USEF: THE PRIVACY AND SECURITY GUIDELINE

A solid foundation for smart energy futures

Intellectual Property Disclaimer

Revision History

Revision	Comments	Issue date
2015	Initial public release	2 Nov 2015

USEF: PRIVACY
AND SECURITY GUIDELINE

RELEASE DATE:
2 NOVEMBER 2015
ISBN:
978-90-824625-2-4

The Universal Smart Energy Framework

The Universal Smart Energy Framework (USEF) provides non-discriminatory access to smart energy systems at acceptable cost-to-connect and cost-to-serve levels.
By providing an open and consistent framework of specifications, designs, and implementation guidelines, USEF enables participants to seamlessly co-create a fully functional smart energy system.
The USEF Foundation acts as the framework’s steward and aspires to establish it as the de facto framework for smart energy products, services, and solutions. In 2020 the foundation wants to be part of 25% of all smart energy systems in at least 5 different markets throughout Europe—and, hopefully, beyond.

To accelerate the development of commercially viable offerings based on the framework, the USEF Foundation has developed a reference implementation. The reference implementation enables stakeholders to develop smart energy products, services, and solutions in an unambiguous, well-defined way. These offerings will in turn enable the large-scale international deployment of smart energy systems.

In the coming years, USEF will be validated in a number of large-scale international demonstration projects, which will support the commoditization of smart energy products, services, and solutions. Currently, USEF is being deployed in the demonstration project “Energiekoplopers” in The Netherlands, in which the potential flexibility of 200 households is activated and aggregated and in Hoog Dalem, where batteries are used to reduce grid peak loads, caused by heat pumps and PV.

Table of Content

1 Privacy & security

Smart energy systems—like most complex information systems - deal with sensitive data and require security and privacy preservation measures. Privacy & security have system-wide implications. Therefore, the protection of individual subsystems/components is not sufficient; the entire system is as strong as its weakest link.

1.1. Scope

USEF follows the principle of privacy & security **by design.**
The privacy & security guideline forms the basis of the design. The design takes the current legal and social views on privacy & security into account and links these to the future directions which
they will likely evolve. Trade-offs between privacy & security and market and energy efficiency opportunities are also discussed.

The guideline is not a purely technical, or technology-driven, document. Rather, it is a policy document with philosophical aspects that presents a balanced view of the increasingly important topic of privacy & security. The security principles listed in this document need to be adhered to when implementing and operating the framework to ensure full USEF compliancy.

1.2. Introduction

Privacy & security issues go beyond the technical realm; they also imply changes in procedures, processes, policies and more. Protection of privacy & security is an ongoing task: privacy measures will need to evolve over time in order to deal with changing societal trends, whereas security measures will need to evolve over time in order to mitigate increasingly sophisticated hacking techniques.

USEF identifies nine “windows” regarding privacy & security. The windows are a result of a brainstorming session held with subject matter experts. The goal of the session was to develop two separate sets of windows that would cover all relevant privacy & security aspects of smart energy systems. After the session the two independent sets were combined into one final set, thereby combining the best outcomes of two separate thought processes. The nine windows presented in Table 1.1 intend to provide a complete view on the privacy & security aspects associated with smart energy systems.

In lieu to the input of subject matter experts, we have outsourced scientific research regarding legal and psychological developments in privacy & security to leading Dutch universities. Specifically, three assignments were given:

- Gustav Bösehans, student at the psychology faculty of the Rijksuniversiteit Groningen has performed a literature review [1], under the supervision of Dr. Jan Willem Bolderdijk, on the factors leading to consumers experiencing privacy issues in systems where large scale data collection, storage and analysis takes place.
- Anya Castillo, PhD student at Johns Hopkins University, Baltimore**,** has written a white paper [2] on trade-offs in privacy and value creation, under the supervision of Dr. Marcel Volkerts, which forms the basis for Section 3 of this guideline, together with the work of Gustav Bösehans.
- Prof. mr. dr. Mireille Hildebrandt of the law faculty of the Radboud Universiteit Nijmegen has written a brief, well-thought out reflection on the legal requirements for a level playing field on which all stakeholders may pursue maximum value creation using smart energy services in a smart grid environment [3]. Her findings served as input for some of the principles in this document.

The results of the aforementioned research are included in the privacy & security guideline.

The nine windows regarding privacy & security are further explored and elaborated upon in this document. Section provides a brief discussion, illustrated with some examples on where, within the scope of USEF, privacy & security issues typically occur. Section 2.1 presents the used definitions of data, information and knowledge, which will be used throughout the remainder of the document as well as a description of roles we distinguish when discussing privacy & security topics in smart energy systems. In addition, the template used for the principles is introduced.

Sections 3 through 11 present USEF’s opinions on privacy & security in smart energy systems from various viewpoints, stated in the form of design principles. Section 12 summarizes the analyses and principles of the preceding sections, resulting in a set of topics that form the heart of the guideline.

1	Privacy-value creation trade-offs	Individuals and business can both benefit from sharing certain privacy sensitive data. It might allow for tailor made propositions to the end-user or more efficient management of the energy system. How do we accommodate all legitimate interests and objectives?
2	Data management	Data management includes, among others, the collection, storing, processing and mining of data. What data are collected and for which purpose? How long are the data retained and why? When should it be possible to trace data back to its origin? Who owns what data?
3	Data communication	Smart energy systems will generate a lot of data that needs to be transported over an infrastructure to the point(s) where they are used. What is the desired security level for different types of data communication?
4	Confidentiality	Confidentiality refers to limiting information access and disclosure to authorized resources and preventing access by or disclosure to unauthorized resources. The consequences of a breach are different for the different stakeholders (loss of privacy for a Prosumer, loss of goodwill, competitive disadvantage for a retailer). What are necessary and acceptable levels of confidentiality for the different parts of the system?
5	Integrity	Integrity means that data cannot be modified undetectably. Where in the smart energy system is integrity more important than availability, or more important than confidentiality?
6	Availability	Availability refers to the availability of information resources including systems, processes and data elements. What are necessary and acceptable levels of availability for the different components of a smart energy system?
7	Disaster Recovery	No (security) system is perfect. What needs to be done in the case of unforeseen situations? How to mitigate the fall-out from a security/privacy breach? How are responsibilities divided between parties?
8	Identification, Authentication, Authorization	Identification is the process of showing who you are. The identification is validated through the process of authentication, which verifies that you are who you say you are. Authorization is the process of verifying that “you are permitted to do what you are trying to do.”
9	**Risk assessment**	Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat.

Table 1.1: Windows on privacy & security in smart energy systems.

1.3. Examples of privacy & security issues

Most people have a certain understanding of the concepts ‘privacy’ and ‘security’. It is however less obvious what the consequences are of privacy & security in smart grids. In order to get a better understanding, in this section, examples of privacy & security issues related to SCADA/smart energy systems are provided. Each of these examples starts with a short description of the issue, followed by what causes the issue and which countermeasures could have been taken—including references to the sections in the remainder of this document.

1.3.1 Remotely control a Jeep Cherokee

In July 2015 two hackers, Charlie Miller and Chris Valasek, remotely took over a Jeep Cherokee that was driven by Andy Greenberg, a journalist of WIRED magazine [4]. The hack started with relatively innocent attacks, like turning on the vents at maximum speed and tuning in on a Hip Hop radio station at full blast. The next attack was already trickier—the windshield wipers were turned on and the glass was blurred with wiper fluid.
The next step in taking over the car was cutting off the transmission. During the attack, Greenberg was not able to interfere with the hacks by Miller and Valasek.

In modern cars all components—both for the actual driving of the car and for the driver’s comfort sake—are connected to each other via the so-called CAN bus for an optimal driving experience. In addition, cars are more and more connected to the outer world—for maintenance and emergency purposes as well as for communication means for the occupants. The combination of the two however introduced an unwanted and potentially very dangerous vulnerability, giving the hackers the possibility to take over almost every aspect of the car, including the breaks and transmission system[1].
The reason for this vulnerability probably lays in the independent development of the communication in the car itself and the communication of the car with the outer world, without taking into account that one of the components, the car audio system, is actually connected to both. To avoid vulnerabilities like this, complex systems like cars and our future energy system need to be designed from the ground up using a holistic approach.

1.3.2 From serious gaming to naming and shaming?

In order to make Prosumers aware of their energy consumption, and to try to make them reduce this consumption, serious gaming can be used. In , an example of such a serious game in Gainesville Florida [5] is provided. On a map the energy consumption of all households are depicted, in order to compare it with the neighborhood. This data can be used to stimulate people to use less energy, but there is a risk that it will be used to name and shame the people who use more than the average amount of energy. In other words, by providing the information in the way provided above, a privacy issue has popped up.

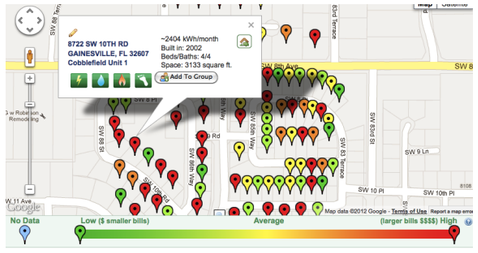


Figure 1-1: Screen shot taken from http://gainesville-green.com/.

It is possible to provide almost the same information to the participants of the game without them giving up privacy, by showing only own information to each participant, in comparison with the average consumption of comparable households. Possibly, social media like Facebook can be used to give insight in the consumption of friends as well, in case explicit permission is given.
Privacy and value creation might conflict with each other; therefore a trade-off must be made (see Section 1.5). In addition, the confidentiality of all data involved must be assessed (see Section 1.8).

[1] Shortly after the publication of the hack, Fiat Chrysler Automobiles announced a patch for the cars vulnerable for the hack.

1.3.3 To trust or not to trust?

The introduction of the smart meter in The Netherlands has been far from smooth. In the original concept, privacy was not taken into account. This was no issue in countries like Italy, where the legacy meters are mostly the outside the homes, but for the Dutch the smart meter was considered to be a privacy breach - a smart meter could be used to see the whereabouts of people based on energy consumption. Additionally, the fact that a smart meter has the possibility to switch off a household remotely made the meter a suspicious matter. As a result, people no longer trusted the smart meter and a strong lobby against the smart meter grew.
New requirements were stated for the smart meter rollout, including technical improvements like encryption and the possibility for people to refuse a smart meter, in order to regain trust.

If privacy was taken into account right from the beginning, less resistance against the smart meter was to be expected. Most people have a healthy resistance against newly introduced technologies, especially when they do not see what is in it for them. Therefore it is important to take into account the—right or wrong—objections against the new technologies. Privacy is one of the subjects that could have been foreseen as a reason for objection—by neglecting it, trust has been jeopardized and provided the opponents to smart meters with ammunition to prevent the introduction of the smart meter.

By taking (technological and procedural) measures to protect the privacy of the Prosumers (privacy/security by design), giving the Prosumers control by requiring an explicit opt-in by the Prosumer for energy companies to use the smart meter readings on a quarterly basis and provide the customer with incentives (Euros, a feeling of being green instead of being greedy) losing trust can be avoided. Trust is the guiding principle for this document; privacy value creation trade-offs are discussed in more detail in Section 1.5.

2 Definitions and concepts

Privacy & security discussions often evolve around protecting data and information from being used inappropriately. But what exactly is information? How does it differ from data? What are the roles we distinguish when discussing privacy & security topics in smart energy systems? This section provides the definitions and concepts used in discussing privacy & security principles and presents a template for formalizing them.

2.1. Data, information & knowledge

It is important to have a clear understanding of the concepts of raw data, information and knowledge, when we reason about security and privacy risks and when discussing potential security architectures. In the remainder of this document, we will use the following definitions, based on the definitions from the European Guide to good Practice in Knowledge Management [6]:

- **Raw Data:** discrete, objective facts (numbers, symbols, figures) without context and interpretation. If they have been subjected to processing steps, then these steps are known and reversible.
- **Information:** data products that arise from using domain knowledge to interpret raw data and/or combining raw data elements. It adds value to the understanding of a subject and in context it is the basis for knowledge.
- **Knowledge:** The combination of data and information, to which is added expert opinion, skills and experience, to result in a valuable (set of) data asset(s) which can be used to aid decision making. Knowledge may be explicit and/or implicit, individual and/or collective.

The following examples may help in understanding these definitions.

2.1.1 Raw data example:

Sensor reading that has been converted from Fahrenheit to Celsius. No information was added, characteristics unchanged, the data remains as is.

2.1.2 Information example

An energy profile that has been created from multiple individual energy readings is an example of information. Note that also the absence of (e.g.) energy readings is information.

2.1.3 Knowledge example

Water consumption spikes at 6:45 PM on June 9 2016. We know it is half time in the Netherlands-Denmark soccer game so we understand, and probably have predicted, the spike. Nothing out of the ordinary is going on here. The same spike at 4 AM on June 10 2016 would on the other hand raise alarms: given our knowledge of the current operating conditions of the water net this is highly suspect. Something is wrong, we need to take action!

2.2. Privacy & Security Roles

Several roles are recognized in the EU concerning privacy. In this section, these roles are described, based on the definitions provided in the Data Protection Directive 95/46/EC [7][2].

- **Data Subject:** the individual whom particular personal data is about. An individual who has died or who cannot be identified or distinguished from others is not counted as a Data Subject.
- **Data Controller**: the natural or legal person (which includes organizations) which - alone or jointly with others - determines the purposes for which and the manner in which any (personal) data are, or are to be, processed. A Data Controller remains responsible for compliance with the General Data Protection Regulation (GDPR) [8], even though he has engaged a data Processor.
- **Data Processor**[3]: any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller. Data Processors are not directly subject to the Regulation; however, most Data Processors will be Data Controllers themselves for other types of data (i.e. HR information of its employees).

[2] The Directive will be replaced by the General Data Protection Regulation (GDPR) [8], which is a proposal at the time of writing. The expected agreement on the GDPR is expected end 2015 with early adoption starting in 2016 and enforcement in 2017. In this proposal references are made to the definitions in the Directive.

[3] Note that although data processing can to large extent automated ultimately a human being will be responsible for such automated processing steps.

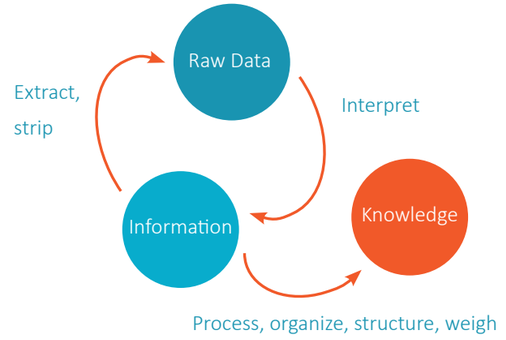


Figure 2-1: Definitions of raw data, information and knowledge.

- **Data Collector:** specialization of Data Processor, collecting data on behalf of a Data Controller. Although not mentioned in the Data Protection Directive, for readability purposes this role is used in some of the principles of this document (instead of using terms like 'Data Processor to whom collecting data is assigned').

Depending on the use case under consideration, the smart energy system actors can fulfill different privacy & security roles. Examples of Data Controllers and Data Processors [9] are given below.

Data Controller example

A government department sets up a database of information about every child in the country. It does this in partnership with local councils. Each council provides personal data about children in its area, and is responsible for the accuracy of the data it provides. It may also access personal data provided by other councils (and must comply with the data protection principles when using that data). The government department and the councils are Data Controllers in common in relation to the personal data on the database.

Data Processor example

A utilities company engages a company that operates call centers to provide many of its customer services functions on its behalf. The call center staff has access to the utilities company's customer records for the purpose of providing those services but may only use the information they contain for specific purposes and in accordance with strict contractual arrangements. The utilities company remains the Data Controller. The company that operates the call center is a Data Processor

2.3. Security principles

In chapters 4-11 the security principles are provided according to a fixed pattern. In the table below, this pattern is described in order to better understand the way the principles are formulated.

Principle	**Each principle starts with a self-explaining name about the principle. It is provided as a short sentence stated in the imperative. Example: 'principles are stated in the imperative'.** **ID#**
Description	In the description, an explanation of the principle is provided. It is limited to the 'what' of the principle, describing what is exactly meant, without giving the reasons. Example: 'a principle is a sentence in the imperative explaining what the principle is about. It contains at least a subject and a predicate; verbs like 'should' are prohibited.'
Rationale	The rationale is the why of the principle. It states why it is important to follow the principle, and what the relevance is of the principle (especially in a smart grid). Example: 'using the imperative indicates that using a principle is not a free choice, but a directive that must be complied with.'
Consequences	Following a principle may have consequences, either positive or negative. This section the possibility to state consequences that are foreseen. Example: 'by explicitly prescribing the format of a principle, commonly used principles might be rephrased (e.g. 'need to know' is reformulated as 'data is processed on a need to know basis').

3 Privacy-value creation trade-offs

Individuals and business can both benefit from sharing certain privacy sensitive data. It might allow for tailor made propositions to the end-user or more efficient management of the energy system. How do we accommodate all legitimate interests and objectives?

3.1 Introduction

The future integration of smart grid technologies is dependent upon two-way communication to facilitate more efficient market and network management. Whereas data and analytics have been the norm in communications-based industries such as mobile apps and online marketing, the access to unlimited data, the potential for crowd sourcing, and the opportunity for analytical services and machine learning with smart grid technologies have the potential to revolutionize the energy value chain.
This trend has already occurred in other traditional business services; for example in the insurance industry: predictive modeling using gigabytes of data has improved policy pricing and coverage options. The data and analytics performed in smart energy systems can result in benefits for individual actors in the system, such as DSOs, Aggregators, Energy Service Companies, Prosumers, third party companies, and society as a whole.

There is a potential downside to this: sharing data on energy production and consumption might result in a (perceived) privacy risk that in turn can hamper the adoption of these new technologies, resulting in higher costs for many stakeholders.
To illustrate this, consider these two examples:

- Exchanging energy production and consumption data enables Aggregators and DSOs to better forecast the inflexible and flexible load on the system, and therefore improve the aggregated flexible load scheduling across all households.
- In a configuration where households with distributed generation are collectively operated as a virtual power plant (VPP),production and consumption data must be exchanged within the VPP in order to reduce its internal peak load.
- Both instances of privacy data sharing suggest that a lack of data disclosure would result in inferior operations and management of the energy system. Customers must be willing to sacrifice some degree of privacy in exchange for benefits to their individual household energy consumption and overall utility costs.

3.2 The value of smart energy services

Many stakeholders can benefit from data sharing and advanced analytics in smart energy systems. The value benefits to DSOs include proactive network maintenance, reduction of adverse events, improved operational efficiency, reduced labor costs, and better asset management.

Prosumers realize efficiency and monetary savings, and depending on the sophistication of smart grid integration, other benefits such as integrated home management and automated and remote energy control.

Partnerships and third party companies like ESCOs realize market expansion in providing (smart energy) services where the (smart energy) service provider is a separate entity from the Supplier and Aggregator, or in utilizing the information shared through smart energy systems for alternative purposes, such as marketing.

Furthermore, social welfare also increases through aggregated savings and the selection of environmentally conscious options.

3.3 The what, why and how of privacy

Before discussing the market for privacy and how to address privacy issues from a legal perspective let us briefly discuss first what we mean by privacy, why privacy is important, when privacy issues arise and how they can be avoided/mitigated.

Why we need privacy

In a broad sense, privacy reflects people's desire to protect themselves by temporarily limiting access to themselves by others [10] and in so doing, reducing vulnerability and increasing decisional and behavioral autonomy. According to Westin, privacy can be achieved in four ways - solitude, intimacy, anonymity and reserve - which he called the "hows" of privacy.

Privacy is crucial to normal psychological functioning and the right to privacy is defined in the United Nations Universal Declaration of Human Rights, Article 12 [11]. Privacy provides room for personal development and autonomy. There simply are times when we want and need to be alone such as when coping with loss, shock or sorrow. Similarly, people may desire privacy in order to take a time-out from the hassle of daily life, to release emotions such as anger or sadness, or just being oneself in exclusion of others. This also reflects on Westin's early perspective on privacy. He suggested that privacy serves the distinct and at times co-occurring purposes of personal autonomy, emotional release, self-evaluation or limited and protected communication, the so-called "whys" of privacy. The first and last purposes map most closely to privacy aspects encountered in smart energy systems.

Invasion of privacy

Generally speaking, perceptions of privacy invasion will be high when people lack control over the disclosure of personal information. People want to maintain control over when and how much or what kind of information is transmitted to others. Also, it has become clear that technological modifications/ mitigations alone cannot reduce privacy concerns effectively. Such modifications may be necessary, yet will not be sufficient unless personal boundaries are considered carefully.

An important factor in people's perception of whether their privacy has been invaded or not, is knowledge or "notice". If people are uncertain or poorly informed about how their personal information is collected, used, and with whom it is shared, people may react by engaging in privacy self-defense (e.g. by withholding or giving false personal information).

Mitigating privacy risks

In general, people will most likely share personal information (and privacy concerns will be lowest) when the perceived benefits (e.g. higher quality service, personalized offers or discounts) of doing so exceed the perceived risks. Trust may thus be understood as the willingness on the part of the Prosumer to disclose personal information to an interaction partner [12]. Trust, once established, also reduces privacy concerns in the long run, thereby increasing the likelihood that the Prosumer will remain with the same organization/interaction partner [13].

A high-perceived risk of disclosing personal information will raise privacy concerns, but is not necessarily related to actual disclosure behavior. In contrast, when Prosumers perceive the interaction partner as trustworthy, privacy concerns will be low and so will be the boundary for sharing personal information.

It is important to realize that privacy is not a "one size fits all" topic. Apart from cultural differences there are also individual differences with respect to privacy concerns. Tanner, Medin and Iliev [14] suggested two orientations that people may hold. On the one hand, people holding a ***deontologist*** perspective are concerned with acting in line with some moral standard. On the other hand, people holding a ***consequentialist*** perspective strive to maximize personal benefits and act according to expected outcomes. One can easily imagine how these orientations might affect privacy concerns.

3.4 The price of privacy

The perceived values of smart energy systems benefits affect the customer's willingness to participate. Although customers sharing their privacy data can enable companies to increase the expected utility of these customers, there is nevertheless a perceived privacy risk that necessitates some level of trust between the transacting parties [15] [16].

Conceivably, low perceptions of risk and high levels of trust induce higher privacy data disclosure between customers and companies although customers with high expected benefits from smart energy services over their current baseline are more willing to share privacy data regardless. Therefore the success of smart energy services somewhat rests in the overall impact such services may have on the customer's baseline and the relationship amongst stakeholders.

Similar to other ecommerce transactions, transactions in smart energy systems between two parties can be increasingly characterized as an exchange of energy and other smart energy services for money and personal information. However, such transactions are more appealing to one party when that party has more or better information than the other. Information asymmetry can increase uncertainties and have implications for the terms of the transaction and the relationship amongst stakeholders. Service providers attempt to signal their reputation and trustworthiness to customers through pricing mechanisms, guarantees, fair information practices and advertising to "resolve" this asymmetry [17]. Thus, regardless of privacy rights being legislatively granted or not, energy service providers and affiliated partners may choose to invest in high-fidelity IT infrastructures in order to procure more customer participation in smart energy systems.

Consequently, there is an incentive to price the cost of implementation. Given that smart energy systems may induce considerable investments from households (of either consumer or Prosumer nature), energy suppliers, communication facilitators, and yet other third-party entities, the aspect of which parties have the rights to payment is highly problematic. Without stringent standardizations in place, there is a plethora of strategies in managing smart energy systems and also in how households participate in the energy market. These different levels of participation require different levels of privacy data sharing and may offer different benefits. Here it should be noted that customers, who do not participate in a smart energy system due to their inability or unwillingness to pay, will still experience increased grid reliability since there is no way to exclude these

non-paying parties[4]. The high fixed costs associated with high-fidelity IT infrastructures, in addition to the costs of the actual smart energy systems, result in a higher likelihood for the market to participate in price discrimination.

In pricing privacy implicitly through smart energy services, companies ostensibly may decide from the following programs:

- To charge each customer their willingness-to-pay;
- To use a taxonomy of subscription options to enable customers to self-select;
- To charge each customer based on a proprietary valuation [18].

Matching the household's willingness and ability to pay is a price discrimination that could enhance market efficiency through maximizing both profits to producers and benefits to Prosumers but exhaustive customization would become increasingly inefficient for the service provider. Since the success of smart energy services critically depends on privacy data and large-scale participation service providers might see it fit to predispose the customer to believing that they are exercising their true preferences while competitively pricing the options for privacy data disclosure, thus make participation even more appealing.

Quintessentially, privacy is an intermediate goal that cannot be treated purely as consumption good, and therefore is difficult to price explicitly and separate from smart energy services. The pricing behavior of companies offering smart energy services often reflects the allocative efficiency gained from the privacy data sharing. A service provider that also provides smart energy services may utilize aggregated privacy data across households to better characterize grid operations for both short- and long-term planning strategies. Knowledge pertaining to the flexibility of loads, distributed generation and voltage profiles of localized areas, for instance, improves forecasting and power quality monitoring as well as defers investments and decreases uncertainty in the company's asset management strategies. In the interest of exclusively facilitating smart grid services, companies may have increased needs for customers to share their privacy data so that the companies can competitively improve their service offerings. Furthermore, companies or even customers themselves may choose to monetize from privacy data sharing by capturing the value created to third-party entities through market transactions. For those stakeholders investing in smart energy systems, a misallocation of resources will persist if there is not a critical mass of participation in smart energy services. A critical mass in smart energy systems results in aggregated privacy data disclosure that creates allocative efficiencies to the company offering the services.

4 Also known as the "Free-rider" problem.

3.5 Legal frameworks

An alternative or complement to a market-based approach in valuing privacy is a government procurement approach. Such an approach is typically founded on the premise that the right to privacy is legally established and therefore as a legal right, the act of maintaining privacy should not be explicitly priced [18]. Where privacy is considered a legal right, government approaches would centrally control legitimate uses of privacy data. However, unsuitable government constraints on the integrity and security of privacy data may result in high transaction costs to the market. Difficulties in defining government intervention arise due to controversy over the "legitimate uses" criteria, the realized benefits and costs of privacy data exchange, and whether the government mechanisms are sufficiently effective.

It is arguable that government intervention focuses either on mechanisms to remove barriers to private contractual agreements, or on institutional reforms to reduce transactions costs. Debatably, rent-seeking behavior in the legislative process may increase transactions costs, which also contributes to deadweight loss in the market. For example, companies with pre-existing investments in smart grid technologies may attempt to capture wealth by manipulating any policy-driven standardization on the IT infrastructure. In such events, nontrivial externalities persist in government intervention approaches because in reality the government prevents the market from working [19].
Objectively judging personal information as private leads to difficult policy choices. Therefore, government intervention needs to be conditioned on the privacy values of the governing society. Although it is probably safe to assume that, at least in the Western world, privacy serves the same distinct functions for people of various cultural backgrounds, it is important to note that perceptions concerning information privacy (such as on the internet or in mobile commerce) are often shaped by the national, socio-economic environment[5].

In the European Union (EU), processing of personal data is covered by the Data Protection Directive [20] which will be replaced in the near future by the recently unveiled draft European General Data Protection Regulation (GDPR) [8]. Privacy is a highly developed area of law in Europe. All member states of the EU have signed the European Convention on Human Rights [21] which provides a right to respect for one's "private and family life, his home and his correspondence" subject to certain restrictions.

The guiding principle for the privacy in the EU is that personal data should not be processed at all, except when certain conditions are met.

5 Despite cultural similarities, the US and the EU have recently taken different approaches to information privacy with the EU taking a fundamental rights approach.

These conditions fall into three categories:

- Transparency: The Data Subject has the right to be informed when his personal data is being processed.
- Legitimate purpose: personal data can only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes.
- Proportionality: personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

As is the case with all EU directives, the Data Protection Directive has to be turned into law at the national level by the individual member states before they are legally binding for citizens. Member states have, and use, some latitude when implementing their own data protection legislation.

This lack of harmonization within the EU can lead to very tangible issues for initiatives like USEF. For example, the Dutch approach to smart meter data privacy would be illegal in Germany because it forces a choice between personal data privacy and energy efficiency and this opt-in approach has been outlawed in Germany.

The design of a smart energy system should therefore take care to craft solutions that can recognize and incorporate these national differences to keep the vision of a scalable, replicable solution alive.

Upon formal legislation, the GDPR will harmonize the current mélange of national data protection laws derived from the Directive.

The Regulation will sport better descriptions of the rights of data subjects and the obligations of Data Controllers and processors, e.g. to implement data security measures, to designate a data protection officer[6] and an obligation to provide notification of personal data breaches.
The Regulation has relaxed the "legitimate uses" limitation principle originally introduced in the Directive. The Regulation allows retention of data for "further processing" which is potentially compatible (or not) with the initial purpose for which the personal data has been collected [21]. Only in the event of further processing for incompatible purposes must the Data Subject be informed.
Although the Regulation introduces three new health-related definitions of sensitive data, data more specific to ecommerce, such as "behavioral data" in online shopping and smart grid services, is still not considered sensitive in nature.
The "special categories of" (sensitive) personal data article in the Regulation is unchanged from the Directive and still does not protect sensitive information extraction from common personal data [21].
Therefore exploitable and actionable information may be legally extracted from behavioral data that is exchanged as privacy data for smart grid services. Notably, the Regulation as currently drafted provides negligible explicit privacy protection to smart grid service customers.

6 A new role foreseen in [8] but not included in [7].

3.6 Recommendations

Successful smart grid integration requires a consistent and non-conflicting approach to privacy & security. The value creation from privacy data varies for participating stakeholders, where the economic and other indirect benefits to these stakeholders could be antagonistic in outcome. To gain more insight into the mechanism underpinning this fairly under-researched subject, thereby maximizing the chances of a positive outcome for parties designing and implementing smart energy systems, five broad recommendations are given.

3.6.1 Performing a Quantitative Analysis of Value Creation

The extent of privacy data exchange that is required for participating stakeholders to achieve the desired benefits from smart grid technologies is ambiguous. Furthermore, the value creation can be wildly different depending on the strategy employed to manage the smart grid technologies and for households to participate in the energy market. A quantitative analysis of the different deployment strategies will result in a more tangible assessment of the potential outcomes, allowing for better business case modeling and risk assessments.

3.6.2 Building a Sustainable IT Infrastructure

Given the fact that smart energy is a relatively new field, both technologically and regulatory, smart energy systems should provide flexibility in addressing privacy & security issues that may surface with the advent of new smart energy systems and/or regulations. In the process of procuring standardizations for smart energy systems, there must be minimal recourse to stakeholders with pre-existing investments in IT infrastructure protocols.
Any nepotism incurred this early on has the potential to hijack developments of a sustainable smart energy system by creating persistent barriers to entry for other companies to participate, and also by creating nontrivial externalities which will prevent the markets from working efficiently and effectively.

3.6.3 "Nudging" Privacy Preferences

Although contracting may reveal some semblance of the customer's true preference, there is substantial literature in behavioral decision and economic research that suggest customers are inconsistent in their choices. Therefore, there are ways to communicate with customers through smart grid interfaces in order to enhance and influence their choices in a

way that increases individual and societal welfare[7].
Through "nudging" privacy preferences, customers of smart energy services actively participate in their own privacy protection by choosing to employ different security strategies depending upon the context of the information being exchanged and the potential privacy concerns involved.

3.6.4 Anticipating Loopholes in the Regulation

The proposed EU GDPR [8] provides negligible privacy protection to Internet, social media, ecommerce, and smart energy service customers included. In light of further drafting and pending legislation, a challenge for smart energy systems is to adhere to this moving target. A conservative approach may fulfill the finalized Regulation without compromising designs for evolving smart energy systems that are to be commercialized in the upcoming decades.

3.6.5 Drafting Contractual Agreements

In situations where the nudging of privacy preferences fails, contractual agreements can be an alternative approach. In this situation, embedding privacy rights in the service level agreements for smart energy services is a mitigative measure worth exploring. This is especially true for territories outside of the EU to where privacy rights are treated differently and legal obligations between participating parties would be favorable for smart energy systems to explore.

[7] For example using labeling comparable to what is used for white goods and cars to indicate privacy risks of energy propositions.

4 Data management

Data management includes, among others, the collection, storing, processing and mining of data. What data are collected and for which purpose? How long are the data retained and why? When should it be possible to trace data back to its origin? Who owns what data?

4.1. Explanation of the subject

All digital systems manage data. As such, they implicitly or explicitly implement some rules. Data management in smart energy systems comprises the collection, storing, retention, processing and sharing of data and its derived products information and knowledge through aggregation, anonymization and the use of (predictive) profiling techniques.

4.2 Rationale of the subject

In smart energy systems, it is particularly important to know what data are managed, why they are used and how actors control the usage of data. Without clearly defining these conditions, end-user trust may not be established which would negatively impact the value creation in smart energy systems and hamper operational security. The advent of Big Data, analytics and machine learning and the technological and the social concerns and emerging legislation accompanying it, require a careful and consistent approach to data management.

4.3 Scoping

Data management in smart energy systems includes the management of all data products as mentioned in Section 2.1 (raw data, information, knowledge) that are created by, processed, or stored in the system. External data (such as weather forecasts) that are only used as input for processing (e.g. analytics) are not subjected to the data management principles laid down in this section while data products resulting from such operations are.

It is important to note that although USEF takes great care in distinguishing raw data and derived data products such as information and knowledge these concepts are often used interchangeably, as can be seen from the definition of personal data stated in the EU Directive "Data Protection Directive 95/46/EC" [7].

Personal Data: "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 [art. 2(a)]".

When in the principles given below the term "Personal Data" is used it meant to include both raw data and derived data products.

The Data Management Principles roughly fall into two main categories. The first one consists of "Minimum Disclosure Principles", the second one of "Ethic of Knowledge Principles".

The Minimum Disclosure Principles are the data management principles related to the end-user (in the role of Data Subject) perspective. They represent a conservative approach where the Data Subject does not a priori trust the peer; therefore he/she accepts to disclose data only if such data:

- Are required for fulfilling the service;
- Provide value for the Data Subject.

The Ethic of Knowledge principles refer to the usage of data by the Data Collector. The Data Collector follows specific ethics on retrieving and using data. This applies to operator of the IT infrastructure.

4.4. Principles

Principle	A Data Policy governs all data in a smart energy system	#01
Description	It is important to have a clear view of used data. The best way to control the usage of data is to apply a policy. The policy includes information like: ■ Who is the Data Subject, - Controller, - Processor? ■ Why does the system need it? ■ What is the lifetime of the data? ■ How can the Data Subject access/control personal data?	
Rationale	The policy allows clarification of the usage of the data. It permits clear explanation to Data Subject. It is a relevant way to enable “User Trust” by generalization of “Data Transparency” of the usage of the information.	
Consequences	■ Data not linked to an explicit policy are not present in the system. ■ The Data Subject, Controller and Processor as well as the lifecycle of all data types present in a smart energy system is registered. ■ The purpose of all data types in smart energy system implementations is explicitly registered.	

Principle	All personal data in a smart energy system are subject to a Data Protection Impact Assessment	#02
Description	A Data Protection Impact Assessment (DPIA) is (Art. 33 of [8]) ‘an assessment of the impact of the envisaged processing operations on the protection of personal data. (…) The assessment contains at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of Data Subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of Data Subjects and other persons concerned’.	
Rationale	A Data Protection Impact Assessments will be mandatory in the upcoming European GDPR. In addition they form a robust part of data policies mentioned above.	
Consequences	DPIAs will need to be performed for all the data managed by the system. The DPIAs need to be auditable by the Data Subject.	

Principle	Data management is designed in a technology and implementation agnostic way using open standards wherever possible	#03
Description	The design of data management in a smart energy system should be independent of the technologies used to implement it, and consequently of the vendors providing the implementations. Deviations from this should be properly motivated. Using open standards not only enhances transparency, it also increases interoperability and arguably security.	
Rationale	Robust and transparent data management is of crucial importance for the viability of smart energy systems as it is a key enabler for trust. Creating an open, interoperable design in which components can be provided by multiple vendors helps to establish a thriving smart energy system.	
Consequences	Designing data management in a technology and implementation agnostic way using open standards increases interoperability and arguably security. Note that in the implementation phase technology choices are unavoidable.	

Principle	Disclosure of data is agreed upon in a transparent way by an explicit agreement between the actors	#04
Description	A service may require the retrieval of Personal Data to perform a service. Users (Data Subjects) can be reluctant to disclose such data; if it is mandatory for the service, the user shall have to disclose the data.	
Rationale	Transparency with respect to data usage is the main enabler for trust. Users are more likely to disclose personal data when they know and understand the purpose of the disclosure. Clearly stating the conditions under which data are disclosed also allows actors to take relevant actions to fulfill certification and regulation obligations related to data storage.	
Consequences	■ This principle implies clear and explicit contractual relationships between actors. ■ Consent is required for the management of personal data. ■ Consent can be withdrawn at any moment.	

Principle	Data are processed as much as possible on the Data Subject side	#05
Description	Data are processed as much as possible on the Data Subject side. This implies that the transformation of “raw data” into “information” takes place at the Data Subject side. Only the information is exchanged, the raw data reside on the client side.	
Rationale	Data are processed as much as possible on the Data Subject side. This implies that the transformation of “raw data” into “information” takes place at the Data Subject side. Only the information is exchanged, the raw data reside on the client side.	
Consequences	Generating information at client side enhances privacy by applying the principle “relevant, adequate and not excessive” and security by generating information only at and for the targeted peer. It also relaxes the security constraints on communication and enables efficient use of network resources.	

Principle	The collected data is fit for purpose	#06
Description	Collected data are adequate, relevant, not excessive and used for a legitimate purpose. It is the server side equivalent of the "data is disclosed only on need to know" basis (principle **#21**)	
Rationale	This principle is part of the guiding principle for privacy in the EU. The principle helps to setup the user contract, fulfill the data storage regulation and enhance trust between actors.	
Consequences	Data Collectors cannot collect all available data by default. They need to justify why data is collected. Data serving different purposes will typically be governed by different data policies, suggesting the implementation of separate data streams.	

Principle	The Data Controller is responsible for the protection of collected data	#07
Description	The Data Controller is responsible for collected data. It needs to fulfill the security and privacy requirements that follow from applicable law and entities it interfaces with. It protects data from being stolen and/or modified by unauthorized systems.	
Rationale	Users disclose information to a Data Collector for a specific purpose. The Data Collector has accepted the disclosed information. The trust of the user in the Data Collector to limit the use of the data to the purposes it was disclosed for should not be violated. Such a violation of trust is not sustainable and would negatively impact the viability of smart energy systems.	
Consequences	The data controller continues to be responsible for the collected data, even when it outsources its data processing to a third-party. The Data Collector implements an IT infrastructure that provides mechanisms for providing confidentiality and integrity and availability of the collected data.	

Principle	The Data Controller allows the Data Subject control over its Personal Data	#08
Description	Personal data—as stated in the user/service provider contract—is owned by the Data Subject, that, as result and therefore should be controlled by the Data Subject.	
Rationale	Personal Data is the property of the Data Subject. The Data Subject shall be able to verify correctness of the data and have means to enforce correction of incorrect data. In addition, Data Subjects need to be provided with (granular) controls to withdraw consent and to move his data to another collector (data portability). This principle is also an enabler for trust.	
Consequences	The data controller requires an IT system that supports data portability, data consultation and granular consent management in an understandable, easy to access manner. ■ The right to withdraw consent at any time means that data streams based on consent cannot be considered stable and can therefore not be used for grid operation purposes. A separation of data stream into those based on necessity and those based on consent is warranted. ■ Easy to use interfaces for Data Subjects to exercise control are needed.	

Principle	Anonymous data is not de-anonymized	#09
Description	Through the combination of anonymized data with metadata and/or ancillary data products might make it possible to perform a de-anonymization operation. This principle states that this is not allowed.	
Rationale	Anonymous data may—implicitly or explicitly according the communication protocol—encompass data that could be used to identify the sender of the data. Future technological developments could also make de-anonymization possible. This principle protects the Data Subject from unwillingly disclosing personal data through advanced profiling techniques.	
Consequences	■ Data mining, analytics and other profiling techniques should be designed in a privacy-preserving manner to prevent de-anonymization. ■ No metadata should be linked to anonymized data that enables de-anonymization. ■ Technological advances might result in today's anonymous data being tomorrow's de-anonymized data. Periodic re-evaluation of de-anonymized data is therefore strongly recommended.	

Principle	Data retention times are specified and motivated	#10
Description	For motivated reasons, system may have to store data in a persistent way. The storage duration is limited.	
Rationale	Firstly, the added value of storing data generally decreases over time. Secondly, this allows reliable implementation of the principle "The Data Controller is responsible for the protection of collected data."	
Consequences	Metadata includes data retention times.	

Principle	Information and Knowledge computed from a single Data Subject is considered to be Personal Data	#11
Description	A system may be able to compute information and knowledge from a single Data Subject. Such data is viewed and processed as Personal data.	
Rationale	Creating information and knowledge often involves techniques such as aggregation or analytics. Although such techniques enhance anonymization the risk of de-anonymization cannot be eradicated. Smart energy system designs should therefore err on the side of caution and treat such information and knowledge as Personal Data.	
Consequences	■ When related to a single Data Subject, knowledge computations shall be specified in user contract. ■ A Service Provider shall explain why it needs such knowledge and how it is obtained and used. ■ Traceability of the origins of such derived data products are built into each system.	

Principle	Knowledge created from aggregated heterogeneous data is owned by its creator	#12
Description	Knowledge obtained from data aggregation or data mining of heterogeneous users (data from different sources but related using one or more criteria), is owned by the entity performing the computation.	
Rationale	Aggregation and data mining are main enablers for smart energy systems. Actors in smart energy arena can obtain a competitive advantage by, among others, creating value through smart profiling and analytics, to the extent that this is covered by the grounds for processing as specified in the EU Data Protection Directive. Any knowledge obtained from this is considered their intellectual property.	
Consequences	■ Knowledge obtained this way is considered as data owned by the system. All references to input data shall be removed. ■ To enhance/enable "Trust", usage of user data shall be clearly stated in the user contract or - if necessary—user shall be notified on new usage of its data, in this case user consent could be required.	

4.5. Conclusion

Data management is a very important topic for smart energy systems. Not only are there many legal obligations that have far-reaching design and implementation consequences for data management (such as the need for consent and data portability) transparent and sophisticated data management is also an important enabler for trust. Mutual trust between Data Subjects, Controllers and Processors based on unambiguous guidelines is a pre-condition for large-scale participation in smart energy systems and a driver for value creation. The data management principles described in this section center around consent, data minimization and protection against unwanted profiling which together provide a solid framework for creating trust.

5 Data communication

Smart energy systems will generate a lot of data that needs to be transported over an infrastructure to the point(s) where they are used. What is the desired security level for different types of data communication?

5.1. Explanation of the subject

Data communication is about the exchange of data between two entities: a sender and a receiver. The sender and receiver require a channel to communicate. The channel is created by means of a medium connecting sender and receiver.
Effective communication requires the sender and receiver to agree on how to set up a connection over the channel, how to transport data over the connection and how to interpret that data. This has been described in formal models like the OSI model [23] which divides data communication into seven layers and the simpler TCP/IP model [24] which recognizes four distinct layers:

- Application layer: the application layer is provided by the program that uses TCP/IP for communication.
- Transport layer: the transport layer provides the end-to-end data transfer by delivering data from an application to its remote peer.
- Internetworking layer: The internetwork layer, also called the internet layer or the network layer, provides the "virtual network" image of an internet (this layer shields the higher levels from the physical network architecture below it).
- Link layer: The network interface layer, also called the link layer or the data-link layer, is the interface to the actual network hardware.

The TCP/IP model provides a good starting point for the understanding of data communication in the context of this document.
Data communication in smart energy systems does not differ markedly from other communication domains like Internet, which—by design—involves different heterogeneous networks. Using the de-facto standard communication protocols of the Internet in a smart energy system is therefore, although not for all purposes[8], obvious.

5.2. Rationale for the subject

A smart energy system is a distributed system that forms a geographically widespread combined energy and IT infrastructure. These systems do not work on their own, but in close cooperation with each other. This implies these systems need to exchange data—in fact, without the data communication between the subsystems a smart energy system reduces to a legacy energy grid.
Smart energy systems like those based on USEF therefore critically depend on trusted, reliable (see Sections 6 to 8 for principles related to reliability) data communication. This includes assuring that during the exchange of data the data is not altered nor intercepted.

5.3. Scoping

The principles described in this section focus on the privacy & security requirements for data communication between the various roles in smart energy systems. Although the principles might be applicable for legacy communication as well—and the reader is most definitely encouraged to explore how application of the guideline might benefit his organization here –this is not the focus of these principles.

[8] Especially in protecting the assets transporting and distributing energy the latency of a TCP/IP connection is too high to be useful.

5.4. Principles

Principle	The communication channel between source and destination does not contain intermediary nodes where the data needs to be disclosed	#13
Description	To exchange data, a communication channel is set up between two entities. This channel must be secured end-to-end, without any nodes in between where the data needs to be disclosed. In case the communication channel is secured, data can be exchanged in a secure way. In the picture below an example is provided of a communication channel that does not comply with the principle, showing that a man in the middle is able to access the data that is exchanged. 	
Rationale	Avoiding intermediate nodes where data is to be revealed reduces number of vulnerability points of the system. By creating a secure channel this way, the sender can guarantee to the receiver that there are no third parties that can access the data during the data exchange.	
Consequences	This principle requires a separation between routing information and content. The routing information is needed for creating the secure channel between sender and receiver, implying this information cannot be encrypted. Besides encrypting the channel, the messages should be encrypted as well (see principle #14)	

Principle	Data secures itself	#14
Description	Operational requirements may require data to be sent from one source to one or many destination peers over an unsecure channel. To ensure this happens securely, the data should secure itself and security should not depend on the transmission medium. 	
Rationale	Exchanging data over an unsecure channel exposes the data to be intercepted by a third party, resulting in integrity and/or confidentiality breaches. Since the Data Controller is obliged to comply with the GDPR, he has to take other measures to avoid these breaches. Securing the data prevents that the data intercepted can be read by the interceptor.	
Consequences	In order to implement this principle, a transport-independent cryptographic scheme is needed. Encrypting an outgoing message using a private digital encryption key results in an opaque blob: the sealed and encrypted message. Unsealing and decrypting this message, using the corresponding private digital encryption key returns the message plaintext after signature verification (which is required to ensure message integrity).	

Principle	Message encryption is based on a proven, independently validated cryptographic scheme	#15
Description	The messages exchanged between the roles in a smart energy system are encrypted using an established proven cryptographic scheme for which robust, state-of-the-art open source implementations are available. Designing a custom cryptographic scheme and functions is not allowed.	
Rationale	Smart energy systems in general and USEF in particular rely heavily on the exchange of messages which origins and contents should be shielded from prying eyes and manipulating hands in order for actors to trust, adopt and successfully use the framework. Cryptography is a highly specialized, highly technical field which complexity should not be underestimated. Home-grown solutions are likely if not guaranteed to contain vulnerabilities and are therefore to be avoided.	
Consequences	Most cryptographic schemes rely on public-private key combinations. Therefore, to fulfil this principle a secure way of managing cryptographic keys is needed.	

Principle	Data communication between roles is controlled	#16
Description	Data communication between different roles in a smart energy system is controlled, assuring that only the necessary communication between the systems of the different roles is possible. All other data communication is rejected.	
Rationale	Limiting the communication between the different smart energy system roles—only systems that must be able to communicate with systems of another smart energy system role are allowed to do so—avoids misuse of systems of by other smart energy system roles.	
Consequences	At least the source- and destination address of messages that need to be exchanged between the smart energy system roles must be inspected. In addition, it is advisable to inspect whether or not a message is expected—a flexibility offer sent without a prior flexibility request indicates a possible breach.	

Principle	Parties that exchange data are able to identify each other	#17
Description	The receiver is able to verify the sender the data originates from; the sender is able to verify the identity of the receiver it wants to send the data to	
Rationale	In order to trust the data that is exchanged, the receiver wants to be sure that the sender is the party it expects the party from to avoid the receiver is acting on data that has been spoofed. In addition, the sender wants to assure that the party it sends data to is the intended receiver, to avoid data leakage to (untrusted) third parties.	
Consequences	In order to exchange messages with other participants in a smart energy system, an implementation needs to determine the appropriate entity address and encryption/signing keys of each participant. This information can be obtained by querying DNS using their Internet domain names. To eliminate the risk of man-in-the-middle attacks, DNS results should be DNSSEC signed, and the implementation should verify these signatures.	

Principle	The receiver is able to verify sent data have not been tampered with.	#18
Description	The receiver of a message wants to be sure that during the data communication the contents of the message have not been altered in any way. In case the contents have been altered, the receiver must be able to notice that. See also principle #	
Rationale	The content of a message is used by the receiver for further actions. Therefore, it must be able to trust it and rely on its contents. Verification of the sender identity is not sufficient; verifying the content has not been tampered with during transportation is required as well.	
Consequences	Messages that are exchanged must be digitally sealed in a way that every change is noticeable upon unsealing, i.e. prior to processing the message its contents. A proven way to achieve this is to digitally sign every message using the private key of the sender, implying the use of a PKI infrastructure.	

Principle	Security aspects of the individual data streams are subject to the security aspects of the system as a whole	#19
Description	A data stream between two entities does not stand on its own, but in most situations plays a role in the entire smart energy system. The rating of the level of confidentiality, integrity and availability of the individual data stream might differ from the rating of the same data in the system as a whole.	
Rationale	A chain is as strong as its weakest link. To achieve the security requirements for the system as a whole, all individual links should at least fulfill the requirements of the system.	
Consequences	Individual data streams cannot be assessed by themselves; the role of the data stream in the system of a whole is what counts. In case the requirements of the system as a whole are higher than those of the individual data stream, additional costs for implementing the stream might be involved.	

Principle	Data communication between roles is resilient	#20
Description	The communication between the roles in a smart energy system is resistant to a temporary unavailability of the receiver. As soon as the receiver is available again, the processes interrupted due to unavailability will continue.	
Rationale	Smart energy systems in general and USEF in particular rely heavily on exchanging messages between different roles. The communication channel, however, might be temporarily unavailable. By implementing a resilient message exchange framework, the robustness of the system is increased.	
Consequences	To realize this principle each participant must operate a message queue, both for outgoing and for incoming messages, in order to achieve fully asynchronous and decoupled operations, that implements retry mechanism. In addition, mechanisms must be in place to confirm the receiving of a message and out-of-bound notification messages that failed to be delivered.	

5.5. Conclusion

A smart grid is a distributed system of systems, mandating data exchange, which in turn requires data communication.
The quality of the data is not be negatively impacted by the communication, nor should it possible by third parties to intercept the data. To achieve this, both the communication channel and the data itself must be secured. In the data exchange, it is important that sending and receiving parties are able to verify each other's identity. In addition, the receiver of the data must be assured the data has not been tampered with.

For increasing robustness of smart energy systems, data communication between roles must be resilient.

6 Confidentiality

Confidentiality refers to limiting information access and disclosure to authorized resources and preventing access by or disclosure to unauthorized resources. The consequences of a breach are different for the different stakeholders (loss of privacy for a Prosumer, loss of goodwill, competitive disadvantage for a retailer). What are necessary and acceptable levels of confidentiality for the different parts of the system?

6.1 Explanation of the subject

Confidentiality is the cornerstone of information security. It aims to keep information which represents a value secret, e.g. market information (money) or information about persons and their behavior (privacy). It is therefore a must-have, both for the persons involved in a smart energy system—to preserve their privacy—as well as for the (commercial) organizations—to protect their valuable assets. In general, one can state that confidentiality mostly relates to privacy-preservation in the part of the (smart) energy system near the end user, and that it mostly relates to asset protection in the other parts of the (smart) energy system. When discussing confidentiality we typically talk about information rather than raw data since it is the context and interpretation that transforms raw data into information that results in data products that are deemed confidential.

Confidentiality can be achieved by (amongst others) restricting information flow and access. For example, access can be granted to information only on a need-to-know basis. Furthermore, granting access also implies that information can (and often will) be copied from one place to another. It is therefore important that those copies of the data are deleted when they are not needed anymore. This is less obvious than it looks—often copies of information become out of reach of the initial Data Controller and/or Subject. Think about sending a document by email to a colleague, who in turn forwards it to another person.

In order to preserve confidentiality information must be accessible only for entities (persons or systems) that have the right to access the data. This implies that confidentiality requires a mechanism to determine the identity of each entity. The higher the confidentiality of information, the more guarantees are needed to assure the identity of the entity. See chapter **10** for more information about identities.

Making confidential information available for other parties than the Data Subject not only requires the determination of identities. It is required that the Data Subject trusts the other parties that they will respect the confidentiality level determined by the Data Subject. In other words, information that is rated as 'confidential' by the Data Subject must not be made publicly available by the receiving party. Exchanging information with a third party is only allowed if the Data Subject is informed and agrees.

6.2 Rationale

In a smart energy system, a vast amount of data is stored and exchanged. Protecting all this data, so the confidentiality can be guaranteed all the time is not only very complex, and thus expensive; it may also negatively impact the functionality of parts of the energy system. Not all data is equally sensitive to violations of confidentiality. The ownership of the data, the conditions under which they are collected, their purpose, the level of anonymization and the potential for de-anonymization are all factors that have to be taken into account by Data Controllers and - Processors when assessing the confidentiality.

For these reasons, optimizing the costs of measuring and the exchanging information, the required level of confidentiality must be determined for all information. The levels range from public information to secret information, with one or two levels in between. For public information, it is not needed for an entity to identify itself before accessing the data, for secret information several checks are made to confirm the identity[9] of the entity.

Handling information with respect to confidentiality is especially important when handling privacy-sensitive information, like customer information, to gain and maintain end-user trust. Some of this information is essential for a proper operation of a smart energy system while other information is essential to enable value creation through, e.g., third-party services. In case customers decide massively to refuse sharing this information with other stakeholders in a smart energy system, the feasibility of a smart energy system can be questioned.

[9] An identity is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons. So usually there is no such thing as "the identity", but several of them, Hansen and Pfitzmann [30].

6.3 Scoping

For all information needed for a smart energy system, confidentiality must be taken into account. This includes, among other things, customer information, meter readings, the status of the grid and pricing information. To avoid a too complex analysis of the confidentiality requirements, this information should be divided into classes and a data policy should detail the requirements for managing information at each confidentiality level.

Although the principles are written with a smart energy system in mind, most, if not all, are relevant for other information as well.

6.4 Principles

Principle	Information is shared on a need to know basis	#21
Description	Access to information other than public information shall be permitted only on a need-to-know basis. In other words, an entity can only access information that is needed to perform the activities it is required to do based on legal or contractual obligations. All other (non-public) information is inaccessible.	
Rationale	The more entities have access to (non-public) information, the higher the risk for privacy and/or security incidents. By reducing the access to information that is needed only, the risk of (un-)intended leakage of confidential information is limited.	
Consequences	For all processes, the information need must be determined. Only then it is possible to determine which information must be made available, to whom and under which conditions. However, the boundaries between information really needed and information that is nice to have is not always as strict as desirable. Therefore, the data policy and the underlying data protection impact assessment play a key role in determining what information is accessible.	

Principle	Information is classified into degrees of confidentiality needed	#22
Description	Not all information has the same sensitivity; therefore information must be classified into degrees of confidentiality needed. Suggested classifications are: ■ **Public**: available for everyone. Can be freely exchanged ■ **Internal**: available within the boundary of an organization. Exchanging with third parties is bounded by certain rules. ■ **Confidential**: available for a limited group within an organization. Exchanging with third parties is restricted. ■ **Secret**: available for certain individuals within an organization only. Cannot be exchanged with other organizations.	
Rationale	Taking measures to limit the access to information costs money and is less convenient (providing credentials to open a document takes more effort than just double-clicking on it). By classifying the information, it is easier to determine which measures must be taken to assure enough confidentiality.	
Consequences	■ Stakeholders must agree upon the data classification of information they exchange. If one of the parties classifies certain information as confidential, the other party must take measures to guarantee this confidentiality. In general, the highest level of confidentiality assigned by a stakeholder determines how the information is treated. ■ Metadata contains the classification level. ■ This principle applies to all information in a smart energy system—meter readings, data used for business analytics, etc. Classifying information is however less obvious than it looks and might differ per organization/country (i.e. in Italy meter readings are considered less sensitive than in the Netherlands).	

Principle	Protect the data, not only the medium	#23
Description	Instead of only protecting the access to the medium where the information is stored, the data products themselves are protected as well. The type of 'defense in depth' that is deployed may vary from data product to data product, depending on the (operational) use of the data and may include additional file level access control, encryption etc. These additional layers of protection avoid unauthorized access to information even in case of a breach in the security of the medium.	
Rationale	In case only the medium is protected instead of the information itself as well, a copy of the information to another medium removes the protection. If the information itself is protected, copying it to another medium does not remove the protection.	
Consequences	For encrypting information, encryption-/decryption keys are needed. The current standard in encryption is using a public/private key combination—information encrypted with the public key can be decrypted with the private key only and vice versa. In order to exchange these keys between the parties involved, a key management infrastructure is needed.	

Principle	Separate information of different confidentiality classifications	#24
Description	The separation of information based on its confidentiality classification needs to be ensured during the entire life cycle of the information, from collection to destruction. Since the confidentiality classification of information may change during this life cycle the aggregation levels and protection measures may change accordingly.	
Rationale	Separating data according to its confidentiality classification allows for the optimal application of protection measures.	
Consequences	In the information models used this splitting must be taken into account in advance. In addition, either the information classifications must be agreed upon, or the splitting must be flexible. This results in more complex information models and handing.	

Principle	Confidentiality is ensured end-to-end	#25
Description	The confidentiality of (privacy) sensitive information is guaranteed during the entire lifecycle, from creation, communication, storing and processing to retention. It is possible that during the lifecycle of an information asset the required confidentiality changes; in that case the measures to be taken must change accordingly (example: confidentiality classification of the financial results of a company is 'confidential'/'secret' before publication, but 'public' after publication).	
Rationale	A chain is a weak as its weakest link. As a result, to ensure confidentiality during the lifecycle all entities involved in this lifecycle must have at least taken measures according to the assigned confidentiality level.	
Consequences	■ In order to be able to guarantee confidentiality end-to-end, the entire chain needs to be identified. For each part of the chain, it must be assured that the specific part can fulfill the confidentiality requirements. The ultimate consequence might be that part of the chain must be replaced due to lack of available measures for that part of the chain. ■ A mechanism is available that modifies access to information when the confidentially classification changes. ■ The confidentiality classification is exchanged between roles.	

Principle	Protection is proportional to potential damage[10]	#26
Description	The level of protection shall be proportional to the potential damage that may result from information leakage. This implies a differentiation is made in measures to be taken for guaranteeing confidentiality for different information in a smart energy system.	
Rationale	A 100% guarantee of meeting confidentiality requirements is neither feasible nor cost-effective. The potential damages of confidentiality breaches need to be understood, using a Data Protection Impact Assessment see principle #02, in order to determine the desired confidentiality protection measures.	
Consequences	The balance between taking measures and taking risks must proportional to balance between the costs for implementing the measures and the (financial) consequences of the recovery in case data leakage has occurred. As a result, some confidentiality breaches will inevitably occur.	

6.6 Conclusions

In a smart energy system, information needs to be classified into different categories of confidentiality. For each category, the right measures must be taken in order to find the right balance between the costs for these measures and the (financial) damage of a violation against the confidentiality needed.
The starting point for the confidentiality is the 'need to know' principle—only information that is needed for proper operation should be available to an entity.

10. Note that similar principles apply to integrity and availability of data (products), see chapters 7 and 8.

7 Integrity

Integrity means that data cannot be modified undetectably. Where in the smart energy system is integrity more important than availability, or more important than confidentiality?

7.1 Explanation of the subject

The concept of integrity concerns the consistency of actions, values, methods, measures, principles, expectations, and outcomes. Data integrity concerns the trustworthiness of data (and the information represented in it) over its entire lifecycle. It is a must-have for trust in a smart energy system: the energy producers, suppliers and Prosumers require correct invoices; the Prosumers need to have trust in the smart energy system that ultimately asks of them to adapt their energy consumption behavior.

A second aspect of data integrity is that the data stored in the IT systems is consistent with the real world it represents. Decision making is based on a representation of the real world stored in IT systems. Only if that representation resembles the real world—in other words, the integrity is guaranteed—the right decisions can be made.

Violation of integrity can have several causes. Some examples are:

- **Wrong input.** There are several ways of putting data into an IT system, like converting a measured (analogue) value (e.g. voltage or current) to a digital value, manually entering data or receiving data from another IT system. If the input is wrong, the integrity of the data, and thus the derived information, is violated. Example: integrity violation through manipulation of (local) power market price information impact both system stability and financial results of connected parties.
- **Wrong processing**. A programming error might result in wrong outcome. Although extensive testing reduces the number of programming errors, part of the programming errors are very hard to find, due to the fact that the processing only goes wrong in exceptional circumstances.
- **Physical**. Although IT systems and the data on it are considered to be digital, the actually systems are still mostly relying on analogue values—voltage (for instance, in a data communication connection), magnetism (storage on hard disks), Although thresholds are chosen to avoid meshing up the binary data (1's and 0's), it might occur due to external influences (radiation) that a 1 changes into a 0 and vice versa. Taking into account that several systems in a smart e are located in highly interferential environments (substations), this must be taken into account.

Achieving data integrity starts with using means to assure the right measurement. The phrase 'garbage in is garbage out' applies to data integrity. Even if all measures are taken to make sure that the integrity of data is guaranteed during the lifecycle in the IT systems—exchanging with other systems, calculating, etc.—as long as the input is wrong, the output will be wrong. Measures to assure the integrity of the input are, among other things, certification (for instance of a smart meter), four eyes principle (for data entry) and testing with data that has a known outcome (for software programs). For limiting the physical influence in highly interferential environments can be achieved by proper shielding the systems.

Ways to achieve data integrity are for instance applying mathematical integrity checks (CRC, MAC, signature), sanity checks (range check, check against context) and/or redundancy (backup copy, parity bits). In the end, data integrity is of course only a means; the real goal is to achieve information integrity.

7.2 Rationale for the subject

Taking the integrity of the data into account is essential for several reasons. First of all, in order to rely on the data in the IT systems the parties involved—Prosumers, Aggregators, BRPs and TSO/DSOs—must at least have the guarantee that the data their business depends on are within the defined reliability interval. The more a party is convinced that the data are correct, the more likely it is they will use the data for decision making—trading flexibility, controlling the grid, adapting energy consumption etc.

In addition, it is expected that integrity helps in reducing the resistance against the introduction of smartness into the energy system. This goes for Prosumers as well as employees in the energy supply chain—it is in human behavior to have a certain ratio of resistance against matters that are outside of the mindset of a human being—it is 'scary' to give certain control to

incomprehensible systems. Showing the integrity is guaranteed, takes away at least part of the fear and establishes trust in the smart grid.

Finally, a smart energy system is needed to use the energy system as optimal as possible. The smartness in the grid is needed to prevent the grid from exceeding its physical limits. If the systems controlling the balance in and load on the grid must rely on data which integrity is not guaranteed, the likelihood increases that the grid will be overloaded, with power outages and diminished trust as a result.

Assuring data integrity requires measures to be taken, which increases the costs for realizing a smart energy system. It is likely that to guarantee data integrity for all data in the system is too expensive to be realistic. It is therefore important to make a distinction between the levels of integrity needed. This implies standard measures must be taken for most components, but additional measures are only implied for critical components. Compare to testing in a production environment—standard measures include that all produced goods are checked basically, only a few samples are tested extensively to represent the entire batch; for critical products however, every produced good is tested extensively.

7.3 Scoping

The integrity principles listed in this guide apply to all the IT systems required to operate a smart energy system and the services enabled by it as well as the analog systems feeding into those IT systems.

7.4 Principles

Principle	Integrity is upheld for actionable information	#27
Description	The integrity of all actionable information in the smart energy system, this is information on which basis action will be taken, is always upheld. Full guarantees may not always be possible, but the level of guarantee shall at least be proportional to the consequence of the decision (see also principle #28).	
Rationale	Decisions are made based on information. To make the right decisions, at least the information on which the decisions are based must be right, i.e. the accuracy and consistency and completeness of such data should be assured Higher information integrity improves information quality, thereby supporting better decision-making.	
Consequences	For each type of actionable information, mean to guarantee the integrity must be defined, proportional to the consequence of action on that information. One can for example: ■ Protect and check the integrity of individual data in a mathematical way using (cryptographic) checksums; ■ Checking that it is consistent with other data and information that is available in the system.	

Principle	The protection level is proportional to the potential damage[11]	#28
Description	The level of protection shall be proportional to the potential damage that may result from incorrect actions/decisions being taken upon invalid information. This implies differentiation is made in measures to be taken for guaranteeing integrity for the different types of components.	
Rationale	Guaranteeing a near 100% of integrity for all data and information is too costly. In addition, the effect of violating the integrity of information has different impact for different information. Therefore, the potential damages of integrity losses need to be understood, using a Data Protection Impact Assessment (see principle #02), in order to determine the desired integrity protection measures.	
Consequences	A small portion of the data and information will be incorrect. In making decisions based on the information, a sanity check is therefore mandatory.	

7.5 Conclusions

The integrity of the data is a measure of the reliability that the data in the (IT) systems is representing the real world. The more critical the data and information are for decision making, the higher the integrity must be.

Integrity is the basis for the trust in the systems. The parties involved in smart grids will only rely on these systems if integrity is within an accepted reliability bandwidth.

In order to determine the optimum data and information integrity, the potential damages from loss of integrity need to be assessed.

11. Similar principles exist for confidentiality and availability, see Sections 6 and 8 Integrity.

8 Availability

Availability refers to the availability of information resources including systems, processes and data elements. What are necessary and acceptable levels of availability for the different components of a smart energy system?

8.1 Explanation of the subject

Most—if not all—people have an intuitive idea about the concept 'availability'. It is nevertheless much harder to realize the consequences of bringing this concept in practice. In fact, it is easier to look at the opposite—'Unavailability'. As long as something is available, it is hard to appreciate the fact that it is available. First if that something becomes unavailable, the real value is discovered.

A definition of availability is [25]: "The degree to which a system, subsystem, or equipment is in a specified operable and committable state at the start of a mission, when the mission is called for at an unknown, i.e., a random, time." Simply put, availability is the proportion of time a system is in a functioning state.
There are two reasons for unavailability: planned and unplanned downtime. Planned downtime is the time a system is down for maintenance and is predictable to a high extent. By planning maintenance outside the service window planned downtime has no impact on the availability from a business perspective. Unplanned downtime is caused by failing systems, and is therefore unpredictable.

There are several aspects to availability that must be taken into account:

- Duration. Several short outages spread over a longer period might be acceptable, whilst a longer single outage—even if the duration of that outage is shorter than the sum of durations of the short outages – can be unacceptable
- Appraisal of planned downtime. For systems that run 24x7, planned downtime has a direct effect on the (business) availability. Even with a relatively low availability of 99.9% per year, measures must be taken to reduce the downtime during maintenance, for instance by having a standby system that takes over functionality of the main system. The maintenance of systems with a limited service window can be planned outside of that window, and therefore probably do not need extra measures.
- Degradation of service. A system might be available, but if the normal service level is degraded substantially, users of the system might consider the system to be unavailable.

To determine which systems need high availability, several methodologies exist, all based on determining the (business) impact of unavailability. High(er) availability comes at cost, which implies that only for systems that really need a high availability measures should be taken.

8.2 Rationale for the subject

In a smart energy system the availability of energy depends not only on the physical components, but also on the IT systems controlling the energy system. This implies the systems responsible for the smartness must have sufficient availability to achieve the overall availability needed. Whether or not availability is sufficient is related to the impact of unavailability on the Prosumers of a system. This impact is related to:

- **Location in the energy grid**: generally, the control systems of a primary substation need higher availability than the control systems in secondary substation[12]. Also, it can be argued that a secondary substation in the center of a large city must have a higher availability than a secondary substation in a rural area. The reason in both cases is the number of customers that are affected.
- **Role in the smart energy system**: systems that are used for controlling the grid and therefore have a 'real-time character' must have a higher availability than systems used for administration—assuming that no data is lost during the unavailability of an administration system.
- **Number of systems involved in the outage**: having a few systems - related to the entire population—unavailable has less impact on the grid than having an outage of all or most of the systems.
- **Time to repair/replace**: the longer it takes to return to a fully operational stage in case of an outage, the more effort should be put in avoiding outages.

[12] In a microgrid, or for topologies with a large amount of decentral generation this might be different.

8.3 Scoping

The primary goal of a smart energy system is to guarantee the optimal dispatch of connected assets in a safe, reliable, affordable and sustainable way. To achieve this, a complex cooperation of systems is needed.

The scope of this section focuses on systems used for flexibility trading such as the market-based coordination mechanism (MCM) proposed by USEF, exchanging the messages between the different roles in a smart energy system (Aggregator, BRP. DSO). Although the principles do apply to other systems used in a smart energy system as well, these systems not part of the (primary) scope of this section.

8.4 Principles

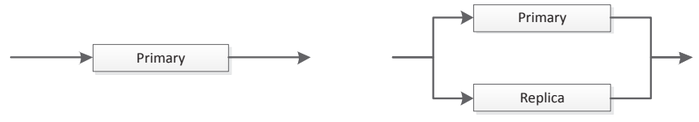
Principle	Assess the vulnerability of assets[13]	#29
Description	The vulnerability of an asset depends on several aspects, like value, location, etc. To determine the vulnerability of an asset, it is needed to investigate these aspects for each asset. Keep in mind it is possible that identical physical assets can have a different vulnerability level due to difference in aspects—a (data communication) cable in a city might be more vulnerable for excavation damage than an identical cable in a recreation area.	
Rationale	Risk is a product of both impact and likelihood. In order to determine whether or not additional mitigating measures are needed for raising availability, it is therefore needed to determine both. The likelihood an asset becomes unavailable depends on the vulnerabilities of that asset—the more vulnerabilities, the bigger the likelihood. Assets with many vulnerabilities therefore probably need countermeasures, especially when the availability of that system is classified as high.	
Consequences	To assess each asset is an extensive job. A pragmatic way is to start with a threat analysis. Based on these threats, it can be determined which assets are likely to be most vulnerable. The assessment should start with these assets to limit the time needed for assessing, and still having a sufficient inside of the vulnerabilities of the grid as a whole.	

Principle	Protection is proportional to potential damage[2]	#30
Description	A smart energy system consists of many different components. Depending on the role and position in the smart grid, the unavailability of the component has more or less impact. The required measures to ensure availability are determined based on the impact unavailability has. To avoid too much granularity in classifications, the M/490 SGIS working group has defined five security levels [26]: ■ **Low:** Assets whose disruption could lead to a power loss under 1 MW; Town/ Neighborhood Incident; ■ **Medium**: Assets whose disruption could lead to a power loss from 1 MW to 100 MW; Regional/Town Incident; ■ **High**: Assets whose disruption could lead to a power loss from above 100 MW to 1 GW; Country/Regional Incident; ■ **Critical:** Assets whose disruption could lead to a power loss from above 1 GW to 10 GW; European/Country Incident; ■ **Highly Critical:** Assets whose disruption could lead to power loss above 10 GW; Pan European Incident. Although these system-level classifications have a strong focus on physical assets they can be augmented and/or replaced by criteria more appropriate to individual USEF roles. In determining the availability needed, it must be taken into account that components are in most cases part of a chain. This might imply the availability of a component in the chain is rated higher than an individual component due to the needed end-to-end availability of the chain.	

[13]. This principle applies not only on the availability of assets, but on confidentiality and integrity (see previous sections) as well.

[14]. Similar principles exist for confidentiality and integrity; see Sections 6 and 7.

Rationale	Assessing the necessary availability of the components is needed in order to determine where additional measures must be taken to keep the smart grid up and running. Because the measures to raise the availability are more than proportional to the availability achieved, making all components highly available is far too costly. By classifying the components, it is possible to determine for which components additional measures are needed, limiting the costs for achieving availability.
Consequences	■ For all components that are either added to the smart energy system or fulfill a different role than in the classic grid, the required availability needs to be assessed. This requires a deep understanding of the role such components play in the overall availability of the systems which in turn requires are processes to be mapped out and documented. Only when the impact of a component on the system as a whole is understood appropriate measures can be put in place. ■ Availability classification is part of the metadata of components.

Principle	Introduce redundancy for systems that need to be highly available	#31
Description	Key for making systems high available is identifying single points of failure (SPOF). These are components of a system that make a system unavailable in case such a component fails. By introducing redundancy, components that are identified as SPOFs are implemented more than once. Redundancy can be implemented in two ways, namely active-passive and active-active. In an active-passive configuration, the redundant component(s) is/are in standby modus as long as the primary component is up and running, and takes over as soon as the primary component fails (this is called a failover). In an active-active configuration, both the primary and the redundant components are in a running state.	
Rationale	To avoid the failure of the entire system due to the failure of a SPOF is to implement this component more than once. In case the primary component fails, (one of) the redundant component(s) takes over the functionality. The picture below provides an example of a non-redundant (left) system and its redundant replacement (right) 	
Consequences	Introducing redundancy comes with several issues: ■ Cost: each redundant component is implemented at least twice (instead of once). In addition, the failover implementation in general adds costs as well; ■ Implementing failover is less trivial as it looks at first sight. Several measures must be taken to avoid unpredictable states of the system.	

Principle	Monitor high-availability systems	#32
Description	Systems that need to be highly available must be monitored. Each failure of these systems must be detected and acted upon. Due to the amount of systems on one hand and the speed of the response needed, the monitoring (and the acting upon the status changes) must be automated. Note that the redundancy of systems (see principle #31) should be monitored too.	
Rationale	If a component of a high-availability system fails, the replica of that component must take over in order to prevent the entire system fails. This taking over is only possible if the failure of the component is determined, which is only possible if it is monitored. The detected failure must not only take care of the failover, but in addition it must start a process to repair the failed component—as long as a failed component is not repaired, the redundancy needed is not available, introducing the risk that a second component failure results in a system failure.	
Consequences	High-availability systems that are 24x7 operational must be monitored 24x7. Although part of the monitoring is executed automatically and recovery processes (see chapter 9) can be triggered automatically, human intervention must be possible as well. This implies the implementation of a service organization that is available 24x7.	

Principle	Unavailability is mitigated by failsafe operation	#33
Description	In case the 'smartness' in a part of the smart energy system is not available, the energy system must switch to a failsafe operation. In this mode, additional services that are needed to optimize the usage of the energy system are not available. This implies, among other things, a stepwise degradation of the connection capacity.	
Rationale	The smartness in a smart energy system provides the ability to optimize the usage of the current energy system. If the smartness is not available, it is more challenging to predict and prevent an overload of the capacity, nor is it possible to safely feed de-centrally generated electricity back into the net. Falling back to failsafe operation in fact implies that the energy system operates in a way it is operating nowadays.	
Consequences	In order to be able to fall back to a failsafe operation, the smart energy system has to be designed with this capability in mind. This requires among others, sensors and actuators and might bring additional costs. Implementation of this operating regime acts as a backstop for regular, market-driven operations and leads to a higher availability of the energy system.	

8.5 Conclusions

With the introduction of smartness into the energy system, a dependency between the availability of the energy system and the IT systems controlling it is introduced. To avoid power and market outages due to failures in these systems, several measures must be taken. This varies from making the flexibility market systems high available as well to realizing a fail-safe mode for the grid itself, where the smart energy system is behaving like a legacy grid in case the smartness is not available. As is the case with confidentiality and integrity, a balance must be made to invest in high(er) availability and the financial damage in case of a failure.

9 Disaster Recovery

No (security) system is perfect. What needs to be done in the case of unforeseen situations? How to mitigate the fall-out from a security/privacy breach? How are responsibilities divided between parties?

9.1 Explanation of the subject

Disaster recovery is a subset of business continuity. Disaster recovery is the area of security planning that deals with protecting an organization's business functions from the effects of significant negative events related to its technology infrastructure.
These negative events can be classified along two axes. We can distinguish between natural disasters such as earthquakes and tornadoes, and man-made disasters such as theft and terrorisms. Additionally, we can classify disasters in terms of breaches of confidentiality, integrity and availability. Different types of disasters call for different control measures [27]:

- Preventive measures - Controls aimed at preventing an event from occurring.
- Detective measures - Controls aimed at detecting or discovering unwanted events.
- Corrective measures - Controls aimed at correcting or restoring the system after a disaster or an event.

Confidentiality breaches are hard to recover from. Once confidential information has become public, it cannot be undone. Mitigation measures against a confidentiality breach therefore focus on prevention and have a strong link to the identification, authentication and authorization of actors. Corrective controls in the realm of confidentiality breaches focus on restoring confidentiality by replacing the now public information with new confidential information.

Recovering from integrity issues is generally speaking easier, and control measures exist in the preventive, detective and corrective domain, ranging from more operational controls like frequent (offsite) backups to error detecting and correcting codes that are part of the design and implementation of a system.

The category that is traditionally most associated with disaster recovery is probably the recovery from availability failure. Preventive controls can be applied effectively to counter availability failures, centered on including redundancy in the system's design and implementation. Preventive controls also assist in enabling corrective controls.

9.2 Rationale

The advent of smart energy systems signals an introduction of information technology in the energy system at a large scale. As a result, recovery from outages or other negative events such as data leaks involving IT systems needs to be considered when designing the future energy system to maximize its proper, uninterrupted operation or in case this temporarily fails, mitigate the consequences for all stakeholders involved and ensure continuous supply of energy to all connected parties.

9.3 Scoping

There are both technical and organizational aspects to disaster recovery. The technical aspects relate to architectural design and implementation choices. Organizational aspects deal with creating and testing recovery plans, assigning responsibilities and defining criteria for declaring a disaster and claiming successful recovery.

The P&S guideline concerns itself with the technical aspects of disaster recovery only and aims to provide principles that allow the disaster recovery to be designed and implemented in a rationalized and where possible quantified fashion. Organizational aspects of disaster recovery are considered out of scope as it is assumed that smart energy systems will be part of larger networked enterprise systems and fall under existing business continuity planning realms. When technical aspects of disaster recovery directly impact organizational aspects or vice versa it will be mentioned in the principles.

9.4 Principles

Principle	Investments in Disaster Recovery are based on a risk assessment	#34
Description	A risk assessment is carried out to assess the (financial, reputational) damage associated with negative events. The results of these assessments are used to determine the type and scope of disaster recovery control measures.	
Rationale	Control measures to prevent, detect and correct negative events resulting from disasters carry a cost. In order to justify these and prevent under- or overspending on disaster recovery the associated risks associated should be quantified.	
Consequences	A risk assessment methodology should be available to consistently assess risks for business processes and systems. Risk-based control measures contribute to balanced investments in disaster recovery.	

Principle	The system architecture supports an implementation that matches industry-standard RTO and RPO times	#35
Description	Disaster recovery capabilities are typically specified in terms of RTO (Recovery Time Objective, the duration of time and a service level within which a business process must be restored after a disaster) and RPO (Recovery Point Objective, the maximum tolerable period in which data might be lost from an IT service due to a major incident). A system architecture puts constraints on the system implementation and therefore on attainable RTO and RPO times.	
Rationale	In order for smart energy systems to be adapted at a large scale its architecture should support an implementation that allows for RTO and RPO times that are at least as good as what is currently considered standard in the energy sector.	
Consequences	Disaster recovery should be a design consideration from the very first stages of system design. During the implementation phase a method should be available for determining RTO and RPO times. For parts of the smart energy system that require very short RTO and RPO times, an implementation that guarantees high-availability is required.	

Principle	Smart energy system elements are prioritized for recovery	#36
Description	In the event of recovery from a disaster, systems are restored according to a predetermined, documented order of priority.	
Rationale	Focus should be on doing the right things as opposed to doing things right. When elements (physical components, functions or data) are prioritized, it is clear to all involved what needs to be done first.	
Consequences	Priority for recovery needs to be specified in recovery plans. This implies not only some (sub) systems are prioritized for recovery but also that for some (sub)systems recovery is postponed on purpose.	

Principle	Smart energy systems are designed as highly-cohesive, loosely coupled	#37
Description	Cohesion refers to the number and diversity of tasks that a building block of the system is designed for. Coupling refers to links between separate building blocks of the system.	
Rationale	A highly cohesive, loosely coupled system design enhances the atomicity of the system and helps to mitigate the fall-out of failures of individual system components.	
Consequences	Applying this principle results in a more robust system. Additional benefits include greater flexibility and extensibility.	

Principle	Backup only what you need to restore	#38
Description	A careful assessment should be made which data should be restored in case of a disaster. There is no point in backing up data if there is no intention to restore it after a disaster.	
Rationale	Business continuity seldom requires all the data ever generated by its processes. Backing up unnecessary data increases the cost of disaster recovery and negatively impacts RTO and RPO times.	
Consequences	Back-up sets are limited in size and therefore easier to manage and more cost effective. Back-up and restore times are reduced. A risk assessment is required to determine which data assets are to be included in backup strategies and which are left out.	

9.5 Conclusions

Efficient and effective recovery is needed to prevent a bad situation becoming worse. Choices, sometimes uneasy ones, have to be made about what to recover first in case of failures. Unplanned downtime of a smart energy system will probably have a negative effect on trust of Prosumers in companies that provide the services in a smart energy system and may, especially in the start-up phase of smart energy systems, impact Prosumers' willingness to participate in a negative way, which, in turn, affects the business case for companies involved in the smart energy system.

There are both operational and design aspects to disaster recovery. In this guideline we limit ourselves to the design aspects of recovery. In the realm of systems design, disaster recovery aspects manifest themselves as design choices that prevent, facilitate detection of and recovery from disasters.

10 Identification, Authentication, Authorization

Identification is the process of showing who you are. The identification is validated through the process of authentication, which verifies that you are who you say you are. Authorization is the process of verifying that "you are permitted to do what you are trying to do."

10.1 Explanation of the subject

A transaction is a communication between one or more actors where information is exchanged, which in turn leads to a relevant (i.e., may impact one or both actors) state change of the system and commercial settlement. Smart energy actors can be devices that supply or demand energy (or storage devices which can take on both roles) or represent a group of such actors as an intermediate.

In this context, the concepts of identification, authentication and authorization mean that an actor involved in a smart energy transaction is able to identify itself to another actor, where necessary can prove its identify to the other party and that it can be verified that an actor is actually authorized to participate in the information exchange or transaction. In some situations this is a reciprocal action, where both actors identify, authenticate and sometimes also determine each other's authorization.

Identification, authentication and authorization are also important in information exchanges that do not (directly) lead to a real-world state change but are used for system monitoring, reporting and auditing.

For a clear understanding of identification, authentication and authorization, it is needed to use unambiguous definitions of the concepts used and their mutual relations. In this document, the following definitions are used:

- **Actor:** an actor is a (physical) entity that acts within a smart energy system. Examples of actors are a Prosumer, the computer of the aggregator serving a local market and a smart meter.
- **Transaction:** a transaction is an exchange between two actors.
- **Identity:** an identity is used to identify an actor. An actor can have several different identities which can be used in different contexts. It is assumed here that an actor has a single identity per context. (Parts of) Other identities that are not used as identifier in a certain context can however be used as attributes/characteristics of the actor. Transactions can have either implicit or explicit identifiers. For example: actor John Doe's energy supplier has assigned him client number 12345. When making a call to his mother he probably identifies himself only with 'John', while in calling his colleagues he will use 'John Doe' as identifier. In contacting his energy supplier 'John Doe' will only be used for user-friendly communication, and thus as an attribute of the actor. The identifier used in this communication is '12345'.
- **Authentication:** authentication is the proof that the identity an actor claims to possess is valid. Depending on the context, stronger proof of identity might be required for authentication. As an example: cashing €100 from your bank account can be done at an ATM—a bank card and pin code are sufficient to proof your identity. However, for cashing €10000, you need to go to the counter and provide, besides your bank pas and pin code, your (registered) passport as well.
- **Authorization**: authorization is the right that is given to the identity an actor has provided. An example of authorizations (in the context of a smart energy system) is the right provided to an ESCo to collect the meter readings of a prosumer (read right).

10.2 Rationale of the subject

In a smart energy system transaction supply and demand come together in a way to reach a desired optimum. Optimal may mean lowest possible financial cost, lowest environmental impact, maximum profit, or optimal resource utilization or other desired and defined goal.

To ensure the envisioned outcome of a transaction, there must be trust between participating actors as in any real-world transaction. Trust means that each actor will fulfill the promise of the transaction, which is to produce or to consume the agreed amount of energy, at the agreed time and—where applicable—fulfill other (e.g., financial) obligations associated with the transaction. Trust will raise the likelihood that actors will continue to participate in future transactions benefitting the system, and that the system will engage enough actors for it to be able to function as a whole.

Trust is enhanced when the identity, authenticity and/or authorization of actors is known and verified. Trust is negatively impacted when actors cannot rely on the authenticity of actors, i.e., when identities can be abused (stolen, faked) or when transactions cannot be properly authorized, i.e. that the identity of an actor is not known as "compromised" or that the transaction is within the preset (agreed upon) limits.

Trust is further enhanced when the actual transactions are also carried out satisfactorily. Transparency of the trustworthiness of actors thus may also enhance the system, e.g. by evaluating or rating actors (e.g., suppliers, prosumers or device types) within the context of a transaction or even publically: rating is "explicit trust". For example regulators may want to publish relevant ratings of the entities they supervise. Rating of individual Prosumers may very well be limited to ensure at least a minimum level of access to the energy market, because of energy's nature as a basic human need and of course privacy concerns.

Authorization is principally the right of the Data Subject but can, and most likely will, be delegated to the Data Controller. In some cases the authentication, authorization and rating may be delegated to a trusted third party that plays no role in the actual transaction. As a special case, this delegation may also preserve the privacy of actors by hiding the "real" identities from the actors participating in the transaction. In certain cases, e.g., in a dispute, the identity of an actor may be restored in a controlled way by the third party.

10.3 Scoping

Although the principles might be applicable in a broader scope, the principles provided in the next section are written with the entities playing a role in a smart energy system in mind. Especially for the roles that exchange data with each other (Aggregator, BRP and DSO) the principles must be taken into account. For actors within a role, for instance the user account of an employee of a DSO, these principles are not a prerequisite for USEF compliancy.

10.4 Principles

Principle	Entities in smart energy systems have unique identifiers within their scope	#39
Description	A well-defined scope (application, time-based, etc.) determines the name space (or named or unnamed context) and the naming scheme of the identifiers used. Together they guarantee these identifiers are unique. The unique identifiers may be permanently or temporarily assigned to an entity, depending on the scope and application. Non-linkable (by certain entities) IDs aid in privacy preservation. A temporary ID is typically, directly or indirectly, linked to another permanent ID, but not linkable by participating entity at the time when a transaction occurs.	
Rationale	Uniqueness of identifiers enables associated entities to participate in transactions, entities to be authenticated, entities to be authorized for a particular transaction, the transactions to be auditable and thus achieving trust and transparency. If identifiers are ambiguous these mechanisms are harder or impossible to implement.	
Consequences	Naming schemes and name spaces should be carefully selected to match all system requirements, to be able to guarantee uniqueness now (and into a defined future), taking into account the projected number of entities and transactions in the system. Identifiers should be globally unique in a global scope: e.g., a MAC address. The scope should determine if portability of identifiers is allowed or prohibited. Privacy Enhancing Technologies (PET) may be used when dealing with identities in a Smart Energy System.	

Principle	Authorization is based on either an (authenticated) identity of an entity or (certified) properties of an entity	#40
Description	Examples of an (Authenticated) ID ■ Serial ■ Pseudo ID Examples of (Certified) properties ■ Product number ■ Manufacturer ■ Location ■ Capabilities ■ Class of product (e.g., Wi-Fi alliance) ■ Role	
Rationale	Keeping track of the provided authorizations requires a lot of administration. Instead of authorize each entity individually it is desirable to authorize a group of entities based on a (sub-) set of their common characteristics to reduce the load on the authorization system. This results in a single authorization to the group instead of an authorization for each single entity.	
Consequences	For each situation, it must be determined which authorization fits better; the authorization of the individual identities or authorization based on common properties. Individual authorizations are more granular and therefore can provide a perfect fit on the 'need to know' principle; the downside however is a substantial administration and the challenge to keep this administration up to date. Authorization based on properties is less granular, and might therefore give more rights than exactly needed; the administration needed however is substantially lower and therefore easier to keep authorizations up to date.	

Principle	Identities have a life cycle	#41
Description	A life cycle means that (de)centrally, identifiers are associated with a state according to a predefined scheme that is part of the name space. The number of implemented states depends on the application, preserving uniqueness means at least two states: Unused and In Use. The following states are proposed (not limitative): ■ Unused ■ Issued ■ In Use ■ Reserved ■ Retired ■ Blocked (abuse) ■ Suspended	
Rationale	A life cycle provides a way to distribute, manage and control the identities assigned to entities and transactions, and a way to derive meaning from the identifiers communicated by an actor to other actors participating in Smart Energy Transactions.	
Consequences	Depending on the size of an identifier, scarcity may require introduction of extra states to support reuse. ■ An identification system meets the performance and availability requirements of the services for which it is used. ■ Authentication mechanisms match the life cycle of the identity of the actors in the system. ■ Metadata elements should be available to record lifecycle states.	

Principle	The use of identity providers is supported	#42
Description	All actors in a smart energy system need an identity to participate. Instead of realizing an own identity provisioning service, an external identity provider can be used. Identity providers aid in issuing identities and typically also authenticate identities to actors participating in a transaction.	
Rationale	Actors may want to delegate identification and authentication to identity providers to achieve economy of scale. Identity providers have standardized interfaces and are also responsible for all supporting processes of the life cycle, with a special focus on granting an identifier to an actor based on other certified credentials. USEF encourages the use of identity providers, because it enables the portability of identities of the actors in the smart energy system, which eases the data portability which is mandatory in the new GDPR.	
Consequences	By using an identity provider for identifying and possibly authenticating actors, the control over the identities and their authenticity is delegated to a third party. This implies an explicit trust of the identity provider by all actors involved. Actors using identity providers must make strict agreements with the identity provider—for individuals, these agreements must preserve their privacy sufficiently, for organizations the authentication of the identities must be sufficient to ensure the needed authenticity.	

Principle	Authentication mechanisms are fit for use	#43
Description	Authentication mechanisms are fit for use implies that they are compatible with resources that are reasonably available for the actors to participate in the transactions. In addition, the authentication mechanisms must have a psychological fit with the actors that need to authenticate. This principle is tightly coupled with the principle 'Authentication mechanisms are risk-based' and is applicable wherever the authentication of entities and transactions is required. Examples of 'fit for use' authentication mechanisms: ■ In a "local" or a "limited risk" application not using authentication may be allowed by the responsible domain: a "trusted id" is used. ■ A standard identification/authentication mechanism for natural persons is the use of a username/password combination ('user credentials'). To assure fit for use, the user credentials are governed by a defined policy on at least password strength and expiration and checked by challenge-response instead of sending it in clear-text. ■ In case a stricter checking of authentication is needed, due to a higher risk profile, tokens are used like one-time passwords or physical-tokens.
Rationale	Authentication mechanisms are needed to verify the identity of an actor to a certain extent. The exact requirements are determined by the value of the authorizations that are linked to the identity that is verified. The higher the value of these authorizations, the more likely it is that a rogue actor will try to gain access to the identity, and thus the stricter the authentication must be. On the other hand, the stricter an authorization mechanism is, the more effort it takes (cost, time, etc.). Having a too strict authentication mechanism for the authorizations to be protected implies wasting resources.
Consequences	In order to determine what is 'fit for use', both a risk assessment is needed and the capabilities of the actors must be known with relation to the authentication mechanism. Note that 'fit for use' can/will change over time, making periodic evaluations of what constitutes 'fit for use' necessary. Using an authentication mechanism that doesn't fit the actors that need to authenticate their identity either prevents the functionality needed entirely (example: popping up a login screen for an automated process will halt the system until the process types in the user credentials) or results in a reduction of security (example: user writing down his hard to remember username and password).

Principle	Authentication mechanisms are risk-based	#44
Description	Authentication mechanisms are based on identified (by risk assessment) risk levels. Risk-based implies that the cost associated with the mechanism substantially outweighs the risks of not using the mechanism.
Rationale	An authentication mechanism is needed to assure an actor has the identity he claims to have to a certain extent. The implementation of such a mechanism is not free; it takes effort in both realizing the mechanism and in using the mechanism. These costs must be in line with the value that must be protected. Higher security risks will lead to stricter requirements on confidentiality and integrity of data. A high risk level will lead to more stringent security requirements, and thus to a stricter authentication mechanism.
Consequences	Risk-based implies a risk assessment is executed. See chapter 11 for a discussion about risk assessment methodologies.

Principle	Authorizations have a life cycle	#45
Description	A life cycle means that authorizations are associated with a state according to a predefined scheme. The numbers of implemented states depend on the application. The following states are proposed (not limitative): ■ Granted ■ Revoked ■ Suspended ■ Expired Authorization can be granted to a particular function or a particular object (or set of objects). Authorization may be one time, or for a certain number of transactions, or for a certain period which may be "indefinite".
Rationale	Authorizations change, depending on actions of actors, authorizations may be granted, revoked or suspended. An identity will always have a limited lifetime. At the end-of-life of an identity, authorizations will expire. Examples of events impacting authorization are: ■ Becoming a member ■ Incompliance with service conditions ■ Failure of a device or a device type ■ Abuse ■ Fraud ■ Expiry after o certain period of time.
Consequences	■ An authorization system meets the functional aspects of the services for which it is used by employing the right granularity of authorizations. ■ An authorization system has mechanisms to manage the authorization levels of actors (granting, viewing and revoking rights). ■ An authorization system supports verification of the authorization for a (single) transaction. ■ An actor is able to verify its own rights (and changes to it) in an authorization system: transparency. ■ An authorization system meets the performance aspects of the services for which it is used. ■ An authorization system has the ability to expire accounts, while giving a warning signal that an account is going to be expired.

Principle	Authorizations are classified into authorization types	#46
Description	An authorization type describes what an actor can do with the data he is authorized for. The minimum set of types is: ■ Read: data can be accessed, but cannot be altered ■ Change: data can be created, read, updated and deleted ■ Manage: type of authorization of data can be altered	
Rationale	Different types of actors have different needs of accessing data—being able to read certain data is sufficient for some actors, while other actors must be able to alter the data as well. Although it is possible to create an authorization for each different action, it is more feasible to combine authorizations to minimize the administration of the authorizations. Making a distinction between 'read', 'change' and 'manage' is in most cases sufficient to prevent unwanted access to data.	
Consequences	By combining authorizations actors can gain more authorization than they actually need. An actor who needs the possibility to change certain data is able to delete it as well, even if he is not supposed to do so. Depending on the data classification, this might be an unwanted situation—in these cases, the authorization categorization must be more granular. An actor with 'manage' authorization does not have the ability to read or change the data (segregation of duties). He can however provide 'read' or 'change' authorization to himself.	

Principle	Detected unauthorized transactions (or attempts to) are managed according to a predefined policy	#47
Description	When a smart energy system detects unauthorized actions, or attempts to unauthorized actions, it needs to generate an event in the system log. Depending on the severity of the action, an alarm that is visible in a maintenance room or dispatch center is generated; in case of a severity of the highest category, automated protection measures must be taken to prevent the breakdown of the system.	
Rationale	In addition to not granting an actor the right to perform a certain transaction, to safeguard system operation additional measures are needed to prevent hacking the system. These measures must be planned for in advance, as are the methods of detecting unauthorized transactions. The system should be able to separate the affected part of the system, to prevent further damage.	
Consequences	When detected, an alarm may be generated upon which defined actions may be taken, in an automated fashion or requiring human intervention or initiation. The system may enter a special "breach" state or special operating mode, followed by a controlled recovery from the special operating mode.	

Principle	An actor's actual behavior feeds back into the identification/authentication system, setting "trust levels" (rating = explicit trust).	#48
Description	Based on the authorizations given, an actor is expected to perform actions. This expected behavior is compared to the actual behavior of the actor. In case actual and expected behavior are in line with each other, the trust level of the actor is raised; in case actual behavior is not in line with the expected behavior, it is lowered.	

Rationale	Identification and authentication are means to assure an actor is actually the entity he claims to be, in order to trust him enough to provide him with the authorization needed to perform certain actions. By using trust levels based on actual behavior, the expected outcome of future actions can be predicted with a higher certainty, making the system more reliable.
Consequences	The algorithms of granting/revoking rights/level must be: ■ Risk-based; ■ Transparent. Rating disputes may lead to the need for arbitration. However, it is recommended to objectively rate the compliance of an actor to the agreed upon transactions or other specified behavior or accuracy, as opposed to rating by human actors who may be biased or use subjective rating criteria. This makes ratings more transparent, and although it does not eliminate the need for arbitration, it does make conflict resolution easier.

10.5 Conclusions

To generate trust and as a result of that, increase the number of transactions by more and more actors in a smart energy system, each actor needs to be able to uniquely identify itself to other actors, where necessary prove its identity and be certain that its counterpart is actually authorized to participate in the transactions.

For this, naming schemes are needed to support unique identification of actors and transactions.
Identity providers may be used, supporting the identification and authentication of actors. Federated identity providers may be used to support the wide array of actors in a smart energy system.

Authorization systems need mechanisms to maintain the authorization levels of actors (granting and revoking rights) and to support verification of the authorization for a single transaction based on the (authenticated) identity or other properties of an actor, and allow for an actor to check its own rights.

An actor's actual behavior may be rated and fed back into the authorization system, setting "trust levels".

11 Risk assessment

11.1 Explanation of the subject

Privacy & security issues can result in all kinds of adverse effects for an organization. These effects vary wildly in scope and severity. Reputation loss from leaking customer data is an issue that is very different from manipulating energy market data, in terms of likelihood of occurrence and severity. How do we decide where to allocate our efforts and capital? This is where risk assessment comes in.

The goal of risk assessment is to understand and where feasible reduce risks. Risk assessments can be qualitative or quantitative. Quantitative methods are preferred, especially when the outcome of risk assessments is to be used to make and/or justify design decisions that carry substantial implementation or operational costs but quantitative risk assessments are not trivial to perform. Many methods for performing risk assessments exist: the ENISA inventory of risk assessment methodologies [28] alone already contains 17 different methodologies. This inventory is far from complete, implying over 25 different methodologies are (more or less widely) used all over the world. An in-depth analysis of the FAIR [29] methodology showed a good fit with USEF's design goals:

- FAIR is an open methodology, developed by the open group;
- The workload associated with a FAIR-based risk assessment is low compared to most other risk assessment methods;
- FAIR is relatively easy to understand for non-security people, as are most of the people working with USEF;
- FAIR is available free of charge.

11.2 Rationale of the subject

During the design and build phases of smart energy systems potential privacy & security issues are likely to be identified. In order to efficiently and cost-effectively implement measures and controls to mitigate these issues the risks associated with them need to be determined in a common and unbiased way. This is where risk assessment comes in. Using an agreed-upon framework for risk assessment, risks can be identified, classified and, depending on the method chosen, quantified, allowing for a rational approach to reducing risks arising from privacy & security issues.

11.3 Scoping

USEF uses a risk assessment method to:

- Identify and quantify or at least classify risks with the aim of improving the privacy & security aspects of the USEF. Risks that are not quantifiable or classifiable are not actionable and therefore of very limited use in a design process.
- Guide the implementation and operationalization of USEF.

The first bullet mandates that risk assessments are an integral part of the design process, safeguarding Privacy & Security by Design. Note that Privacy & Security by Design requirements are derived from Legal Protection by Design requirements.

The second bullet states that risk assessment provides the boundaries for the implementation of smart energy systems and provides input for the risk management process of organizations implementing, or interacting with, smart energy systems such as USEF.

The Security in Privacy & Security relates to Cyber security, not physical security. USEF does not make statements about the quality of door locks or the ferociousness of guard dogs. It is however assumed that the implementation of physical security does not weaken overall system security.

Cyber security relies on information security, application security, network security, and Internet security (ISO/IEC 27032:2012). Risk Management is the identification, assessment, and prioritization of risk. It deals with operational processes and we therefore consider it to be outside the realm of USEF.

11.4 Principles

Principle	Risks are categorized or quantified	#49
Description	All risks are categorized (using a fixed set of categories like low, medium, high) or quantified (using a numeric scale) using a risk assessment methodology which is most appropriate for the management and control of the respective types of risk.	
Rationale	Risk assessments identify the risks present in a smart energy system with the purpose of being able to gauge which mitigating actions need to be implemented to meet the specified risk appetite. To this end, risk assessments need to yield at least categorized but preferably quantified. Using quantified risks mitigating actions are more easily justified and communicated to stakeholders. When resorting to qualified risks only, proportional measures are difficult to identify.	
Consequences	Not all commonly used risk assessment methodologies are appropriate for use in a smart energy environment. Especially during the design and implementation phases risk assessment methods that yield quantifiable risks should be used.	

Principle	Risk assessments are integrated into the smart energy system life-cycle	#50
Description	A smart energy system's life cycle encompasses, at a minimum, design, implementation, operation and decommissioning phases. During all these phases risks exist which should be identified, quantified and mitigated where needed[2].	
Rationale	Modern systems, such as our energy system, are complex and dynamic systems that change during their life-cycle. Designs change, new designs lead to new implementations and the context in which a system is operated can change. Each of these changes can induce new risks or change existing risks. In addition, risk mitigating measures change the risk profile of (sub)systems. In order to have a firm handle on risks during all stages of the life cycle of a smart energy system, risk assessments should be an integral part of life-cycle management.	
Consequences	■ The triggers for and frequency of risk assessments is documented and communicated for all life-cycle stages. ■ The responsibility for performing risk assessments for all life-cycle stages is documented and communicated.	

Principle	Risk assessment is based on an auditable method	#51
Description	Risk assessments are performed using a method that is auditable, i.e. it yields results that are reproducible and independently verifiable. Audits can be organized internally where the goal is internal control and promptly recognize and mitigate identified vulnerabilities. External audits may be organized when external monitoring or compliance with laws and regulations is required.	
Rationale	Audits help to detect possible vulnerabilities and to recognize implementation errors that can subsequently be resolved in cooperation with the audit committee. Audits thus help to improve designs, implementation and operations of smart energy systems and therefore help to establish trust and acceptance. Since risk assessments are an important tool in guiding design and implementation choices the method used for risk assessments should be auditable.	
Consequences	■ The results of risk assessments are documented. ■ The results of both internal and external audits are used as input for improving the risk assessment process. ■ The results of external audits include risk assessment data.	

11.5 Conclusions

Risk assessment plays an important role in categorizing and quantifying risks, which is a prerequisite for rationally managing design and implementation trade-offs that arise from identified privacy & security issues. To do so, a method needs to be selected for performing risk assessments. After a selection and review process USEF has decided to recommend the FAIR methodology, which is a good fit with USEF's design goals , for the design and implementation phase. Together with a set of risk assessment principles this can be used to guide the application of many of the privacy & security principles laid out in this guideline.

12 Summary

12.1 Value creation

The introduction of smart energy systems will see an explosion of available, granular data on energy production and consumption. There is value in this privacy data for all stakeholders but the economic and other indirect benefits to these stakeholders could be antagonistic in outcome. DSOs and Aggregators profit from proactive network maintenance and improved operational efficiency, for example, where customers can realize efficiency and monetary savings, and enjoy new services such as integrated home management. Social welfare increases through aggregated savings and environmentally preferred choices. Perceived privacy risks, occurring when people lack control over the disclosure of personal information, can however hamper the introduction of smart energy services. Privacy concerns will be lowest when the perceived benefits exceed the perceived risks. In order to maximize the chance of a successful introduction of smart energy systems energy companies should build trust and strive for maximum transparency.

12.2 Need to know

A fundamental cornerstone of security is the principle of "Need to Know": access to data or information is only granted after having established that the intended recipient needs access to perform his or her legal and/or contractual obligations. This principle is extended to the collection and processing of data. In the first case it means that a proper method for identification, authentication and authorization must be in place anywhere data is collected, processed and stored. In the last case it means that data should only be collected for a specific, well-defined, purpose and should not be more than absolutely necessary for said purpose. Data should not be kept longer than necessary: the proper disposal of the data is as important as the collecting of it.

12.3 Data Management

Data management is a very important topic for USEF. Not only are there many legal obligations that have far-reaching design and implementation consequences for data management, such as the need for consent and data portability, transparent and sophisticated data management is also an important enabler for trust. Mutual trust between Data Subjects, Controllers and Processors based on unambiguous guidelines is a pre-condition for large-scale participation in smart energy systems and a driver for value creation. Data Management in smart energy systems centers on two main topics: data minimization principles, representing a conservative approach where the Data Subject does not a priori trust the peer and ethic of knowledge principles which refer to the usage of data by the Data Collector.

12.4 Operations Management

Operations Management deals with the design and management of smart energy products, processes, services and supply chains. It concerns the acquisition, development, and utilization of resources that businesses need to deliver and receive energy on the smart grid at the moment their clients want it. The scope of OM ranges from strategic to tactical and operational levels.

Typical strategic issues include determining the size and location of the smart energy chain, deciding on the structure of service and telecommunications networks and designing smart energy technology supply chains. Making privacy & security an integral part of the design one can achieve a higher levels of security at lower costs. Tactical issues include sustainable smart energy architectures, project management methods and smart device selection and replacement. Operational issues include privacy & security, energy production scheduling and control, inventory management, quality control and inspection, and equipment maintenance policies and last but not least compliancy with the relevant legislation.

12.5 Authorization

Identification is the process of showing who you are, Authentication is the process of verifying that "you are who you say you are" and Authorization is the process of verifying that "you are permitted to do what you are trying to do". In the context of a Smart Energy System, a Smart Energy Actor, a device which supplies or demands energy or represents a group of such actors as an intermediate, needs to be able to identify itself to other actors, where necessary prove its identity and be certain that its counterpart is actually authorized to participate in the transaction and vice versa.

For this, naming schemes are needed to support unique identification of actors. Identity providers may be used, supporting the identification and authentication of actors. Federated identity providers may be used to support the wide array of actors in a Smart Energy System. Authorization systems need mechanisms to maintain the authorization levels of actors (granting and revoking rights) and to support verification of the authorization for a single transaction and for an actor to check its own rights.

An actor's actual behavior may even feedback into the authorization system, setting "trust levels". The availability and performance requirements of a Smart Energy System greatly impact the design and implementation of its authorization system.

12.6 Rules and policies

Rules play an important role when it comes to privacy & security aspects of smart energy systems. European legislation and the national laws derived from it set the boundary conditions for all actors in a smart energy system, for example with respect to privacy. Where the existing legal framework is unclear or insufficient, parties can enter into a contract to resolve any ambiguities. The governing laws and contracts are typically translated into more technical and operational policies for data management, user authorization etc., down to the level of password rules and rules for 3rd party access.

Outside the realm of legislation, policies come into play as well, when it comes to policies asset security classification, compliance and recovery procedures.

Appendix 1 Glossary

BRP	Balance Responsible Party
DSO	Distribution System Operator
ESCo	Energy Service Company
EV	Electric Vehicle
GDPR	General Data Protection Regulation
Grid	Network for the transport and distribution of energy
MCM	Market-based Coordination Mechanism
P&S	Privacy & Security
Prosumer	A consumer which is capable of producing energy as well
Settlement	Determining the energy production and consumption and used flexibility as preparation for the billing process.
Supplier	Has a contractual relationship with Prosumers to source, supply and invoice energy
TSO	Transmission System Operator
USEF	Universal Smart Energy Framework

Bibliography

[1] G. Bösehans, „Privacy concerns: When they are raised and how they can be avoided – A literature review,“ Rijksuniversiteit Groningen, Groningen, 2012.

[2] A. Castillo, "Smart Grid Integration: Tradeoffs in Privacy and Value Creation," DNV KEMA, Groningen, 2012.

[3] M. Hildebrandt, “Legal Protection by Design in the Smart Grid,” Smart Energy Collective, Arnhem, 2013.

[4] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," Wired magazine, 21 July 2015. [Online]. Available: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/#. [Accessed 20 October 2015].

[5] EnergyIT.com, "Gainsvill Green," 14 5 2014. [Online]. Available: http://gainesville-green.com/.

[6] CEN, "European Guide to good Practice in Knowledge Management - Part 5: KM Terminology," CEN, Brussels, 2004.

[7] European Parliament, "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," 23 November 1995. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. [Accessed 27 May 2014].

[8] European Commission, "Proposal for a 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)," 25 1 2012. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF. [Accessed 28 5 2014].

[9] Information Commisioner's Office, "Key definitions of the Data Protection Act," 15 5 2014. [Online]. Available: http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions.

[10] A. Westin, Privacy and Freedom, NewYork: Atheneum, 1967, pp. 487-.

[11] United Nations, "The Universal Declaration of Human Rights," 12 5 2014. [Online]. Available: http://www.un.org/en/documents/udhr/index.shtml.

[12] R. Mayer, J. Davis and F. Schoorman, "An integrative model of organizational trust," Academy of Management Review, pp. 709-734, 1995.

[13] G. Gundlach and P. Murphy, "Ethical and legal foundations of relational marketing exchanges," Journal of Marketing, pp. 35-46, 1999.

[14] C. Tanner, D. Medin and R. Iliev, "Influence of deontological versus consequentialist orientations on act choices and framing effects: When principles are more important than consequences," European Journal of Social Psychology, pp. 757-769, 2008.

[15] P. Schwartz and D. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information," New York University Law Review, p. 1814, 2011.

[16] A. Beldad, T. Van der Geest and M. Steehouder, "Shall I Tell You Where I Live and Who I Am? Factors Influencing the Behavioral Intention to Disclose Personal Data for Online Government Transactions," International Journal of Human-Computer Interaction, pp. 163-177, 2012.

[17] A. Benlian and T. Hess, "The Signaling Role of IT Features in Influencing Trust and Participation in Online Communities," International Journal of Electronic Commerce, pp. 7-56, 2011.

[18] A. Kapczynski, "The Cost of Price: Why and How to Get Beyond Intellectual Property Internalism," UCLA Law Review Vol. 59, Iss. 4, pp. 970-1026, 2012.

[19] A. Barnett and B. Yandle, "The End of the Externality Revolution," Social Philosophy and Policy. Vol. 26, pp. 130-150, 2009.

[20] European Commission, 14 5 2014. [Online]. Available: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

[21] P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals," Computer Law & Security Review. Vol. 28, pp. 130-142, 2012.

[22] I. Jamieson, "Smart Meters - Smarter Practices Addemdum March 2012," EM Radiation Research Trust, Leicester, 2012.

[23] Wikipedia, "OSI model," 15 5 2014. [Online]. Available: http://en.wikipedia.org/wiki/OSI_model.

[24] L. Parziale, D. T. Britt, C. Davis, J. Forrester, W. Liu, C. Matthews and N. Rosselot, TCP/IP Tutorial and Technical Overview, International Business Machines Corporation, 2006.

[25] Wikipedia, "Availability," 23 May 2012. [Online]. Available: http://en.wikipedia.org/wiki/Availability. [Accessed 22 June 2012].

[26] CEN-CENELEC-ETSI Smart Grid Coordination Group, "Smart Grid Information Security," CEN-CENELEC-ETSI, 2012.

[27] Wikipedia, "Disaster recovery," [Online]. Available: http://en.wikipedia.org/wiki/Disaster_recovery#Classification_of_disasters. [Accessed 15 5 2014].

[28] ENISA, "Inventory of Risk Management / Risk Assessment Methods," [Online]. Available: http://rm-inv.enisa.europa.eu/methods/rm_ra_methods.html. [Accessed 15 5 2014].

[29] "Factor analysis of information risk," [Online]. Available: http://en.wikipedia.org/wiki/Factor_analysis_of_information_risk. [Accessed 06 01 2015].

[30] M. Hansen and A. Pfitzmann, "Privacy Terminology," July 2010. [Online]. Available: http://tools.ietf.org/html/draft-hansen-privacy-terminology-00#page-39. [Accessed 20 5 2014].

A solid foundation for smart energy futures

www.usef.energy