access micro-segment A. Authentication is possible either with EAP-MD5 or EAP-AKA authentication method.
- X sends EAP-MD5 or EAP-AKA authentication message to (WLAN) network interface towards Micro-segmentation Enabler (MSE).
- MSE will intercept the EAP-message, checks the authentication status with the help of hostpad/radius.
- If the authentication is successful, and authentication method is valid for that micro-segment, MSE will add that node to the microsegment A.
- X can start sending packets to the microsegment A.
- It is possible to check the Trustworthiness level of the micro-segment by the use of Micro-segment monitoring enabler (MSME) and Trust Metric Enabler (TME).
- Trustworthiness level is shown by printing traffic light to the screen.
- Yellow is shown when EAP-MD5 is used, since the method is lightweight and suitable for IoT but vulnerable for man in the middle attacks.
- Green is shown when EAP-AKA is used, since it provides better privacy.

The demo includes three enablers: MSE, MSME, and TME. MSE is used for creating and deleting micro-segments, adding and deleting nodes from micro-segments, and providing access control to the micro-segment. TME will provide information about the trustworthiness of a micro-segment. MSME will monitor behaviour inside the micro-segment and detect any anomalous behaviour. Figure 9 shows the architecture of the scenario.



Client:
- wpa_supplicant -Dwired (TIIT modified)

Emulator:
- mininet
- hostpad (TIIT modified)
- microsegmentation,
- microsegment monitor
- trust metric

Server:
- web service

Flow
1) start EAP-AKA / EAP-user/pw authentication through EAP over LAN
2) intercept the EAPoL message, check authentication using hostapd. If OK, add to the micro-segment
3) Send ARP request, wait ARP response
4) find the correct end host inside micro-segment. If not found in Mininet, try to find from outside
5) IP packet(s) flow

Figure 9: Scenario architecture.