FP7 Grant Agreement N° 607109

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

D1.4 Final report on the security & privacy goals

Due date of deliverable: 01/10/2016
Actual submission date: 30/9/2016
Work package: WP1 Use Cases and Security Goals
Number of pages: 41
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 D1.4 the *final set* of security & privacy goals for the SEGRID use cases is defined. This deliverable is the final update of the first report on the security & privacy goals (D1.3).

A security goal is defined as "*a specific need to protect a certain interest of a stakeholder"*. The focus of the deliverable has been on drafting security goals on:

- traditional information security properties (i.e. *confidentiality*, *integrity* and *availability*)
- system security properties, such as: *system integrity*, *robustness* and *resilience.*

These security properties have been elaborated on, and a stepwise approach has been defined to draft security goal.

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 recently accepted 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 "Privacy Design Strategies" by J.-H. Hoepman [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. This stepwise approach has been applied to draft the set of privacy goals for the three SEGRID use cases which cover elements where personal data is collected, transferred, processed and/or stored.

Author	Frank Fransen (TNO)
Contributors	Johanneke Siljee (TNO) Eric Luiijf (TNO) Pei-Hui Lin (ENCS) Nuno Medeiros (EDP Distribuição) Rolf Blom (SICS) Marco Tiloca (SICS) Judith Rossebo (ABB) Johan Rambi (Alliander) Exabier Bilbao Hernandez (ZIV)

Security Assessment	**See deliverables table for security assessment requirements**
Approval Date	September 30th 2016
Remarks	None

TABLE OF CONTENTS

1 INTRODUCTION – RATIONALE OF THIS DOCUMENT 5
1.1 The SEGRID project objectives 5
1.2 Work Package 1 – Use Cases and Security Goals 6
1.3 The structure of Deliverable D1.4 7
2 METHOD FOR ESTABLISHING SECURITY AND PRIVACY GOALS 8
2.1 Introduction 8
2.2 Properties for defining security goals 8
2.2.1 Security properties for information assets 9
2.2.2 Security properties for system assets 10
2.3 Properties for defining privacy goals 14
2.4 Methodology 16
3 SEGRID USE CASES 17
3.1 UC1: Smart meter used for on-line reading of consumption and technical data 17
3.2 UC2: Load balancing renewable energy centrally 18
3.3 UC3: Dynamic power management for smart homes, smart offices, and electric vehicles 20
3.4 UC4: Load balancing renewable energy regionally (substation automation) 22
3.5 UC5: Automatic reconfiguration of the power grid 23
4 SECURITY GOALS 26
4.1 Security goals for information assets 26
4.1.1 Customer (Household) 26
4.1.2 Customer (MV DER) 26
4.1.3 Energy supplier 26
4.1.4 Distribution System Operator 27
4.1.5 Data Hub 28
4.1.6 CSO 28
4.2 Security goals for the system assets 28
4.2.1 Smart Meter 29
4.2.2 Household concentrator 30
4.2.3 SCADA 30
4.2.4 RTU (primary substation & secondary substation) 30
4.2.5 Communication network 31
5 PRIVACY GOALS 32
5.1 UC1: Smart meter used for on-line reading of consumption and technical data 32
5.2 UC3: Dynamic power management for smart homes, smart offices, electric vehicles 33
5.3 UC4: Load balancing renewable energy regionally (substation automation) 34
6 GLOSSARY 36
7 REFERENCES 39
APPENDIX A – MAPPING BETWEEN STAKEHOLDER INTERESTS AND ASSETS 41

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 the coming years, the level of automation in electricity distribution grids will grow substantially. Smart meters will be deployed at home premises, and remote terminal units (RTUs) will be placed in distribution substations. The increased automation should provide a better view of how electricity flows to the medium and low voltage grids, and provide grid operators increased control to influence that flow. But the increased automation also has major consequences for the cyber security posture of the electricity grid. By nature, automation adds new attack vectors through which cyber attackers can enter and attack the networks of grid operators, and offers other possibilities to cause physical damage to the electricity grid itself. Moreover, there is an increased risk of physical damage to the electricity grid due to inadvertent events in the cyber domain of Smart Grids (e.g. malware, technical dependencies, and human errors).

From a technical point of view, it is not sufficient to only consider all the different components in a Smart Grid separately; they will together form a truly integrated system-of-systems and 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 methods for 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. A number of new cyber security issues become critical in this context.

This new utility-wide system(-of-systems) will not come into existence overnight; the Smart Grid will be composed of a mix of old, even legacy, and new components. Therefore, we look upon the Smart Grid as a gradually evolving system in which new functionalities are added to accommodate new use cases with the challenge to maintain security, privacy and dependability of the Smart Grid as a whole. The required security solutions to cope with this situation range from improvements in current security, privacy and operational solutions and procedures to the introduction of new security and privacy paradigms.

The term 'Smart Grid' is used for a wide variety of developments related to the automation of electricity grid. Focusing on the efforts of the project, SEGRID will work on five concrete use cases, shown in Figure 1. These have been further elaborated in the deliverable D1.1 of the project. The five SEGRID use cases are:

1. Smart meters 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);

Automatic reconfiguration of the power grid.

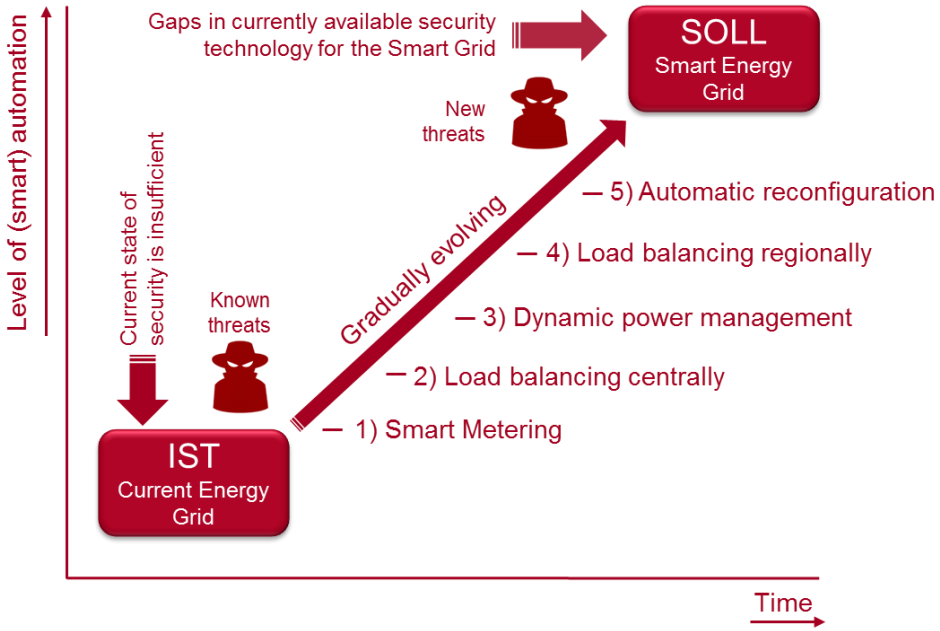

Figure 1: SEGRID storyline

The SEGRID use cases reflect important steps of Smart Grid developments until 2020 and beyond, and will cover the most relevant security and privacy issues that will arise from the increasing complexity of Smart Grids.

SEGRID will formulate privacy and security goals for the use cases defined (WP1) and perform a risk analysis of these use cases (WP2). Vulnerability assessment frameworks and tools to identify these risks in real systems will be developed (WP3) and gaps in the currently available security solutions will be identified (WP2). Solutions for some of these gaps will be developed in WP4. Selected vulnerability assessment tools and novel security solutions will then be tested in SITE (WP5).

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.

SEGRID deliverable D1.1 [11] defines and describes the SEGRID architecture and the five SEGRID use cases. 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. This deliverable D1.4, contains the final report on the security & privacy goals. The figure below depicts the dependencies between the WP1 deliverables.

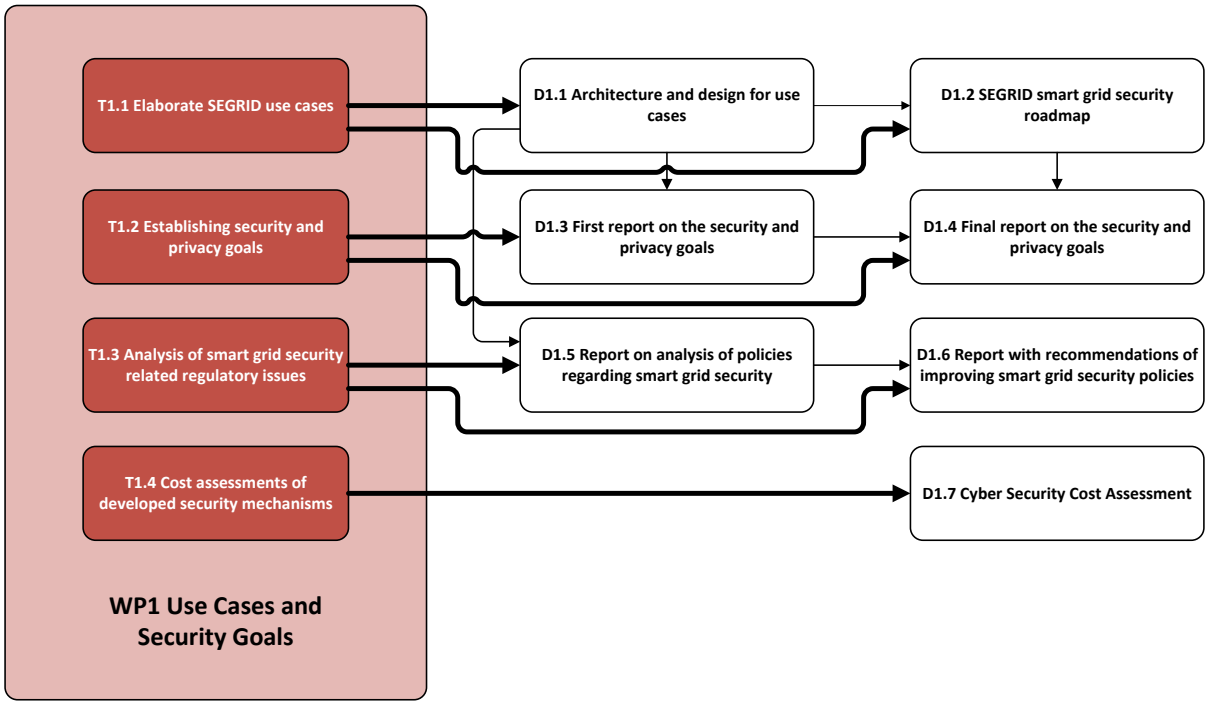

Figure 2 - Dependencies between the WP1 deliverables

1.3 The structure of Deliverable D1.4

Chapter 2 describes the methodological approach for drafting security and privacy goals. Next, the SEGRID use cases are briefly described, including an assessment of the stakeholders, their interests and the information and system assets that play a role each of the use cases. The following two chapters subsequently present the set of security goals and the privacy goals for the SEGRID use cases.

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. For instance, 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. We have decided to define security goals at an abstract level based on the stakeholders interests. As part of WP2, risk assessments on SEGRID use cases have been performed. Based on the results of these risk assessments more use case specific security requirements to mitigate particular threats can be defined.

In the following two sections we will discuss what security and privacy concerns are considered for the definition of security & privacy goals in each of the SEGRID use cases.

2.2 Properties for defining 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.

In D1.1 we distinguish between information assets and system assets. A system asset is defined as a physical component that processes information assets. A set of interacting or interdependent system assets make up the system that performs the business function or the service described in the SEGRID use case.

In the following sections, the security properties which can be used to define security goals are explored. This is done for both information assets and system assets.

2.2.1 Security properties for information assets

Security properties for information assets 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 of this series, 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.

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

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

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.

Since accountability is more a property of a system it will be included in the following section.

2.2.2 Security properties for system assets

2.2.2.1 Introduction

System security properties can be applicable for individual system assets as well as the system-as-a-whole. In this section, we will consider security properties for both systems and individual system assets. Note that in standards, such as IEC 62443 [13], system assets are typically referred to as components.

When considering a system asset it makes sense to further distinguish between the hardware, software (including firmware, operating system, and applications) and data (both configuration data and process data), see Figure 3. Software and data are information assets. For those types of assets we can define security goals using the properties defined in Section 2.2.1.

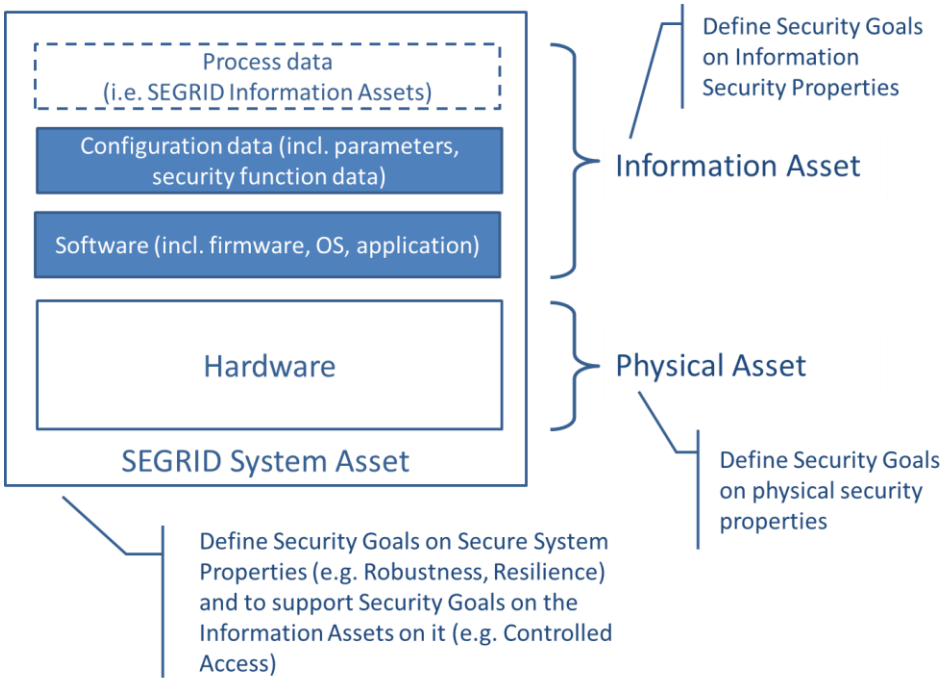

Figure 3: Elements of a system asset (i.e. component)

2.2.2.2 Security properties

Security properties for systems and system assets are less well defined as those for information assets. In fact, it is common to define security controls and mechanisms instead of the particular properties that need to be preserved. In this section, we have collected a set of system security properties that are relevant in the context of Smart Grids.

The properties **availability** and **integrity** have a slightly different meaning, if they are considered in the context of a system or system asset. A good definition for availability in the context of a system is given in IEEE Standard Glossary of Software Engineering Terminology, i.e. IEEE Std 610.12-1990 [12]:

> **System Availability** - the degree to which a system or component is operational and accessible when required for use. Often expressed as a probability.

Note that the definition refers to a degree. This is relevant as the impact of the duration of unavailability can vary significantly. As security goals are defined at an early stage of the design phase it may be difficult to specifically quantify the degree of the desired system availability. In this document, we will therefor will only specify security goals on the system availability of a system or system assets if its disturbance has a direct severe impact on a certain interest of a stakeholder.

System Availability is directly related to the properties **robustness**, and **resilience** that have been defined in SEGRID deliverable D4.1 [14]:

> **Robustness -** the ability of a system or network (component) to remain secure and operational despite some of its components (subcomponents) have been compromised or have been subjected to disturbance events.

> **Resilience -** the ability of a system, network or entity exposed to threats to resist, absorb, accommodate to and recover from the effects of cyber-attacks in a timely and efficient manner, including the preservation and restoration of its essential basic structures and functions.

As the latter two are more specific regarding the particular behaviour of the system or system asset during a cyber-attack (or disturbance), it is relevant to consider these properties in the context of the SEGRID project. As we define security goals based on the need to protect a certain interest of a stakeholder, it might however be difficult to distinguish whether a system (asset) needs to be *robust* or *resilient*.

Regarding integrity in the context of a system, IEEE Std 610.12-1990 [12] also has a definition. This definition, however, is a slightly outdated as it focuses only on the prevention of unauthorized access. With integrity of a system, we currently mean that the system performs its intended function correctly. We will therefor use the definition from [15] and [16]:

> **System integrity** - The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

This definition does seem similar to what is typically meant with reliability. The definition of information security in the previous section also mentioned reliability as an additional property of information security. In ISO/IEC27000:2014 reliability is defined as: property of consistent intended behaviour and results. In IETF RFC 4949 a more specific definition is given [17]:

> **Reliability** - The ability of a system or component to perform its required functions under stated conditions for a specified period of time.

We will typically refer to **reliability** for the property of a system to execute its intended function, and to **system integrity** when we specifically want to stress the property that a system can execute its intended function in an unimpaired manner, free of unauthorized manipulation. The execution of critical processes or security functions are typical examples for which execution on a component with high **system integrity** is recommended. Note that particularly in the case of security functions the

confidentiality and *integrity* of stored and processed data needs to be protected as well (e.g. to protect cryptographic keys and other security parameters). It is common to require that such functions be executed within a Trusted Execution Environment (TEE) as it protects the execution of the security functions and the data stored in and processed by the TEE. The capability of a component to protect resources such as the software, configuration data and process data on it, is referred to as access control. As this is an important capability we decided to include the security property **Controlled Access** for components:

> **Controlled Access -** the ability of a system or component to enable authorised entities to use or access a resource (e.g. function, software, configuration data, and process data) while preventing unauthorised use or access of that resource.

Related to this is accountability as defined in the previous section. If it is relevant for a system or system asset to ensure that the actions of an entity may be traced uniquely to the entity we will define **accountability** as a security goal.

Another important aspect for cyber security of Smart Grids is the **physical security** of a system or system asset. In energy transmission and distribution systems, equipment will typically be distributed across decentralized sites, ranging from control rooms and data centres within the organization's building, to peripheral (potentially unoccupied) sites and customer premises. Physical security is about preventing unauthorised physical access to the system assets which are relevant for a certain interest of a stakeholder.

In some cases, however, breaching the physical perimeter of a system asset ~~access~~ cannot be prevented. For instance, the smart meter is located at the premises of the customer. When a third party with physical access has an interest in tampering with the equipment, it is important to further protect the equipment against tampering. Typical security properties or capabilities are: **tamper detection**, **tamper response, tamper evident** and **tamper resistant.** Since the specific tamper protection that needs to be apply depends on the threats and risks an organisation wants to mitigate, we will not define specific tamper protection goals. When relevant we will define a security goal on the physical security of system asset and mention the need for tamper protection.

2.2.2.3 Security life-cycle management properties

Security goals can also be defined for a particular phase in the life-cycle of a system or a component. In D4.1, the security life-cycle management has been defined with the following phases: manufacture phase, deployment phase, and operational phase. We have added decommission phase, as it is relevant to consider security and potential threats when disposing of components.

Manufacture phase

With respect to the manufacture phase it is relevant to mention that the component should be securely engineered. Nowadays more and more standards are being developed on security engineering and secure (software) development process, such as the NIST Special Publication 800-160 [18]. Also certification schemas that provide assurance on the secure development process are being developed, such as ISASecure Security Development Lifecycle Assurance (SDLA) Certification that is based on ISA/IEC 62443-4-1 [19].

In addition, it is also possible to require assurance on the security functions of a product. The typical framework for this is Common Criteria (CC), which is specified in ISO/IEC 15408 [20]. CC enables products to be certified on a specific assurance levels. The specific security properties to be assessed depend on each particular product. These are typically defined for categories of products in so called Protection Profiles. The actual certification is done against a Security Target which describes in a

formal manner the security needs for the specific product that is identified as the Target of Evaluation (TOE).

Another product security certification schemes relevant in the context of Smart Grids is ISASecure Embedded Device Security Assurance (EDSA) Certification based on the ISA/IEC 62443-4-2 specification [13] containing the technical security requirements for industrial automation control system components. The ISASecure certification has four security assurance levels (SAL) that are defined in ISA/IEC 62443.

With respect to defining security goals for the manufacture phase we can thus define security assurance with a specific assurance level with respect to:

- the secure development process applied by the manufacturer of a particular component;
- the security functions of a particular component.

Deployment phase

As to the deployment phase it is important that the components is securely handed over from the manufacturer to the operator, and securely deployed within a power grid system. For some components (e.g. smart meters) the manufacturer can pre-install cryptographic key material that will be used to securely load the operational keys, additional software and configuration data during the deployment phase. These so called trust anchors need to be securely handed over from the manufacturer to the operator (or system integrator). A security goal can be defined for components to support **Secure handover of Trust Anchors**.

As it is still quite common that components are being deployed with an insecure configuration (e.g. unpatched, default passwords, open ports), an important step during the deployment phase is ensuring that components will be deployed in a secure configuration. This is typically referred to as **Secure configuring** and **Hardening**. The latter includes locking down the functionality of the component to prevent unauthorized access or changes, remove unnecessary functions or features, and patch any known vulnerabilities. Although the manufacturer should lead or at least assist with this processes, this support is not always provided. For common components (e.g. Windows systems, Cisco routers) secure configuration guidelines exist, such as the Security Configuration Benchmarks from Center for Internet Security[1]. Security goals can thus be defined for deployment of components in a **secure configuration**.

Operational phase

During the operational phase, the threat landscape will change as new types of attacks and new security vulnerabilities are discovered. In addition, the level of protection provided by particular security mechanisms (e.g. a cryptographic algorithm) will degrade over time or can even be disruptively jeopardized. It is relevant to ensure that a component's software and hardware, and in particular the security protection mechanisms, can be updated. A component should thus be **Maintainable** and **Upgradable**:

- **Maintainability** – the ease with which a software system or component can be modified to correct faults, improve performance or other attributes, or adapt to a changed environment [12].

- **Upgradability** – the property of a system to support upgrades of system functions, including security functions.

[1] https://benchmarks.cisecurity.org/

In SEGRID deliverable D4.1 [14] these component properties are defined as Future-Proof.

Decommission phase

Ìn the decommission phase it is important that confidential data on the components is removed, zeroised or destroyed in another way before disposal or redeployment of the component. This is, however, rather an information security management control then a specific security property of a system asset.

2.3 Properties for defining privacy goals

Privacy protection is a major concern of the European Commission (EC) 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. This has been replaced by the European Commission data protection regulation, General Data Protection Regulation (GDPR) [7], which is an EU wide law to strengthen and unify data protection within the EU. The GDPR is particularly more specific regarding developments new system that handles personal data. For example, article 25 mandates data protection by design and by default, and article 35 mandates the carrying out of a Data Protection Impact Assessment (DPIA). This is very relevant in the context of Smart Grids, as the introduction of smart meters has, for example, led to debates on privacy. The EU Smart Grid Task Force Expert Group 2 has developed a DPIA Template for Smart Grid and Smart Metering Systems [21].

Privacy protection is concerned with safeguarding "personal data". In GDPR "personal data" is defined in article 4 as:

> *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"*

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 processes 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. Otherwise, the privacy goals would 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 focused 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.

Method for drafting Security Goals

The following stepwise approach has been developed to draft the security goals for each of the SEGRID use cases:

Step 1. Identify the stakeholders and their interest for the specific SEGRID use case;

Step 2. Identify the information assets and system assets for the specific 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 & system assets need to be preserved to ensure the stakeholder interests;

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

Method for drafting Privacy Goals

The following stepwise approach has been developed to draft the privacy goals for each of the SEGRID use cases in which privacy concerns play a role:

Step 1. Determine if in the specific use case personal data is collected, transferred, processed and/or stored. In that 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 for this particular use case.

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

Each of the 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.

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	Energy consumption
	Compensation for energy production
	Correct invoice for energy consumption and production
	Protection of personal data
Energy supplier	Purchase energy
	Perform billing (invoicing) (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)

Information Assets:

- Measurement Data
- Switch Data
- Configuration Data
- Monitoring Data
- Fault Data (incl. location)
- Outage Data
- Distribution network model

System Assets:

- Smart Meter
- Display
- Actuator (Switch)
- Sensors
- Meter Data Concentrator
- IT DSO: Smart Metering Information system (AMI)
- SCADA
- Data Hub: Exchange System
- Energy Supplier System
- Call Centres
- Outage Management System (OMS)

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 for use case 2 (UC2).

Table 3-2 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	Correct invoice for energy production
	Compensation for energy production
DSO	Energy distribution
	Power quality management (1)
	Energy balancing (2)

Information Assets:

- Sensor Data
- Load Forecast Data
- kWh Data
- Set Points
- Configuration Data
- Monitoring Data

System Assets:

- Intelligent Electronic Devices
- RTU: secondary substation
- RTU: primary substation
- SCADA front-end
- SCADA
- TSO System
- Access to TSO Data (ICCP)
- SCADA Vendor Access
- DSO IT
- Data Historian
- Maintenance front-end
- Element Manager (e.g. https, SSL/TLS)
- Time synchronization e.g. (SNTP)

- Monitoring system (e.g. SNMP)
- RTU: DER Meter
- Display
- Set Point Actuator (Switch)
- Meter Data Concentrator
- IT DSO: Smart Metering Information system (AMI)
- Data Hub: Exchange system
- Energy Supplier System

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

Dynamic Power Management for smart homes, smart offices, and 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 a) home or b) public charge spot. To prevent a peak loads due to EV charging, the DSO is able to influence charging of EVs.
    a) The customer has to inform the DSO of how much the EV must be charged and by when the vehicle must be loaded to the required capacity level. The DSO can then execute EV charging to optimally balance energy production and consumption.
    b) The charge spot operator (CSO) creates a charge plan for this EV ('EV Charge Plan') and submits the charge plan to the DSO for approval. If the charge plan does not fit within all constraints, the DSO responds with a request for a new plan and provides information on the available capacity in the network segment. The CSO can change the charge plan accordingly.

In the table below the main stakeholders and their high level interests are listed for use case 3 (UC3).

Table 3-3 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
CSO	Charge EV
Energy supplier	Purchase energy
	Energy sales & billing (invoicing)

Information Assets:

- Measurement Data
- Sensor Data
- Switch Data
- Change consumption/generation command
- Consumption Priorities
- Current Status Data
- Set points
- Monitoring Data
- Load Forecast Data
- Dynamic Network Topology Data
- EV Charge Data
- EV Charge Plan

System Assets:

- Household Concentrator
- Smart Household Appliance
- Charging Point
- Smart Meter
- Display
- Sensors
- Actuator (switcher)
- Meter Data Concentrator
- IT DSO: Smart Metering Information system (AMI)
- RTU at substation
- SCADA
- SCADA Front-End
- TSO System
- Data Hub: Exchange system
- Energy Supplier System
- Electric Vehicle (EV)

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).

Table 3-4 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

Information Assets:

- Analogue Data
- Sensor Data

- Measurement Data
- kWh Data
- Change consumption/generation command
- Consumption Priorities
- Current Status Data
- Set points
- Switch Data
- Monitoring Data
- Fault Data: Breaker State Data
- Sensor Data: Feeder Data
- Load Forecast Data
- Dynamic Network Topology Data

System Assets:

- Analogue Sensor
- Actuator (switcher)
- Sensors
- Intelligent Electronic Devices
- RTU at Power generation MV
- RTU at substation
- Short Circuit Indicators
- Feeder Protection
- HMI
- kWh meter
- SCADA
- Access to TSO Data
- Smart Meter
- Display
- Household concentrator
- Smart Household Appliance
- Meter Data Concentrator
- IT DSO: Smart Metering Information system (AMI)
- Data Hub: Exchange system
- Energy Supplier System

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).

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

Stakeholders	Interest
DSO	Energy distribution
	Outage management
	Minimise grid losses

Information assets:

- Sensor Data
- Set points
- Switch Data
- Fault Data: Breaker State Data
- Fault Data: Feeder Data
- Configuration Data: Line Parameters (e.g. impedances)
- Dynamic Network Topology Data
- Flow Model
- Load Forecast Data
- Configuration Data

System Assets:

- Actuator (switcher)
- Sensors
- Intelligent Electronic Devices
- RTU: secondary substation
- RTU: primary substation
- HMI

- Short Circuit Indicators
- Feeder Protection
- SCADA front-end
- SCADA
- View on TSO Systems
- Maintenance front-end
- Element Manager
- Time synchronization
- Monitoring system

4 Security goals

This chapter presents the 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.

In Appendix A a combined mapping is given of the specific interests of the set of stakeholders for each of the identified information and most important system assets based on the analysis of the five SEGRID use cases.

4.1 Security goals for information assets

For the information assets the security goals have been defined per stakeholder.

4.1.1 Customer (Household)

In order to receive correct invoice for energy consumption and production in UC1 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 UC3 and UC4, the household customer has the following security goal:

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

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

4.1.2 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).

4.1.3 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 and monitoring data processed by the data hub.

4.1.4 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 measurement data (i.e. Measurement Data, Sensor Data, kWh Data) and monitoring data (e.g. Current Status Data) during transfer and storage.

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

DSO_SG03 ensure *data integrity* and *authenticity* of control messages send from the DSO to the DER (e.g. Set Point) and to households (e.g. Change Consumption/Generation Command) to change production or consumption.

In order to correctly perform market facilitation in accordance with the SLA with the data hub and applicable legal requirements and regulations (o.a. UC1, UC3) the DSO has the following security goals[2]:

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.

DSO_SG08 ensure *data integrity* and *authenticity* of monitoring data during transfer and storage.

For the local load balancing renewable energy (UC4) & local automatic reconfiguration of the power grid (UC5), it is important that the topology model (i.e. Dynamic Network Topology Data) is correct at substation level. To this end, the DSO has the following security goal:

DSO_SG09 ensure *data integrity* and *authenticity* of monitoring data (e.g. Fault data, Sensor data) and network topology data (e.g. Dynamic Network Topology Data) during transfer and storage.

[2] Since DSO_SG04 from D1.3 has been removed the identifier is not used in this document.

In addition, the DSO has the following security goal for local automatic reconfiguration of the power grid (UC5):

DSO_SG10 ensure *data integrity* and *authenticity* of switching commands (i.e. Switch Data) from RTU to Actuator within substations.

In order to ensure correct functioning of elements (e.g. RTUs, IEDs, smart meters) and support remote element management the DSO has the following security goals:

DSO_SG11 ensure *data integrity* and *authenticity* of configuration data of elements (i.e. Configuration Data) during transfer and storage.

DSO_SG12 ensure *data integrity* and *authenticity* of software of elements during transfer and storage.

4.1.5 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.

4.1.6 CSO

In order to correctly charge EV, and support DSO with load balancing, the CSO has the following security goals:

CSO_SG01 ensure *data integrity* and *authenticity* of EV charging data (i.e. EV Charge Data, EV Charge Plan) during transfer and storage.

CSO_SG02 ensure *data integrity* and *authenticity* of control data (i.e. Set Point) from the DSO during transfer and storage.

4.2 Security goals for the system assets

When assessing the system assets for defining security goals, it was acknowledged that it was not such a straightforward process when compared to information assets. System assets are typically related to or owned by a particular stakeholder and are often used for multiple functions, many not described in the SEGRID use cases. This would thus extend the assessment beyond the scope of the SEGRID use cases. Moreover, it was identified that the best practice security controls should in general be applied to all system assets[3]. For system assets that are specifically relevant to ensure a stakeholders interests

[3] In D1.3 state of the art of best practices security and privacy protection controls and countermeasures for smart metering and Smart Grids have been given. For instance, IEC 62443-3-3 and IEC 62443-4-2 are particularly relevant in the context of system assets.

within a SEGRID use case or the smart energy grid in general, specific security goals can been defined. It was then decided that we would identify the system assets for which it made sense to specify specific security goals. In addition, we defined a security goal that is applicable for all system assets:

GE_SG01 Ensure that system asset specific *best practice security controls* are applied to each of the system assets.

GE_SG02 Ensure that *best practice security principles* are applied to each of the system assets and the system as a whole.

The system assets for which we have defined specific additional security goals are:

- Smart Meter
- Household concentrator
- SCADA
- RTU primary substation
- RTU secondary substation
- Communication network

In Appendix A a combined mapping can be found of the specific interests of the set of stakeholders for these system assets based on the analysis of the five SEGRID use cases.

4.2.1 Smart Meter

In order to ensure:

- correct measurement data such that the energy supplier can produce a correct invoice for energy consumption and/or production, and
- correct use (and prevent misuse) of the remote switching function,

the following security goals have been defined:

SM_SG01 Ensure *system integrity* of the smart meters.

SM_SG02 Ensure *controlled access* to information assets (i.e. process data, configuration data and software) on the smart meters.

Since the smart meter is located at the customer's premises and is a potential target for tampering the following security has been defined

SM_SG03 Ensure *physical security (e.g. tamper detection, tamper response, tamper evident, tamper resistant)* of the smart meters.

Security life-cycle management

To ensure the security throughout the life-cycle of the smart meter the following security goals have been defined:

SM_SG04 Ensure secure *maintainability* of the security functions of the smart meters.

SM_SG05 Ensure secure *upgradability* of the security functions of the smart meter.

The manufacturer can pre-install security function data (e.g. cryptographic key material) on the Smart Meter to securely load the operational (security) function data. To support this process the following security goal has been defined:

SM_SG06 Ensure support for a *secure handover of trust anchors* (e.g. cryptographic keys) from the manufacturer to the owner/operator (e.g. DSO).

4.2.2 Household concentrator

In order to ensure that the customer's smart appliances are operated correctly and not misuse the following security goal has been defined:

HC_SG01 Ensure *controlled access* to information assets (i.e. process data, configuration data and software) on the household concentrator.

Security life-cycle management

To ensure the security throughout the life-cycle of the household concentrator the following security goals have been defined:

HC_SG02 Ensure secure *maintainability* of the security functions of the household concentrator.

HC_SG03 Ensure secure *upgradability* of the security functions of the household concentrator.

4.2.3 SCADA

As continuity, availability and reliability of the SCADA system are of high importance for the to (centrally) manage the energy grid (e.g. distribution of energy, power quality, and energy load balancing), the following security goals have been defined:

SC_SG01 Ensure *robustness* and *resilience* of the SCADA system.

SC_SG02 Ensure *system integrity* of the SCADA system.

SC_SG03 Ensure *controlled access* to information assets (i.e. process data, configuration data and software) on the SCADA system.

4.2.4 RTU (primary substation & secondary substation)

The RTUs in the primary and secondary substations are of high importance for the DSO to (regionally) manage the energy grid (e.g. distribution of energy, power quality, energy load balancing, and outage management), the following security goals have been defined:

RT_SG01 Ensure *system integrity* of the RTUs.

RT_SG02 Ensure *controlled access* to information assets (i.e. process data, configuration data and software) on the RTUs.

RT_SG03 Ensure *robustness* and *resilience* of the RTUs.

RT_SG04 Ensure *physical security (e.g. physical access, tamper detection)* of the RTUs.

Security life-cycle management

To ensure the security throughout the life-cycle of the RTUs the following security goals have been defined:

RT_SG05 Ensure secure *maintainability* of the security functions of the RTUs.

RT_SG06 Ensure secure *upgradability* of the security functions of the RTUs.

4.2.5 Communication network

The availability of a communication network is in many of the SEGRID use cases important to ensure the stakeholder's interests. Therefore we have defined the following specific security goal:

CN_SG01 Ensure *robustness* and *resilience* of the Smart Grid communication network.

5 Privacy goals

This chapter presents the 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.

In addition to the use case specific privacy goals, we would like to point the reader to the list of privacy and data protection targets in the annex of the DPIA Template for Smart Grid and Smart Metering Systems [21] as they present good comprehensive generic set of the privacy goals for Smart Grid developments. These targets are[4]:

- Safeguarding quality of personal data
- Legitimacy of processing sensitive personal data
- Compliance with the data subject's right to be informed
- Compliance with the data subject's right of access to data, correct and erase data
- Compliance with the data subject's right to object
- Safeguarding confidentiality and security of processing
- Compliance with notification requirements
- Compliance with contractual requirements between data controller and data processor
- Compliance with data retention requirements
- Privacy by design
- Privacy by default

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.

[4] The authors have been informed that DPIA template will be updated based comments received during the test phase. The updated list of privacy targets has been included. See for more information: https://ec.europa.eu/energy/en/test-phase-data-protection-impact-assessment-dpia-template-smart-grid-and-smart-metering-systems

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 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 type of 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, CSO	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, CSO	DSO, CSO	DSO,CSO
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.

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 Glossary

This glossary serves as inventory of abbreviations used in the document.
This is a standard glossary, used for all technical SEGRID deliverables

Acronym	Description
ABAC	Attribute-Based Access Control
AMI	Advanced Metering Infrastructure
API	Application programming interface
APT	Advance Persistent Threat
ASLR	Address Space Layout Randomization
BLP	Bell-LaPadula
BYOD	Bring Your Own Device
CAPEC	Common Attack Pattern Enumeration and Classification
CC	Common Criteria
CDF	Cumulative Distribution Function
CEN	European Committee for Standardization.
CENELEC	European Committee for Electrotechnical Standardization.
CERT	Computer Emergency Response Team
CIS	Customer information system
CPS	Cyber-Physical System
CSO	Charge Spot Operator.
CVE	Common Vulnerabilities and Exposures
DAC	Discretionary Access Control
DAN	Distribution automation node
DC	Data Concentrator.
DEP	Data Execution Prevention
DER	Distributed Energy Resources
DMS	Distribution management system
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
DoW	Description of Work
DPIA	Data Protection Impact Assessment
DRAACS	Demand-response analysis and control system
DSO	Distribution System Operator.
Dx.y	Deliverable x.y
EA	Enterprise Architecture
EAM	Enterprise asset repository
EC	European Commission
EDSA	Embedded Device Security Assurance
EMS	Energy management system
EMSP	E-Mobility Service Provider.
ERP	Enterprise resource planning
ETSI	European Telecommunications Standards Institute.
EU	European Union
EV	Electric Vehicle.
FE	Front end
FHS	Filesystem Hierarchy Standard
FS	Forecasting system

FTP	File transfer protocol
G3	Alliance for PLC technology.
GIS	Geographical Information System.
GDPR	General Data Protection Regulation
GMS	Generation management system
GOOSE	Generic Object Oriented Substation Event
GPRS	General Packet Radio Service.
GPS	Global Positioning System
GSSE	Generic Substation State Events
GUI	Graphical User Interface.
HAN	Home area network
HE	Head End
HES	Head-End System.
HMI	Human Machine Interface.
HTTPS	Hypertext transfer protocol secure
HV	High Voltage.
ICC	Inter Control Center
ICCP	Inter Control center Communications Protocol
ICS	Industrial Control System
ICS-CERT	Industrial control systems computer emergency response team
ICT	Information and Communication Technology
IDS	Intrusion detection system
IEC	International Electro technical Commission (ISO)
IED	Intelligent Field Device
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol (IPvx = IP version x)
IPS	Intrusion prevention system
IPSec	IP Security
ISO	International Organization for Standardization.
IT	Information Technology
LAN	Local area network
LCA	Latent Credibility Analysis
LDAP	Lightweight Directory Access Protocol
LN	Local Network.
LV	Low Voltage.
MAC (1)	Media Access Control
MAC (2)	Mandatory Access Control
MDMS	Meter Data Management System.
MMS	Meter management system
MOF	Meta object facility
MU	Merging unit
micro-CHP	Micro combined heat and power.
MV	Medium (level) Voltage.
NAN	Neighborhood area network
NMS	Network management system
NN	Neighbouring Network.
NTP	Network Time Protocol
NVD	National Vulnerability Database
OMS	Outage Management System
OS	Operating System
OSCP	Open Smart Charging Protocol

OSGP	Open Smart Grid Protocol
OSI	Open Systems Interconnection
OT	Operational technology
OTP	One-Time Password
PCT	Programmable communicating thermostat
PHP	PHP: Hypertext Preprocessor (a recursive acronym
PLC	Power Line Communication.
PQ	Power Quality
PV	Photovoltaic
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RF	Radio frequency
RFC	Request for Comments
RTU	Remote Terminal Unit.
SAL	Security Assurance Level
SCADA	Supervisory Control and Data Acquisition.
SCS	Substation control system
SDLA	Security Development Lifecycle Assurance
SE	Secure Element.
SEGRID	*S*ecurity for smart *E*lectricity *GRID*s.
SFTP	SSH File Transfer Protocol
SGAM	Smart Grid Architecture Model.
SG-CG	Smart Grids Coordination Group (ETSI).
SMITP	Smart metering Information and Telecommunication Protocol.
SNTP	Simple Network Time Protocol
SSH	Secure Shell
SUC	System under Consideration, or Subject under Consideration
TCP/IP	Transmission Control Protocol / Internet Protocol
TEE	Trusted Execution Environment
TEPT	Trained Execution Path Tree
TOE	Target Of Evaluation
TSO	Transmission System Operator.
TTC	Time To Compromise
Tx.y	Task w.y
UC	Use Case
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VLAN	Virtual LAN
VPN	Virtual private network
WAMS	Wide Area Monitoring System
WAN	Wide area network
WAP	Wireless Application Protocol
WMS	Workforce management system
WPx.y	Work Package x.y
XACML	Extensible Access Control Markup Language
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformations
3G / 4 G	Third/ Forth generation mobile communication.

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 (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, , 27 April 2016, Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[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"; version 1.2; October 2016.

[12] IEEE Std 610.12-1990 IEEE Standard Glossary of Software Engineering Terminology Approved September 28, 1990 (Reaffirmed September 2002)

[13] ISA/IEC 62443-4-2, Industrial communication networks - Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components; draft text; Ed. 1; 2015-07-22

[14] SEGRID Deliverable D4.1; "Preliminary Security and Privacy Architecture"; October 2015.

[15] NIST Special Publication 800-27 Rev A; Engineering Principles for Information Technology Security (A Baseline for Achieving Security); Revision A; June 2004

[16] Committee on National Security Systems Instruction (CNSSI) No. 4009, Committee on National Security Systems (CNSS) Glossary, April 2015. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[17] R. Shirey, Internet Security Glossary, Version 2, IETF RFC 4949, August 2007

[18] RON ROSS, et. al.; NIST Special Publication 800-160; Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems; May 2016; Second Public Draft

[19] ISA/IEC 62443-4-1, Industrial communication networks – Network and system security –Part 4-1: Product development requirements; Draft 1, Edit 9, April 2013

[20] ISO/IEC 15408, Information technology — Security techniques — Evaluation criteria for IT security; Part 1 – 3; 3rd edition, 2009.

[21] DPIA Template for Smart Grid and Smart Metering Systems; Smart Grid Task Force 2012-14; Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment; 18.03.2014

[22] SEGRID Deliverable D2.1; "Threat vulnerability and risk assessment applied to SEGRID use cases"; 05/10/2015.

Appendix A – Mapping between stakeholder interests and assets

	Stakeholder	Customer					DER Customer		energy supplier			DSO						DSO-AMI		Data Hub		CSO
	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	Charging of EV
Information assets	Measurement data	•	•	•		•			•	•				•	•		•		•		
	Sensor Data									•			•	•	•	•			•		
	kWh Data						•	•		•			•	•			•		•		
	Current Status Data	•			•	•								•							
	Monitoring data												•	•	•			•			
	Switch data	•	•		•	•				•	•			•	•	•		•	•	•	
	EV Charge Data	•				•								•							•
	EV Charge Plan	•												•							•
	Change C/G command	•			•					•				•					•		
	Set Points	•					•			•			•	•		•	•		•		•
	Configuration data												•		•		•				
	Consumption Priorities	•			•	•								•							
	Load Forecast Data												•	•	•	•					
	Dynamic Network To-pology Data														•	•					
	Fault Data														•						
	Outage Data														•						
System Assets	Smart Meter	•	•	•	•	•			•	•	•			•	•		•	•			
	Household Concentrator	•			•	•								•							
	SCADA	•	•									•	•	•	•	•					•
	RTU primary substation	•										•	•	•	•	•					
	RTU secondary substation	•			•		•					•	•	•	•	•					
	Communication network	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	

Classification level: Public