FP7 Grant Agreement N° 607109

***S*ecurity for smart *E*lectricity *GRID*s**

D1.3 First report on the security & privacy goals

Due date of deliverable: 31/03/2015
Actual submission date: 01/04/2015
Work package: WP1 Use Cases and Security Goals
Number of pages: 42
Revision: Version 1
Classification level: Public

Project type:	Collaborative project – small or medium scale focused research project
Thematic Priority:	FP7-SEC-2013-1
Start date of project:	October 1st, 2014
Duration:	36 months

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 607109

Management summary

The SEGRID project has defined five use cases that are exemplary for the gradually evolving system concept of smart grids in Europe. The use cases will be used to identify new cyber-threats and vulnerabilities as well as the gap between available and needed cyber security solutions for smart grids. The SEGRID use cases have been selected considering:

1. the relevance for new business, economic growth, and supporting the introduction of more sustainable and locally generated power, and
2. addition of new functionality and components that inherently will introduce new vulnerabilities and a wider cyber-attack surface.

In this deliverable D1.3 the *initial set* of security & privacy goals for the SEGRID use cases is defined. This deliverable will be updated later during the SEGRID project by the final report on the security & privacy goals (D1.4).

A security goal is defined as *"a specific need to protect a certain interest of a stakeholder"*. In this initial stage, the focus of the deliverable has been on drafting security goals based on the traditional information security properties: *Confidentiality*, *Integrity* and *Availability*. These information security properties have been elaborated on and a stepwise approach has been defined.

A privacy goal is defined as "*a specific need to protect personal data when it is collected, transferred, processed, and/or stored by a stakeholder*". For the drafting of privacy goals we have assessed the EU Data Protection Directive 95/46/EC [8], the upcoming General Data Protection Regulation (GDPR) [7], and the set of eleven privacy principles for ICT systems as defined in ISO/IEC 29100:2011 [9].

However, since SEGRID is a technical oriented project focused on enhancing the protection of smart grids against cyber-attacks, the eight privacy design strategies defined in [10] better match with this purpose. These privacy design strategies are: *Minimise, Hide, Separate, Aggregate, Inform, Control, Enforce,* and *Demonstrate*. Also for drafting privacy goals a stepwise approach has been defined. In three of the SEGRID use cases personal data is collected, transferred, processed and/or stored. This stepwise approach has been applied to draft the initial set of privacy goals for the SEGRID use cases.

To achieve the identified security and privacy goals for the SEGRID use cases, security and privacy protection controls need to be applied. Over the last couple of years, several organisations have establish best practices with security and privacy protection controls and countermeasures for smart metering and smart grids. In order to assist the work in other SEGRID work packages, in particular the gap analysis in WP2, this deliverable presents an overview of the state of the art in security and privacy protection controls for smart metering and smart grids. This state of the art overview contains a brief description of the work performed under Mandate M/490, the sets of security measures for smart grids established by ENISA and Expert Group 2, and the standards ISO/IEC TR 27019:2013 [21], NISTIR 7628 [22] and IEC 62351 [15].

Author	Frank Fransen (TNO)
Contributors	Johanneke Siljee (TNO) Eric Luiijf (TNO) Christiane Peters (ENCS) Nuno Medeiros (EDP Distribuição) Rolf Blom and Marco Tiloca (SICS) Judith Rossebo (ABB) Exabier Bilbao Hernandez (ZIV)

Security Assessment	**See deliverables table for security assessment requirements**
Approval Date	31/03/2015
Remarks	None

TABLE OF CONTENTS

1 INTRODUCTION – RATIONALE OF THIS DOCUMENT 6
1.1 The SEGRID project objectives 6
1.2 Work Package 1 – Use Cases and Security Goals 7
1.3 Deliverable D1.3 – First report on the security & privacy goals 7
1.4 The structure of Deliverable D1.3 8
2 METHOD FOR ESTABLISHING SECURITY AND PRIVACY GOALS 9
2.1 Introduction 9
2.2 Security goals 9
2.3 Privacy goals 11
2.4 Methodology 13
3 SEGRID USE CASES 15
3.1 UC1: Smart meter used for on-line reading of consumption and technical data 15
3.2 UC2: Load balancing renewable energy centrally 17
3.3 UC3: Dynamic power management for smart homes, smart offices, electric vehicles 18
3.4 UC4: Load balancing renewable energy regionally (substation automation) 20
3.5 UC5: Automatic reconfiguration of the power grid 22
3.6 Summary 23
4 SECURITY GOALS 26
4.1 Customer (Household) 26
4.2 Customer (MV DER) 26
4.3 Energy supplier 26
4.4 Distribution System Operator 27
4.5 Data Hub 27
5 PRIVACY GOALS 28
5.1 UC1: Smart meter used for on-line reading of consumption and technical data 28
5.2 UC3: Dynamic power management for smart homes, smart offices, electric vehicles 28
5.3 UC4: Load balancing renewable energy regionally (substation automation) 30
6 STATE OF THE ART ON SECURITY & PRIVACY CONTROLS 32
6.1 SGCG - Smart Grid Information Security 32
6.1.1 Smart grid information security standards landscape 33
6.1.2 Privacy protection 35
6.2 Sets of security measures for smart grids 35
6.2.1 ENISA - Security measures for smart grids 35
6.2.2 Expert Group 2 – Proposal for a list of security measures for smart grids 36
6.3 Security and privacy controls standards 37
6.3.1 ISO/IEC TR 27019:2013 37
6.3.2 NISTIR 7628 rev 1 38
6.3.3 IEC 62351 38

Classification level: Public

7 REFERENCES.....40

Classification level: Public

1 Introduction – Rationale of this document

This chapter introduces the SEGRID project and defines the goals of this deliverable as well as explains the context for the use cases in this document.

1.1 The SEGRID project objectives

SEGRID's main objective is to enhance the protection of Smart Grids against cyber-attacks. In a Smart Grid, it is not sufficient to consider all the different components separately; they will together form a truly integrated system-of-systems. The Smart Grid will neither be completely owned, nor completely controlled, by a single power system operator. There will be many Smart Grid services and components that are operated by other organisations, such as public telecom networks and third party-delivered (outsourced) application services. There will potentially be many new channels of connecting with various Smart Grid applications using a diverse set of communication channels, such as local connection interfaces, distributed web access, and smart apps on smart phones.

This new utility-wide system (-of-systems) will not come into existence overnight. Therefore, the Smart Grid will be composed of a mix of old, even legacy, and new components. This is why we introduce the concept of a gradually evolving system in which new functionalities are added to accommodate new use cases with the challenge to maintain the security (and privacy) of the Smart Grid as a whole.

We have selected five use cases that clearly demonstrate this gradual evolving system concept. The SEGRID use cases have been selected based on the work already done by ENISA along with the working parties involved in the EC Mandates M/441 [1] and M/490 [2] as well as based on the work and competence of the project partners.

The rationale for the five SEGRID use cases is based on:

- Relevance for new business, economic growth, and supporting the introduction of more sustainable and locally generated power;
- Addition of new functionality and components that inherently will introduce new vulnerabilities and a wider cyber-attack surface.

The five SEGRID use cases are:

1. Smart meter used for on-line reading of consumption and technical data;
2. Load balancing renewable energy centrally;
3. Dynamic power management for smart homes, smart offices, and electric vehicles;
4. Load balancing renewable energy regionally (substation automation);
5. Automatic reconfiguration of the power grid.

We believe that the SEGRID use cases reflect important steps in the European Smart Grid developments until 2020 and beyond (SEGRID storyline, see Figure 1). Moreover, the

SEGRID use cases will cover the most relevant security and privacy issues that will arise from the increasing complexity of the evolving Smart Grids.

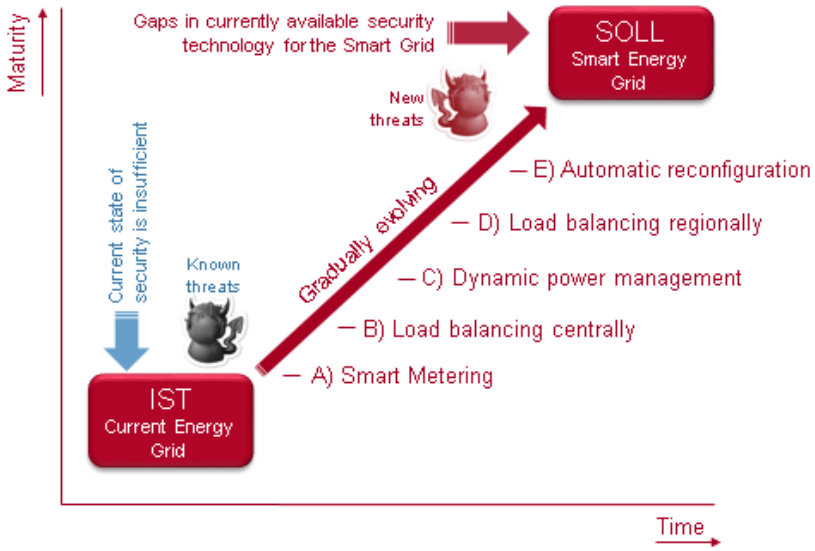

Figure 1: SEGRID storyline

1.2 Work Package 1 – Use Cases and Security Goals

Work Package 1 is a key building block for the SEGRID project, setting the basis for all activities within SEGRID.

The Work Package 1 main objectives are:

- Elaborate on the SEGRID reference architecture and describe the five use cases.
- Establish the security & privacy goals for each of the SEGRID use cases.
- Identify points of improvement with respect to Smart Grid security and privacy in policies and regulations related to the identified SEGRID use cases.
- Assess the cost of implementing security and privacy protection technologies that are developed in WP4 for each of the Smart Grids use cases.

1.3 Deliverable D1.3 – First report on the security & privacy goals

SEGRID deliverable D1.1 [11] defines and describes the SEGRID architecture and the five SEGRID use cases. This deliverable D1.3 defines the initial security & privacy goals for these SEGRID use cases. In addition, this deliverable provides an overview of the state of the art in smart grid security and privacy controls. D1.3 is the initial SEGRID report on the security & privacy goals and will be revised in SEGRID deliverable D1.4, the final report on the security & privacy goals. The figure below depicts the dependencies between the WP1 deliverables.

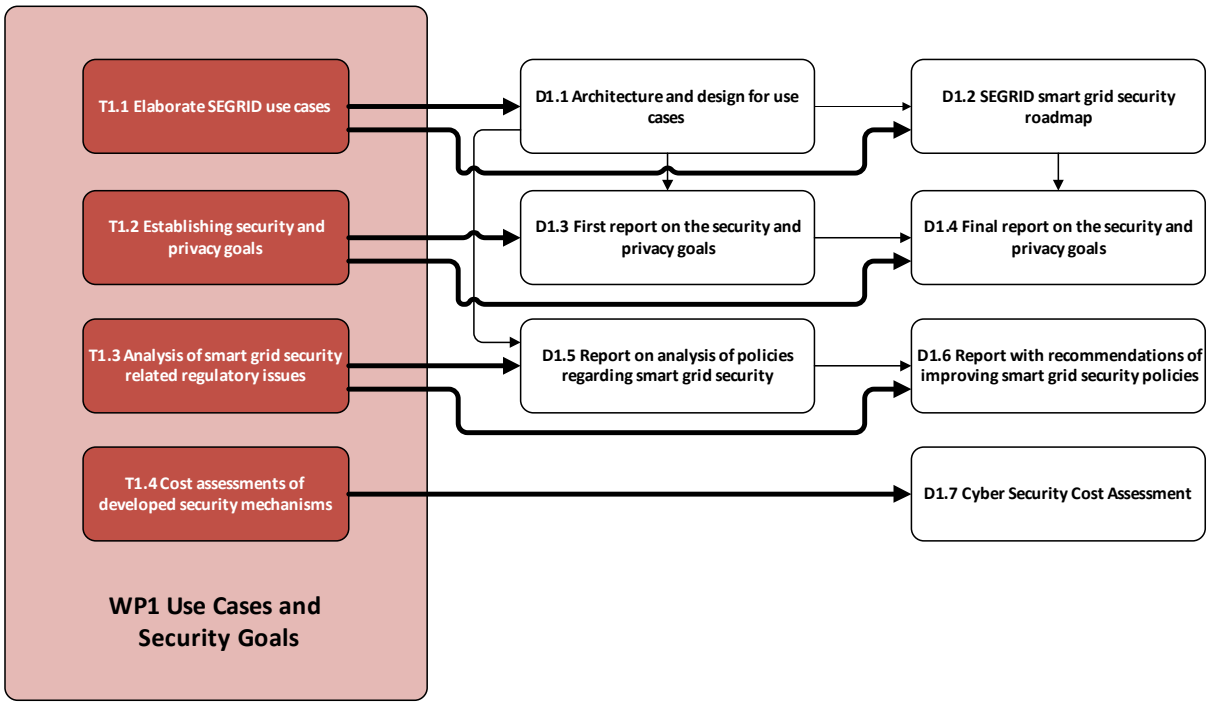

Figure 2 - Dependencies between the WP1 deliverables

1.4 The structure of Deliverable D1.3

Chapter 2 describes the methodological approach for drafting security and privacy goals. Next, the SEGRID use cases are described, including an assessment of the stakeholders, their interests and the information assets that play a role each of the use cases. The following two chapters subsequently present the initial set of security goals and the privacy goals for the SEGRID use cases. Chapter 6 provides the state of the art security and privacy controls that can be applied to ensure the security and privacy goals.

2 Method for Establishing Security and Privacy Goals

2.1 Introduction

This chapter describes the method to establish security and privacy goals for the SEGRID use cases. First, we will describe what we mean with goals. In requirements engineering the usage of goals has been widely recognised [3]. A goal has been defined as "*an objective the system under consideration should achieve*". A goal thus refers to an intended property that needs to be ensured. Goals can cover both functional and non-functional concerns of the system under consideration. Non-functional concerns are, for instance, related to performance, scalability, usability, safety, security, and privacy. This deliverable focusses on the latter two concerns.

We have the following understanding of a security goal and a privacy goal:

- A *security goal* is a specific need to protect a certain interest of a stakeholder.
- A *privacy goal* is a specific need to protect personal data when it is collected, transferred, processed, and/or stored by a stakeholder.

These goals therefore describe WHAT properties need to be ensured and WHY this is necessary for a particular stakeholder. These security and privacy goals are defined independent of a particular threat.

In requirements engineering, the typical reasons why the definition of goals is important are: motivating requirements, achieving requirements completeness, and goal-driven identification of requirements [3]. Within the SEGRID project we define security & privacy goals for the SEGRID use cases to help focus the work in other WPs by providing guidance on what security properties and privacy principles need to be ensured. The security & privacy goals will be used in WP2 to assist and guide the risk and threat assessments.

Goals can be formulated at different levels of abstraction ranging from strategic level concerns to low-level technical concerns. In the following two sections we will discuss what security and privacy concerns are considered for the definition of security & privacy goals for the SEGRID use cases.

2.2 Security goals

The stakeholder interests are related to a particular (business) goal or function which will be elaborated upon in each of the specific SEGRID use cases. Security goals are related to specific architectural assets (information, function, system and/or network) that are critical to achieve these goals or functions. By determining what security properties of these assets need to be preserved in order to ensure the stakeholders interests, the security goals can be defined.

The property types are typically derived from the information security domain. A well-known and renowned set of standards for Information Security Management is the ISO/IEC 27000 series. The first standard ISO/IEC 27000:2014 [4] provides the set of definitions and terms. Information security is defined as:

> **Information security** – preservation of *confidentiality*, *integrity* and *availability* of information.

Note: In addition, other properties, such as *authenticity*, *accountability*, *non-repudiation*, and *reliability* can also be involved.

Here confidentiality, integrity and availability are defined as follows:

Confidentiality – property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity – property of accuracy and completeness.

Availability – property of being accessible and usable upon demand by an authorized entity.

The property **availability** is applicable to information as well as to a (information processing) function, process or system. In the context of smart grids, availability is often regarded as the most important property [5]. Ensuring availability of the power supply is indeed very important. The availability of information or of an information processing function is not necessarily more important than the integrity of the information to ensure the availability of power supply.

Confidentiality can easily be applied within the context of smart grids, although the property is often regarded as less important for this domain (see for instance section 6 of [5]). Note that confidentiality of security function data (such as symmetric encryption keys) is important.

Integrity is the more difficult, and much debated, property of the three. The definition for integrity from ISO/IEC 27000 is not easy to apply. A more traditional definition for data integrity that was first defined in ISO 7498-2:1989 [6] is:

Data integrity – property that data has not been altered or destroyed in an unauthorized manner.

A common debate on data integrity is whether it also means that the data is correct. Therefore, *correctness integrity* is sometimes included as an additional property. Moreover, the authenticity of the origin of information is also not included in the definition above. *Data origin integrity* or *authenticity* is commonly addressed as a separate property.

Authenticity is defined in ISO/IEC 27000 as follows:

Authenticity – property that an entity is what it is claiming to be.

For the definition of security goals of the SEGRID use cases we will use both *data integrity* & *authenticity* as aspects of integrity. The security goal shall make clear which of the two, or if both are meant.

In the definition of information security above, **accountability** is mentioned as an additional property that is sometimes relevant. Within the context of smart grids we expect that accountability is relevant. ISO/IEC 27000:2014 does not contain a definition of this property. ISO 7498-2:1989 provides the following definition of accountability:

Accountability – property that ensures that the actions of an entity may be traced uniquely to the entity.

A specific type of accountability is **non-repudiation**, which is defined as:

Non-repudiation – ability to prove the occurrence of a claimed event or action and its originating entities.

The definition of information security above mentions **reliability** as an additional property, and in ISO/IEC27000:2014 it is defined as:

> **Reliability –** property of consistent intended behaviour and results.

This property is related to the behaviour of the information system or process, and not to the information itself. With respect to information, it is better to refer to *data quality* or *correctness integrity* when considering for example the reliability of acquired/sensed data. Within the context of smart grids reliability is a relevant system property to consider.

In this initial version of the SEGRID deliverable on security & privacy goals, we will limit ourselves to define of security goals on the typical information security properties for the information assets. In the update of this deliverable (i.e. SEGRID deliverable D1.4) the scope will be extended to security goals on properties, such as system security and security life cycle management. In addition, the methodology to determine security goals will be re-assessed and possibly enhanced to a more process-oriented security approach.

2.3 Privacy goals

Privacy protection is a major concern of the European Commission and Member States and is regulated by European law. In particular, the EU Data Protection Directive 95/46/EC [8] sets the basic legislative rules that have to be implemented in national law of each of the Member States. The upcoming European Commission data protection regulation, General Data Protection Regulation (GDPR) [7], will replace this Directive and introduce new regulation. For example, article 23 mandates data protection by design and by default. This is particularly relevant in the context of smart grids. The introduction of smart meters, for example, has led to debates on privacy.

Privacy protection is concerned with safeguarding “personal data”. In EU directive 95/46/EC "personal data" is defined as:

> *Article 2a: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;*

Privacy goals express specific needs (WHAT and WHY) to protect personal data collected, transferred, processed, and/or stored by a stakeholder. The following roles are typically distinguished in privacy protection are:

- **Data subject** - the natural person to whom the personal data relates. The data subject can be identified, directly or indirectly, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;
- **Controller** - the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data;
- **Processor** - a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

- **Recipient** - a natural or legal person, public authority, agency or any other body to which the personal data are disclosed.

For defining the privacy goals for a SEGRID use case it is relevant to assign these roles to the stakeholders. In order to express the privacy goals in a more specific manner we need to establish a set of privacy concepts. Else the privacy goals will be at a very abstract level, e.g. "the smart meter data is personal data and has to be protected according to applicable data protection laws". In ISO/IEC 29100:2011 [9] a privacy framework is specified, including a set of eleven *privacy principles* for ICT systems and the development of privacy management systems to be implemented within the organisation's ICT systems. These privacy principles are:

1. **Consent and choice** – inform data subjects, present the available choices and obtain consent.
2. **Purpose legitimacy and specification** – ensure that the purpose complies with data protection legislation and inform data subjects of this purpose.
3. **Collection limitation** – limit the data collection to what is allowed by data protection legislation and needed for the purpose.
4. **Data minimisation –** minimise the amount of personal data collected, minimise the number of privacy stakeholders and people to whom personal data is disclosed, offer as default non-privacy invasive options, and delete personal data whenever the purpose for processing has expired.
5. **Use, retention and disclosure limitation** – limit the use, retention and disclosure of personal data to the specified purpose and for which consent was given by the data subjects.
6. **Accuracy and quality** – ensure the data is accurate, up-to-date, adequate and relevant for the purpose of use, and establish mechanisms to periodically check this.
7. **Openness, transparency and notice** – inform data subjects about the data controller policies, procedures and practices, including notices that personal data is being processed, and provide information on how data subjects can access, correct and remove personal data.
8. **Individual participation and access** – provide data subjects with the ability to access and review their personal data, allow data subjects to challenge the accuracy and completeness, and provide the ability to amend, correct or remove personal data.
9. **Accountability** – document and communicate policies, procedures and practices, assign the duty to implement privacy policies to specified individuals in the organisation, provide suitable training, inform data subjects about privacy breaches, etc.
10. **Information security** – ensure the integrity, confidentiality and availability of the personal data, and implement the right controls, based on an appropriate risk assessment and security standards.
11. **Privacy compliance** – verify and demonstrate that the processing meets relevant data protection laws, and have appropriate internal controls and supervision mechanisms that assure compliance.

These principles cover legal, procedural and technical aspects. Since SEGRID is a technical oriented project focussed on enhancing the protection of smart grids against cyber-attacks, we focus here on those privacy goals that will help to identify gaps and privacy protection techniques for smart grids. In [10], a set of eight privacy design strategies are defined that better match with this purpose. These privacy design strategies are:

- Strategy #1: MINIMISE – The amount of personal data that is processed should be restricted to the minimal amount possible.
- Strategy #2: HIDE – Any personal data, and their interrelationships, should be hidden from plain view.
- Strategy #3: SEPARATE – Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
- Strategy #4: AGGREGATE – Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
- Strategy #5: INFORM – Data subjects should be adequately informed whenever personal data is processed.
- Strategy #6: CONTROL – Data subjects should be provided agency over the processing of their personal data.
- Strategy #7: ENFORCE – A privacy policy compatible with legal requirements should be in place and should be enforced.
- Strategy #8: DEMONSTRATE – Be able to demonstrate compliance with the privacy policy and any applicable legal requirements.

For the definition of privacy goals we will focus on the identifying privacy protection needs using these privacy design strategies.

2.4 Methodology

This section describes the approach for drafting security and privacy goals for the SEGRID use cases. For this initial deliverable on the security & privacy goals for the SEGRID use cases, we have decided to define security goals at a generic level. The reasons are:

- The definition of the use cases (in D1.1) and the definition of these security and privacy goals (in this deliverable) take place simultaneously, which complicates the process;
- For the purpose of this initial version of the security and privacy goals it is sufficient to define them at a generic level.

In addition, in WP2 a risk assessment on the SEGRID use cases will be performed that will result in more use case specific security requirements.

The following stepwise approach has been developed to draft the security goals.

Method for drafting Security Goals

Step 1. Identify the stakeholders and their interest for each of the SEGRID use cases.

Step 2. Identify the information assets for each of the SEGRID use cases and related these assets to the stakeholder interests.

Step 3. Analyse what information security properties, described in section 2.2, of these information assets need to be preserved to ensure the stakeholder interests.

Step 4. Define the security goals based on the analysis in step 3.

The following stepwise approach has been developed to draft the privacy goals.

Method for drafting Privacy Goals

Step 1. Determine if in a use case personal data is collected, transferred, processed and/or stored. For those use cases where this is the case, continue with the following steps:

Step 2. Identify what type of personal data is collected and how it will be collected, used, and disseminated (at an architectural level).

Step 3. Identify the privacy roles per stakeholder within the particular use case.

Step 4. Define privacy goals on based the privacy aspects described in section 2.3.

Goals will be drafted in a statement of one sentence containing the WHAT needs to be preserved i.e. security properties and privacy aspects), and WHY (i.e. to ensure stakeholder interests).

3 SEGRID use cases

In SEGRID deliverable D1.1 [11] the SEGRID use cases are described in detail. These use cases that are exemplary for the gradually evolving system concept of smart grids in Europe. Moreover, the SEGRID use cases will cover the most relevant security issues that will arise from the increasing complexity of the emerging European smart grids.

In this chapter each of the use cases is briefly described. For each of the five use cases, the stakeholders and their (high level) interests have been identified. Next, the Information Assets that play a role in the use cases are listed. Finally, a mapping is made between the stakeholder's interests for all the SEGRID use cases and the Information Assets.

3.1 UC1: Smart meter used for on-line reading of consumption and technical data

The smart meter is a device at the customer's premises that records consumption of electricity (and possibly gas, heat, and water) in short intervals and provides remote access to this consumption data. This data is collected for various purposes including billing and grid management. The smart meter may routinely send the data to the Distribution System Operator (DSO) or the data may be read out remotely by the DSO. The DSO facilitates the collection and delivery of consumption data to the energy supplier, possibly via a data hub. In addition to power consumption data, the smart meter may also measure the voltage and phase to support the DSO with the management and operation of the (smarter) power grid.

The smart meter may also provide remote switching of customers, by means of a disconnect switch in the smart meter. The main purpose of this is to remotely disconnect customers who have failed to pay their bills in time.

The following three scenarios are described for this use case:

1. *Metering* – Automatically sending or reading measurement data by a Data Concentrator (DC) of the DSO. Acquired meter data will be send to a head-end system and Meter Data Management System (MDMS). The DSO will send the consumption data to the energy supplier, possibly via an aggregator.
2. *Remote power switching* – the DSO will remotely switch on or off customers upon request of the energy supplier. The communication between the energy supplier and the DSO may go via an aggregator.
3. *Outage management* – in this scenario, smart meters are equipped with a so called last gasp function which will send a message to the utility's Outage Management System (OMS) before the meter loses power. This message can assist the DSO with determining which and how many customers are affected by a power outage or when a customer contacts the DSO call centre.

Based on the description of this use case in SEGRID deliverable D1.1, the following stakeholders and their high level interests have been identified. In Table 3-2 the information assets used in this use case are listed.

Table 3-1 List of stakeholders and their (high level) interests in SEGRID use case 1. The number in brackets refers to the particular use case scenario.

Stakeholders	Interests
Customer	Insight in own energy consumption
	Insight in own energy production
	Correct invoice for energy consumption and production
	Protection of personal data
Energy supplier	Purchase energy
	Perform billing (invoicing) (1)[1]
	Reduce fraud or illegal usage by disconnecting customers (2)
DSO	Outage management (3)
	Element management of the smart meters
	Market facilitation • Collect smart meter measurement data and make available to data hub (1) • Facilitate switching upon request from data hub (2)
Data hub	Market facilitation • Collect smart meter measurement data from DSO and make available to energy supplier (1) • Facilitate switching for energy supplier (2)

Table 3-2 List of information assets for SEGRID use case 1.

Information Assets	Description
Measurement Data	Measurement Data are smart meter measurements about the energy consumption or energy production at a connection on the LV-level.
Switch Data	Switch Data are the commands from the control systems in order to switch on-off a device. In case of the smart meter it is to switch on or off the customer's connection to the grid.
Configuration Data	Configuration Data incorporates a lot of parameters to describe the smart meter, but also parameters to control the execution of the smart meter. An examples of the first category is the device identity. Examples of the second category are communication periods, cryptographic keys, etc. etc. Configuration Data is defined at Maintenance system and downloaded to different types of control system and meters, such as the Smart Meters.
Monitoring Data	Monitoring Data includes information stored in devices like Smart Meters concerning logging, power quality, outage times, etc. Monitoring Data can be collected by Monitoring system to build reports about process behaviour, device- and the total system behaviour. The last gasp message from the smart meter is also considered Monitoring Data.
Fault Data	Fault Data is information from special equipment in the grid about faults in the distribution grid. In use case 1, the Fault Data are error reports from customer to a call centre on the lack power.
Outage Data	Outage Data is information calculated by the Outage Management System (OMS) to localize a fault in the grid. The OMS uses Fault Data from various sources to decide the probable location of a fault to enable a quick repair.
Dynamic Network Topology Data	Dynamic Network Topology Data is a real-time model of the distribution grid state represented as a bus-branch model but without power flow. The Dynamic topology model is built by the SCADA or RTU system based on the static topology from Configuration Data and from the real time states of binary devices like breakers and isolators, i.e. open or closed. In use case 1 this data is used to determine where the

[1] Use case scenario number is shown between brackets.

	most probable fault location is.

3.2 UC2: Load balancing renewable energy centrally

Load balancing renewable energy is a way to automatically controlling the distributed generation, to balance the renewable energy supply to the demand, in a way that regional congestion is avoided. In this specific use case load balancing renewable energy is performed centrally. A head-end SCADA system is responsible for receiving and processing all the metering information, and deciding whether to increase or decrease the MV Distribution Energy Resources (DER) generation to balance it with the demand. The decision making is done by the DSO. Additionally, the SCADA system is also used for managing the quality of the energy supplied by the DER.

The following two scenarios are described for this use case:

1. *Managing Power Quality* – in this scenario the DSO is responsible for defining production limits and energy quality parameters for the MV DER. When deviations from these limits are detected, the DSO will react – either by switching off the production unit entirely or adjusting the power production set points – to make sure that the injected power will not have a negative impact on the grid stability.
2. *Balancing MV renewable generation centrally* - in this scenario the DSO will send new set points to Remote Terminal Units (RTUs) to either decrease or increase the power generation at the MV DER.

In the table below the main stakeholders and their high level interests are listed/tabled/…. for use case 2 (UC2). In Table 3-4 the information assets used in this use case have been listed.

Table 3-3 List of main stakeholders and their interests in SEGRID use case 2. The number in brackets refers to the particular use case scenario.

Stakeholders	Interests
DER producer	Insight in own energy production
	Compensation for energy production
DSO	Energy distribution
	Power quality management (1)
	Energy balancing (2, 3)

Table 3-4 List of information assets for SEGRID use case 2.

Information Assets	Description
Sensor Data	Sensor Data are (smart) grid measurements about the binary states of breaker and isolator.
Load Forecast Data	Load forecasts are a predication of future loads in the distribution system. It is calculated based on historical data and other parameters like weather data, special days (e.g., holidays), etc.
kWh Data	kWh Data ae company meter measurements on the MV-level about the energy consumption or energy production at a certain load/generation point. kWh data is a special case of Measurements but useful to distinguish in the SEGRID use cases.
Set Points	Set points are used to control process devices with continuous regulation like generation units. This can limit the supply of DER in emergency situations.
Configuration data	Configuration Data incorporates a lot of parameters to describe the electrical grid

	but also parameters to control the execution of the control systems. Examples of the first category are device identity, static topology, i.e. how devices are statically connected, line impedances, operational limits, etc. Examples of the second category are communication parameters, RTU connections, execution periods, cryptographic keys, etc. etc. Configuration Data is defined at Maintenance system and downloaded to different types of control system and meters lie SCADA, RTU, Smart Meters, etc.
Monitoring data	Monitoring Data includes information stored in devices. Monitoring Data can be collected by Monitoring system to build reports about process behaviour, device- and the total system behaviour. In use case 2 monitoring data is collected from the RTU of the DER producer.

3.3 UC3: Dynamic power management for smart homes, smart offices, electric vehicles

Dynamic Power Management for smart homes, smart offices, Electric Vehicles (EV) is based on the use of flexibility in demand and supply. At the customer premises a device agent can control the customer's loads such as home appliances (e.g. fridges, washing machine, air conditioners) and charging station of an electric vehicle. The DSO can remotely interact with this device agent to increase or decrease load, with the purpose of reshaping the consumption profile of a given area. The objective is to improve grid efficiency, hosting capabilities for DER and maintainability. Customers need to establish an agreement with the DSO to hand over – to a certain extent – the control of the devices to the DSO.

The following three scenarios are described for this use case:

1. *Centralised control of available loads* – in this scenario customers provide direct control of loads, such as air conditioners, refrigerators, swimming pool heating, to the DSO as a service. The DSO continuously monitors the power grid and compares the collected data with predefined optimal values. When deviations are detected the DSO can control (a group of) customer devices in order to increase or decrease demand. The client is informed through individual notification and/or monthly service usage report that its services have been used.
2. *Load shifting – Centralised control and automation of home appliances* - in this scenario customers set up appliances (e.g. a loaded washing machine) to be started upon command from the DSO. The customer will inform the DSO of the available load and possibly time frame in which the start of the load should take place. The DSO will continuously monitor the power grid and may activate the customers load to increase the demand.
3. *Optimised charging of EV* – the customer has an electric vehicle and connects it to a charging station at home. To prevent a peak loads due to EV charging when people come home from work, the DSO is able to schedule and start the charging of EVs and possibly configure the charging program. The customer has to inform the DSO of how much the EV must be charged and when the vehicle must have been loaded to the required capacity level. The DSO can then execute EV charging to optimally balance energy production and consumption.

In the table below the main stakeholders and their high level interests are listed for use case 3 (UC3). In Table 3-6 the information assets use in this use case have been listed.

Table 3-5 List of main stakeholders and their interests in SEGRID use case 3.

Stakeholders	Interests
Customer (Small Office, Household, EV owner)	Correct invoice for energy consumption
	Loads and appliances operate correctly
	EV charged upon demand
DSO	Energy distribution
	Energy balancing
	Power quality management
Energy supplier	Purchase energy
	Energy sales & billing (invoicing)

Table 3-6 List of information assets for SEGRID use case 3.[2]

Information Assets	Description
Measurement Data	Measurement Data are smart meter measurements about the energy consumption or energy production at a connection on the LV-level.
Sensor Data	Sensor Data are (smart) grid measurements about the binary states of breaker and isolator.
Switch Data	Switch Data are the commands from the control systems in order to switch on-off a device. In case of the smart meter it is to switch on or off the customer's connection to the grid.
Change consumption /generation command	Change consumption/generation command is a special type of command to give instructions to Smart Meters and household appliances to start, reduce consumption or to increase/decrease generation. In use case 3 this is used to control customer devices and smart household appliances.
Consumption Priorities	Consumption Priorities are in use case 3 used to communicate to the DSO that a particular smart household appliance is ready to be started by the DSO within certain time frame.
Current Status Data	Current status data is a special case of Binary measurements to indicate the state of a Smart Household Appliance.
Set points	Set points are used to control process devices with continuous regulation like generation units. In use case 3 set points are used to control the EV charging point.
Monitoring Data	Measurement data are smart household meter measurements give information about the energy consumption or energy production at a connection on the LV-level.
Load Forecast Data	Load forecasts are a predication of future loads in the distribution system. It is calculated based on historical data and other parameters like weather data, special days (e.g., holidays), etc.
Dynamic Network Topology Data	Dynamic Network Topology Data is a real-time model of the distribution grid state represented as a bus-branch model but without power flow. The Dynamic topology model is built by the SCADA or RTU system based on the static topology from Configuration Data and from the real time states of binary devices like breakers and isolators, i.e. open or closed.

[2] At the time of drafting D1.3, use case 3 was not yet ambiguously defined in D1.1 [11]. In particularly, the description of the System Assets and Information Assets needed to be more aligned with the description of use case 3. In the final version of the security and privacy goals for SEGRID use cases (SEGRID Deliverable D1.4) an updated version of use case 3 will be included.

3.4 UC4: Load balancing renewable energy regionally (substation automation)

Similar to use case 2, this use case focusses on enabling the DSO to load balance renewable energy. The difference with *UC2 load balancing renewable energy centrally* is that in UC4 the control is shifted to automated subsystems. These automated systems could be on the scale of a primary MV substation or even on an underlying secondary MV/LV substation. The goal is to balance the renewable energy supply with the (local) demand in order to avoid congestion and/or local power quality problems like unacceptable voltages. The control is done by automated subsystems in the RTUs which, under the SEGRID reference architecture, are present on the scale of a MV primary and secondary substation.

In D1.1, three scenarios are described for this use case. In all three scenarios the local distributed power generation and consumption is monitored by the DSO and aggregated at the substation level by the DSO's primary RTUs. The RTUs continuously keep track of the network topology by supervision of circuit breaker status. They gather information from all the loads that are connected to the substation and the generation facilities. Based on energy forecast performed on a day-ahead basis (incl. estimated consumption for that substation), the centralised generation that will be injected by the HV/MV substation and the MV and LV distributed generation, the RTU can determine if there is any deviation in demand or generation. Three scenarios have been defined as to how the RTU can act:

1. *Balancing MV renewable generation* – the DSO will send a new set point to a set of RTUs at the MV DER producers' premises, to either increase or decrease their power generation.
2. *Balancing LV renewable generation* – the DSO will send a switch on or off command to the smart meter at the LV producers' premises, in order to switch on or off the supply to the power grid.
3. *Balancing LV energy consumption locally* – the DSO will send a reduce consumption order to customers. Customers may specify consumption priorities for their energy consuming appliances that will be used to reduce the consumption upon request from the DSO. If the limitation does no longer exist, the DSO will inform the customers after which their appliances may go back to normal operation.

In the table below the main stakeholders and their high level interests are listed for use case 4 (UC4). In Table 3-8 the information assets for this use case have been listed.

Table 3-7 List of main stakeholders and their interests in SEGRID use case 4.

Stakeholders	Interests
Customer (Household)	Compensation for energy production
	Compensation for provided flexibility in load and/or production
	Protection of personal data
Customer (MV DER Producer)	Compensation for energy production
	Compensation for provided flexibility in production
DSO	Energy distribution
	Energy balancing

Table 3-8 List of information assets for SEGRID use case 4. The number in brackets refers to the particular use case scenario.

Information Assets	Description
Analogue Data	Analogue Data ae (smart) grid measurements about the state of the electrical grid like currents, voltage, active and reactive power (i.e., measurement with continuous values) (3)
Sensor Data	Sensor Data are (smart) grid measurements about the state of the electrical grid like currents, voltage, active and reactive power but also breaker and isolator states. (1 and 3)
Measurement Data	Measurement Data are smart meter measurements about the energy consumption or energy production at a connection on the LV-level. (2)
kWh Data	kWh Data are company meter measurements on the MV-level give information about the energy consumption or energy production at a certain load/generation point. kWh data is a special case of Measurements but useful to distinguish in the SEGRID use cases. (1)
Change Consumption/ Generation Command	Change consumption/generation command is a special type of command to give instructions to Smart Meters and Household Appliances to either reduce consumption or to increase/decrease generation. This command type is used in the SEGRID user cases for clarification. (3)
Consumption Priorities	Consumption Priorities is a special case of Configuration Data where the customers can set priorities to their household devices which could be switched off or reduce loads in case the household receives a Change Consumption/Generation Command. (3)
Current Status Data	Current status data is a special case of Binary measurements to indicate the state of a Smart Household Appliance. (3)
Set Points	Control to process devices with continuous regulation like generation units. This can limit the supply of DER in emergency situations. (1)
Switch Data	Switch Data are the commands from the control systems in order to switch on-off a device. In use case 2 it is to switch on or off the locally generated LV supply to the power grid. (2)
Monitoring Data	Monitoring Data includes information stored in devices like Smart Meters Household Concentrator concerning logging, power quality, outage times, etc. Monitoring Data can be collected by Monitoring system to build reports about process behaviour, device- and the total system behaviour. (3)
Fault Data: • **Breaker State Data** • **Feeder Data**	Fault Data is information from special equipment in the grid about faults in the distribution grid. The most common is fault indicators that show the existence of a short circuit and the direction of the fault and feeder head protection that open the feeder breaker in the primary substation in case of a fault. The feeder head protection can disconnect the feeder to protect primary equipment and human life. Fault Data is use in this use case to create status of the network topology ('Dynamic Network Topology Data'). (3)
Load Forecast Data	Load forecasts are a predication of future loads in the distribution system. It is

	calculated based on historical data and other parameters like weather data, special days (e.g., holidays), etc. (1, 2, and 3)
Dynamic Network Topology Data	Dynamic Network Topology Data is a real-time model of the distribution grid state represented as a bus-branch model but without power flow. The Dynamic topology model is built by the SCADA or RTU system based on the static topology from Configuration Data and from the real time states of binary devices like breakers and isolators, i.e. open or closed. (3)

3.5 UC5: Automatic reconfiguration of the power grid

In this use case, technology is introduced in the power grid to automatically localise, isolate and repair faults through automatic (re)configuration, also referred to as self-healing. The objective is to improve the quality of service of power supply by decreasing the number of and duration of power interruptions, at the same time minimising the affected area. The automatic reconfiguration might be done locally or centrally. Similarly, the need for reconfiguration might be identified locally or centrally.

The following three scenarios are described for this use case:

1. *Centrally decided isolation and restoration at faults in MV network* – in this scenario the primary substation RTU monitors the MV grid parts under its responsibility and identifies parts of the network where a fault has occurred. Isolation can be done by the operators at the central dispatch or by automatic commands by the primary substation RTU. When the fault is isolated the primary RTU will try to re-energise customers.
2. *Distributed isolation and restoration at faults in the MV network* – in this locally and distributed decided scenario the smaller RTUs of each secondary substation will decide the dynamic topology of the MV network by questioning its neighbouring substations. To do this, a peer-to-peer communication between substations is used. By combining the information, a dynamic topology model can be created at secondary substation RTUs. With this information each of the substations can decide by itself to open or close load breakers under its control in order to isolate faults in network parts and/or restore the energy to sections without a fault.
3. *Minimisation of losses in the MV network using switching* – in this scenario the primary substation RTU receives information about the static topology and line parameters (e.g. impedances) from a central engineering system where all data of the MV grid is defined. All secondary substations RTUs communicate with the RTU in the primary substation and send real-time information about currents, active and reactive power, phase angles and voltages as well as information about load breaker states. The primary substation RTU can calculate a dynamic topology state and an optimal power flow with minimal losses and optimal voltage profiles. Based on the forecasted loads the primary substation RTU calculates load flows with and without switching. The primary RTU decides if a switching action has to be performed in order to reach a more optimal load flow state.

In the table below the main stakeholders and their high level interests have been listed for use case 5 (UC5). In Table 3-10 the information assets used in this use case have been listed.

Table 3-9 List of main stakeholders and their interests in SEGRID use case 5.

Stakeholders	Interest
DSO	Energy distribution
	Outage management
	Minimise grid losses

Table 3-10 List of information assets for SEGRID use case 5.

Information Assets	Description
Sensor Data	Sensor Data are (smart) grid measurements about the binary states of breaker and isolator.
Set Points	Set Points are used to control process devices with continuous regulation like generation units. This can limit the supply of DER in emergency situations.
Switch data	Switch Data are the commands from the control systems in order to switch on-off a device.
Configuration data	Configuration Data incorporates a lot of parameters to describe the electrical grid but also parameters to control the execution of the control systems. Examples of the first category are device identity, static topology, i.e. how devices are statically connected, line impedances, operational limits, etc. Examples of the second category are communication parameters, RTU connections, execution periods, cryptographic keys, etc. etc. Configuration Data is defined at Maintenance system and downloaded to different types of control system and meters lie SCADA, RTU, Smart Meters, etc.
Load Forecast Data	Load forecasts are a predication of future loads in the distribution system. It is calculated based on historical data and other parameters like weather data, special days (e.g., holidays), etc.
Dynamic Network Topology Data	Dynamic Network Topology Data is a real-time model of the distribution grid state represented as a bus-branch model but without power flow. The Dynamic topology model is built by the SCADA or RTU system based on the static topology from Configuration Data and from the real time states of binary devices like breakers and isolators, i.e. open or closed.
Flow Model	The Flow model represents the power flows in the distribution grid. It is calculated by a Power Flow calculation in the SCADA or RTU systems using real-time analogue measurements, the bus-branch model from the dynamic topology and line parameters from Configuration Data.
Fault Data • **Breaker State Data** • **Feeder Data**	Fault Data is information from special equipment in the grid about faults in the distribution grid. The most common is fault indicators that show the existence of a short circuit and the direction of the fault and feeder head protection that open the feeder breaker in the primary substation in case of a fault. The feeder head protection can disconnect the feeder to protect primary equipment and human life.

3.6 Summary

The SEGRID use cases reflect a diverse set of smart grids developments. The common technological development in these use cases is that there will be an increase of metering (i.e. Measurement data, Sensor Data, kWh Data) that will lead to central or distributed control by switching (i.e. Switch data, Change consumption/generation command) or re-configuring (i.e. Set Points, Configuration Data) loads, production or network topology. The motivation for this control differs: load balancing, power quality management, grid optimisation (operation,

maintenance and loss reduction), or fraud reduction. In addition, smart metering will enable collection of consumption data in short intervals from consumers' households.

In Table 3-11 a mapping is made between the stakeholder's interests for all the SEGRID use cases and the Information Assets.

Table 3-11 Mapping of stakeholder interest in the SEGRID use cases and the Information Assets.

	Stakeholder	Customer					DER Customer		energy supplier			DSO					DSO-AMI		Data Hub	
	Interests	Energy consumption (incl. EV charging)	Compensation for energy production	Correct invoice (for consumption and production)	Loads / appliances operated correctly	Protection of personal data	Compensation for energy production	Correct invoice (for production & service)	Energy purchasing	Perform billing (invoicing)	Reduce fraud by disconnecting	Distribution of energy	Power quality management	Energy load balancing	Outage management	Minimize grid losses	Market facilitation - measurement data acquisition & delivery	Market facilitation - switching	Market facilitation - data exchange	Market facilitation - switching
Information assets	Measurement data	•	•	•		•			•	•				•	•		•		•	
	Sensor Data									•			•	•	•	•			•	
	kWh Data						•	•		•			•	•			•		•	
	Current Status Data	•			•	•								•						
	Monitoring data												•	•	•			•		
	Switch data	•	•		•	•				•	•			•	•	•		•	•	•
	Change C/G command	•	•		•					•				•					•	
	Set Points	•					•			•			•	•		•	•		•	
	Configuration data												•		•		•			
	Consumption Priorities	•			•									•						
	Load Forecast Data												•	•	•	•				
	Dynamic Network To-pology Data														•	•				
	Fault Data														•					
	Outage Data														•					

Classification level: Public

4 Security goals

This chapter presents the initial set of security goals for the SEGRID use cases. These security goals have been established by means of the approach described in section 2.4.

4.1 Customer (Household)

In order to receive correct invoice for energy consumption and production the household customer has the following security goals:

CH_SG01 ensure *data integrity* and *authenticity* of measurement data for the energy supplier.

CH_SG02 ensure *availability* of measurement data for the energy supplier.

In order to have appliances correctly started within given constraints and their EV correctly charged within given constraints in use case 3 and 5, the household customer has the following security goal:

CH_SG03 ensure *data integrity* and *authenticity* of control messages from the DSO (e.g. Change Consumption/Generation Command, Set Points).

Protection of the customer personal data is discussed in chapter 5.

4.2 Customer (MV DER)

In order to:

- optimise energy production
- receive correct compensation for energy production, and
- receive correct compensation for provided production flexibility as a services,

the MV DER customer has the following security goals:

CD_SG01 ensure *data integrity* and *authenticity* of energy production limits (i.e. Set Points) received from the DSO.

CD_SG02 ensure *data integrity* and *authenticity* of measurement data (i.e. kWh data).

4.3 Energy supplier

In order to correctly perform billing for energy production and consumption the energy supplier has the following security goals:

ES_SG01 ensure *data integrity* and *authenticity* of measurement data received from the data hub.

ES_SG02 ensure *data integrity* and *authenticity* of tariff related configuration data in the smart meters.

ES_SG03 ensure *availability* of measurement data.

In order to correctly perform switching on/off of customers the energy supplier has the following security goals:

ES_SG04 ensure *data integrity* and *authenticity* of switch data processed by the data hub.

4.4 Distribution System Operator

In order to correctly perform power quality management and energy load balancing the DSO has the following security goals:

DSO_SG01 ensure *data integrity* and *authenticity* of meter data (i.e. Measurement Data, Sensor Data, kWh Data) and monitoring data during transfer and storage.

DSO_SG02 ensure the *availability* of measurement and monitoring data.

In order to correctly perform outage management the DSO has the following security goals:

DSO_SG04 ensure *availability* of the sensor data and monitoring data (incl. last gasp message).

In order to correctly perform market facilitation in accordance with the SLA with the data hub and applicable legal requirements and regulations the DSO has the following security goals:

DSO_SG05 ensure *data integrity* and *authenticity* of measurement data during transfer and storage.

DSO_SG06 ensure *availability* of measurement data during transfer and storage.

DSO_SG07 ensure *data integrity* and *authenticity* of switch data during transfer and storage.

4.5 Data Hub

In order to correctly perform market facilitation in accordance with the SLA with the energy supplier and applicable legal requirements and regulations the data hub has the following security goals:

DH_SG01 ensure *data integrity* and *authenticity* of measurement data during transfer and storage.

DH_SG02 ensure *availability* of measurement data during transfer and storage.

DH_SG03 ensure *data integrity* and *authenticity* of switch data during transfer and storage.

5 Privacy goals

This chapter presents the initial set of privacy goals for the SEGRID use cases. In three of the SEGRID use cases personal data is collected, transferred, processed and/or stored: use case 1, use case 3, and use case 4. For these use case the steps described in section 2.4 were followed.

5.1 UC1: Smart meter used for on-line reading of consumption and technical data

The following information assets are considered personal data:

- *measurement data* at short intervals from the smart meter with an *identifier* that can be related to a specific household customer (UC1 - scenario 1); and
- *switch data* (switch on/off and identifier) (UC 1 – scenario 2)

Table 5-1 Assessment of privacy roles per identified personal data for use case 1.

Privacy role	Measurement data	Switch data
Data subject	Customer	Customer
Controller	DSO	Energy supplier
Processor	DSO, Data Hub	Energy supplier, DSO, Data Hub
Recipient	Energy supplier	-

The following privacy goals have been identified:

UC1_PG01 Ensure that minimal measurement data is collected, transferred, processed, stored, and/or disclosed.

UC1_PG02 Ensure that measurement data is hidden from plain view.

UC1_PG03 Ensure that switch data is hidden from plain view.

UC1_PG04 Ensure that measurement data is aggregated at the highest level of aggregation and with the least possible detail in which it is (still) useful.

UC1_PG05 Ensure that measurements data and identifier data is separated whenever possible.

UC1_PG06 Ensure that the customer is informed adequately on the personal data (i.e. power consumption data and switching data) that is collected and processed

UC1_PG07 Ensure that the customer can exercise control over the collection, processing, storage and disclosing of his personal data (i.e. power consumption data and switching data).

UC1_PG08 Ensure that the energy supplier, DSO, and aggregator are able to demonstrate compliance with the privacy policy and any applicable personal data protection legislation.

5.2 UC3: Dynamic power management for smart homes, smart offices, electric vehicles

The following information assets[3] are considered personal data:

- *Client-supplier contract information* (signed contract between energy supplier and client) stored at energy supplier's systems;
- *Client's devices' service offer* (a client's device offering itself as a configurable power consumption service, including schedules and charging configurations) sent from client's device to the DSO;
- *Client's devices' configuration* (program (or charging) execution schedule and configuration for a certain device, includes device identifier) sent from DSO to the device at the client's home;
- *Service usage notification* (client is informed when (and which) of his devices are (about to be) used to optimise the grid, and when they are not used anymore) sent from DSO to client;
- *Service usage data (*log of how, when, how much its services are being used) stored in the DSO's central systems and sent from DSO to client on an e.g. monthly basis.

Table 5-2 Assessment of privacy roles per identified personal data for use case 3.

Privacy role	Client data and information	Client-supplier contract information	Client's devices' service offer
Data subject	Customer	Customer	Customer
Controller	Energy supplier	Energy supplier	Energy supplier
Processor	DSO, Data Hub	Energy supplier	DSO
Recipient			

	Client's devices' configuration	Service usage notification	Service usage data
Data subject	Customer	Customer	Customer
Controller	Energy supplier	Energy supplier	Energy supplier, Data Hub
Processor	DSO	DSO	DSO
Recipient			

The following privacy goals have been identified:

UC3_PG01 Ensure that minimal client data is collected, transferred, processed, stored, and/or disclosed.

UC3_PG02 Ensure that minimal device's service offer data is requested, processed, stored, and/or disclosed.

UC3_PG03 Ensure that minimal device's configuration data is transferred, stored, and/or disclosed.

UC3_PG04 Ensure that the service usage notification contains the minimal amount of information necessary.

UC3_PG05 Ensure that minimal service usage data is collected, transferred, processed, stored, and/or disclosed.

UC3_PG06 Ensure that client data and information is hidden from plain view

[3] The Information Assets in the description of Use Case 3 were not final at the time of drafting the privacy goals. The information assets listed here are based on an initial version of the use case 3 description. In the final version of the Security & Privacy Goals for SEGRID use cases (SEGRID Deliverable D1.4) this will be updated.

UC3_PG07 Ensure that client-supplier contract information is hidden from plain view

UC3_PG08 Ensure that client's devices' service offer is hidden from plain view

UC3_PG09 Ensure that client's devices configuration is hidden from plain view

UC3_PG10 Ensure that service usage notification is hidden from plain view

UC3_PG11 Ensure that service usage data is hidden from plain view

UC3_PG12 Ensure that service usage data is aggregated at the highest level of aggregation and with the least possible detail in which it is (still) useful.

UC3_PG13 Ensure that client identifier data is separated from device data whenever possible.

UC3_PG14 Ensure that the customer is informed adequately on the personal data (i.e. client data and information, client-supplier contract information, but also which devices are registered for a client, devices service offers, device configurations, service usage notifications and service usage data) that is collected and processed

UC3_PG15 Ensure that the customer can exercise control over the collection, processing, storage and disclosing of his personal data (i.e. client data and information, client-supplier contract information, but also which devices are registered for a client, devices service offers, device configurations, service usage notifications and service usage data).

UC3_PG16 Ensure that the energy supplier and DSO are able to demonstrate compliance with the privacy policy and any applicable personal data protection legislation.

5.3 UC4: Load balancing renewable energy regionally (substation automation)

The following information assets are considered personal data:

- *power production data* (measurements data and customer identifier) collected at short intervals are considered personal data if the producer is a household (UC 4 – scenario 2)
- *'Measurement Data' because of the 'Switch Data'* (information on the service provided by producers to help balance energy on the grid) (UC4 – scenario 2)

Privacy role	Power production data	'Measurement Data' because of the 'Switch Data'
Data subject	Customer	Customer
Controller	Energy supplier	Energy Supplier
Processor	DSO, Data Hub	DSO, Data Hub
Recipient		

The following privacy goals have been identified:

UC4_PG01 Ensure that minimal power production data is collected, transferred, processed, stored, and/or disclosed.

UC4_PG02 Ensure that minimal *'Measurement Data' because of the 'Switch Data'* is collected, transferred, processed, stored, and/or disclosed.

UC4_PG03 Ensure that power production data is hidden from plain view.

UC4_PG04 Ensure that *'Measurement Data' because of the 'Switch Data'* is hidden

from plain view.

UC4_PG05 Ensure that power production data is aggregated at the highest level of aggregation and with the least possible detail in which it is (still) useful.

UC4_PG06 Ensure that *'Measurement Data' because of the 'Switch Data'* is aggregated at the highest level of aggregation and with the least possible detail in which it is (still) useful.

UC4_PG07 Ensure that power production measurements data and identifier data is separated whenever possible.

UC4_PG08 Ensure that *'Measurement Data' because of the 'Switch Data'* and identifier data is separated whenever possible.

UC4_PG09 Ensure that the customer is informed adequately on the personal data (i.e. power production data and *'Measurement Data' because of the 'Switch Data'*) that is collected and processed

UC4_PG10 Ensure that the customer can exercise control over the collection, processing, storage and disclosing of his personal data (i.e. power production data and *'Measurement Data' because of the 'Switch Data'*).

UC4_PG11 Ensure that the energy supplier, DSO, and Data Hub are able to demonstrate compliance with the privacy policy and any applicable personal data protection legislation.

6 State of the Art on Security & Privacy Controls

Over the last couple of years several organisations have established best practices with security and privacy protection controls and countermeasures for smart metering and smart grids. These controls and countermeasures can be applied to ensure the security and privacy goals for the SEGRID use cases. In SEGRID WP2 we will perform a risk assessment on the SEGRID use cases to identify the potential threats and risk factors. In addition, a gap analysis on security solutions for the SEGRID use cases will be performed to identify the current state of the art security solutions and gaps compared to what is needed to mitigate the identified threats and risks.

This chapter presents a high level overview on the state of the art in security and privacy protection controls for smart metering and smart grids that have been composed over the last couple of years. This overview will assist and guide the gap analysis in WP2.

The chapter is structured as follows. First, studies performed under Mandate M/490 with respect to state of the art on security and privacy controls are described. Next, the sets of security measures for smart grids that have been established by ENISA and Expert Group 2 are described. And finally an overview of security and privacy control standards for smart metering and smart grids is provided.

6.1 SGCG - Smart Grid Information Security

In March 2011, the European Commission and EFTA issued the Smart Grid Mandate M/490 which was accepted by the three European Standards Organizations (ESOs), CEN, CENELEC and ETSI in June 2011. M/490 requests CEN, CENELEC and ETSI to develop a framework to enable ESOs to perform continuous standard enhancement and development in the smart grid field. The ESOs combined their strategic approach and established the CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG), being responsible for coordinating the reply to M/490[4]. Part of the mandate requested specific work to be done on information security and data privacy. For this purpose a Smart Grid Information Security Working Group was established. In 2012, the SG-CG SGIS working group produced their first report on information security and data privacy [5].

During the end of 2012, the Smart Grid Mandate M/490 was extended until the end of 2014. The objective of the extension was to allow the SG-CG to fine-tune the Smart Grid methodology developed in 2012 and to develop an extended set of standards supporting Smart Grid deployment in Europe. As part of this extension the SG-CG SGIS working group produced their second Smart Grid Information Security report [12].

Both in 2012 and in 2014 SGIS working group studied the smart grid information security standards landscape. In the second working period, the SG-CG SGIS working group also worked on privacy protection. In the following section we will first present an overview of the work on the smart grid information security standard landscape, followed by an overview of privacy protection work.

[4] http://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force

6.1.1 Smart grid information security standards landscape

The work in [5] identified and analysed the following first set of standards:

- ISO/IEC 27001:2013 [13],
- ISO/IEC 27002:2013 [14],
- IEC 62351 [15],
- NERC CIP (US Standard) [16], and
- NISTIR-7628 (US Guidelines) [17].

These standards were analysed with respect to: 1) their relevance for *organisations* (Smart Grid operators) and *products and services* (product manufacturer and service providers), and with respect to 2) their relevance from a *technical point of view* and from *an organisational point of view*. The five standards were plotted along these two angles, see Figure 3. The conclusion of the first study of the smart grid information security standard landscape was that the basis for standards are available but IEC-62351 and ISO/IEC 27002 could be made more smart grid specific. ??? adapted to SG?

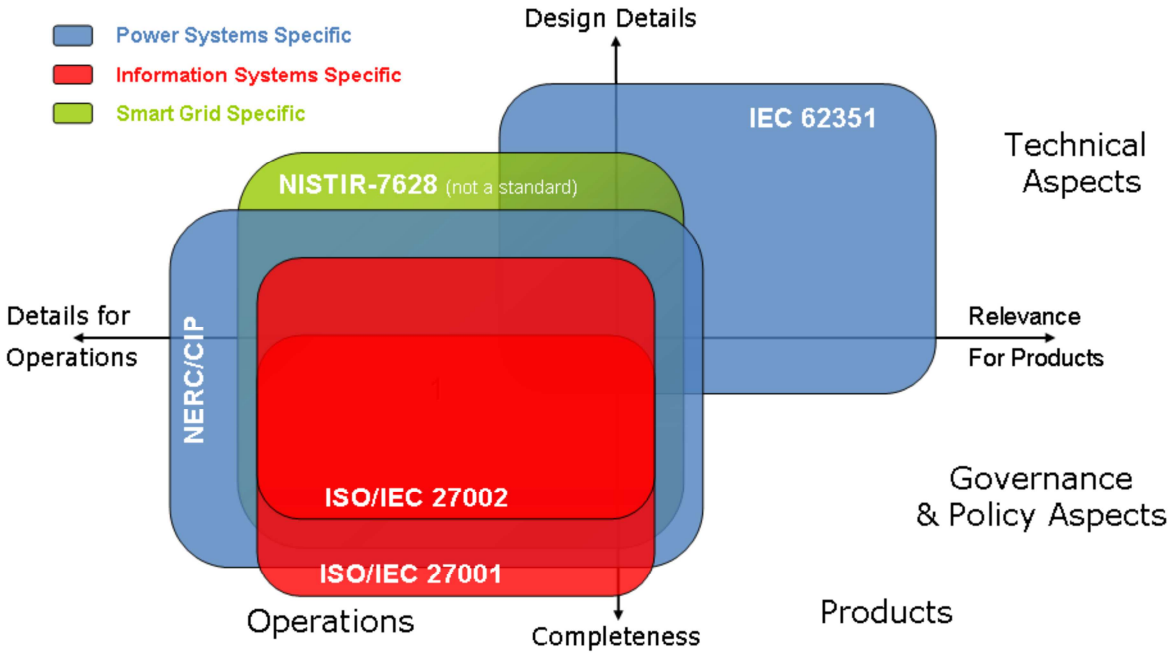

Figure 3. Figure from [5] depicting the analysis of information security standard landscape.

In addition, in 2012 the SGIS working group concluded that analysing the smart grid information security standards landscape is a continuous exercise integrating the evolution of the smart grid information security needs. In 2014 the SGIS working group therefore continued its study of the standards landscape. The focus was to study IEC-62351 further, to study ISO/IEC TR 27019:2013 (an energy domain specific set of controls based on ISO/IEC 27002), and to identify and analyse the further security standards. In particular, with the focus on security standards from ISO, IEC and IETF targeting the implementation of security measures. The selected standards were divided into requirements and solution standards and

are listed in the tables below. These standards were also mapped along the same axis as the first set of standards, see Figure 4.

Table 6-1 Requirement standards considered (The 'What') in [12]

Number	Title
ISO/IEC 15408	Information technology — Security techniques — Evaluation Criteria for IT security
ISO/IEC 18045	Information technology — Security techniques — Methodology for IT Security Evaluation
ISO/IEC 19790	Information technology — Security techniques — Security requirements for cryptographic modules
ISO/IEC TR 27019:2013	Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
IEC 62443-2-4	Security for industrial automation and control systems - Network and system security - Part 2-4: Requirements for Industrial Automation Control Systems (IACS) solution suppliers
IEC 62443-3-3	Security for industrial automation and control systems, Part 3-3: System security requirements and security levels
IEC 62443-4-2	Security for industrial automation and control systems, Part 4-2: Technical Security Requirements for IACS Components
IEC 62443-2-1	Security for industrial automation and control systems - Network and system security - Part 2-1: Industrial automation and control system security management system
IEEE 1686	Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities
IEEE C37.240	Cyber Security Requirements for Substation Automation, Protection and Control Systems

Table 6-2 Solution standards considered (The 'How') in [12]

Number	Title
ISO /IEC 15118-2	Road vehicles – Vehicle-to-Grid Communication Interface, Part 2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements
IEC 62351-x	Power systems management and associated information exchange – Data and communication security
IEC 62056-5-3	DLMS/COSEM Security
IETF RFC 6960	Online Certificate Status Protocol
IETF RFC 7252	CoAP Constrained Application Protocol
IETF draft-weis-gdoi-iec62351-9	IEC 62351 Security Protocol support for the Group Domain of Interpretation (GDOI)
IETF RFC 7030	Enrolment over Secure Transport

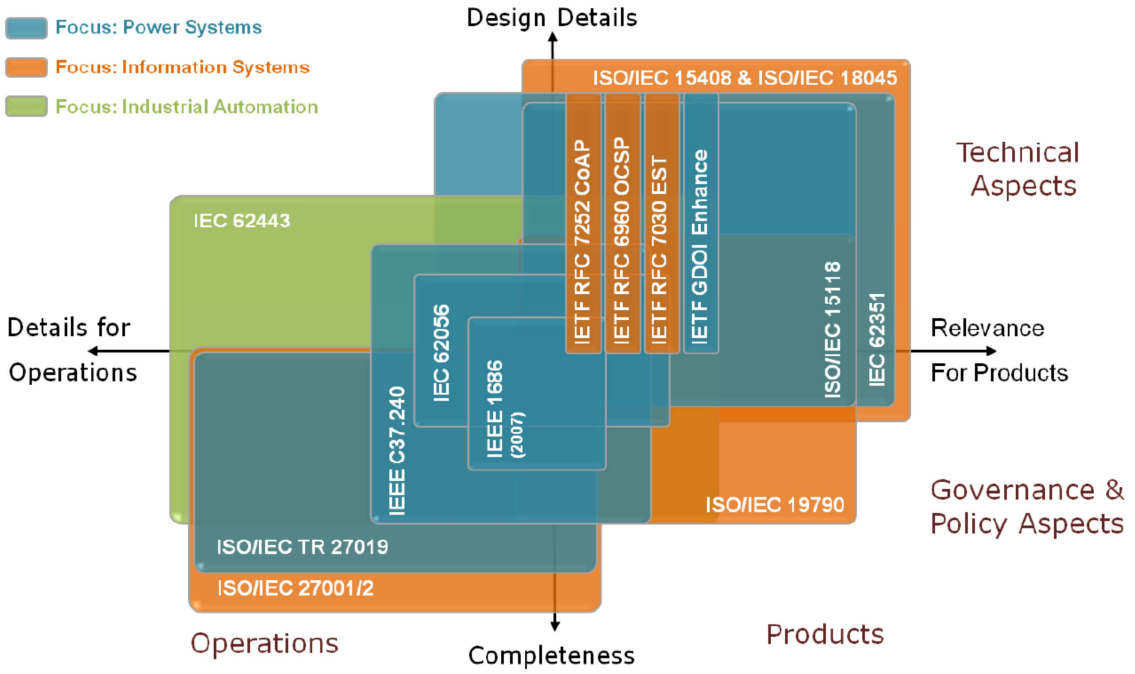

Figure 4. Figure from [12] depicting the analysis of information security standard landscape.

The selected set of standards has also been mapped to the Smart Grid Architecture Model (SGAM), and gaps were identified regarding their resolution in the associated standardisation committees. this analysis is well documented in [12].

6.1.2 Privacy protection

The SG-CG SGIS working group has performed an extensive analysis of data protection issues for smart grids, in particularly in the context of smart metering and electric vehicles. The working group performed an analysis on emerging Privacy Enhanced Technologies (PET) to support privacy by design. In [12] an overview of the state of the art of privacy enhancing technologies for smart metering and for electric vehicles is presented.

The working group also studied the Data Protection Impact Assessment (DPIA) template that was developed by the EU Smart Grid Task Force Expert Group 2 (SGTF EG2). In particular, the working group assessed DPIA template in relation to the SGIS Toolbox, described in annex B of [5], and the SGIS Framework [12]. It was suggested that data protection impact assessment is considered separately in the pre-assessment of the SGIS Framework, since an identical approach to security cannot be applied for data privacy.

6.2 Sets of security measures for smart grids

6.2.1 ENISA - Security measures for smart grids

In 2012 ENISA has issued two reports on smart grid security. The first report [18] *'Smart Grid Security: Recommendations for Europe and Member States'* was the result of a study to identify the risks and challenges related to cyber security aspects of smart grids, and study the

national and European initiatives related to smart grids security. The report presents ten recommendations for stakeholders, both from public and private sector, aimed at providing useful and practical advice in order to improve current initiatives, enhancing co-operation, raising awareness, developing new measures and good practices, and reducing barriers to information sharing.

The second report [19] *'Appropriate security measures for smart grids'* is a technical document with a set of minimum security measures. It is intended for smart grid stakeholders to provide guidance and help improve the minimum level of their cyber security services. The security measures are organised into three sophistication levels and ten domains, namely:

- Domain 1: Security governance & risk management;
- Domain 2: Management of third parties;
- Domain 3: Secure lifecycle process for smart grid components/systems and operating procedures;
- Domain 4: Personnel security, awareness and training;
- Domain 5: Incident response & information knowledge sharing;
- Domain 6: Audit and accountability;
- Domain 7: Continuity of operations;
- Domain 8: Physical security;
- Domain 9: Information systems security; and
- Domain 10: Network security.

The document also provides a mapping between the proposed measures and the controls from ISO/IEC 27002 [14], NISTIR 7628 [22] and ISO/IEC TR 27019:2013 [21] standards.

This ENISA report was the basis for the *proposal for a list of security measures for smart grids*, of the Smart Grid Task Force - Expert Group 2, described in the following section.

6.2.2 Expert Group 2 – Proposal for a list of security measures for smart grids

The European Commission Smart Grids Task Force was established in 2009 to advice on issues related to smart grid deployment and development. Expert Group 2 for Regulatory recommendations for privacy, data protection and cyber security in the smart grid environment produced several documents that are relevant in the context of this state of the art overview.

The *Proposal for a list of security measures for smart grids* is a technical report to help smart grid asset owners define what is good practice rather than to provide them with a set of minimum or appropriate security measures [20]. The document provides a catalogue of 45 available security measures, grouped in 11 domains, that might help smart grid providers in improving the level of the cyber security of their installations. The report stresses that this list is intended as guidance and not a mandatory list. The smart grid asset owners should first perform a risk assessment (define appropriateness) and use the security measures catalogue for control selection for risk mitigation. The proposed security measures do not address data privacy which is out of scope of the document.

The ENISA report on *Appropriate security measures for smart grids* [19] was used as a starting point. The first 10 domains are similar and only a couple of measures have been added. The security measures catalogue contains an additional domain:

- Domain 11: Resilient and robust design of critical core functionalities and infrastructures.

In addition, the report provides an overview of smart grid assets, a threat landscape for smart grids and a mapping between the appropriate security measures, assets and threats.

6.3 Security and privacy controls standards

6.3.1 ISO/IEC TR 27019:2013

The *Information Security Management System (ISMS)* set of standards by ISO, also known as the ISO/IEC 27000 series, has been developed to be applicable to all organisations, regardless of type, size or nature'. These standards can thus also be applied to the energy domain, and more specifically the smart grid domain. In the ISO/IEC 27000 series the ISO/IEC 27002:2013 [14] is the code of practice for information security controls, and contains 14 security control clauses collectively containing a total of 35 main security categories and 114 controls.

Since ISO/IEC 27002 contains best practice information security controls applicable for all types of organisations, domain specific best practice controls are not included. Moreover, the implementation guidance given for each control will typically not provide domain specific guidance. As a consequence, some sectors have developed sector specific sets of information security controls based on ISO/IEC 27002. For the energy sector a sector specific Technical Report, ISO/IEC TR 27019:2013 [21], was prepared by DIN Deutsches Institut für Normung and was adopted by ISO and IEC, under a special "fast-track procedure". It is expected that ISO will start a revision process soon, since the technical report was based on the ISO/IEC 27002:2005, which was revised in 2013.

The ISO/IEC TR 27019:2013 [21] contains guidelines based on ISO/IEC 27002:2005 for process control systems specific to the energy utility industry. The scope of ISO/IEC TR 27019:2013 is defined as 'process control systems used by the energy utility industry for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes.' The technical report contains the following additions:

- energy sector specific implementation guidelines to ISO/IEC 27002:2005 controls
- 4 new energy sector specific control objectives, and
- 11 new energy sector specific controls.

Energy utility organisations that implement an ISMS based on ISO/IEC 27001 can use the ISO/IEC 27002 and the ISO/IEC TR 27019:2013 [21] for the control selection to mitigate the risks identified in a risk assessment. Note that *risk assessment* and *control selection using ISO/IEC 27002* are mandatory requirements in ISO/IEC 27001. It will be possible to perform

an ISO/IEC 27001 certification of an ISMS that used ISO/IEC 27002 and the ISO/IEC TR 27019:2013 for control selection. This is being specified in ISO/IEC 27009 – Sector-specific application of ISO/IEC 27001[5].

6.3.2 NISTIR 7628 rev 1

NIST Interagency Report 7628 [22], Guidelines for Smart Grid Cyber Security, consists of three volumes:

1. Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements
2. Privacy and the Smart Grid
3. Supportive Analyses and References

It presents an analytical framework that organisations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related characteristics, risk factors, and vulnerabilities.

The initial version [17] of Guidelines for Smart Grid Cyber Security was developed as a consensus document by the Cyber Security Working Group (CSWG) of the Smart Grid Interoperability Panel (SGIP), a public-private partnership launched by NIST in January 2010. Since 2010, new insights and changes in regulatory requirements regarding privacy necessitated an updates, resulting in NISTIR 7628 Rev. 1 [22].

- Volume 1 provides a general set of requirements for *logical architecture and interfaces of the smart grid* that were established using a high-level risk assessment process. In addition, Volume 1 also identifies technical cryptographic and key management issues and alternatives solutions (e.g. existing standards, methods, or technologies) across the scope of systems and devices found in the smart grid.
- Volume 2 provides among other things a discussion of the concept and terminology of privacy, identified personal activities within the smart grid, provides an in-depth look at privacy issues and concerns, particularly in the context of electric vehicles, and a brief discussion of fifteen emerging smart grid privacy risk factors for which organisations and consumers should stay aware. It is important to note that volume 2 of NIST is based on USA regulatory requirements and approaches on privacy, which do differ from the European regulatory requirements approach.
- Volume 3 provides more in-depth analysis in support of volume 1. Including among others an overview of vulnerability classes, bottom-up security analysis, overview of relevant standards, and an analysis of key use cases that are architecturally significant with respect to security requirements for the smart grid. For each of the use cases high-level requirements of confidentiality, integrity, and availability (CIA) have been defined.

6.3.3 IEC 62351

IEC 62351 [15] is a multi-part standard developed for handling the security of protocols developed by the IEC Technical Committee 57. IEC TC57 is responsible for development of standards for information exchange for power systems and other related systems including

[5] At the moment of writing this deliverable ISO/IEC 27009 was still under development; status committee draft.

Energy Management Systems, SCADA, and distribution automation. IEC 62351 was developed and is maintained by IEC TC57 working group 15 (WG15).

IEC 62351 addresses different security objectives and include authentication of data transfer through digital signatures, ensuring only authenticated access, prevention of eavesdropping, prevention of playback and spoofing, and intrusion detection. In the table below, the different parts are listed. An overview of the IEC TC57 WG15 standard is given in [23].

Table 6-3 overview of the IEC 62351 parts.

Number	Title
IEC 62351-1	Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues
IEC 62351-2	Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms
IEC 62351-3	Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP (incl. TLS Encryption, Node Authentication, and Message Authentication)
IEC 62351-4	Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS
IEC 62351-5	Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives
IEC 62351-6	Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850
IEC 62351-7	Power systems management and associated information exchange - Data and communications security - Part 7: Network and system management (NSM) data object models
IEC 62351-8	Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control
IEC 62351-9	Power systems management and associated information exchange - Data and communications security - Part 9: Key Management
IEC 62351-10	Power systems management and associated information exchange - Data and communications security - Part 10: Security architecture guidelines
IEC 62351-11	Power systems management and associated information exchange - Data and communications security - Part 11: Security for XML Files

7 References

[1] M/441 EN; "*Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability*"; European Commission Directorate-General For Energy; Brussels; 12th March 2009.

[2] M/490 EN; "*Smart Grid Mandate Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment*"; European Commission Directorate-General For Energy; Brussels; 1st March 2011.

[3] Axel van Lamsweerde; "*Goal-Oriented Requirements Engineering: A Guided Tour*"; In: RE, IEEE Computer Society (2001); 249.

[4] ISO/IEC 27000:2014, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, ISO, Switzerland.

[5] SG-CG/M490/D_ Smart Grid Information Security, CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Information Security, November 2012. Available at: ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf

[6] ISO/IEC 7498-2:1989, Information Processing Systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture, ISO, Switzerland.

[7] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('General Data Protection Regulation'); This document is based on the latest (unofficial) Version of the GDPR: INOFFICIAL CONSOLIDATED VERSION AFTER LIBE COMMITTEE VOTE, PROVIDED BY THE RAPPORTEUR, 22 October 2013, Available at http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf.

[8] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data". Available on Eur-lex.europa.eu.

[9] ISO/IEC 29100, "Information technology – Security techniques – Privacy framework", ISO, Geneva, Switzerland, 2011

[10] J.-H. Hoepman, "Privacy Design Strategies", In IFIP TC11 29th Int. Conf. on Information Security (IFIP SEC 2014), pages 446-459, June 2-4 2014. A preliminary version was presented at the Amsterdam Privacy Conference (APC 2012) and the

Privacy Law Scholars Conference (PLSC 2013). Available at: http://www.cs.ru.nl/~jhh/publications/pdp-sec.pdf

[11] SEGRID Deliverable D1.1; "Architecture and design for use cases"; April 2015.

[12] SG-CG/M490/H_ Smart Grid Information Security; CEN-CENELEC-ETSI Smart Grid Coordination Group; 2014-12. Available at: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf

[13] ISO/IEC 27001:2013; *Information technology —Security techniques — Requirements*; Second edition; 2013-10-01.

[14] ISO/IEC 27002:2013; *Information technology —Security techniques — Code of practice for information security management*; Second edition; 2013-10-01

[15] IEC 62351; "*Power systems management and associated information exchange - Data and communications security*"; IEC.

[16] NERC CIP; Available at: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[17] NISTIR 7628; *"Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements"*; August 2010.

[18] *"Smart Grid Security - Recommendations for Europe and Member States"*; ENISA; 2012-07-01.

[19] *"Appropriate security measures for smart grids - Guidelines to assess the sophistication of security measures implementation"*; ENISA; 2012-12-06.

[20] SMART GRID TASK FORCE Expert Group 2; Proposal for a list of security measures for smart grids. 9/12/2013. Available at: https://ec.europa.eu/energy/sites/ener/files/documents/20140409_enisa_0.pdf

[21] ISO/IEC TR 27019:2013; *Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*; 2013-05-07

[22] NISTIR 7628 Revision 1; *"Guidelines for Smart Grid Cybersecurity. Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements"*; September 2014. Available at: http://dx.doi.org/10.6028/NIST.IR.7628r1

[23] Frances Cleveland; “IEC TC57 WG15. IEC 62351 Security Standards for the Power. System Information Infrastructure.”, IEC, June 2012; Available at: http://iectc57.ucaiug.org/wg15public/Public Documents/White Paper on Security Standards in IEC TC57.pdf