700416 SUCCESS

D3.12 v1.0

Integration and Validation Plan. Test and certification specifications, V3

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700416.

Project Name	SUCCESS
Contractual Delivery Date:	31.10.2018
Actual Delivery Date:	31.10.2018
Contributors:	ENG, P3C, ISMB, RWTH, SYN
Workpackage:	WP3 - Securing Smart Devices
Security:	PU
Nature:	R
Version:	v1.0
Total number of pages:	67

Abstract:

This deliverable presents the outcome of the SUCCESS consortium work within tasks T3.5 and T3.6, that concentrated on the integration of WP3 components, including the interfacing between the CI-SOC, NORM and the Distribution Grid. This document is mainly focused on the testing activity and describes the execution of the functional tests identified and reported in the previous version of the deliverable, D3.11.

Keyword list:

Security, communication, Utility, Architecture, Threat, Countermeasure, Integration, Validation, Testing

Disclaimer:

All information provided reflects the status of the SUCCESS project at the time of writing and may be subject to change.

Executive Summary

This deliverable documents the current status of the Integration and Validation Plan Test and certification specifications.

It is the third version of deliverable reporting activities related to integration and validation of components developed within Workpackage 3. It updates D3.11 with the execution and the description of the tests identified and reported in the second version of the deliverable.

The testing activity covered by this document has been carried out on the integrated component, i.e. NORM and CI-SOC work together, allowing both a single component validation and pairwise integration. Performed tests enabled also to validate the whole flow of information, from measures detected by smart meters and PMU to messages formatted by the Security Agent on NORM and later received by CI-SOC, that processes them in order to detect potential threats and take appropriate actions to mitigate them.

The same approach on the certification preparation, complete integration and validation of SUCCESS Security solution has been adopted in testing activities described in deliverable D4.9 [1].

Authors

P3C		
	Paschalidis, Panagiotis	Panagiotis.Paschalidis@p3-group.com
ENGINEERING (ENG)		
	Antonello Corsi	antonello.corsi@eng.it
	Giampaolo Fiorentino	giampaolo.fiorentino@eng.it
	Claudia Pandolfo	claudia.pandolfo@eng.it
SYNELIXIS (SYN)		
	Artemis Voulkidis	voulkidis@synelixis.com
Rheinisch-Westfaelische Technische Hochschule Aachen(RWTH)		
	Padraic McKeever	PMcKeever@eonerc.rwth-aachen.de
ISMB		
	Mikhail Simonov	simonov@ismb.it

Table of Contents

1. Introduction

1.1 Scope of this Deliverable

This document is the third and final version of the test and validation plan for integrating and testing SUCCESS components in the area of monitoring and controlling Neighbourhood Area Network (NAN) assets, namely the Next-generation Open Real-time Meter (NORM) and the Critical Infrastructures Security Operations Centre (CI-SOC). It is a natural extension of D3.10 [2], describing the main interactions between the two components in terms of expected behaviour and protocols for communication, and D3.11 [3], that identifies and reports the test cases executed and described in this deliverable.

CI-SOC and NORM constitute the local part of the SUCCESS solution that act as first security layer. The methodology for integrating and testing both NORM and CI-SOC from a logical and functional point of view, that is the subject of [3], is briefly reported for reference in this document as well, together with the description of the test cases, whose execution and results are the outcome of the validation activity and represent the focus of the present deliverable.

The main objective of this document is to validate through testing the interaction between CI-SOC and the NORM, in order to assess they can properly interface and work together in real-life scenarios.

The main audience of the present deliverable is represented by the SUCCESS project partners, as responsible for components involved in the testing activities or for the certification processes followed during the integration and validation activities.

In addition to them, this document could be of potential interest to the following Smart Grid actors:

Utilities / Critical Infrastructures Operators

Utilities and critical infrastructure operators could be interested in checking whether their current software and hardware portfolio satisfies the advanced security specifications through the tests identified and executed during the activities described in this deliverable and in its previous versions.

Smart grid assets manufacturers

They could be interested in evaluating whether their products are able to support SUCCESS solutions.

Smart metering products manufacturers

NORM, one of SUCCESS' primary offerings, is a flexible combination of an open hardware platform (Raspberry PI3 [4]) coupled with advanced software and hardware services to support modern and legacy smart meters. Certification against the identified integration requirements would imply compliance to a large range of smart meters and services, as well as to the security guidelines as identified by the SUCCESS security experts.

1.2 Relationship to the work of the project

This deliverable is directly related to the activities performed by the SUCCESS consortium within WP3, in the context of securing the Smart Grid at NAN level:

- Task 3.3 - “DSO Security Monitoring Centre”, since this document is focused on the tests executed on the overall CI-SOC;
- Task 3.4 - “Development of next generation Smart Meter for trials (NORM)”, because also the components composing the NORM have been extensively tested;
- Task 3.5 - “Information Security Management Integration and Testing”, since the integration planning and testing is the activity detailed in this deliverable;

- Task 3.6 - “Certification feature catalogue, feature specifications and test plans”, since they share context with regards to both feature catalogue and specifications and test plans, better described in the previous version of this document, D3.11 [3]

From the certification perspective, this deliverable is also loosely coupled with the certification centre activities carried out in Task 6.2.

The methodology and structure followed in the Integration, Testing and certification activities has been also adopted in D4.9 [1].

1.3 How to Read This Document

This deliverable updates and deprecates D3.11 [3], that targets the identification of test cases for NAN assets that fare of interest to SUCCESS. The main difference with the previous version of this deliverable is the outcome of the Validation and Test activity, i.e. the results of the identified test cases.

Section 2 gives an overview of the test and certification methodology adopted in the validation and testing activity. It has been already illustrated in the previous version of this deliverable and has been reported for completeness.

Section 3 reports the test cases identified and defined in [3]. Acronyms used to identify functionalities and test cases have been modified to reflect DSOSMC renaming to CI-SOC, therefore the final test cases description is intended to be the one included in the present document.

Annex A can be used as a quick reference to test cases, while test results are presented in Annex B.

Assisting the comprehension of the present results and their importance under a holistic security by design approach, the interested reader is requested to refer to deliverable D4.2 [5] that presents the SUCCESS Security Solution architecture and offers a high-level introduction on the SUCCESS project mission, goals and approach. Deliverable D3.14 [6] documents the individual testing activities and specifications and acts as the basis of the integrated features definitions. For a further understanding of the features and technical specifications, D3.6 [7] offers details on CI-SOC design and implementation. With regard to NORM, its technical specification can be found in D3.9 [8], which provide information related to the NORM specifications. Lastly, a good understanding of D1.2 [4] is required to be aware of the core threats against which the SUCCESS Security Solution intends to offer protection, documented as the features described in the aforementioned deliverables

2. Integration and validation test and certification methodology

Building on the output of deliverables D3.10[2], D3.11[3] and D3.14 [6], yet under an integrated functionality perspective, this deliverable largely follows the methodology documented in D3.14 [6]. Integrated validation and testing will be pursued in two directions, namely on the basis of:

1. pairwise, interface-level testing among the various components, effectively performing in a real environment the individual tests described in D3.14 [6] (many times assisted by simulated component functionality);
2. integrated testing among the various components, essentially validating the logical functionality of the SUCCESS NAN- and DSO-level developments, covering the co-existence of NORM and CI-SOC.

With respect to the second point, since the focus of this deliverable is put on the NAN level assets of the Smart Energy Grid (NORM, in particular), and the security infrastructure managing their security context (in the context of the SUCCESS Security solution, the CI-SOC), only the relevant functionalities are being discussed, leaving the discussion on the integration and validation test and certification methodology related to CI-SOC and the rest of the SUCCESS components (excluding NORM) to deliverable D4.9 [1].

With respect to pairwise testing, this may include testing:

1. the interfacing of sub-components inside the same component (e.g. testing that the CI-SOC Monitoring component is able to actually communicate with CI-SOC Analytics component, as described in D3.6 [7]) or
2. the interfacing of specific components residing in NORM and CI-SOC (e.g. test that the local NORM Physically Unclonable Function agent is able to properly communicate with an instance of the CI-SOC Key Management Module – see D3.14 [6], D3.6 [7], D3.9 [8]).

The relevant features for the pairwise testing have been documented in D3.10 [2] and are, therefore, left out of the analysis of the present document.

With respect to integrated testing, the pairwise testing pertains to validating that the logic behind a realistically-framed scenario covering end-to-end functionalities is properly implemented. Evidently, the integrated testing should consider scenarios where the maximum possible set of independent functionalities is tested, spanning operations from both NORM and CI-SOC components.

2.1 Adopted methodology

The methodology for defining and documenting the integration and validation test and certification procedures will follow the pattern extensively documented in D3.14 [6], naturally focusing on an integrated approach rather than a stand-alone, component-sandboxed perspective followed by D3.14 [6].

The test and certification specifications will follow a step-wise approach composed of eight steps as follows:

1. Identification of integrated smart grid components to be tested
2. Grouping of functional features
3. Identification of functional features of identified, integrated components
4. Mapping of the integrated components' functional features to technical specifications
5. Definition of test templates
6. Specification of test cases
7. Define test and certification time schedule
8. Test cases validation

It should be highlighted that step 5 pertaining to the definition of the test templates has already been conducted in the context of [2]. However, the updated templates of [6] are adopted in this deliverable. Similarly, the tables presenting the technical specifications in this deliverable follow the structure of the templates adopted in [6].

2.2 Application of the methodology to SUCCESS developments

2.2.1 Identification of integrated smart grid components to be tested

In the context of integration and validation testing and certification specification processes that this document addresses, the integrated smart grid components of interest are the CI-SOC and the NORM. For naming reasons, the integrated system referring to their coordinated interfacing is notated as *CSNM*[1]. This notation has been changed as a consequence of having renamed DSOSMC in CI-SOC. Since DSOSMC has been renamed in CI-SOC all notations and acronym including DSOSMC have been changed as a consequence. Because this document updates the previous versions of this deliverables, the notations to refer to for testing are the ones used here and reported in the following sections.

2.2.2 Grouping of functional features

The groups of functional features have been extensively documented in [9] (Table 4) and are tabulated below for reasons of document clarity.

Table 1: SUCCESS groups of functional features

ID	Title	Description
G1	AAA	Authentication, authorization and accounting features. Though not all of these may be supported (e.g. accounting), mechanisms to ensure that unauthorized access to any kind of service or data is prohibited should be implemented.
G2	Streams protection	Features related to the protection of the data residing within a shared medium, be it a transmission link or a physical storage device (e.g. a hard disk).
G3	Metering services	As the core concept of SUCCESS Security Solution is based on the continuous monitoring of non-personal, network data such as voltage, frequency, etc., the existence of metering services is considered necessary. In this group, such services residing at devices level are classified.
G4	State monitoring	This group pertains to the non-device oriented counterparts of the metering services, namely systems that can evaluate the metering services output and assess the security status of the grid.
G5	Asset management	Features related to managing the behaviour of various assets of the Smart Grid, spanning from devices at NAN level up to pan-European security monitoring entities.
G6	Time synchronization	As SUCCESS evangelizes that the large-scale use of PMUs is beneficial to the security monitoring processes, this group is related to ensuring that proper services for time synchronization are deployed at PMU level.
G7	Threats management	Features related to identifying and assessing threats. This group includes the local security agent of NORM, as well as

[1] CSNM stands for CISOC ↔ NORM. In [3] this interaction was indicated with the acronym DSNM (representing DSOSMC↔NORM)

		the threat identification processes of the CI-SOC and the E-SMIS (though the latter is out of the context of this document)
G8	Countermeasures management	This group includes the broad countermeasures-related features. In SUCCESS, countermeasures are meant to be managed at CI-SOC and ESMC level.
G9	User Interaction	This group includes features related to handling the control of a component behaviour to the component end-user through user-friendly interfaces.
G10	End-to-end	Generic group referring to functional features referring to multiple groups and features. Should be used for rationality and overall functionality checking only.

2.2.3 Identification of functional features of identified, integrated components

In the framework of two-level testing and certification specification, the interface-level pairwise functional features are defined as the combination of the individual component features documented in [9]. The relevant (fused) features are tabulated below.

Table 2: CSNM Features

CSNM feature ID	CSNM feature name	§
CSNM:G1:F1	Authentication of Physically Unclonable Functions (PUF)-enabled NORM devices	2.2.3.1
CSNM:G1:F2	Periodic update of the active challenge-response pair (CRP) of PUF-enabled NORM devices	2.2.3.2
CSNM:G2:F1	Encryption and decryption of reported data	2.2.3.3
CSNM:G2:F2	Channel encryption	2.2.3.4
CSNM:G3:F1	Integrated NORM metrology services	2.2.3.5
CSNM:G7:F1	Support for standard security services	2.2.3.6
CSNM:G10:F1	Mitigation of incidents implying compromise of the SMM or the low-cost PMU module of NORM devices	2.2.3.7
CSNM:G10:F2	Mitigation of incidents implying malware/virus infection on the NORM devices	2.2.3.8
CSNM:G10:F3	Mitigation of incidents where remote software attestation fails	2.2.3.9
CSNM:G10:F4	Mitigation of incidents where remote hardware attestation fails	2.2.3.10
CSNM:G10:F5	Mitigation of incidents where firewall configuration is unexpected	2.2.3.11
CSNM:G10:F6	Mitigation of incidents where NORM devices are unavailable	2.2.3.12

CSNM:G10:F7	Mitigation of incidents where NORM devices cannot authorize themselves	2.2.3.13

In the following subsections, the descriptions of the integrated CSNM functional features mentioned in Table 2 are provided.

As pointed out in section 2.2.1, due to renaming DSOSMC to CI-SOC, notations have been modified; the base CI-SOC features are now identified with the following format: CISOC:G_i:F_i, where G_i indicates a group of functional feature and F_i a functional feature itself.

2.2.3.1 Feature CSNM:G1:F1 – Authentication of PUF-enabled NORM devices

Base Features: CISOC:G1:F1, NORM:G1:F1

Feature Type: Pairwise

Consolidating the functional features CISOC:G1:F1 and NORM:G1:F1, this integrated functional features refers to the ability of the CI-SOC and the NORM to interwork with a view to leverage on the hardware security capabilities granted to NORM by the PUF module [8]. This interworking includes the ability of CI-SOC to i) bootstrap NORM devices, ii) manage the CRPs of the supported NORM devices and iii) verify their authenticity effectively implementing NORMs authentication, authorization and accounting (AAA).

2.2.3.2 Feature CSNM:G1:F2 – Periodic update of the active CRP of PUF-enabled NORM devices

Base Features: CISOC:G1:F2, NORM:G1:F1

Feature Type: Pairwise

As per CISOC:G1:F2, the CI-SOC should be able to periodically or on-demand update the active CPR of the NORM devices supported by the CI-SOC instance.

2.2.3.3 Feature CSNM:G2:F1 – Encryption and decryption of reported data

Base Features: CISOC:G2:F1, NORM:G2:F1

Feature Type: Pairwise

As reported in [9][7][8] the NORM devices should be able to send encrypted data to the CI-SOC as a further security measure on top of the communication channel encryption (see §2.2.3.4 for details). The encryption of the data should be performed by the PUF hardware security module integrated in the NORM (with the help of the Security Agent on NORM), whereas the decryption of the data should be performed on the CI-SOC side (with the help of the KMM).

2.2.3.4 Feature CSNM:G2:F2 – Channel encryption

Base Features: NORM:G2:F5

Feature Type: Pairwise

The communications between the NORMs and the entities receiving the measured data (e.g. metrology, PMU-related, configuration etc.) should be performed over encrypted channels to ensure that the communications cannot be overheard by threat agents applying man-in-the-middle or eavesdropping attacks[10]. This feature, together with CSNM:G2:F1 would ensure that the SUCCESS Security solution features 2-level encryption on the devices-reported data streams.

2.2.3.5 Feature CSNM:G3:F1 – Integrated NORM metrology services

Base Features: CISOC:G2:F1, CISOC:G4:F1, NORM:G2:F1, NORM:G2:F3, NORM:G2:F4, NORM:G3:F1, NORM:G3:F2

Feature Type: Pairwise, End to end depending on the configuration

A NORM device should be able to report to the CI-SOC (possibly other actors as well, depending on the currently active policy for data reporting [8]) an encrypted set of meaningful measurements originating from either the integrated Smart Meter (metrology data) or the integrated low-cost PMU. On the other side, the CI-SOC should be in the position to, first, decode the data (see §2.2.3.3), then properly handle them (this includes data pre-processing and storage).

2.2.3.6 Feature CSNM:G7:F1 – Support for standard security services

Base Features: CISOC:G7:F1, NORM:G7:F2, NORM:G7:F3, NORM:G7:F4, NORM:G7:F5

Feature Type: Pairwise

The NORMs should expose interfaces that make feasible their remote security attestation by the CI-SOC services. These security attestation capabilities should guarantee that the CI-SOC is able to:

- Retrieve information or notifications about the integrity of the software deployed on each NORM (NORM:G7:F2);
- Retrieve information or notifications about the hardware integrity of the NORM per se (NORM:G7:F3);
- Retrieve information or notifications about the antivirus software activity running on the NORM devices (NORM:G7:F4);
- Assess and/or retrieve information or notifications about the security status of the firewall running on the NORM devices (NORM:G7:F5);
- Retrieve the log file of the NORM security services.

This data should be used by the CI-SOC Analytics module (see [7] for details) to derive the security status of each supported NORM device.

2.2.3.7 Feature CSNM:G10:F1 – Mitigation of incidents implying compromise of the SMM or the low-cost PMU module of NORM devices

Base Features: CSNM:G1, CSNM:G2, CSNM:G3, CSNM:G7, CISOC:G4, CISOC:G7, CISOC:G8, NORM:G3

Feature Type: End to end

Incident ID: N/A

The CI-SOC should be in a position to understand that a certain set of NORMs have been compromised, by means of exploiting features CSNM:G1, CSNM:G2, CSNM:G3, CSNM:G7 as well by means of applying advanced monitoring and analytics (CISOC:G4, CISOC:G7) and algorithmic processes to detect situations that might imply the emergence of a security incident, as described in [11], pertaining to manipulation of either the SMM or the low-cost PMU (abnormal measurements activity). Upon detection of such a situation, the CI-SOC should select the appropriate countermeasures strategy to mitigate the identified threat (CISOC:G8), e.g. by temporarily disconnecting the meter.

2.2.3.8 Feature CSNM:G10:F2 – Mitigation of incidents implying malware/virus infection on the NORM devices

Base Features: CSNM:G7:F1, NORM:G7:F4

Feature Type: End to end

Incident ID: CS-4

The CI-SOC should be able to understand that a certain set of NORMs has been compromised by malware, rootkits or viruses, by means of exploiting features CSNM:G7:F1 and all features falling under NORM:G7:F4. Upon detection of such a situation, the CI-SOC should select the appropriate countermeasures strategy to mitigate the identified threat (CISOC:G8), e.g. by enforcing periodic antimalware, anti-rootkit and antivirus checks and instructing the relevant software signatures updates more frequently, until the problem is resolved. This feature relates to Incident-Countermeasure CS-4 as defined in [11].

2.2.3.9 Feature CSNM:G10:F3 – Mitigation of incidents where remote software attestation fails

Base Features: CSNM:G7:F1, NORM:G7:F2

Feature Type: End to end

Incident ID: CS-2

The NORM has local software attestation capabilities (NORM:G7:F2) which should be exposed to the CI-SOC either in the form of an API, or in the form of a report, so that the latter may act as deemed appropriate (CSNM:G7:F1). In case the software attestation fails, the CI-SOC should send a disconnection command to the NORM, then either try to re-flash the correct software image to the NORM filesystem or send a physical maintenance unit to do it. In all cases, the NORM authentication credentials (active CRP) should be reset to ensure secure and private communications. This feature relates to Incident-Countermeasure CS-2 as defined in [11].

2.2.3.10 Feature CSNM:G10:F4 – Mitigation of incidents where remote hardware attestation fails

Base Features: CSNM:G7:F1, NORM:G7:F3

Feature Type: End to end

Incident ID: PS-2

Similar to CSNM:G10:F3, but referring to hardware attestation (e.g. case opening or equipment replacement). As the NORM features mechanisms (implemented by the local security agent, feature NORM:G7:F3) to identify its hardware configuration status, this information should be acknowledged to the CI-SOC. In case such an unplanned hardware configuration change is detected, the CI-SOC should send a disconnection command to the NORM, then send a physical maintenance unit to check and repair the configuration of the compromised NORM device(s). In all cases, the NORM authentication credentials (active CRP) should be reset to ensure secure and private communications. This feature relates to Incident-Countermeasure PS-2 as defined in [11].

2.2.3.11 Feature CSNM:G10:F5 – Mitigation of incidents where firewall configuration is unexpected

Base Features: CSNM:G7:F1, NORM:G7:F5

Feature Type: End to end

Incident ID: N/A

Similar to CSNM:G10:F2, but referring to the status of the firewall of the NORM devices; since the NORM needs to integrate with the CI-SOC and other services and actors, several network ports would need to be open in order to allow the internal NORM services to communicate with the corresponding external services. In any case, the configuration of the firewall should be the same for all NORM devices. If a port scanning indicates that the default configuration has been altered (e.g. leaving more ports in a listening state), then a command to reset the firewall configuration should be sent to the NORM device(s).

2.2.3.12 Feature CSNM:G10:F6 – Mitigation of incidents where NORM devices are unavailable

Base Features:	CSNM:G7:F1, CI-SOC:G4:F1, CI-SOC:G7:F1
Feature Type:	End to end
Incident ID:	PS-3, PS-4, PS-5

There are multiple reasons why a NORM device is not available (namely direct communication with it is not possible), including communication links failure, power supply failure or other, unknown generic reason failure. In the case that a NORM device is found to be unreachable, then the CI-SOC, having acknowledged the issue, should send an alert to the Utility security staff through the Dashboard that a maintenance unit should be sent on-site to fix the issue. This feature relates to Incident-Countermeasure PS-3, PS-4 and PS-5 as defined in [11].

2.2.3.13 Feature CSNM:G10:F7 – Mitigating incidents where NORM devices cannot authorize themselves

Base Features:	CSNM:G1, CSNMM:G2, CSNM:G7:F1, CISOC:G1, CISOC:G2, NORM:G1, NORM:G2
Feature Type:	End to end
Incident ID:	CS-3

This feature refers to cases where the validation of the NORM devices fails, or there emerge repeating decryption service failures, indicating that either the synchronization of the PUF component of the NORMs has been broken, or the PUF hardware security module has been compromised/replaced/broken. In every case, the CI-SOC services should be able to detect the issue and accordingly i) try to re-establish the authentication synchronization with the NORM by activating a new CRP or ii) send a maintenance unit to check the NORM physically. This feature relates to Incident-Countermeasure CS-3 as defined in [11].

3. Integrated CI-SOC and NORM testing and validation

3.1.1 Technical Specifications

The technical specifications of NORM and CI-SOC have been extensively documented in [8] [7] and their presentation is excluded in this document for conciseness. For CSNM, no further technical specification can be provided as it refers to the fusion of the functionalities of the two above components, without offering any additional functionality.

3.1.2 Test templates

The test template used for testing has been provided in [9] and will be adopted as such.

3.1.3 Test cases

Test cases defined in [3] are reported in the following sections. The new notation[2], due to renaming DSOSMC to CI-SOC, has been used.

An overall test reference is reported in Annex A. Test results are documented in Annex B.

3.1.3.1 Test cases for feature CSNM:G1:F1

Table 3: Test case CSNM:G1:F1:T1

Test ID	CSNM:G1:F1:T1		
Test Description	Test that the CI-SOC can bootstrap a PUF-enabled NORM, by registering sets of CRP.		
Test location	At the premises of SYN	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G1:F1		
Product requirement	The CI-SOC should be able to bootstrap a NORM device.		
Test environment	An active CI-SOC instance and a NORM device.		
Preparation	N/A		
Dependencies	N/A		
Steps	1. The NORM should send a message to the CI-SOC KMM indicating that it needs to be bootstrapped, specifying its ID; 2. The CI-SOC KMM sends a list of 5000 distinct challenges to the NORM; 3. NORM responds to the CI-SOC KMM with 5000 different response strings; 4. The KMM registers 5000 pairs of challenge-response strings in its challenge-response database.		
Pass criteria	5000 distinct challenge-response are stored in the challenge-response database of the KMM.		
Suspension criteria	N/A		

[2] DSNM → CSNM and DSOSMC → CISOC

Table 4: Test case CSNM:G1:F1:T2

Test ID	CSNM:G1:F1:T2		
Test Description	Test that the CI-SOC KMM can identify a PUF-enabled NORM device.		
Test location	At the premises of SYN.	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G1:F1		
Product requirement	The CI-SOC should be able to uniquely identify a NORM device.		
Test environment	An active CI-SOC instance and at least two NORM devices.		
Preparation	N/A		
Dependencies	Test case CSNM:G1:F1:T1 should have been successfully executed right before this test, considering at least two NORM devices		
Steps	1. The two NORM devices are fed with a set of active challenges, based on the set of CRPs already stored in the Key Management module challenge-response database as of test CISOC:G1:F1:T1 2. The two NORM devices attempt to validate themselves using false response strings; 3. The two NORM devices attempt to validate themselves using correct response strings; 4. Repeat the above for at least 1000 times		
Pass criteria	The CI-SOC KMM is able to correctly validate the two NORM devices.		
Suspension criteria	N/A		

3.1.3.2 Test cases for feature CSNM:G1:F2

Table 5: Test case CSNM:G1:F2:T1

Test ID	CSNM:G1:F2:T1		
Test Description	Test whether the CI-SOC can refresh the active PUF challenge of the various NORMs deployed on the field.		
Test location	At the premises of SYN	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G1:F2		
Product requirement	The authentication configuration of the various metering devices supported should be periodically and often updated.		
Test environment	An active CI-SOC instance and at least two NORM devices.		
Preparation	N/A		

Dependencies	Test cases CSNM:G1:F1:T1 and CSNM:G1:F1:T2 should have been successfully executed right before this test, considering at least two NORM devices.
Steps	1. Configure the CI-SOC KMM to update the PUFs active challenge every 1 minute; 2. Record the active challenge of the fake PUFs every minute; 3. Compare the (each minute) recorded active challenges of the fake PUFs with the corresponding challenges sent by the KMM.
Pass criteria	At any given moment, the active challenge of a PUF should be different than the one in the minute before and should match the one designated by the CI-SOC KMM.
Suspension criteria	N/A

3.1.3.3 Test cases for feature CSNM:G2:F1

Table 6: Test case CSNM:G2:F1:T1

Test ID	CSNM:G2:F1:T1		
Test Description	Test whether data reported by the NORM devices are encrypted and can be decrypted by the CI-SOC if they have not been tampered with.		
Test location	At the premises of SYN	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G2:F1		
Product requirement	The CI-SOC should be able to decrypt messages encrypted by the NORM PUF hardware security mechanism.		
Test environment	An active CI-SOC instance and at least two NORM devices.		
Preparation	A predefined message to be encrypted should have been agreed upon.		
Dependencies	All test cases referring to features belonging to CSNM:G1 should have been successfully applied.		
Steps	1. The CI-SOC bootstraps and periodically updates the active challenges of the NORM PUF modules; 2. The NORM devices encrypt the predefined message structure and send it to the CI-SOC; 3. The CI-SOC should be able to decrypt the message;		
Pass criteria	The decrypted message matches the pre-defined one.		
Suspension criteria	N/A		

Table 7: Test case CSNM:G2:F1:T2

Test ID	CSNM:G2:F1:T2		
Test Description	Test whether on-channel data tampering is possible to be detected by the CI-SOC.		
Test location	At the premises of SYN	**Partner**	SYN
Component	CI-SOC, NORM		

Features under test	CSNM:G2:F1
Product requirement	The CI-SOC should be able to detect if the messages sent by the NORM devices have been tampered with on-channel (detect man-in-the-middle attacks)
Test environment	An active CI-SOC instance and at least two NORM devices.
Preparation	A predefined message to be encrypted should have been agreed upon. Also, a service emulating a threat agent listening to the channel (e.g. having broken the VPN connection between the NORM and the CI-SOC) should be available.
Dependencies	All test cases referring to features belonging to CSNM:G1 should have been successfully applied.
Steps	1. The CI-SOC bootstraps and periodically updates the active challenges of the NORM PUF modules; 2. The NORM devices encrypt the predefined message structure and feeds a third-party service emulating the threat agent; 3. The threat agent emulating service alters the message, changing either the NORM ID, or the encrypted message string, or the timestamp of the encryption reported; 4. The threat agent emulating service forwards the altered message to the CI-SOC for decryption; 5. The CI-SOC should be able to detect the message manipulation and raise an alarm;
Pass criteria	The CI-SOC identifies the decryption failure indicating data manipulation.
Suspension criteria	N/A

3.1.3.4 Test cases for feature CSNM:G2:F2

Table 8: Test case CSNM:G2:F2:T1

Test ID	CSNM:G2:F2:T1		
Test Description	Ensure ability of the NORM to connect through a VPN-encrypted channel to the CI-SOC granted that the credentials and installed certificates are valid.		
Test location	In the premises of REC	**Partner**	REC
Component	CI-SOC, NORM		
Features under test	CSNM:G2:F2		
Product requirement	N/A		
Test environment	An active CI-SOC instance and at least two NORM devices, all configured to connect to the same OpenVPN service.		
Preparation	Configure the OpenVPN client on the NORM and the CI-SOC to use a set of valid credentials and a set of valid certificates.		
Dependencies	N/A		
Steps	1. Power up the NORM and the CI-SOC and set the OpenVPN client to auto-start on boot; 2. Try to connect to the OpenVPN service;		

	3. Ensure that the connection was successful (a new virtual interface has been created in both NORM and CI-SOC, holding an IP address different than the IP address of the NORM physical networking interface). 4. Ensure that the NORM can communicate with the DSOSCM (e.g. executing CSNM:G1:F2:T1).
Pass criteria	The NORM and the CI-SOC can communicate properly, their channel being VPN-encrypted.
Suspension criteria	N/A

3.1.3.5 Test cases for feature CSNM:G3:F1

Table 9: Test case CSNM:G3:F1:T1

Test ID	CSNM:G3:F1:T1		
Test Description	Smart metrology metering services refer to the fact that NORM can extract the metrology related data from its SMM component, which are available for readout from actors having the right to access this data and send the relevant data to the CI-SOC.		
Test location	In the premises of REC	**Partner**	REC
Component	CI-SOC, NORM		
Features under test	CSNM:G3:F1		
Product requirement	The CI-SOC should be able to receive SMM data from the NORM SMM services.		
Test environment	An active CI-SOC instance and at least one NORM device is assumed, configured to use one metrology meter used in the project.		
Preparation	Ensure that the SMM is correctly attached to the NORM.		
Dependencies	N/A		
Steps	1. Power up the NORM and wait a period of at least one week gathering data and sending them encrypted to the CI-SOC; 2. Enter in the system with administrator rights and download the file with the records; 3. Perform readout of energy indexes from the log file; 4. Compare the indexes from file with the indexes received by CI-SOC.		
Pass criteria	The indexes from two sources are the same for the same timestamp.		
Suspension criteria	N/A		

Table 10: Test case CSNM:G3:F1:T2

Test ID	CSNM:G3:F1:T2		
Test Description	The same as CSNM:G3:F1:T1 but with respect to low-cost PMU measurements		
Test location	In the premises of RWTH	**Partner**	RWTH
Component	CI-SOC, NORM		
Features under test	CSNM:G3:F1		

Product requirement	The CI-SOC should be able to receive PMU data from the NORM low-cost PMU services.
Test environment	An active CI-SOC instance and at least one NORM device is assumed, configured to use a low-cost PMU.
Preparation	Ensure that the low-cost PMU has been successfully attached to the NORM device and configure it to send at least 10 messages/second.
Dependencies	The tests CSNM:G2:F1:T1 and all tests falling under CSNM:G1 should have been successfully executed.
Steps	1. Power up the NORM and wait for at least one day sending encrypted PMU data to the CI-SOC; 2. Collect the data recorded by the low-cost PMU; 3. Compare the data retrieved by the NORM with the ones received by CI-SOC.
Pass criteria	The indexes from two sources are the same for the same timestamp.
Suspension criteria	N/A

Table 11: Test case CSNM:G3:F1:T3

<table>
<tr><td><b>Test ID</b></td><td colspan="3">CSNM:G3:F1:T3</td></tr>
<tr><td><b>Test Description</b></td><td colspan="3">Test the ability of the CI-SOC to handle multiple data streams coming at high rates.</td></tr>
<tr><td><b>Test location</b></td><td>At the premises of REC</td><td><b>Partner</b></td><td>REC, RWTH, ENG, SYN</td></tr>
<tr><td><b>Component</b></td><td colspan="3">CI-SOC, NORM</td></tr>
<tr><td><b>Features under test</b></td><td colspan="3">CSNM:G3:F1</td></tr>
<tr><td><b>Product requirement</b></td><td colspan="3">The CI-SOC Monitor module should be able to handle a high traffic of incoming messages.</td></tr>
<tr><td><b>Test environment</b></td><td colspan="3">An active CI-SOC instance and at least ten NORM devices are assumed, configured to use a low-cost PMU.</td></tr>
<tr><td><b>Preparation</b></td><td colspan="3">Same as CSNM:G3:F1:T2</td></tr>
<tr><td><b>Dependencies</b></td><td colspan="3">The tests CSNM:G2:F1:T1, CSNM:G3:F1:T2 and all tests falling under CSNM:G1 should have been successfully executed.</td></tr>
<tr><td><b>Steps</b></td><td colspan="3">1. Configure the NORM devices to send at least 10 data packets every second for at least 1 hour;
2. Check that all packets were processed (encrypted, transferred and decrypted at the CI-SOC backend) as expected.</td></tr>
<tr><td><b>Pass criteria</b></td><td colspan="3">All packets should have been successfully retrieved and processed by the Monitor module.</td></tr>
<tr><td><b>Suspension criteria</b></td><td colspan="3">There might be cases where physical resources are simply not enough to accommodate the injected traffic. In this case, scalability of the solution should be tested on IT infrastructures of larger capacity else. The correspondence between IT capacity and traffic should be researched and discussed.</td></tr>
</table>

Table 12: Test case CSNM:G3:F1:T4

Test ID	CSNM:G3:F1:T4

Test Description	Test the ability of CI-SOC to handle data streams containing irrelevant information.		
Test location	At the premises of RWTH	**Partner**	ENG, REC, RWTH, SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G3:F1		
Product requirement	The CI-SOC should only analyse data that are relevant.		
Test environment	An active CI-SOC instance and at least ten NORM devices are assumed.		
Preparation	Same as CSNM:G3:F1:T2 or CSNM:G3:F1:T3, assuming that all NORMs have been configured to send irrelevant data at random times.		
Dependencies	N/A		
Steps	1. Configure the NORM devices to send irrelevant data at a percentage of 10% of the messages sent. The message emission rate can be at the range of 10 messages per second; 2. Run the service for at least 1 week; 3. Check if all relevant data have been processed and irrelevant data have been discarded.		
Pass criteria	All relevant data should have been processed whereas all irrelevant data should have been discarded.		
Suspension criteria	N/A		

3.1.3.6 Test cases for feature CSNM:G7:F1

Table 13: Test case CSNM:G7:F1:T1

Test ID	CSNM:G7:F1:T1		
Test Description	Check if NORM can perceive changes in its software configuration and accordingly alert the CI-SOC.		
Test location	At the premises of ENG	**Partner**	ENG
Component	CI-SOC, NORM		
Features under test	CSNM:G7:F1		
Product requirement	The CI-SOC should be able to be aware of the software status on the NORM side (either performing remote software attestation or by means being notified about the result of a local software attestation).		
Test environment	An active CI-SOC instance and a NORM device are assumed.		
Preparation	Two files should be a priori available to the NORM, one completely new to the overall NORM software stack and one constituting a slight change to an existing/well known file of the NORM software.		
Dependencies	The tests CSNM:G3:F1:T2 and all tests falling under CSNM:G1 should have been successfully executed		
Steps	1. Perform a software attestation to check that everything is normal on the current NORM configuration; 2. Add a new executable file (script or binary) in the NORM filesystem; 3. Perform software attestation and let the CI-SOC know about the result;		

	4. Remove the file and replace another file with an alteration; 5. Perform software attestation and let the CI-SOC know about the result; 6. Replace the altered file with the original; 7. Perform software attestation and let the CI-SOC know about the result.		
Pass criteria	Steps 3 and 5 should indicate that the filesystem has changed. Step 7 should report that the NORM condition is normal.		
Suspension criteria	N/A		

Table 14: Test case CSNM:G7:F1:T2

Test ID	CSNM:G7:F1:T2		
Test Description	Check that the NORM is able to identify changes in its overall integrated configuration and accordingly alert the CI-SOC.		
Test location	At the premises of ENG	**Partner**	ENG, REC, RWTH, SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G7:F1		
Product requirement	The CI-SOC should be able to be aware of the hardware status on the NORM side (either performing remote hardware attestation or by means being notified about the result of a local hardware attestation).		
Test environment	An active CI-SOC instance and a NORM device are assumed.		
Preparation	N/A		
Dependencies	The tests CSNM:G3:F1:T2 and all tests falling under CSNM:G1 should have been successfully executed		
Steps	1. Verify the validity of the NORM/SMM/PUF configuration; 2. Alter the configuration by replacing one of the above elements; 3. Verify that the change is detected and appropriately reported to the CI-SOC; 4. Repeat steps 2-3 until all possible alteration combinations have been tested.		
Pass criteria	The change is always detected and the CI-SOC is aware of the change.		
Suspension criteria	N/A		

Table 15: Test case CSNM:G7:F1:T3

Test ID	CSNM:G7:F1:T3		
Test Description	The NORM should be protected by an antivirus mechanism and the CI-SOC should be aware of its status		
Test location	At the premises of SYN	**Partner**	ENG, SYN, REC
Component	CI-SOC, NORM		
Features under test	CSNM:G7:F1		

Product requirement	NORM should be protected by an antivirus software without affecting real-time actions and the CI-SOC should be aware of threats detected.
Test environment	An active CI-SOC instance and a NORM device are assumed.
Preparation	N/A
Dependencies	The tests CSNM:G3:F1:T2 and all tests falling under CSNM:G1 should have been successfully executed.
Steps	1. Run an antivirus scan; 2. Check if the virus has been detected and the CI-SOC has been notified.
Pass criteria	The virus should have been detected and removed (quarantined) and the CI-SOC informed.
Suspension criteria	The NORM does not have enough resources to run the antivirus software. In this case, other options may be analysed, such as external analysis by a trusted party.

Table 16: Test case CSNM:G7:F1:T4

Test ID	CSNM:G7:F1:T4		
Test Description	The NORM should be protected by a firewall and the CI-SOC should be aware of its state.		
Test location	At the premises of SYN	**Partner**	ENG, SYN, REC
Component	NORM		
Features under test	CSNM:G7:F1:T4		
Product requirement	All NORM traffic should be protected by a firewall software and CI-SOC should be aware of the status of the NORMs firewall.		
Test environment	An active CI-SOC instance and a NORM device are assumed.		
Preparation	N/A		
Dependencies	The tests CSNM:G3:F1:T2 and all tests falling under CSNM:G1 should have been successfully executed		
Steps	1. Retrieve from the CI-SOC the list of ports that should be open; 2. Scan all ports of the NORM and send a report to the CI-SOC if a port that does not belong to the list of a-priori known ones is open.		
Pass criteria	All ports should be closed except for the a-priori known ones; in any other case, an alert is sent to the CI-SOC.		
Suspension criteria	N/A		

Table 17: Test case CSNM:G7:F1:T5

Test ID	CSNM:G7:F1:T5
Test Description	Ensure that the CI-SOC is able to retrieve the logs of the security components of the NORM

Test location	In the premises of SYN	**Partner**	SYN, ENG
Component	CI-SOC, NORM		
Features under test	CSNM:G7:F1		
Product requirement	The CI-SOC should be able to retrieve security logs from the NORM.		
Test environment	An active CI-SOC instance and a NORM device are assumed.		
Preparation	N/A		
Dependencies	The tests CSNM:G3:F1:T2 and all tests falling under CSNM:G1 should have been successfully executed.		
Steps	1. Select a NORM from the CI-SOC dashboard and ask for their logs; 2. The logs should be properly retrieved.		
Pass criteria	The NORM logs should be available to the CI-SOC.		
Suspension criteria	N/A		

3.1.3.7 Test cases for feature CSNM:G10:F1

Table 18: Test case CSNM:G10:F1:T1

Test ID	CSNM:G10:F1:T1		
Test Description	Disconnection of NORM devices with compromised SMM or low-cost PMU[3]		
Test location	At the premises of ENG	**Partner**	ENG, SYN, REC, ISMB
Component	CI-SOC, NORM		
Features under test	CSNM:G10:F1		
Product requirement	The CI-SOC should be able to deduce that a certain set of NORMs has been compromised (SMM and/or low-cost PMU manipulation) and temporarily disconnect them.		
Test environment	An active CI-SOC instance and at least two NORM devices are assumed, out of which, one is “compromised”, namely set to send erroneous measurements.		
Preparation	The CI-SOC demand and production Analytics and Monitor modules are trained and configured to provide reliable results. The “compromised” NORM has reported enough measurements so that the Analytics module has been properly trained to detect the abnormal values.		
Dependencies	All CSNM:G1-CSNM:G7 test cases should have been successfully executed.		
Steps	1. Verify that CI-SOC automatically obtains encrypted real-time measures from NORM; 2. Verify that only relevant data are handled, the irrelevant ones being ignored; 3. Verify that the reported data are not altered and the decryption process is successfully performed;		

[3] When allowed by national law

	4. Verify that analytic is performed on the data and the compromised NORMs are detected; 5. The CI-SOC should identify a certain set of countermeasures, the first of whose should be to disconnect the meter from the grid.
Pass criteria	The "compromised" NORM gets disconnected from the grid.
Suspension criteria	The CI-SOC Analytics module does not recognise the "compromised" NORM due to improper or inadequate training. In this case, allow the "compromised" NORM to send data without any alteration for enough time, then execute the test again.

3.1.3.8 Test cases for feature CSNM:G10:F2

Table 19: Test case CSNM:G10:F2:T1

Test ID	CSNM:G10:F2:T1		
Test Description	Ensure that the CI-SOC is aware of the software security status of the NORM and can appropriately act in case of virus/malware/rootkit detection		
Test location	At the premises of ENG	**Partner**	ENG, SYN, REC, RWTH
Component	NORM, CI-SOC		
Features under test	CSNM:G10:F2		
Product requirement	The CI-SOC should be aware of the security state of the NORMs in terms of antivirus, anti-rootkit and anti-malware		
Test environment	An active CI-SOC instance and one NORM device are assumed.		
Preparation	Three files are assumed to be available, acting as i) virus, ii) malware, iii) rootkit. These files should be successively placed into the NORM device.		
Dependencies	All CSNM:G1-CSNM:G7 test cases should have been successfully executed.		
Steps	1. Instruct the NORM to perform a security scan; 2. Notify the CI-SOC about the scan outcome; 3. Place the file containing the virus in the NORM filesystem; 4. Instruct the NORM to perform a security scan; 5. Notify the CI-SOC about the scan outcome; 6. After one hour, place the file containing the malware in the NORM filesystem; 7. Repeat steps 4, 5 8. After one hour, place the file containing the rootkit in the NORM filesystem; 9. Repeat steps 4, 5		
Pass criteria	Step 1 should result in no threat detection, in contrast to step 4, which should always result in detecting the infected files. At all times, the CI-SOC should be informed and the countermeasures taken should be: 1. Instruction to quarantine the infected files if not already quarantined; 2. Instruction to periodically (short-ranged and frequently) run the security inspection; 3. Perform software attestation of the node; 4. If the remote attestation fails, the CI-SOC should request a software re-flash on the NORM (be this intervention physical, namely by sending a security crew on-site, or cyber, namely by remote software flashing).		

Suspension criteria	The infected files are not detected by the security software. In this case, alternatives as to this specific software should be investigated.

3.1.3.9 Test cases for feature CSNM:G10:F3

Table 20: Test case CSNM:G10:F3:T1

Test ID	CSNM:G10:F3:T1		
Test Description	The CI-SOC should be aware of software attestation failures and be able to mitigate them.		
Test location	At the premises of ENG	**Partner**	ENG, SYN, RWTH, REC
Component	CI-SOC, NORM		
Features under test	CSNM:G10:F3		
Product requirement	SUCCESS should be able to verify the authenticity of the software operating in the NORM devices and act either to fix the issue or to notify the DSO security staff to fix it.		
Test environment	An active CI-SOC instance and one NORM device are assumed.		
Preparation	At least one SUCCESS source or binary file should be available after being slightly or heavily modified.		
Dependencies	All CSNM:G1-CSNM:G7 test cases should have been successfully executed.		
Steps	1. The CI-SOC instructs the NORM to perform a software attestation; 2. The NORM informs the CI-SOC of the result of the software attestation (performed by the local security agent); 3. Place the modified file in the NORM filesystem replacing the original one; 4. Repeat steps 1-2 5. The CI-SOC notifies the DSO security staff about the event through the Dashboard; 6. The CI-SOC tries to mitigate the issue; a. The CI-SOC tries to flash a new version of the NORM device software; b. The CI-SOC informs the DSO security staff through the Dashboard that a maintenance unit should be sent to fix the issue.		
Pass criteria	Step 2 should result in a report stating that everything is normal. Step 4 should result in a report stating that the software attestation failed. Step 6 should be completed, either using option a or option b.		
Suspension criteria	N/A		

3.1.3.10 Test cases for feature CSNM:G10:F4

Table 21: Test case CSNM:G10:F4:T1

Test ID	CSNM:G10:F4:T1		
Test Description	The CI-SOC should be aware of hardware attestation failures and be able to mitigate them.		
Test location	At the premises of ENG	**Partner**	ENG, SYN, REC, RWTH
Component	CI-SOC, NORM		

Features under test	CSNM:G10:F4
Product requirement	SUCCESS should be able to verify the validity of the hardware configuration of the NORM devices and notify the DSO security staff to fix possible misconfigurations.
Test environment	An active CI-SOC instance and one NORM device are assumed, the NORM being equipped with PUF and one of SMM or low-cost PMU.
Preparation	If the NORM is equipped with a low-cost PMU, another low-cost PMU should be available. If the NORM is equipped with a SMM, another SMM should be available.
Dependencies	All CSNM:G1-CSNM:G7 test cases should have been successfully executed.
Steps	1. The CI-SOC instructs the NORM to perform a hardware attestation; 2. The NORM informs the CI-SOC over the result of the hardware attestation (performed by the local security agent); 3. Replace the metering (SMM/low-cost PMU) equipment of the NORM with the replacement, or simply remove it. 4. Repeat steps 1-2 5. The CI-SOC notifies the DSO security staff about the event through the Dashboard; 6. The CI-SOC should inform the DSO security staff through the Dashboard that a maintenance unit should be sent to fix the issue;
Pass criteria	Step 2 should result in a report stating that everything is normal. Step 4 should result in a report stating that the software attestation failed. Step 6 should be completed.
Suspension criteria	N/A

3.1.3.11 Test cases for feature CSNM:G10:F5

Table 22: Test case CSNM:G10:F5:T1

Test ID	CSNM:G10:F5:T1		
Test Description	Ensure that the CI-SOC is aware of the firewall status of the NORM and can appropriately act in case of firewall misconfiguration detection.		
Test location	At the premises of ENG	**Partner**	ENG, SYN, REC, RWTH
Component	CI-SOC, NORM		
Features under test	CSNM:G10:F5		
Product requirement	The CI-SOC should be aware of the security state of the NORMs in terms of firewall configuration.		
Test environment	An active CI-SOC instance and one NORM device are assumed.		
Preparation	N/A		
Dependencies	All CSNM:G1-CSNM:G7 test cases should have been successfully executed.		
Steps	1. Instruct the CI-SOC to perform a security scan on the particular NORM; 2. Notify the CI-SOC about the firewall scan outcome; 3. Change the firewall configuration of the NORM; 4. Repeat steps 1, 2.		

	5. The CI-SOC, being aware of the firewall misconfiguration, sends to the NORM a valid configuration; 6. The NORM device applies the new configuration; 7. Instruct the CI-SOC to perform a security scan on the particular NORM.
Pass criteria	Step 1 should result in no firewall misconfiguration detection, in contrast to step 4, which should always result in detecting the firewall rules change. At all times, the CI-SOC should be informed and the countermeasures taken should be: 5. Send to the NORM a valid configuration; 6. Perform a new firewall scan; 7. Perform a remote attestation (see CSNM:G7:F1) If the remote attestation fails, the CI-SOC should request a software re-flash on the NORM (be this intervention physical, namely by sending a security crew on-site, or cyber, namely by remote software flashing).
Suspension criteria	N/A

3.1.3.12 Test cases for feature CSNM:G10:F6

Table 23: Test case CSNM:G10:F6:T1

Test ID	CSNM:G10:F6:T1		
Test Description	Test the ability of the CI-SOC to identify unreachable NORM devices and appropriately inform the DSO security staff though the CI-SOC dashboard.		
Test location	At the premises of ENG	**Partner**	ENG, SYN, REC, RWTH
Component	CI-SOC, NORM		
Features under test	CSNM:G10:F6		
Product requirement	SUCCESS should be able to detect situations when a NORM is not reachable and notify the DSO security staff.		
Test environment	An active CI-SOC instance and one NORM device are assumed.		
Preparation	N/A		
Dependencies	All CSNM:G1-CSNM:G7 test cases should have been successfully executed.		
Steps	1. Leave the NORM to operate normally for one hour; 2. Plug the NORM out of power; 3. After 5 minutes, plug it in again; 4. Configure the NORM to not use the internet; 5. After 5 minutes, configure it to use the internet.		
Pass criteria	In both step 2 and step 4, the CI-SOC should inform the DSO security staff through the Dashboard that a maintenance unit should be sent to fix the issue.		
Suspension criteria	N/A		

3.1.3.13 Test cases for feature CSNM:G10:F7

Table 24: Test case CSNM:G10:F7:T1

Test ID	CSNM:G10:F7:T1

Test Description	Test that the CI-SOC is able to identify situations of repeating NORM authentication errors and appropriately acts to fix the issue.		
Test location	At the premises of SYN	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G10:F7		
Product requirement	The CI-SOC should identify situations of repeating NORM authentication errors and appropriately act to fix the issue.		
Test environment	An active CI-SOC instance and one NORM device are assumed.		
Preparation	N/A		
Dependencies	All CSNM:G1-CSNM:G7 test cases should have been successfully executed.		
Steps	1. Let the NORM operate normally for one hour; 2. Change the code that handles the PUF-related processes; 3. Instruct the CI-SOC to ask for a NORM validation; 4. Leave the NORM to operate for one hour 5. The CI-SOC should identify that: a. The validation always fails; b. The decryption processes always fail. 6. The CI-SOC attempts to update the active CRP of the NORM and informs it about it; 7. If this does not fix the problem, the CI-SOC instructs the NORM to perform a software and hardware attestation; 8. If this does not fix the problem, the DSO security staff are informed that a maintenance unit should be sent on-site to fix the issue;		
Pass criteria	The remote software attestation should identify the problem.		
Suspension criteria	N/A		

4. Potential Future Work

This deliverable equipped with certification feature it is a blueprint for the definition of an aligned security solution useful for center operators and integrated field devices and can be adopted by security solution tailored to mitigate threat against Critical Infrastructure. At this purpose an extension of the work taking in account all the cyber-physical menaces is ongoing in the DEFENDER Project with the aim to quantify the risk of a CEI.

The integration and feature schemas allow to create a certification solution that could be exploited by every project with the aim to connect the lower part of the infrastructure even to the highest pan european coordination level.

For this reason the easiest way to extend this certification schemas and related integration tests is to apply them, following by design policy, also to the new security solution tailored to act in the Pan-european level and also to all the overarching solution designed from scratch.

5. Conclusions

In this deliverable the final step of the Validation and Test of components developed within Workpackage 3 has been performed and the outcome of the overall activity, represented by the results of the integration tests, is presented. Validation and testing represents the basis for ensuring the SUCCESS integration, by assessing that NORM and CI-SOC successfully co-operate from both a logical and functional perspective. This is particularly important in view of the WP5 trials, because tests can highlight problems that may occur when deploying the SUCCESS Security solution in WP5.

Functional features of NORM and CI-SOC have been tested according to the test cases identified and defined during the Validation and testing activity on the basis of the SUCCESS Security solution certification framework. Tests have been carried out in laboratory using NORM and CI-SOC deployed in Ireland and at RWTH site respectively. Both components are reachable through VPN connection. The approach adopted during Validation and test activities has ensured the verification of system core functionalities in terms of successful operation testing and integrated performance.

6. References

[1] SUCCESS, «Deliverable D4.9: Integration and Validation Plan - Test and certification specifications, V3,» October 2018.

[2] SUCCESS, «Deliverable D3.10: Integration and Validation Plan. Test and certification specifications, V1,» 2017.

[3] SUCCESS, «Deliverable D3.11: Integration and Validation Plan. Test and certification specifications, V2,» 2017.

[4] «Raspberry PI,» [Online]. Available: https://www.raspberrypi.org/.

[5] SUCCESS, «Deliverable D4.2: Solution Architecture and Solution Description, V2,» 2017.

[6] SUCCESS, «Deliverable D3.14: Smart Grid Test & Certification specifications, V2,» May 2018.

[7] SUCCESS, «Deliverable D3.6: Information Security Management Components and Documentation, V3,» 2018.

[8] SUCCESS, «Deliverable D3.9: Next Generation Smart Meter, V3,» November 2018 .

[9] SUCCESS, «Deliverable D3.13: Smart Grid Test & Certification Specifications, V1,» 2017.

[10] SUCCESS, «Deliverable D1.2: Identification of existing threats V2,» 2017.

[11] SUCCESS, «Deliverable D4.5: Description of available components for SW functions, infrastructure and related documentation, V2,» 2017.

[12] SUCCESS, «Deliverable D3.9: Next Generation Smart Meter, V3,» 2018.

7. List of Tables

8. List of Abbreviations

AAA	Authentication authorization accounting
AMI	Advanced Metering Infrastructure
AMR	Automatic Meter Reading
CAPEX	Capital Expenditure
CEI	Critical Energy Infrastructure
CI-SAN	Critical Infrastructure Security Analytics Network
CI-SOC	Critical Infrastructures Security Operations Centre
CRP	Challenge Response Pair (referring to PUF-enabled NORM devices)
CSNM	CI-SOC ↔ NORM (integrated system)
DSO	Distribution System Operator
EDM	Event Driven Meter
GPS	Global Positioning System
KMM	Key Management Module (CI-SOC context)
KPI	Key Performance Indicator
NAN	Neighbourhood Area Network
NORM	Next Generation Open Real Time Smart Meter
OS	Operating System
PMC	PTP Management Client
PMU	Phasor Measurement Unit
PPS	Pulse Per Second
PTP	Precise Time Protocol
PUF	Physical Unclonable Function
ROCOF	Rate of Change Of Frequency
SCADA	Supervisory Control And Data Acquisition
SGAM	Smart Grid Architecture Model
SMG	Smart Meter Gateway
SMM	Smart Metrology Meter
SSH	Secure Shell

SUCCESS	Securing Critical Energy Infrastructures
TVE	Total Vector Error
VM	Virtual Machine
VPN	Virtual Private Network
WP	Work Package

A. Test cases reference

#	Test case ID	Component	Short Description	§	Page
1	CSNM:G1:F1:T1	CI-SOC, NORM	Test that the CI-SOC can bootstrap a PUF-enabled NORM, by registering sets of CRP	3.1.3.1	15
2	CSNM:G1:F1:T2	CI-SOC, NORM	Test that the CI-SOC KMM can identify a PUF-enabled NORM device	3.1.3.1	16
3	CSNM:G1:F2:T1	CI-SOC, NORM	Test whether the CI-SOC can refresh the active PUF challenge of the various NORMs deployed on the field.	3.1.3.2	16
4	CSNM:G2:F1:T1	CI-SOC, NORM	Test whether data reported by the NORM devices are encrypted and can be decrypted by the CI-SOC if they have not been tampered.	3.1.3.3	17
5	CSNM:G2:F1:T2	CI-SOC, NORM	Test whether on-channel data tampering is possible to be detected by the CI-SOC.	3.1.3.3	17
6	CSNM:G2:F2:T1	CI-SOC, NORM	Ensure ability of the NORM to connect through a VPN-encrypted channel to the CI-SOC granted that the credentials and installed certificates are valid.	3.1.3.4	18
7	CSNM:G3:F1:T1	CI-SOC, NORM	Test that the SMM measurements are correctly fed to the CI-SOC	3.1.3.5	19
8	CSNM:G3:F1:T2	CI-SOC, NORM	Test that the low-cost PMU measurements are correctly fed to the CI-SOC	3.1.3.5	19
9	CSNM:G3:F1:T3	CI-SOC, NORM	Test the ability of the CI-SOC to handle multiple data streams coming at high rates.	3.1.3.5	20

10	CSNM:G3:F1:T4	CI-SOC, NORM	Test the ability of CI-SOC to handle data streams containing irrelevant information.	3.1.3.5	20
11	CSNM:G7:F1:T1	CI-SOC, NORM	Check if NORM can perceive changes in its software configuration and accordingly alert the CI-SOC.	3.1.3.6	21
12	CSNM:G7:F1:T2	CI-SOC, NORM	Check that the NORM is able to identify changes in its overall integrated configuration and accordingly alert the CI-SOC.	3.1.3.6	22
13	CSNM:G7:F1:T3	CI-SOC, NORM	The NORM should be protected by an antivirus mechanism and the CI-SOC should be aware of its status	3.1.3.6	22
14	CSNM:G7:F1:T4	CI-SOC, NORM	The NORM should be protected by a firewall and the CI-SOC should be aware of its state.	3.1.3.6	23
15	CSNM:G7:F1:T5	CI-SOC, NORM	Ensure that the CI-SOC is able to retrieve the logs of the security components of the NORM	3.1.3.6	23
16	CSNM:G10:F1:T1	CI-SOC, NORM	Disconnection of NORM devices with compromised SMM or low-cost PMU (disconnection possible when allowed by national law)	3.1.3.7	24
17	CSNM:G10:F2:T1	CI-SOC, NORM	The CI-SOC is aware of the software security status of the NORM and can appropriately act in case of virus/malware/rootkit detection	3.1.3.8	25
18	CSNM:G10:F3:T1	CI-SOC, NORM	The CI-SOC is aware of the software security status of the	3.1.3.9	26

			NORM and can appropriately act in case of virus/malware/rootkit detection		
19	CSNM:G10:F4:T1	CI-SOC, NORM	The CI-SOC is aware of the software security status of the NORM and can appropriately act in case of virus/malware/rootkit detection	3.1.3.10	26
18	CSNM:G10:F5:T1	CI-SOC, NORM	The CI-SOC should be aware of the firewall status of the NORM and can act in case of firewall misconfiguration detection	3.1.3.11	27
21	CSNM:G10:F6:T1	CI-SOC, NORM	The CI-SOC is aware of the software security status of the NORM and can appropriately act in case of virus/malware/rootkit detection	3.1.3.12	28
19	CSNM:G10:F7:T1	CI-SOC, NORM	Test that the CI-SOC is able to identify situations of repeating NORM authentication errors and appropriately acts to fix the issue.	3.1.3.13	28

B. Tests results against the specification

All tests have been performed using NORM (including SMM, PMU and Security Agent) deployed in Ireland and CI-SOC deployed at RWTH premises. Both were reachable by connecting via VPN with OpenVPN.

B.1 Test results for functional features CSNM:G1

B.1.1 Test results for feature CSNM:G1:F1

Test results for feature CSNM:G1:F1 are reported in the following tables.

Table 25: Test case CSNM:G1:F1:T1 results

Test ID	CSNM:G1:F1:T1		
Test location	At the premises of SYN/ESB	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G1:F1		
Test preparation comments	N/A		

Detailed test steps and result	1. The NORM was left to operate unattended for a period of time, until its valid CRPs where almost depleted (only 100 left). The relevant CRP KMM database shows:
	`pufkm=# select count(*) from entry where puf_status = 'inactive';`
	`count`
	`-------`
	`100`
	`(1 row)`
	2. The KMM initiates the procedure of CRP updating, by instructing the NORM PUF firmware to bootstrap itself. The relevant logs were:
	`2018-10-23 08:57:43,390 -- [ lpa: bootstrap: 271] -- INFO -- Bootstrap executed to ESB`
	3. At the same time, the logs of KMM indicate that 600 new CRPs were added to the KMM CRP database:
	`pufkm=# select count(*) from entry where puf_status = 'inactive';`
	`count`
	`-------`
	`700`
	`(1 row)`		

Comments	The test was successful		

Table 26: Test case CSNM:G1:F1:T2 results

Test ID	CSNM:G1:F1:T2		
Test location	At the premises of SYN	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G1:F1		

Test preparation comments	Two NORM devices (one real and one emulated) were registered against the CI-SOC.

Detailed test steps and result	1. The two NORMs were bootstrapped against the CI-SOC.
	2. Entering the NORM consoles, we bypassed the PUF processes (namely the response to a given challenge was not generated by the PUF hardware). Afterwards, we left the NORM operation unattended. Upon verification request, the response was always as follows, indicating that the identity verification failed:
	`[lpa        :   verify: 354] --     INFO -- [src: 10.12.0.1] Got signal to verify myself to ESB.`
	`[key_manager: validate: 357] --    ERROR -- Could not validate myself to ESB. Code: 401`
	`[lpa        :   verify: 359] -- CRITICAL -- Could not verify myself to ESB!`
	3. We then reverted the PUF bypass and tried again. The log of the NORM was as follows, with no indication of an error:
	`[ lpa:   verify: 354] --     INFO -- [src:     10.12.0.66] Got signal to verify myself to ESB.`
	4. We let the configurations of steps 2 and 3 active until at least 1000 verification requests were issued by the KMM.

Comments	The test was successful.

B.1.2 Test results for feature CSNM:G1:F2

Test results for feature CSNM:G1:F2 are reported in the following tables.

Table 27: Test case CSNM:G1:F2:T1 results

Test ID	CSNM:G1:F2:T1		
Test location	At the premises of SYN	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G1:F2		
Test preparation comments	Two NORMs, a physical and an emulated one were connected to the same CI-SOC instantiation.		

Detailed test steps and result	1. The CI-SOC KMM was configured to refresh the PUF challenges every 5 minutes.
	2. The logs of the NORMs were as follows:
	…
	`2018-10-23 10:16:34,935 -- [       lpa:update_challenge: 137] --     INFO -- [src:       10.12.0.1] Updated challenge for DSOSMC: ESB`
	`2018-10-23 10:26:34,913 -- [       lpa:update_challenge: 137] --     INFO -- [src:       10.12.0.1] Updated challenge for DSOSMC: ESB`
	`2018-10-23 10:36:35,011 -- [       lpa:update_challenge: 137] --     INFO -- [src:       10.12.0.1] Updated challenge for DSOSMC: ESB`
	`2018-10-23 10:46:35,011 -- [       lpa:update_challenge: 137] --     INFO -- [src:       10.12.0.1] Updated challenge for DSOSMC: ESB`		

	2018-10-23 10:56:35,021 -- [lpa:update_challenge: 137] -- INFO -- [src: 10.12.0.1] Updated challenge for DSOSMC: ESB 2018-10-23 11:06:35,002 -- [lpa:update_challenge: 137] -- INFO -- [src: 10.12.0.1] Updated challenge for DSOSMC: ESB 2018-10-23 11:16:35,012 -- [lpa:update_challenge: 137] -- INFO -- [src: 10.12.0.1] Updated challenge for DSOSMC: ESB 2018-10-23 11:26:34,950 -- [lpa:update_challenge: 137] -- INFO -- [src: 10.12.0.1] Updated challenge for DSOSMC: ESB 2018-10-23 11:27:37,172 -- [lpa:update_challenge: 137] -- INFO -- [src: 10.12.0.1] Updated challenge for DSOSMC: ESB 2018-10-23 11:30:20,352 -- [lpa:update_challenge: 137] -- INFO -- [src: 10.12.0.1] Updated challenge for DSOSMC: ESB
Comments	The test was successful. For security reasons, checking the challenge of each NORM was not possible, by design. Hence, we decided to encrypt the same string each time the active CRP was updated and, every time, the resulting encoded string was different, indicating that the CRP response part (used as encryption key) was different, hence the challenge part was also different).

B.2 Test results for functional features CSNM:G2

B.2.1 Test results for feature CSNM:G2:F1

Test results for feature CSNM:G2:F1 are reported in the following tables.

Table 28: Test case CSNM:G2:F1:T1 results

Test ID	CSNM:G2:F1:T1		
Test location	At the premises of SYN/ESB	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G2:F1		
Test preparation comments	Tests of group CSNM:G1 were successfully conducted. The message content to be decrypted was set to: `{"data": "CSNM:G2:F1:T1 test"}`		

Detailed test steps and result	1. The NORM device was left to operate unattended as per CSNM:G1 tests.
	2. We issued an encryption request to the NORM:
	`curl -X POST \`
	`  http://10.12.0.26:8080/utilities/ESB/encode \`
	`  -H 'Content-Type: application/json' \`
	`  -d '{"data":"CISOC:G2:F1:T1 test"}'`
	`{`
	`    "data": "60220815abdb8daffc9f74a705b7c1e9ac37c7f14a574b4036ff2317578fa3c3",`
	`    "timestamp": "2018-10-23T11:55:53.090508Z"`		

	`}`
	3. Then, we issued a command to KMM to decode the encrypted data:
	`curl -X POST \`
	`  http://10.12.0.1:80/success/cisoc/kmm/dso/ESB/decode \`
	`  -H 'Content-Type: application/json' \`
	`  -d '{`
	`    "pufId":`
	`"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae",`
	`    "data":`
	`"60220815abdb8daffc9f74a705b7c1e9ac37c7f14a574b4036ff2317578fa3c3",`
	`    "timestamp": "2018-10-23T11:55:53.090508Z"`
	`}'`
	
	`{`
	`    "data": "CISOC:G2:F1:T1 test"`
	`}`

Comments	The test was successful.

Table 29: Test case CSNM:G2:F1:T2 results

Test ID	CSNM:G2:F1:T2		
Test location	At the premises of SYN/ESB	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G2:F1		
Test preparation comments	Tests of group CSNM:G1 were successfully conducted. The message content to be decrypted was set to: `{“data”: “CSNM:G2:F1:T2 test”}`		
Detailed test steps and result	1. The NORM device was left to operate unattended as per CSNM:G1 tests. 2. The SECA was set to issuing data encoding requests every five seconds (to forward the SMX data to CI-SOC). 3. We tuned the SECA to slightly alter the encrypted data after retrieval effectively emulating that it has been hacked (i.e. acting like a threat agent). We performed the same test also altering the PUF ID or the timestamp of the message. 4. The SECA forwarded the tampered messages to the KMM for decryption; 5. The KMM would not decrypt the message, and the Monitor component issued attacks of type “Decrypted message”. 6. The above procedure was tested for over 1000 times.		
Comments	The test was successful.		

B.2.2 Test results for feature CSNM:G2:F2

Test results for feature CSNM:G2:F2 are reported in the following tables.

Table 30: Test case CSNM:G2:F2:T1 results

Test ID	CSNM:G2:F2:T1		
Test location	At the premises of SYN/ESB	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G2:F2		
Test preparation comments	Tests of group CSNM:G1 were successfully conducted.		

Detailed test steps and result	1. The NORM device was left to operate unattended as per CSNM:G1 tests, with the OpenVPN connection active at all times.
	2. The logs of the NORM indicated that frequent communication was possible (e.g. see results of CSNM:G1:F2:T1).
	3. A new tun0 interface (created by the VPN software) was also active and transmitting (see sent packets size):
	`pi@SMX43-ESB002:~/puf-client/rPI/API$ ifconfig`
	`. . .`
	`tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00`
	`          inet addr:10.12.0.26  P-t-P:10.12.0.26  Mask:255.255.254.0`
	`          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1`
	`          RX packets:581331 errors:0 dropped:0 overruns:0 frame:0`
	`          TX packets:482215 errors:0 dropped:238 overruns:0 carrier:0`
	`          collisions:0 txqueuelen:100`
	`          RX bytes:93982733 (89.6 MiB)  TX bytes:160785359 (153.3 MiB)`
	`. . .`		

Comments	The test was successful.		

B.3 Test results for functional features CSNM:G3

B.3.1 Test results for feature CSNM:G3:F1

Test results for feature CSNM:G3:F1 are reported in the following tables.

Table 31: Test case CSNM:G3:F1:T1 results

Test ID	CSNM:G3:F1:T1		
Test location	At the premises of ENG	**Partner**	ENG
Component	CI-SOC, NORM		
Features under test	CSNM:G3:F1		
Test preparation comments	N/A		

Detailed test steps and result	1. We took some of the messages including SMM data, in particular frequencies, sent in one week by Security Agent on NORM (about 3·10^5):
	{"hashed_data":"E4EE7EB43ABABB3252AFBCBF482C61B2E1032B26F494235FA35669B650420A7F","norm_data":"8543a6847761d29370f34091291e851d 2018-09-25T10:22:18.328832Z 187b1e369c0e15d991ac796a20b9e9e6762ec3cb6c11e8246c63cc4e5f476004273af7a17cead0f17f849f289e63a706e82f7de6ef98598c109e7c6db2870c422e13e0dca0649a98bc0a57065f43d065a8cd4a200bce9146c0ef6d695e4ddd96351a23408fd9bf3e837a45f7394a6c44","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_b6f427371540420668752","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1537870939011}
	{"hashed_data":"F7BCE63D166545DF56F5CC0A87B0AC93B12A99316BC44A7A1A8AD4A00BA57048","norm_data":"8543a6847761d29370f34091291e851d 2018-09-25T10:22:20.432530Z 187b1e369c0e15d991ac796a20b9e9e6762ec3cb6c11e8246c63cc4e5f476004273af7a17cead0f17f849f289e63a706e82f7de6ef98598c109e7c6db2870c422e13e0dca0649a98bc0a57065f43d065fad8e2b7662912822efd776abd4e41b7351a23408fd9bf3e837a45f7394a6c44","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_055169681540420668932","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1537870941203}
	{"hashed_data":"B7711B32B626253B1972C4213F3C98ADB3081025EB0759D6C2B906922B32F523","norm_data":"8543a6847761d29370f34091291e851d 2018-09-25T10:22:22.572595Z 187b1e369c0e15d991ac796a20b9e9e6762ec3cb6c11e8246c63cc4e5f476004273af7a17cead0f17f849f289e63a706e82f7de6ef98598c109e7c6db2870c422e13e0dca0649a98bc0a57065f43d0655fe162a56ef45d94b1f557bae040f771351a23408fd9bf3e837a45f7394a6c44","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_53e542271540420669065","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1537870942972}
	{"hashed_data":"5F376D9E591CC5D1E60B3DCA03D0535A3F51930B6D0EBB038630802D65472B32","norm_data":"8543a6847761d29370f34091291e851d 2018-09-25T10:22:24.696298Z 187b1e369c0e15d991ac796a20b9e9e6762ec3cb6c11e8246c63cc4e5f476004273af7a17cead0f17f849f289e63a706e82f7de6ef98598c109e7c6db2870c422e13e0dca0649a98bc0a57065f43d065a7f66020832ae4b446881f2afc18ea5acb82132eb00b79d6ac64615775cf809b","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_f396a3831540420669188","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1537870944816}
	2. All messages sent by (SecA on) NORM were received by CI-SOC under the topic “NORM/DSOSMC/SECAGENT”. An extract of CI-SOC log showing the reception of the above messages is reported in the following.
	18/09/25 10:22:20 WARN EventConverter: EVENT RECEIVED: {"hashed_data":"E4EE7EB43ABABB3252AFBCBF482C61B2E1032B26F494235FA35669B650420A7F","norm_data":"8543a6847761d29370f34091291e851d 2018-09-25T10:22:18.328832Z		

```
187b1e369c0e15d991ac796a20b9e9e6762ec3cb6c11e8246c63cc4e5f476004273
af7a17cead0f17f849f289e63a706e82f7de6ef98598c109e7c6db2870c422e13e0
dca0649a98bc0a57065f43d065a8cd4a200bce9146c0ef6d695e4ddd96351a23408
fd9bf3e837a45f7394a6c44","norm_ip":"10.12.0.18","request_id":"HASH_
REQUEST_b6f427371540420668752","norm_id":"26977d6ab89b65e061ed48b7f
2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1537870939011}

encoded NORM data: 8543a6847761d29370f34091291e851d 2018-09-
25T10:22:18.328832Z
187b1e369c0e15d991ac796a20b9e9e6762ec3cb6c11e8246c63cc4e5f476004273
af7a17cead0f17f849f289e63a706e82f7de6ef98598c109e7c6db2870c422e13e0
dca0649a98bc0a57065f43d065a8cd4a200bce9146c0ef6d695e4ddd96351a23408
fd9bf3e837a45f7394a6c44

KMM service response is:
{"data":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa
417bae frequency 1537870936000 50.059 OK SMM"}

decoded NORM message:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870936000 50.059 OK SMM

Storing detected data...

26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870936000 50.059 OK SMM

18/09/25 10:22:20 WARN ThresholdFilter: Analysing event to detect
out of range:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870936000 50.059 OK SMM



18/09/25 10:22:22 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"F7BCE63D166545DF56F5CC0A87B0AC93B12A99316BC44A7A1A8
AD4A00BA57048","norm_data":"8543a6847761d29370f34091291e851d 2018-
09-25T10:22:20.432530Z
187b1e369c0e15d991ac796a20b9e9e6762ec3cb6c11e8246c63cc4e5f476004273
af7a17cead0f17f849f289e63a706e82f7de6ef98598c109e7c6db2870c422e13e0
dca0649a98bc0a57065f43d065fad8e2b7662912822efd776abd4e41b7351a23408
fd9bf3e837a45f7394a6c44","norm_ip":"10.12.0.18","request_id":"HASH_
REQUEST_05516968154042066893 2","norm_id":"26977d6ab89b65e061ed48b7f
2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1537870941203}

encoded NORM data: 8543a6847761d29370f34091291e851d 2018-09-
25T10:22:20.432530Z
187b1e369c0e15d991ac796a20b9e9e6762ec3cb6c11e8246c63cc4e5f476004273
af7a17cead0f17f849f289e63a706e82f7de6ef98598c109e7c6db2870c422e13e0
dca0649a98bc0a57065f43d065fad8e2b7662912822efd776abd4e41b7351a23408
fd9bf3e837a45f7394a6c44

KMM service response is:
{"data":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa
417bae frequency 1537870938000 50.059 OK SMM"}

decoded NORM message:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870938000 50.059 OK SMM

Storing detected data...

26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870938000 50.059 OK SMM

18/09/25 10:22:22 WARN ThresholdFilter: Analysing event to detect
out of range:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870938000 50.059 OK SMM



18/09/25 10:22:24 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"B7711B32B626253B1972C4213F3C98ADB3081025EB0759D6C2B
906922B32F523","norm_data":"8543a6847761d29370f34091291e851d 2018-
09-25T10:22:22.572595Z
187b1e369c0e15d991ac796a20b9e9e6762ec3cb6c11e8246c63cc4e5f476004273
af7a17cead0f17f849f289e63a706e82f7de6ef98598c109e7c6db2870c422e13e0
dca0649a98bc0a57065f43d0655fe162a56ef45d94b1f557bae040f771351a23408
fd9bf3e837a45f7394a6c44","norm_ip":"10.12.0.18","request_id":"HASH_
```

```
REQUEST_53e542271540420669065","norm_id":"26977d6ab89b65e061ed48b7f
2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1537870942972}

encoded NORM data: 8543a6847761d29370f34091291e851d 2018-09-
25T10:22:22.572595Z
187b1e369c0e15d991ac796a20b9e9e6762ec3cb6c11e8246c63cc4e5f476004273
af7a17cead0f17f849f289e63a706e82f7de6ef98598c109e7c6db2870c422e13e0
dca0649a98bc0a57065f43d0655fe162a56ef45d94b1f557bae040f771351a23408
fd9bf3e837a45f7394a6c44

KMM service response is:
{"data":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa
417bae frequency 1537870940000 50.058 OK SMM"}

decoded NORM message:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870940000 50.058 OK SMM

Storing detected data...

26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870940000 50.058 OK SMM

18/09/25 10:22:24 WARN ThresholdFilter: Analysing event to detect
out of range:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870940000 50.058 OK SMM


18/09/25 10:22:26 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"5F376D9E591CC5D1E60B3DCA03D0535A3F51930B6D0EBB03863
0802D65472B32","norm_data":"8543a6847761d29370f34091291e851d 2018-
09-25T10:22:24.696298Z
187b1e369c0e15d991ac796a20b9e9e6762ec3cb6c11e8246c63cc4e5f476004273
af7a17cead0f17f849f289e63a706e82f7de6ef98598c109e7c6db2870c422e13e0
dca0649a98bc0a57065f43d065a7f66020832ae4b446881f2afc18ea5acb82132eb
00b79d6ac64615775cf809b","norm_ip":"10.12.0.18","request_id":"HASH_
REQUEST_f396a3831540420669188","norm_id":"26977d6ab89b65e061ed48b7f
2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1537870944816}

encoded NORM data: 8543a6847761d29370f34091291e851d 2018-09-
25T10:22:24.696298Z
187b1e369c0e15d991ac796a20b9e9e6762ec3cb6c11e8246c63cc4e5f476004273
af7a17cead0f17f849f289e63a706e82f7de6ef98598c109e7c6db2870c422e13e0
dca0649a98bc0a57065f43d065a7f66020832ae4b446881f2afc18ea5acb82132eb
00b79d6ac64615775cf809b

KMM service response is:
{"data":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa
417bae frequency 1537870942000 50.06 OK SMM"}

decoded NORM message:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870942000 50.06 OK SMM

Storing detected data...

26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870942000 50.06 OK SMM

18/09/25 10:22:26 WARN ThresholdFilter: Analysing event to detect
out of range:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870942000 50.06 OK SMM
```

Therefore the decrypted messages are:

```
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870936000 50.059 OK SMM

26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870938000 50.059 OK SMM

26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870940000 50.058 OK SMM

26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1537870942000 50.06 OK SMM
```

<table>
<tr><td></td><td>Detection timestamps in date format are, respectively: 09/25/2018 10:22:16, 09/25/2018 10:22:18, 09/25/2018 10:22:20 and 09/25/2018 10:22:22

3. We have accessed the file storing measures observed in that period; (an extract of) the entries corresponding to the above timestamps are:
<table>
<tr><th>COMPUTER_TIME</th><th>InstFrequency</th><th>Voltage L1-L2</th><th>Voltage L1-N</th></tr>
<tr><td>2018-09-25 10:22:16</td><td>50.059</td><td>383.218</td><td>221.711</td></tr>
<tr><td>2018-09-25 10:22:18</td><td>50.059</td><td>383.220</td><td>221.742</td></tr>
<tr><td>2018-09-25 10:22:20</td><td>50.058</td><td>383.265</td><td>221.767</td></tr>
<tr><td>2018-09-25 10:22:22</td><td>50.060</td><td>383.303</td><td>221.782</td></tr>
</table>
The log shows that the frequency values are the same of the ones received and processed by CI-SOC</td></tr>
<tr><td><b>Comments</b></td><td>The test was successful</td></tr>
</table>

Table 32: Test case CSNM:G3:F1:T2 results

Test ID	CSNM:G3:F1:T2		
Test location	At the premises of ENG	**Partner**	ENG
Component	CI-SOC, NORM		
Features under test	CSNM:G3:F1		
Test preparation comments	N/A		

Detailed test steps and result	1. We took some of the messages including PMU data, in particular rate of change of frequency (ROCOF), sent in one day by Security Agent on NORM (17.062 messages). Security Agent receives PMU data by subscribing to `SUCCESS/NORM/ESB001/PMU/Values` and sends them to CI-SOC by publishing to the same topic used for SMM data (i.e. `NORM/DSOSMC/SECAGENT`). They can be distinguished by looking at the `source` attribute of SecA decrypted messages, that can be SMM or PMU. The messages that will be examined in this test are:
	{"hashed_data":"7C58FD0FF945DD964817B5A4B76CC59722B5D9D53015A47AA78364B21BF26E4B","norm_data":"8543a6847761d29370f34091291e851d 2018-10-02T12:11:40.211393Z 62e40c2f86e0e8ec393672ece2aa7fa3894f25a81c72d7ce4c1175b4a4d58212c12f430ebf991aa326176e38f2970f561ead2781b422d6933b98b627eadd610301828ee8d630ad6ebd56206e3f81618b70e2308e3d1751523a5b809d86d787e430affd38904200bbf0b834716ef8128c0fcc972cdf0f1b97501126df3adce712","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_72d0e2d11540426283422","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1538482300971}
	
	{"hashed_data":"0630AF2FD12B42F3ECB87533776495E64A75E32173BC04943E6D75B79004F0A9","norm_data":"8543a6847761d29370f34091291e851d 2018-10-02T12:11:45.140795Z 62e40c2f86e0e8ec393672ece2aa7fa3894f25a81c72d7ce4c1175b4a4d58212c12f430ebf991aa326176e38f2970f561ead2781b422d6933b98b627eadd61035d412ce5ba376c28deb3f603f8a7e3dbd9df074303c0aa6544badb408a446770ef2808c061dd87b61c809d8c9de0b387feab07cf1e6ae726411ad809ae0e5e54","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_2b0877cb1540426287441","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1538482305958}		

```
{"hashed_data":"4EFE3727A47EB95CA046B8CF4EF62C43876EB5E6240B5C1682EFDE0D2
B26D0BE","norm_data":"8543a6847761d29370f34091291e851d 2018-10-
02T12:11:50.133005Z
62e40c2f86e0e8ec393672ece2aa7fa3894f25a81c72d7ce4c1175b4a4d58212c12f430eb
f991aa326176e38f2970f561ead2781b422d6933b98b627eadd61035d412ce5ba376c28de
b3f603f8a7e3dbdb62b8d66741d742c02b6e4ff314c11fba91da446730651b3f69508a5b4
68ee40fcc972cdf0f1b97501126df3adce712","norm_ip":"10.12.0.18","request_id
":"HASH_REQUEST_4d43bd011540426292432","norm_id":"26977d6ab89b65e061ed48b
7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1538482311015}
```

```
{"hashed_data":"065402917D54BA99D2C06EAE1BF9E01600B4DE4293149428D20E50BB6
C0D6C61","norm_data":"8543a6847761d29370f34091291e851d 2018-10-
02T12:11:55.131015Z
62e40c2f86e0e8ec393672ece2aa7fa3894f25a81c72d7ce4c1175b4a4d58212c12f430eb
f991aa326176e38f2970f561ead2781b422d6933b98b627eadd6103a5787f88b671b15558
57ecb30384d0d63cb41fc61290595e0650701eb54d36ce1294af8a22a25b930fd6209c602
75c110fcc972cdf0f1b97501126df3adce712","norm_ip":"10.12.0.18","request_id
":"HASH_REQUEST_680ec6351540426297439","norm_id":"26977d6ab89b65e061ed48b
7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1538482316102}
```

4. All messages sent by (SecA on) NORM were received by CI-SOC under the topic "NORM/DSOSMC/SECAGENT". An extract of CI-SOC log showing the reception of the above messages is reported in the following.

```
18/10/02 12:11:41 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"7C58FD0FF945DD964817B5A4B76CC59722B5D9D53015A47AA78
364B21BF26E4B","norm_data":"8543a6847761d29370f34091291e851d 2018-
10-02T12:11:45.140795Z
62e40c2f86e0e8ec393672ece2aa7fa3894f25a81c72d7ce4c1175b4a4d58212c12
f430ebf991aa326176e38f2970f561ead2781b422d6933b98b627eadd610301828e
e8d630ad6ebd56206e3f81618b70e2308e3d1751523a5b809d86d787e430affd389
04200bbf0b834716ef8128c0fcc972cdf0f1b97501126df3adce712","norm_ip":
"10.12.0.18","request_id":"HASH_REQUEST_72d0e2d11540426283422","nor
m_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa41
7bae","timestamp":1538482300771}

KMM service response is:
{"data":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa
417bae rocof 1538482298000 -0.0016925039235502481 OK PMU"}

decoded NORM message:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482298000 -0.0016925039235502481 OK PMU

Storing detected data...

26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482298000 -0.0016925039235502481 OK PMU

18/10/02 12:11:41 WARN ThresholdFilter: Analysing event to detect
out of range:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482298000 -0.0016925039235502481 OK PMU


18/10/02 12:11:46 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"0630AF2FD12B42F3ECB87533776495E64A75E32173BC04943E6
D75B79004F0A9","norm_data":"8543a6847761d29370f34091291e851d 2018-
10-02T12:11:45.140795Z
62e40c2f86e0e8ec393672ece2aa7fa3894f25a81c72d7ce4c1175b4a4d58212c12
f430ebf991aa326176e38f2970f561ead2781b422d6933b98b627eadd61035d412c
e5ba376c28deb3f603f8a7e3dbd9df074303c0aa6544badb408a446770ef2808c06
1dd87b61c809d8c9de0b387feab07cf1e6ae726411ad809ae0e5e54","norm_ip":
"10.12.0.18","request_id":"HASH_REQUEST_2b0877cb1540426287441","nor
m_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa41
7bae","timestamp":1538482305958}

KMM service response is:
{"data":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa
417bae rocof 1538482303000 -8.742402424104512E-4 OK PMU"}
```

```
decoded NORM message:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482303000 -8.742402424104512E-4 OK PMU

Storing detected data...

26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482303000 -8.742402424104512E-4 OK PMU

18/10/02 12:11:46 WARN ThresholdFilter: Analysing event to detect
out of range:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482303000 -8.742402424104512E-4 OK PMU



18/10/02 12:11:51 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"4EFE3727A47EB95CA046B8CF4EF62C43876EB5E6240B5C1682E
FDE0D2B26D0BE","norm_data":"8543a6847761d29370f34091291e851d 2018-
10-02T12:11:50.133005Z
62e40c2f86e0e8ec393672ece2aa7fa3894f25a81c72d7ce4c1175b4a4d58212c12
f430ebf991aa326176e38f2970f561ead2781b422d6933b98b627eadd61035d412c
e5ba376c28deb3f603f8a7e3dbdb62b8d66741d742c02b6e4ff314c11fba91da446
730651b3f69508a5b468ee40fcc972cdf0f1b97501126df3adce712","norm_ip":
"10.12.0.18","request_id":"HASH_REQUEST_4d43bd011540426292432","nor
m_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa41
7bae","timestamp":1538482311015}

KMM service response is:
{"data":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa
417bae rocof 1538482308000 -3.3485351013951004E-4 OK PMU"}

decoded NORM message:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482308000 -3.3485351013951004E-4 OK PMU

Storing detected data...

26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482308000 -3.3485351013951004E-4 OK PMU

18/10/02 12:11:51 WARN ThresholdFilter: Analysing event to detect
out of range:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482308000 -3.3485351013951004E-4 OK PMU



18/10/02 12:11:56 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"065402917D54BA99D2C06EAE1BF9E01600B4DE4293149428D20
E50BB6C0D6C61","norm_data":"8543a6847761d29370f34091291e851d 2018-
10-02T12:11:55.131015Z
62e40c2f86e0e8ec393672ece2aa7fa3894f25a81c72d7ce4c1175b4a4d58212c12
f430ebf991aa326176e38f2970f561ead2781b422d6933b98b627eadd6103a5787f
88b671b1555857ecb30384d0d63cb41fc61290595e0650701eb54d36ce1294af8a2
2a25b930fd6209c60275c110fcc972cdf0f1b97501126df3adce712","norm_ip":
"10.12.0.18","request_id":"HASH_REQUEST_680ec6351540426297439","nor
m_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa41
7bae","timestamp":1538482316102}

KMM service response is:
{"data":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa
417bae rocof 1538482313000 -0.0023801170755177736 OK PMU"}

decoded NORM message:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482313000 -0.0023801170755177736 OK PMU

Storing detected data...

26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482313000 -0.0023801170755177736 OK PMU

18/10/02 12:11:56 WARN ThresholdFilter: Analysing event to detect
out of range:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482313000 -0.0023801170755177736 OK PMU
```

Therefore the decrypted messages are:

```
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
rocof 1538482298000 -0.0016925039235502481 OK PMU
```

	26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae rocof 1538482303000 -8.742402424104512E-4 OK PMU 26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae rocof 1538482308000 -3.3485351013951004E-4 OK PMU 26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae rocof 1538482313000 -0.0023801170755177736 OK PMU We can see that these values have been detected by PMU because the last part of the decrypted SecA messages is always set to PMU. The values detected by PMU and sent by secA to CI-SOC are the same that CI-SOC successfully receives, decrypts and processes on its side.
Comments	The test was successful

Table 33: Test case CSNM:G3:F1:T3 results

Test ID	CSNM:G3:F1:T3		
Test location	At the premises of ENG	**Partner**	ENG, REC, RWTH, SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G3:F1		
Test preparation comments	At the moment of testing in Ireland there were not 10 complete NORMs available, therefore, to emulate the high traffic of data we simply increased the rate by 10. To do that, a Security Agent (SecA) simulator was developed. It receives frequency values transmitted every 2 seconds by smart meters by subscribing to topic "`SUCCESS/NORM/ESB001/wally1/Values`" and generates and sends to CI-SOC ten messages (instead of one) with the same frequency value.		

Detailed test steps and result	1. We configured the Security Agent simulator to emulate 10 devices by generating ten messages, instead of one, per each frequency value transmitted by NORM in Ireland for about one hour (17.862 messages). An example of messages sent to CI-SOC is reported below:
	{"hashed_data":"AEE286E2E1E1355741CA83E7419C4C7CA8DEF61A21EA7D3178754DB5A6D36F64","norm_data":"8543a6847761d29370f34091291e851d 2018-10-24T16:50:20.144337Z f70ad5d367ce9ae5484367319bc6a5f4b52ebc0cf766c5cdf2635178da2f86123e0f924c2d05426e2b9b8099cdb40506f30c1c46f54acb162a28234512107d8a1f3a1d83b9e03a911dc204647c5e634c3a0af1d719c928d5f7ae7bbc30a72fa980a31213a77aa8415d23ed86f9d00632","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_4bb72b241540399805269","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1540399805357}
	{"hashed_data":"E519A64A9EEBF82768BC8B860D79F2905B7DAC616B569F5710C6E801EC2D9BD2","norm_data":"8543a6847761d29370f34091291e851d 2018-10-24T16:50:20.272607Z bd4c59427d8f715f60bed44ae47ce785cd8960b4c01b9bfbaf7022d25b9050435dd524b94b037c65ef57e934f5a4b08773b0e2962b0d61d1847d8db05acbd48f1f3a1d83b9e03a911dc204647c5e634c19d9b22d30b4036492dda88553d8965280a31213a77aa8415d23ed86f9d00632","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_d893ef371540399805395","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1540399805453}
	{"hashed_data":"FFEFF62842EF0C3C086C5A2106C714C7F7A5092C70D9EA17AAB6381D7CCB0C2D","norm_data":"8543a6847761d29370f34091291e851d 2018-10-24T16:50:20.400594Z c42e0a9fe75c0260154cb86b6b80c2765b28e0fbb839d3e92db9888db508185b9d50cb4f5b2163e0fd997222335cd76d265ad5913640a460efd7d4984722faeb1f3a1d83b9e03a911d		

```
c204647c5e634c75328520c9a6ef5de1bc30aa2bfd78c980a31213a77aa8415d23ed86f9d
00632","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_4466668d15403998
05523","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b
2fa417bae","timestamp":1540399805553}


{"hashed_data":"92D7A1D77139372B8AC6DBCD6A4DF666935606048F64A55E618502CCF
F52B7F0","norm_data":"8543a6847761d29370f34091291e851d 2018-10-
24T16:50:20.521078Z
b78e174412926b25a0b4d71e5d5871d40fb79d0503b3d2cfde6b1340437b0ed76ad40b70b
19e8dea1229c9679a6b937989fd92ed28a795358857d86c4d77c8321f3a1d83b9e03a911d
c204647c5e634c19d9b22d30b4036492dda88553d8965280a31213a77aa8415d23ed86f9d
00632","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_8a83ebc115403998
05643","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b
2fa417bae","timestamp":1540399805677}


{"hashed_data":"83216D6EEA93B01CAACCB83E6B933102307153017C72873A33A596691
F94101B","norm_data":"8543a6847761d29370f34091291e851d 2018-10-
24T16:50:20.649327Z
6923be7c5b8c3f69a866d0b8f9582f7c7b1c068ea324f9aa9589769440d116ec8e1732678
8e9801a37ec4bb6a1c4e2527a4d3266475eb6e702686c543b57b5181f3a1d83b9e03a911d
c204647c5e634cc62cbd19f332ff14f6957153d2ecbd4980a31213a77aa8415d23ed86f9d
00632","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_a9943caf15403998
05774","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b
2fa417bae","timestamp":1540399805808}


{"hashed_data":"1A81226B84F056B026FED969C7D206A8217A5AE13398E50F68BED35AF
CEEB812","norm_data":"8543a6847761d29370f34091291e851d 2018-10-
24T16:50:20.770845Z
6b29c945bbd43517dc519a0c801ddc8320c909a0b06b92c944c3221311d949646feac2d28
1f8e5b5e3993967c8577d74507e3b60823b735cab27104e7bd9b3251f3a1d83b9e03a911d
c204647c5e634cd4ae4c7c28364b9fbe56effdd23d156c80a31213a77aa8415d23ed86f9d
00632","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_e1456d0b15403998
05894","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b
2fa417bae","timestamp":1540399805929}


{"hashed_data":"D6568B6B4801074BD4DCCF8911138962496892DC30BCBD20756057166
413051E","norm_data":"8543a6847761d29370f34091291e851d 2018-10-
24T16:50:20.889286Z
824a2da1773c48b175a5dedcc304ba8103ec848a41e0a8b430a56e5bc2caaa2b5b8ecd086
ac73d9df7044b729f82b1eaebe3ac0daa11a3217b423d2971c822201f3a1d83b9e03a911d
c204647c5e634cbbe6ff6bd5c84ab8960d389a6edc137680a31213a77aa8415d23ed86f9d
00632","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_9f4e0de815403998
06013","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b
2fa417bae","timestamp":1540399806055}


{"hashed_data":"B87883D8ACC566522D947E889CF27105252337926ED0954278038F40C
E9A86DE","norm_data":"8543a6847761d29370f34091291e851d 2018-10-
24T16:50:21.011536Z
f4c7cf817b8be88c8b6fff5ffac06b14e1087b1f5db53fb67b34b208c56be194bf9a824c2
b8dad2f9fb28d1b0a06bc0bfacae5d61a135d671583d53a21bfee3f1f3a1d83b9e03a911d
c204647c5e634c2f873760b07ba646fd5a9beb6b11d3c880a31213a77aa8415d23ed86f9d
00632","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_982f3e9d15403998
06141","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b
2fa417bae","timestamp":1540399806219}


{"hashed_data":"FAB267227D0005A999B0AF754CF8AB847B8A99AF609902F7DEAFEB0FD
2273471","norm_data":"8543a6847761d29370f34091291e851d 2018-10-
24T16:50:21.137852Z
51f2ff63ec73b438926aca22966f9b691a163994b2b5d9414b74c34a8bb96902e07c846fa
5ca4c24592e98c1cd22a77100d0fdd6baa20e4d9a4aa36f944d198f1f3a1d83b9e03a911d
c204647c5e634c6601860022b15e5a3d54294c6fd21a7780a31213a77aa8415d23ed86f9d
00632","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_c8c180b015403998
06282","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b
2fa417bae","timestamp":1540399806321}
```

```
{"hashed_data":"5B1A930B4ACFF5CD6A19AA21A85102C2609F67D9A088170176862F717
642B46C","norm_data":"8543a6847761d29370f34091291e851d 2018-10-
24T16:50:21.277151Z
e3724c8120faa0cfba49313630aa8ec240bd9bc1a025113c6b13de7383e8e6c61dfa5f8a6
2e8386495c085657b14957c09141bd6c153c6191cf9ac22a7905b851f3a1d83b9e03a911d
c204647c5e634cb06b9e4fa3df43c1bf5f915c346b481d80a31213a77aa8415d23ed86f9d
00632","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_5f78b22315403998
06398","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b
2fa417bae","timestamp":1540399806431}
```

All messages are published under the topic NORMS/DSOSMC/SECAGENT (i.e. the one CI-SOC is subscribed to to receive NORM values), and include the `norm_data` attribute, i.e. SecA formatted messages previously encrypted by local PUF agent on NORM.

5. Check the processing at CI-SOC side. CI-SOC Monitor component first verifies data integrity by validating the hash included in messages sent by SecA, with the help of DCS Agent. If this verification fails a threat is notified to CI-SOC dashboard. Then encrypted message are decrypted by KMM and checked to see whether it is compliant with the format used by SecA. If no error is found, the message is stored in Influx DB and sent to the CI-SOC Analytics module for further processing. An extract of CI-SOC output, related to the first two messages above, is reported below:

```
18/10/24 16:50:21 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"AEE286E2E1E1355741CA83E7419C4C7CA8DEF61A21EA7D31787
54DB5A6D36F64","norm_data":"8543a6847761d29370f34091291e851d 2018-
10-24T16:50:20.144337Z
f70ad5d367ce9ae5484367319bc6a5f4b52ebc0cf766c5cdf2635178da2f86123e0
f924c2d05426e2b9b8099cdb40506f30c1c46f54acb162a28234512107d8a1f3a1d
83b9e03a911dc204647c5e634c3a0af1d719c928d5f7ae7bbc30a72fa980a31213a
77aa8415d23ed86f9d00632","norm_ip":"10.12.0.18","request_id":"HASH_
REQUEST_4bb72b241540399805269","norm_id":"26977d6ab89b65e061ed48b7f
2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1540399805357}

encoded NORM data: 8543a6847761d29370f34091291e851d 2018-10-
24T16:50:20.144337Z
f70ad5d367ce9ae5484367319bc6a5f4b52ebc0cf766c5cdf2635178da2f86123e0
f924c2d05426e2b9b8099cdb40506f30c1c46f54acb162a28234512107d8a1f3a1d
83b9e03a911dc204647c5e634c3a0af1d719c928d5f7ae7bbc30a72fa980a31213a
77aa8415d23ed86f9d00632



KMM service response is:
{"data":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa
417bae frequency 1540392620001 49.971 OK SMM"}

decoded NORM message:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1540392620001 49.971 OK SMM

Storing detected data...

26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1540392620001 49.971 OK SMM

18/10/24 16:50:24 WARN ThresholdFilter: Analysing event to detect
out of range:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1540392620001 49.971 OK SMM



18/10/24 16:50:24 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"E519A64A9EEBF82768BC8B860D79F2905B7DAC616B569F5710C
6E801EC2D9BD2","norm_data":"8543a6847761d29370f34091291e851d 2018-
10-24T16:50:20.272607Z
bd4c59427d8f715f60bed44ae47ce785cd8960b4c01b9bfbaf7022d25b9050435dd
524b94b037c65ef57e934f5a4b08773b0e2962b0d61d1847d8db05acbd48f1f3a1d
83b9e03a911dc204647c5e634c19d9b22d30b4036492dda88553d8965280a31213a
77aa8415d23ed86f9d00632","norm_ip":"10.12.0.18","request_id":"HASH_
```

	REQUEST_d893ef371540399805395","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1540399805453} {"data":"e252d4a7991d3007e38caa6f28b455ff09467fb4aed7d15682bdd34baa1307ee frequency 1540392620251 49.971 OK SMM"} decoded NORM message: e252d4a7991d3007e38caa6f28b455ff09467fb4aed7d15682bdd34baa1307ee frequency 1540392620251 49.971 OK SMM Storing detected data... e252d4a7991d3007e38caa6f28b455ff09467fb4aed7d15682bdd34baa1307ee frequency 1540392620251 49.971 OK SMM 18/10/24 16:50:24 WARN ThresholdFilter: Analysing event to detect out of range: e252d4a7991d3007e38caa6f28b455ff09467fb4aed7d15682bdd34baa1307ee frequency 1540392620251 49.971 OK SMM We can see message received by NORMs (having the same format of the ones reported in step 1), that are printed in clear after decryption performed by KMM. They have the following format: NormId valuetype timestamp value consistency source and we can understand that values were frequencies detected by smart meters (SMM) and that consistency check between SMM and PMU was ok. This indicates that (encrypted) messages sent by NORM are correctly decrypted and pre-processed by CI-SOC.
Comments	The test was successful

Table 34: Test case CSNM:G3:F1:T4 results

Test ID	CSNM:G3:F1:T4		
Test location	At the premises of ENG	**Partner**	ENG
Component	CI-SOC, NORM		
Features under test	CSNM:G3:F1		
Test preparation comments	At the moment of testing in Ireland there were not 10 complete NORMs available, therefore, to emulate 10 NORMs we simply increased the rate by 10. To do that, a Security Agent (SecA) simulator was developed. It receives frequency values transmitted every 2 seconds by smart meters by subscribing to topic "SUCCESS/NORM/ESB001/wally1/Values" and generates and sends to CI-SOC ten messages (instead of one) with the same frequency value.		
Detailed test steps and result	1. The Security Agent simulator was configured to emulate 10 devices by generating ten messages, instead of one, per each frequency value transmitted by NORM in Ireland for about one week (about 3·10^5 messages). The simulator was also configured to send irrelevant data at a percentage of 10%, i.e. 1 device sends events where the SecA formatted message is simply a string and is not compliant to the format NormId valueType timestamp value consistency source. An example of messages sent to CI-SOC is reported below. {"hashed_data":"77C4333451E97F0594C48A6D1D14668BF21FB9198298A2B7AD6BD18C6F219138","norm_data":"8543a6847761d29370f34091291e851d 2018-09-27T09:45:51.269966Z 822208e356b32894e4700cd710d05c895206db8da7099cef7413a415b82981af2a14a91abc568e8f56ebd8b0d377ac67f8eebc1dfdd7db24a4c31020eedbfc2b5b12eea3e71126c22edc3428a4e1c522f3833b9ac616f285180f923ff477cc1b8f801d19712d5d741949a0f74d9fb03a","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_39e72fcf1540431738366","norm_id":"26977d6ab8		

```
9b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timesta
mp":1538041553072}


{"hashed_data":"33F1D5AE7B7F9C10C56F5150E7A83A7209073E5584B5B814
FB8298ACA3EA6E4C","norm_data":"8543a6847761d29370f34091291e851d
2018-09-27T09:45:51.394731Z
4221a077752d9ae91cecf951bc0c2bd259004e9aa20c49010da5d1a2fbcb2722
4f9d0c3158e6e7ee4184927a6f4295a7db8eae37d155ba57517fefe54520561c
5b12eea3e71126c22edc3428a4e1c5226ef7dc2b78a0b95d29a03f44c6ee1bb0
8f801d19712d5d741949a0f74d9fb03a","norm_ip":"10.12.0.18","reques
t_id":"HASH_REQUEST_09d780871540431738489","norm_id":"26977d6ab8
9b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timesta
mp":1538041553456}


{"hashed_data":"AF2C55CA4B713FB7F46A0D579847058F8EBF14BDFE30FC0C
2E0F93A1C553D733","norm_data":"8543a6847761d29370f34091291e851d
2018-09-27T09:45:51.518891Z
94a5207039585deb902cbb1540212d305acbad025324a5ed08980d8efec3b4cf
780c4246b0cf86cac1b19e9266f95527a91ab8d277a6ddc3b79ffc841c245e8d
5b12eea3e71126c22edc3428a4e1c5222674e95e2a80be6d40037a9f8c382d2f
8f801d19712d5d741949a0f74d9fb03a","norm_ip":"10.12.0.18","reques
t_id":"HASH_REQUEST_002c032e1540431738613","norm_id":"26977d6ab8
9b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timesta
mp":1538041553520}


{"hashed_data":"E240C9144DE2033340AEDBA1A991A08613B0E74E51781EC2
D0F73127440B7B26","norm_data":"8543a6847761d29370f34091291e851d
2018-09-27T09:45:51.644487Z
ede43d69db39a0d24b486646a7367f6ef57df63a2c23a658ae37ed39cde42b86
6335af3abe8145289d81cd4bfa1ab446d4a5f0e8c12078760215a67016cc972f
5b12eea3e71126c22edc3428a4e1c5222fee9f988e14d958075851071c73b989
8f801d19712d5d741949a0f74d9fb03a","norm_ip":"10.12.0.18","reques
t_id":"HASH_REQUEST_f188acd61540431738734","norm_id":"26977d6ab8
9b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timesta
mp":1538041553602}


{"hashed_data":"FAB1A667CFB741F604574C623F6D6A28A9B7D47298FA0801
92ACDF2F57C30363","norm_data":"8543a6847761d29370f34091291e851d
2018-09-27T09:45:51.762579Z
0d4e4ed1f87a9348eb67deee52e20099cdff3bedf0baf1d20afd2b241cccfebf
","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_297031571540
431738868","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b41320
8b25b34ee9f9b2fa417bae","timestamp":1538041553595}


{"hashed_data":"7B4CD77B6BA0A41A427F0B5F0946A68B8409931ECA0D9808
FFB00DD147534E9E","norm_data":"8543a6847761d29370f34091291e851d
2018-09-27T09:45:51.897175Z
83ba27cc3961ae61c96e932b5d864eac3da6d59e3c79744390b55c8ce85d4235
269e69c9588aa6ab90bddb9297c44bdc97eb53cf5a957c536ea5aab23ac0c07f
5b12eea3e71126c22edc3428a4e1c522898ac3e5c8c8453af3bf1c23c0dcf36a
8f801d19712d5d741949a0f74d9fb03a","norm_ip":"10.12.0.18","reques
t_id":"HASH_REQUEST_13ee64341540431738997","norm_id":"26977d6ab8
9b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timesta
mp":1538041553733}


{"hashed_data":"C2F04FC7C524C2290E4C6A8949717589BBFE57EA616BACB8
5A3B22B33424B107","norm_data":"8543a6847761d29370f34091291e851d
2018-09-27T09:45:52.025017Z
eb0659c1c72ff893d3242879d47b146ae1a04da830e38bb858f90ed57d1a1619
b7bd3b9e27200b042be5cdd53996a6bfda7ce8481be6d1c9fdbfae680f069191
5b12eea3e71126c22edc3428a4e1c522e14d940ae5c13427c4084d9615b8dcef
8f801d19712d5d741949a0f74d9fb03a","norm_ip":"10.12.0.18","reques
t_id":"HASH_REQUEST_f2ca362a1540431739123","norm_id":"26977d6ab8
9b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timesta
mp":1538041553797}
```

```
{"hashed_data":"C7610EE62B24CCB177DED2FF4338A75314A3A4BF41673F22
604D19AC0AD321D9","norm_data":"8543a6847761d29370f34091291e851d
2018-09-27T09:45:52.150685Z
e38a7f1adc30258b98a1c91e48342c9ed3dd843c9fe6e302553620265697d0e4
8d92da31f54634971ac05a00e539fd675d4b51d388bda0a63b8aef60bdf6c5bc
5b12eea3e71126c22edc3428a4e1c522549abcd2a8cea7b8839948f3fc5e6641
8f801d19712d5d741949a0f74d9fb03a","norm_ip":"10.12.0.18","reques
t_id":"HASH_REQUEST_be0e234a1540431739253","norm_id":"26977d6ab8
9b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timesta
mp":1538041553804}
```

```
{"hashed_data":"3C171291C094720EA9ED040B234D9EBF03A7088439A917E7
89396D2D12E37F20","norm_data":"8543a6847761d29370f34091291e851d
2018-09-27T09:45:52.281106Z
da22a1b84b71e88f699ee23ea90309d7aa1e6c58ba1064d5454450032ead933d
3b6387be8235d9bb40a10206117c1352e8958506d038310bb6fa1b2d7819a581
5b12eea3e71126c22edc3428a4e1c5221af2eb570d3ae361f6c48be401af1f28
8f801d19712d5d741949a0f74d9fb03a","norm_ip":"10.12.0.18","reques
t_id":"HASH_REQUEST_1bd370c61540431739382","norm_id":"26977d6ab8
9b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timesta
mp":1538041553838}
```

```
{"hashed_data":"CD5B66A4F5244C40FC88D008BB8D5829ED367276134C1A9B
E52371D197D99389","norm_data":"8543a6847761d29370f34091291e851d
2018-09-27T09:45:52.035687Z
0d4e4ed1f87a9348eb67deee52e20099cdff3bedf0baf1d20afd2b241cccfebf
","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_dfe652c91540
431740148","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b41320
8b25b34ee9f9b2fa417bae","timestamp":1538041553916}
```

One of the above message, randomly chosen, is replaced by the following, including irrelevant NORM data:

```
{"hashed_data":"ab4bcfa7763817f70961729ef73753411af62215","norm_
data":"jdfhu488djhjkkjl834jjkfdflk","norm_ip":"161.27.62.300","r
equest_id":"HASH_REQUEST_44a78b3d1523265631837","timestamp":1523
265643733}
```

One of the above messages contains irrelevant data.

2. Check the processing performed by CI-SOC Monitor, that first verifies data integrity then decrypts NORM data with KMM support. If encrypted and decrypted data is not properly formatted, or includes incorrect values, the related event is discarded and not further processed by the Analytics module to detect threshold exceeding. Moreover, a potential threat is notified to CI-SOC Dashboard. An extract of CI-SOC output, is reported below. In particular, we have included CI-SOC output messages related to the processing of a "correct" message and of an "incorrect" one.

```
18/09/27 09:45:55 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"33F1D5AE7B7F9C10C56F5150E7A83A7209073E5584B5B814
FB8298ACA3EA6E4C","norm_data":"8543a6847761d29370f34091291e851d
2018-09-27T09:45:51.394731Z
4221a077752d9ae91cecf951bc0c2bd259004e9aa20c49010da5d1a2fbcb2722
4f9d0c3158e6e7ee4184927a6f4295a7db8eae37d155ba57517fefe54520561c
5b12eea3e71126c22edc3428a4e1c5226ef7dc2b78a0b95d29a03f44c6ee1bb0
8f801d19712d5d741949a0f74d9fb03a","norm_ip":"10.12.0.18","reques
t_id":"HASH_REQUEST_09d780871540431738489","norm_id":"26977d6ab8
9b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timesta
mp":1538041553456}

KMM service response is:
{"data":"e252d4a7991d3007e38caa6f28b455ff09467fb4aed7d15682bdd34
baa1307ee frequency 1538041550381 50.075 OK SMM"}

decoded NORM message:
e252d4a7991d3007e38caa6f28b455ff09467fb4aed7d15682bdd34baa1307ee
frequency 1538041550381 50.075 OK SMM

Storing detected data...
```

<table>
<tr><td></td><td><pre>e252d4a7991d3007e38caa6f28b455ff09467fb4aed7d15682bdd34baa1307ee
frequency 1538041550381 50.075 OK SMM

18/09/27 09:45:55 WARN ThresholdFilter: Analysing event to
detect out of range:
e252d4a7991d3007e38caa6f28b455ff09467fb4aed7d15682bdd34baa1307ee
frequency 1538041550381 50.075 OK SMM</pre>
<p>After having verified data integrity, the attribute <code>norm_data</code> encrypted by the Security Agent, is extracted and, if properly formatted, sent to KMM for decrypting it. Finally, the decoded data, if properly formatted and including a correct NormId, further processed by the CI-SOC Analytics module to detect eventual threshold exceeding.</p>
<pre>18/09/27 09:45:55 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"CD5B66A4F5244C40FC88D008BB8D5829ED367276134C1A9B
E52371D197D99389","norm_data":"8543a6847761d29370f34091291e851d
2018-09-27T09:45:52.035687Z
0d4e4ed1f87a9348eb67deee52e20099cdff3bedf0baf1d20afd2b241cccfebf
","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_dfe652c91540
431740148","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b41320
8b25b34ee9f9b2fa417bae","timestamp":1538041553916}

KMM service response is: {"data":"sdk37GG9um593Y0co"}

decoded NORM message: sdk37GG9um593Y0co

18/09/27 09:45:55 ERROR EventConverter: NORM data not properly
formatted. It should be: normId valueType timestamp value
consistency source

18/09/27 09:45:55 WARN ThresholdFilter: Analysing event to detect
out of range: null</pre>
<p>The same processing is being performed but, in this case, the decrypted messages is not properly formatted, as explained in the CI-SOC message. This event is discarded and not further processed to discover possible threats.</p></td></tr>
<tr><td><b>Comments</b></td><td>The test was successful</td></tr>
</table>

B.4 Test results for functional features CSNM:G7

B.4.1 Test results for feature CSNM:G7:F1

Test results for feature CSNM:G7:F1 are reported in the following tables.

Table 35: Test case CSNM:G7:F1:T1 results

<table>
<tr><td><b>Test ID</b></td><td colspan="3">CSNM:G7:F1:T1</td></tr>
<tr><td><b>Test location</b></td><td>At the premises of ENG</td><td><b>Partner</b></td><td>ENG</td></tr>
<tr><td><b>Component</b></td><td colspan="3">CI-SOC, NORM</td></tr>
<tr><td><b>Features under test</b></td><td colspan="3">CSNM:G7:F1</td></tr>
<tr><td><b>Test preparation comments</b></td><td colspan="3">Software configuration verification is performed by checking the SHA-256 checksum of the jar file containing SecA agent (<code>NormSecurityAgent.jar</code>).</td></tr>
<tr><td><b>Detailed test steps and result</b></td><td colspan="3">1. In the first iteration the correct NormSecurityAgent.jar file has been used. SecA generates the checksum at startup and sends it to CI-SOC via MQTT, as shown below:
<pre>PUF endpoint: http://10.12.0.26:8080/ - vendor: ESB
JerseyWebTarget { http://10.12.0.26:8080/id }</pre></td></tr>
</table>

	`/id - HTTP Response Status: 200`
	`*********** NormId has been generated: 26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae`
	`Connecting to broker: tcp://127.0.0.1:1883`
	`Connected to broker: tcp://127.0.0.1:1883`
	`subscribed to topic NORM/SECAGENT/DCSAGENT`
	`subscribed to topic SUCCESS/NORM/ESB001/wally1/Values`
	`subscribed to topic SUCCESS/NORM/ESB001/PMU/Values`
	`NORM software configuration checksum is: DA6577E156CBAE95C0245B8AB3B26F743BF8A2651B1968A9CA6A7CD153E22885`
	`Publication completed: DA6577E156CBAE95C0245B8AB3B26F743BF8A2651B1968A9CA6A7CD153E22885`
	2. Once received the checksum from SecA, CI-SOC verifies that it corresponds to the value stored in CI-SOC configuration file:
	`Connecting to broker: tcp://10.12.0.18:1883`
	`Connected to broker: tcp://10.12.0.1:1883`
	`subscribed to topic NORM/CHECKSUM`
	`18/10/04 10:31:01 WARN NativeCodeLoader: Unable to load native-hadoop library for your platform... using builtin-java classes where applicable`
	`18/10/04 10:31:10 WARN SUCCESSMonitor: NORM software configuration successfully checked`
	3. In the second iteration the file NormSecurityAgent.jar file has been replaced with another jar file oif about the same size, keeping the same name of course. SecA generates the checksum at startup and sends it to CI-SOC via MQTT, as shown below:
	`PUF endpoint: http://10.12.0.26:8080/ - vendor: ESB`
	`JerseyWebTarget { http://10.12.0.26:8080/id }`
	`/id - HTTP Response Status: 200`
	`*********** NormId has been generated: 26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae`
	`Connecting to broker: tcp://127.0.0.1:1883`
	`Connected to broker: tcp://127.0.0.1:1883`
	`subscribed to topic NORM/SECAGENT/DCSAGENT`
	`subscribed to topic SUCCESS/NORM/ESB001/wally1/Values`
	`subscribed to topic SUCCESS/NORM/ESB001/PMU/Values`
	`NORM software configuration checksum is:`
	`65BDADCB6576C882BAFA9F2A038467547EC596F6AC4CE8E73D65994DD26DC878`
	`Publication completed: 65BDADCB6576C882BAFA9F2A038467547EC596F6AC4CE8E73D65994DD26DC878`
	4. Once received the checksum from SecA, CI-SOC verifies that it corresponds to the value stored in CI-SOC configuration file. The verification fails, therefore an error is reported and a threat is notified to the Dashboard, as displayed below:
	`Connecting to broker: tcp://10.12.0.18:1883`
	`Connected to broker: tcp://10.12.0.1:1883`
	`subscribed to topic NORM/CHECKSUM`
	`18/10/04  10:34:07 WARN NativeCodeLoader: Unable to load native-hadoop library for your platform... using builtin-java classes where applicable`
	`18/10/04 10:34:15 ERROR SUCCESSMonitor: NORM software configuration has been changed`

Comments	The test was successful.

Table 36: Test case CSNM:G7:F1:T2 results

Test ID	CSNM:G7:F1:T2		
Test location	At the premises of ENG	**Partner**	ENG
Component	CI-SOC, NORM		
Features under test	CSNM:G7:F1		
Test preparation comments	Security Agent on NORM generates the `NORMId` at startup from `RPIId`, `PMUId`, `SMMId` and `PUFId` values (as described in [8]). The first three values		

	are stored in the SecA configuration file, while PuFId is returned at runtime by the Local PUF Agent. CI-SOC has stored on its side all the valid NORM identifiers.

Detailed test steps and result	1. In the first iteration the correct identifiers of the hardware components belonging to NORM are used: `smxRaspberryId`=0000000072057ed7 and `pmuRaspberryId`=00000000d7a6cdf8. Therefore SecA generates the correct `NORMId` at startup, then transmits detected frequencies to CI-SOC as usual:
	`PUF endpoint: http://10.12.0.26:8080/ - vendor: ESB`
	`JerseyWebTarget { http://10.12.0.26:8080/id }`
	`/id - HTTP Response Status: 200`
	`********** hardware configuration: pmuId: 00000000d7a6cdf8 rpiId: 0000000072057ed7 pufId: 8543a6847761d29370f34091291e851d`
	`*********** NormId has been generated:`
	`26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae`
	`Connecting to broker: tcp://127.0.0.1:1883`
	`Connected to broker: tcp://127.0.0.1:1883`
	`subscribed to topic NORM/SECAGENT/DCSAGENT`
	`subscribed to topic SUCCESS/NORM/ESB001/wally1/Values`
	`subscribed to topic SUCCESS/NORM/ESB001/PMU/Values`
	`NORM software configuration checksum is:`
	`DA6577E156CBAE95C0245B8AB3B26F743BF8A2651B1968A9CA6A7CD153E22885`
	`Publication completed:`
	`DA6577E156CBAE95C0245B8AB3B26F743BF8A2651B1968A9CA6A7CD153E22885`
	
	`{"hashed_data":"839484988B28C24DD356CB1571E3805C8D2562412D1616D7AFC6CFC3DF2F4394","norm_data":"8543a6847761d29370f34091291e851d 2018-10-25T10:29:35.178459Z 32e866152462cecfe0265eaf8501fc9ae2e73d939e0b1cb18963994e27af068d219bf9bed14ec17632bc16455341de7e0f4e74fda81b45937929dfb4b671b36a69be418995141b10203bc6ce22218e1596101d1ebc98356156eeb409d440dca2","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_569547c41540463359192","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1540463359255}`
	2. On its side, CI-SOC receives NORM data and correctly decrypts and processes it
	`18/10/25 12:29:49 WARN EventConverter: EVENT RECEIVED: {"hashed_data":"839484988B28C24DD356CB1571E3805C8D2562412D1616D7AFC6CFC3DF2F4394","norm_data":"8543a6847761d29370f34091291e851d 2018-10-25T10:29:35.178459Z 32e866152462cecfe0265eaf8501fc9ae2e73d939e0b1cb18963994e27af068d219bf9bed14ec17632bc16455341de7e0f4e74fda81b45937929dfb4b671b36a69be418995141b10203bc6ce22218e1596101d1ebc98356156eeb409d440dca2","norm_ip":"10.12.0.18","request_id":"HASH_REQUEST_569547c41540463359192","norm_id":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1540463359255}`
	
	`KMM service response is:`
	`{"data":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae frequency 0 50.05 OK SMM"}`
	`decoded NORM message:`
	`26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae frequency 0 50.05 OK SMM`
	`18/10/25 12:29:49 WARN EventConverter: NormId succesfully verified`
	`Storing detected data...`
	`26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae frequency 0 50.05 OK SMM`
	`18/10/25 12:29:49 WARN ThresholdFilter: Analysing event to detect out of range:`
	`26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae frequency 0 50.05 OK SMM`

3. In the second iteration the identifiers of the hardware components have been changed: : smxRaspberryId=0000000072057ef8 and have been modified: smxRaspberryId= 0000000072057ef8 and pmuRaspberryId=00000000d7a6cee8. SecA generates a wrong NORM identifier and formats messages with an incorrect identifier. SecA messages are encrypted anyway and sent to CI-SOC:

```
PUF endpoint: http://10.12.0.26:8080/ - vendor: ESB
JerseyWebTarget { http://10.12.0.26:8080/id }
/id - HTTP Response Status: 200
********** hardware configuration: pmuId: 00000000d7a6cee8 rpiId:
0000000072057ef8 pufId: 8543a6847761d29370f34091291e851d
*********** NormId has been generated:
3de5dab73ef7f670778562be408a922d79a592f482a30c66fd8f85a058c22cea
Connecting to broker: tcp://127.0.0.1:1883
Connected to broker: tcp://127.0.0.1:1883
subscribed to topic NORM/SECAGENT/DCSAGENT
subscribed to topic SUCCESS/NORM/ESB001/wally1/Values
subscribed to topic SUCCESS/NORM/ESB001/PMU/Values
NORM software configuration checksum is:
DA6577E156CBAE95C0245B8AB3B26F743BF8A2651B1968A9CA6A7CD153E22885
Publication completed:
DA6577E156CBAE95C0245B8AB3B26F743BF8A2651B1968A9CA6A7CD153E22885


{"hashed_data":"C83A4EBAC6BC1C17D3BB9EE3B3C7FF39A995EEFCF1D451C6239
32729342C5457","norm_data":"8543a6847761d29370f34091291e851d 2018-
10-25T10:34:50.271297Z
7e98918b15e4c7c9c019734d8e7c194e12019c56a1ac1a32f1944ce8a05990bf37e
c76d42acce0c86da4d8b1f0a9659251f517540f8a114c72cfcddfa26d09cf69be41
8995141b10203bc6ce22218e1548e2f6a91d60c93860eabfe1a81aea78","norm_i
p":"10.12.0.18","request_id":"HASH_REQUEST_97e04c3a1540463670810","
norm_id":"3de5dab73ef7f670778562be408a922d79a592f482a30c66fd8f85a05
8c22cea","timestamp":1540463670855}
```

4. CI-SOC receives NORM data but does not succeed in decrypting it because of an error raised by KMM due to the invalid NORMId

```
18/10/25 12:34:58 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"C83A4EBAC6BC1C17D3BB9EE3B3C7FF39A995EEFCF1D451C6239
32729342C5457","norm_data":"8543a6847761d29370f34091291e851d 2018-
10-25T10:34:50.271297Z
7e98918b15e4c7c9c019734d8e7c194e12019c56a1ac1a32f1944ce8a05990bf37e
c76d42acce0c86da4d8b1f0a9659251f517540f8a114c72cfcddfa26d09cf69be41
8995141b10203bc6ce22218e1548e2f6a91d60c93860eabfe1a81aea78","norm_i
p":"10.12.0.18","request_id":"HASH_REQUEST_97e04c3a1540463670810","
norm_id":"3de5dab73ef7f670778562be408a922d79a592f482a30c66fd8f85a05
8c22cea","timestamp":1540463670855}
KMM service response is: 406
18/10/25 12:34:58 ERROR EventConverter: KMM decoding error: NormId
has not been recognized
18/10/25 12:34:58 WARN ThresholdFilter: Analysing event to detect
out of range: null
```

Comments	The test was successful

Table 37: Test case CSNM:G7:F1:T3 results

Test ID	CSNM:G7:F1:T2		
Test location	At the premises of SYN	**Partner**	SYN
Component	CI-SOC, NORM		

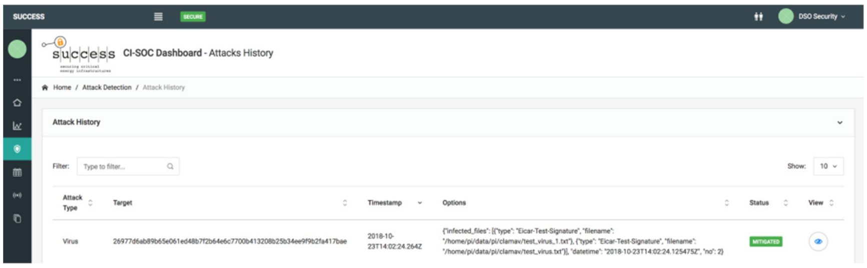
<table>
<tr><td><b>Features under test</b></td><td>CSNM:G7:F1</td></tr>
<tr><td><b>Test preparation comments</b></td><td>The tests CSNM:G3:F1:T2 and all tests falling under CSNM:G1 were successfully conducted.</td></tr>
<tr><td><b>Detailed test steps and result</b></td><td>
1. An hourly scan was setup at NORM side in order to check for viruses.
2. At some point, we downloaded the EICAR[4] virus test file and placed it under a NORM filesystem directory:
<pre>
pi@SMX43-ESB002:~/clamav$ curl
https://www.eicar.org/download/eicar.com.txt >
test_virus.txt
pi@SMX43-ESB002:~/clamav$ curl
https://www.eicar.org/download/eicar.com.txt >
test_virus_1.txt
pi@SMX43-ESB002:~/clamav$ ls
test_virus_1.txt test_virus.txt
pi@SMX43-ESB002:~/clamav$ pwd
/home/pi/data/pi/clamav
</pre>
3. When the time for the scan came, the CI-SOC was notified that the virus was detected and removed:
<pre>
pi@SMX43-ESB002:~/clamav$ ls
pi@SMX43-ESB002:~/clamav$ pwd
/home/pi/data/pi/clamav
</pre>
And at the CI-SOC side we got an indication that the viruses were detected and deleted:

SUCCESS
SECURE
DSO Security
success
securing critical energy infrastructures
CI-SOC Dashboard - Attacks History
Home / Attack Detection / Attack History
Attack History
Filter:
Type to filter...
Show: 10
<table>
<tr><th>Attack Type</th><th>Target</th><th>Timestamp</th><th>Options</th><th>Status</th><th>View</th></tr>
<tr><td>Virus</td><td>26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae</td><td>2018-10-23T14:02:24.264Z</td><td>{"infected_files": [{"type": "Eicar-Test-Signature", "filename": "/home/pi/data/pi/clamav/test_virus_1.txt"}, {"type": "Eicar-Test-Signature", "filename": "/home/pi/data/pi/clamav/test_virus.txt"}], "datetime": "2018-10-23T14:02:24.125475Z", "no": 2}</td><td>MITIGATED</td><td></td></tr>
</table>
</td></tr>
<tr><td><b>Comments</b></td><td>The test was successful.</td></tr>
</table>

Table 38: Test case CSNM:G7:F1:T4 results

<table>
<tr><td><b>Test ID</b></td><td colspan="3">CSNM:G7:F1:T4</td></tr>
<tr><td><b>Test location</b></td><td>At the premises of SYN/ENG</td><td><b>Partner</b></td><td>SYN</td></tr>
<tr><td><b>Component</b></td><td colspan="3">CI-SOC, NORM</td></tr>
<tr><td><b>Features under test</b></td><td colspan="3">CSNM:G7:F1</td></tr>
<tr><td><b>Test preparation comments</b></td><td colspan="3">The tests CSNM:G3:F1:T2 and all tests falling under CSNM:G1 were successfully conducted.</td></tr>
<tr><td><b>Detailed test steps and result</b></td><td colspan="3">
1. The open ports of the NORM should be 22 (SSH), 8080 (PUF firmware), 80/443 (SMX) and 1883 (MQTT).
2. We run an nmap command against the NORM to check the open ports:
<pre>
$ nmap -p- 10.12.0.26
Starting Nmap 7.70 (https://nmap.org) at 2018-10-23
16:20 EEST
Nmap scan report for 10.12.0.26 (10.12.0.26)
</pre>
</td></tr>
</table>

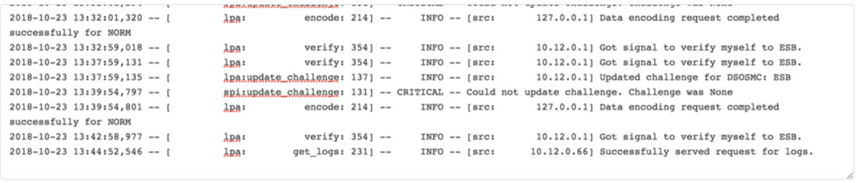
[4] http://www.eicar.org/86-0-Intended-use.html

	`Host is up (0.13s latency).`
	`Not shown: 65530 filtered ports`
	`PORT      STATE  SERVICE`
	`22/tcp    open   ssh`
	`80/tcp    open   http`
	`443/tcp   closed https`
	`1883/tcp  open   mqtt`
	`8080/tcp  open   http-proxy`

Comments	The test was successful.

Table 39: Test case CSNM:G7:F1:T5 results

Test ID	CSNM:G7:F1:T5		
Test location	At the premises of SYN	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G7:F1		
Test preparation comments	N/A		

Detailed test steps and result	1. After logging into the Dashboard, we clicked on the “Testing suite” tab.
	2. The deployed NORM was selected and the logs were available as per the figure below.
	
	`2018-10-23 13:32:01,320 -- [          lpa:           encode: 214] --     INFO -- [src:       127.0.0.1] Data encoding request completed successfully for NORM`
	`2018-10-23 13:32:59,018 -- [          lpa:           verify: 354] --     INFO -- [src:       10.12.0.1] Got signal to verify myself to ESB.`
	`2018-10-23 13:37:59,131 -- [          lpa:           verify: 354] --     INFO -- [src:       10.12.0.1] Got signal to verify myself to ESB.`
	`2018-10-23 13:37:59,135 -- [          lpa:update_challenge: 137] --     INFO -- [src:       10.12.0.1] Updated challenge for DSOSMC: ESB`
	`2018-10-23 13:39:54,797 -- [          spi:update_challenge: 131] -- CRITICAL -- Could not update challenge. Challenge was None`
	`2018-10-23 13:39:54,801 -- [          lpa:           encode: 214] --     INFO -- [src:       127.0.0.1] Data encoding request completed successfully for NORM`
	`2018-10-23 13:42:58,977 -- [          lpa:           verify: 354] --     INFO -- [src:       10.12.0.1] Got signal to verify myself to ESB.`
	`2018-10-23 13:44:52,546 -- [          lpa:         get_logs: 231] --     INFO -- [src:      10.12.0.66] Successfully served request for logs.`		

Comments	The test was successful.		

B.5 Test results for functional features CSNM:G10

B.5.1 Test results for feature CSNM:G10:F1

Test results for feature CSNM:G10:F1 are reported in the following tables.

Table 40: Test case CSNM:G10:F1:T1 results

Test ID	CSNM:G10:F1:T1		
Test location	At the premises of ENG	**Partner**	ENG
Component	CI-SOC, NORM		
Features under test	CSNM:G10:F1		
Test preparation comments	At the moment of testing in Ireland there was only one complete NORM available, therefore, to emulate two NORMs we simply duplicate messages. To do that, a Security Agent (SecA) simulator was developed. It receives frequency values transmitted every 2 seconds by smart meters by subscribing to topic “`SUCCESS/NORM/ESB001/wally1/Values`” and generates and sends to CI-SOC two messages (instead of one): one with		

	the detected value and the other with an increased value in order to trigger a threshold exceeding and distinguish between the two situations for testing purposes. Instead of using irrelevant data, shoes proper management has been tested in DSNM:G3:F1:T4, we decided to treat as "compromised" the devices measuring too high frequencies.
Detailed test steps and result	1. The Security Agent was configured simulator to emulate two devices by generating two messages, instead of one, per each frequency value transmitted by NORM in. The simulator was also configured to send increased frequency to trigger a threshold exceeding threat. An example of messages sent to CI-SOC is reported below: {"hashed_data":"02A736C2A36BA3358C21ECBDBFC525FF31040E25787D0AC90FC 239D840A28387","norm_data":"8543a6847761d29370f34091291e851d 2018- 10-25T12:13:15.134266Z 56c77b5b736a14b4aad4e114302621608f1dd338d2de8e6ebb8437656024238e3c1 abb6c565d05aa367d07bed471fe69d77f6134d384179615705eec1a20e06f2e58b9 a1f367b0e66dee5596f9f864ee30ba0c92cb83c633babe7acc25ceea1385bb50e51 d75a48684df4436c06a62f4","norm_ip":"10.12.0.18","request_id":"HASH_ REQUEST_92ccc3a51540469574122","norm_id":"26977d6ab89b65e061ed48b7f 2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1540469574212} {"hashed_data":"5225A35BB11E544CF160A8E738DDCC1FA99319EAE553EFBAF1A F64462000595F","norm_data":"8543a6847761d29370f34091291e851d 2018- 10-25T12:13:15.260290Z d93b2c03754634ca3dc1c2467e757acb5745ad98c640a0d386a408960716b12de90 e564dad53ad08cd1fa7f0ddce5346a4328a75e1efc52cac7c8d05fa2fdc7d2e58b9 a1f367b0e66dee5596f9f864ee40d8179d0c2e336c1513b628b47acf7f85bb50e51 d75a48684df4436c06a62f4","norm_ip":"10.12.0.18","request_id":"HASH_ REQUEST_31d720e91540469574246","norm_id":"e252d4a7991d3007e38caa6f2 8b455ff09467fb4aed7d15682bdd34baa1307ee","timestamp":1540469574330} {"hashed_data":"BF4CBCA5B1F8E78C70D450D64F14193F534D75619E5E22E3FEE 1EF40F00BC4A3","norm_data":"8543a6847761d29370f34091291e851d 2018- 10-25T12:13:15.435528Z 56c77b5b736a14b4aad4e114302621608f1dd338d2de8e6ebb8437656024238e3c1 abb6c565d05aa367d07bed471fe69d77f6134d384179615705eec1a20e06f2e58b9 a1f367b0e66dee5596f9f864ee30ba0c92cb83c633babe7acc25ceea1385bb50e51 d75a48684df4436c06a62f4","norm_ip":"10.12.0.18","request_id":"HASH_ REQUEST_a9ad57201540469574421","norm_id":"26977d6ab89b65e061ed48b7f 2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1540469574463} {"hashed_data":"E0CC78B9A7D691EDE1FFD048DE1764D0073FD1B9F5E2A893186 50B67ACBE6CF1","norm_data":"8543a6847761d29370f34091291e851d 2018- 10-25T12:13:15.563364Z d93b2c03754634ca3dc1c2467e757acb5745ad98c640a0d386a408960716b12de90 e564dad53ad08cd1fa7f0ddce5346a4328a75e1efc52cac7c8d05fa2fdc7d2e58b9 a1f367b0e66dee5596f9f864ee40d8179d0c2e336c1513b628b47acf7f85bb50e51 d75a48684df4436c06a62f4","norm_ip":"10.12.0.18","request_id":"HASH_ REQUEST_3fe11f451540469574553","norm_id":"e252d4a7991d3007e38caa6f2 8b455ff09467fb4aed7d15682bdd34baa1307ee","timestamp":1540469574610} {"hashed_data":"5D19260FCCAF561B62AF6155A7985A650A280C1E710DE6617CD 85D88FA28284B","norm_data":"8543a6847761d29370f34091291e851d 2018- 10-25T12:13:20.129791Z 56c77b5b736a14b4aad4e114302621608f1dd338d2de8e6ebb8437656024238e3c1 abb6c565d05aa367d07bed471fe69d77f6134d384179615705eec1a20e06f2e58b9 a1f367b0e66dee5596f9f864eecbc607864767ecc0768c28edf96a79f5bd6386fce 33edd696ceb2c67d2c125f5","norm_ip":"10.12.0.18","request_id":"HASH_ REQUEST_b362898d1540469579115","norm_id":"26977d6ab89b65e061ed48b7f 2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1540469579206} {"hashed_data":"146AB6A7EAB89871482A0378B435DC3C1B3155B0E5D43FBDE28 F56A2191A18C9","norm_data":"8543a6847761d29370f34091291e851d 2018- 10-25T12:13:20.250692Z d93b2c03754634ca3dc1c2467e757acb5745ad98c640a0d386a408960716b12de90 e564dad53ad08cd1fa7f0ddce5346a4328a75e1efc52cac7c8d05fa2fdc7d2e58b9 a1f367b0e66dee5596f9f864eeff060101f6209863e1cda0f11e818f1dbd6386fce 33edd696ceb2c67d2c125f5","norm_ip":"10.12.0.18","request_id":"HASH_ REQUEST_76d3a2571540469579243","norm_id":"26977d6ab89b65e061ed48b7f 2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1540469579289} 2. CI-SOC receives NORM messages and processed them by verifying data integrity, decrypting them with KMM features and processing them

to detect potential threat. We report in the following how CI-SOC manages the two different situations considered in this test: normal situation, when frequencies measured by NORM fall in the predefined range, and abnormal situation, when detected frequencies are out of range and the NORM measuring them is considered as compromised.

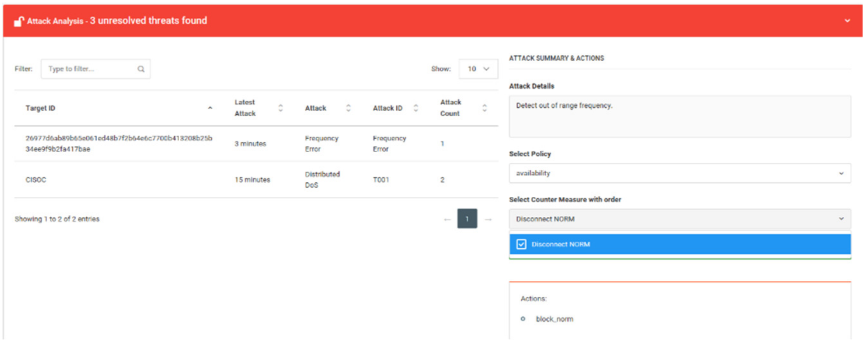
3. CI-SOC processing of in-range frequencies is shown below:

```
18/10/25 14:13:02 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"5225A35BB11E544CF160A8E738DDCC1FA99319EAE553EFBAF1A
F64462000595F","norm_data":"8543a6847761d29370f34091291e851d 2018-
10-25T12:13:15.260290Z
d93b2c03754634ca3dc1c2467e757acb5745ad98c640a0d386a408960716b12de90
e564dad53ad08cd1fa7f0ddce5346a4328a75e1efc52cac7c8d05fa2fdc7d2e58b9
a1f367b0e66dee5596f9f864ee40d8179d0c2e336c1513b628b47acf7f85bb50e51
d75a48684df4436c06a62f4","norm_ip":"10.12.0.18","request_id":"HASH_
REQUEST_31d720e91540469574246","norm_id":"e252d4a7991d3007e38caa6f2
8b455ff09467fb4aed7d15682bdd34baa1307ee","timestamp":1540469574330}
encoded NORM data: 8543a6847761d29370f34091291e851d 2018-10-
25T12:13:15.260290Z
d93b2c03754634ca3dc1c2467e757acb5745ad98c640a0d386a408960716b12de90
e564dad53ad08cd1fa7f0ddce5346a4328a75e1efc52cac7c8d05fa2fdc7d2e58b9
a1f367b0e66dee5596f9f864ee40d8179d0c2e336c1513b628b47acf7f85bb50e51
d75a48684df4436c06a62f4
18/10/25 14:13:03 ERROR EventConverter: Norm Id NormId succesfully
verified
18/10/25 14:13:03 WARN ThresholdFilter: Analysing event to detect
out of range: null
KMM service response is:

{"data":"e252d4a7991d3007e38caa6f28b455ff09467fb4aed7d15682bdd34baa
1307ee frequency 1538041550381 50.066 OK SMM"}

decoded NORM message:
  e252d4a7991d3007e38caa6f28b455ff09467fb4aed7d15682bdd34baa1307ee
frequency 1538041550381 50.066 OK SMM
8543a6847761d29370f34091291e851d 2018-10-25T12:13:15.260290Z
Storing detected data...
e252d4a7991d3007e38caa6f28b455ff09467fb4aed7d15682bdd34baa1307ee
frequency 1538041550381 50.066 OK SMM
18/10/25 14:13:03 WARN ThresholdFilter: Analysing event to detect
out of range:
 e252d4a7991d3007e38caa6f28b455ff09467fb4aed7d15682bdd34baa1307ee
frequency 1538041550381 50.066 OK SMM
```

No further message is reported, indicating that processing performed by the Analytics module did not detect a threshold exceeding

4. CI-SOC processing of out-of-range frequencies is displayed in the following

```
18/10/25 14:13:01 WARN EventConverter: EVENT RECEIVED:
{"hashed_data":"02A736C2A36BA3358C21ECBDBFC525FF31040E25787D0AC90FC
239D840A28387","norm_data":"8543a6847761d29370f34091291e851d 2018-
10-25T12:13:15.134266Z
56c77b5b736a14b4aad4e114302621608f1dd338d2de8e6ebb8437656024238e3c1
abb6c565d05aa367d07bed471fe69d77f6134d384179615705eec1a20e06f2e58b9
a1f367b0e66dee5596f9f864ee30ba0c92cb83c633babe7acc25ceea1385bb50e51
d75a48684df4436c06a62f4","norm_ip":"10.12.0.18","request_id":"HASH_
REQUEST_92ccc3a51540469574122","norm_id":"26977d6ab89b65e061ed48b7f
2b64e6c7700b413208b25b34ee9f9b2fa417bae","timestamp":1540469574212}
encoded NORM data: 8543a6847761d29370f34091291e851d 2018-10-
25T12:13:15.134266Z
56c77b5b736a14b4aad4e114302621608f1dd338d2de8e6ebb8437656024238e3c1
abb6c565d05aa367d07bed471fe69d77f6134d384179615705eec1a20e06f2e58b9
a1f367b0e66dee5596f9f864ee30ba0c92cb83c633babe7acc25ceea1385bb50e51
d75a48684df4436c06a62f4
WARN EventConverter: NormId succesfully verified
KMM service response is:
{"data":"26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa
417bae frequency 1538041550131 52.066 OK SMM"}
decoded NORM message:
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1538041550131 52.066 OK SMM
Storing detected data...
26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae
frequency 1538041550131 52.066 OK SMM
```

	`18/10/25 14:13:02 WARN ThresholdFilter: Analysing event to detect out of range: 26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae frequency 1538041550131 52.066 OK SMM`
	`18/10/25 14:13:02 ERROR EventAggregator: Detected frequency is out of bounds: 26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae frequency 1538041550131 52.066 OK SMM`
	Since a threshold exceeding has been discovered, CI-SOC Dashboard is notified of the out of range frequency threat via MQTT, i.e. publishing on the topic dedicated to this threat: `success/frequency/{norm_id}`. The payload of the MQTT message is `26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae frequency 1538041550131 52.066 OK SMM`
	Having detected the error, the Dashboard provided the option to disconnect the NORM device:
	
	Attack Analysis - 3 unresolved threats found
	Filter: Type to filter... Show: 10
	Target ID | Latest Attack | Attack | Attack ID | Attack Count
	26977d6ab89b65e061ed48b7f2b64e6c7700b413208b25b34ee9f9b2fa417bae | 3 minutes | Frequency Error | Frequency Error | 1
	CISOC | 15 minutes | Distributed DoS | T001 | 2
	Showing 1 to 2 of 2 entries
	ATTACK SUMMARY & ACTIONS
	Attack Details
	Detect out of range frequency.
	Select Policy
	availability
	Select Counter Measure with order
	Disconnect NORM
	☑ Disconnect NORM
	Actions:
	○ block_norm
	When clicked, the BRGW should be informed as per an MQTT message sent to the BRGW/DSOSMC/COUNTERMEASURE/BLOCKNORM with the ID of the NORM set as payload.

Comments	The test was successful

B.5.2 Test results for feature CSNM:G10:F2

Test results for feature CSNM:G10:F2 are reported in the following tables.

Table 41: Test case CSNM:G10:F2:T1 results

Test ID	CSNM:G10:F2:T1		
Test location	At the premises of SYN	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G10:F2		
Test preparation comments	The test CSNM:G7:F1:T3 has been successfully conducted		
Detailed test steps and result	As per CI-SOC:G7:F1:T3, the required functionality is already onboarded, configured as an automated countermeasure at NORM side. The CI-SOC is only notified of both the attack and the countermeasure.		
Comments	The test was successful.		

B.5.3 Test results for feature CSNM:G10:F5

Test results for feature CSNM:G10:F5 are reported in the following tables.

Table 42: Test case CSNM:G10:F5:T1 results

Test ID	CSNM:G10:F5:T1		
Test location	At the premises of SYN	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G10:F5		
Test preparation comments	All CSNM:G1- CSNM:G7 test cases were successfully executed.		

Detailed test steps and result	1. CI-SOC was configured to periodically scan the NORM's firewall configuration, by sending the correct configuration each time.
	2. At some point, we enabled incoming traffic from port 5000 using the command:
	`$ sudo iptables -A INPUT -p tcp --dport 5000 -j ACCEPT`
	nmap showed that the port was open:
	`$ nmap -p- 10.12.0.26`
	`Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-23 17:24 EEST`
	`Nmap scan report for 10.12.0.26 (10.12.0.26)`
	`Host is up (0.13s latency).`
	`Not shown: 65528 filtered ports`
	`PORT     STATE  SERVICE`
	`22/tcp   open   ssh`
	`80/tcp   open   http`
	`443/tcp  closed https`
	`1883/tcp open   mqtt`
	`5000/tcp closed upnp`
	`8080/tcp open   http-proxy`
	3. After less than an hour, the CI-SOC automatically checked the firewall configuration of the NORM and closed the port 5000:
	`2018-10-23 14:51:33,622 - [ lpa: check_firewall: 326] -- INFO - [src: 10.12.0.66] Successfully applied 9 rules.`
	Also, nmap showed that port 5000 was closed:
	`$ nmap -p- 10.12.0.26`
	`Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-23 17:56 EEST`
	`Nmap scan report for 10.12.0.26 (10.12.0.26)`
	`Host is up (0.13s latency).`
	`Not shown: 65528 filtered ports`
	`PORT     STATE  SERVICE`
	`22/tcp   open   ssh`
	`80/tcp   open   http`
	`443/tcp  closed https`
	`1883/tcp open   mqtt`
	`5000/tcp closed upnp`
	`8080/tcp open   http-proxy`
	4. When the CI-SOC checked again for the ports, no relevant action was taken and no relevant trace in the logs was found.		

Comments	The test was successful. Slightly deviating from the original test plan, the CI-SOC firewall check was performed automatically as per CI-SOC configuration.		

B.5.4 Test results for feature CSNM:G10:F7

Test results for feature CSNM:G10:F7 are reported in the following tables.

Table 43: Test case CSNM:G10:F7:T1 results

Test ID	CSNM:G10:F7:T1		
Test location	At the premises of SYN	**Partner**	SYN
Component	CI-SOC, NORM		
Features under test	CSNM:G10:F7		
Test preparation comments	All CSNM:G1- CSNM:G7 test cases were successfully executed.		
Detailed test steps and result	N/A. Since CISOC:G1-CISOC:G7 tests were successfully conducted, this test is automatically passed; the test steps combine the successive conduction of the steps of CISOC:G1-CISOC:G7.		
Comments	The test was successful.		

B.6 Significant notice

The current list of features is the same as the one documented in deliverable D3.11 [3]. However, some features were effectively removed from consideration. Regarding hardware attestation, it is not possible to understand with certainty whether a device has been tampered with or not; with the current SUCCESS design, if a component has been tampered with, its ID will change and all relevant requests will fail to enter the CI-SOC area since they will be dropped by the CI-SOC KMM module. Hence, all hardware attestation tests fell out of scope. Regarding software attestation, the relevant features were removed since their implementation would introduce new attack vectors in the attack surface of both CI-SOC and the NORM; if an attack agent would successfully attack CI-SOC, they would be able to massively attack all NORMs in the area of responsibility of the Utility. The relevant attack identification could be implemented as part of the advanced reporting values monitoring of SUCCESS, namely through the successfully identification of false data injection (e.g. through outliers detection).