TASK FORCE SMART GRIDS

EXPERT GROUP 2: REGULATORY RECOMMENDATIONS FOR DATA SAFETY, DATA HANDLING AND DATA PROTECTION

REPORT

ISSUED: FEBRUARY 16, 2011

TABLE OF CONTENTS

1 INTRODUCTION AND SCOPE OF REPORT

To facilitate and support the process of an EU-wide Smart Grid roll-out, the European Commission decided to set up a Task Force on Smart Grids. The Commission invited all relevant institutional actors and market stakeholders to the first Steering Committee meeting. The Steering Committee agreed to establish three Expert Groups who will jointly develop a common vision for the implementation of Smart Grids in Europe and identify regulatory recommendations and key issues that need to be resolved.

The ultimate goal of this Work Program is to identify and produce a set of regulatory recommendations to ensure EU-wide consistent and fast implementation of Smart Grids, while achieving the expected Smart Grids' services and benefits for all users involved.

The key deliverable of the Smart Grid Expert Group two (EG2) is to identify the appropriate regulatory scenario and recommendations for data handling, data security and data protection. The aim is to establish a data privacy and data security framework that both protects and enables. In particular, the expert group was asked to focus on the following topics:

- Identify the benefits and concerns of customers when becoming active actors in the Smart Grids' retail markets.
- Overview of European legislation on data protection and checking whether further protective measures should be put in place
- Identify possible risks in the handling of data, security and data protection, include data exchange issues.
- Identify ownership of data and access rights.
- Identify responsible parties for data protection
- Analyse how these issues should be handled along the value chain
- Develop a framework in which data can be used
- Recommendations for Information and Communication of Smart Grid benefits to consumers and politicians

In the report the different areas have not been given equal weighting, focus of the Expert Group has been on data security and privacy.

2 EXECUTIVE SUMMARY

This report is the output of Expert Group 2 which focused on identifying the appropriate regulatory scenario and recommendations for data handling, security and data protection.

It was recognized that although there were many common Smart Grid definitions already used in the development of EU Standards and within the legislative framework, that there were no common definitions related to Smart Grids. The appropriate definitions necessary are specified within the body of the report for such terms as technical data, location data, etc. Wherever legal compliance is required, we use terminology as defined in the appropriate EU directives, e.g., personal data as defined in Directive 95/46 EC.

The legal base in Europe is founded on the “European data protection legal framework”. The basic privacy and data protection issues that derive from the EU Privacy Directives and treaties require that an assessment needs to be undertaken to ascertain if the data being processed is of a personal nature or not. If it is personal data then there are privacy issues that need to be addressed and that this processing of personal data must be based on a sound legal foundation.

Whereas, in Europe energy theft and privacy are the most important concerns related to Smart Grid implementation, in other parts of the world (e.g. in the US) it is energy theft and malevolent attacks that are the main concerns.

The purpose, design, functionalities and implementation of the Smart Metering system determines to a large extent whether or not it will comply with privacy and data protection legislation. Therefore, from the beginning, legislation on privacy and data protection must be taken into account as important requirements in the design of Smart Metering systems.

Introducing Smart Grid/Meter functionalities as laid out in the 3rd Energy Package raises a number of issues and expectations from various stakeholders e.g. Grid Users, End Customers, Consumer Groups, etc. Whilst there is a general consensus that Smart Grid/Meters are beneficial for all involved, as with any new technology there are new risks, these include certain concerns in relation to data security, handling and data protection.

Specific for the data privacy aspects, the European consumer groups are asking for clear regulation around frequency of meter reading and usage of data. It is stressed that only data necessary to perform Smart Grid tasks should be collected and utilised. The use of personal data for other purposes than the legal duties of the DSO requires freely given specific and informed consent from the customer.

At the same time, whilst acknowledging benefits, Smart Grid/Meters and wider related infrastructure should be designed for both privacy and security to levels that are in line with the risks for concerning stakeholders, as well as ensure the realisation of potential benefits of Smart Grids/Meters.
The report provides detail of other industries experiences in the area of data security, privacy and data handling and draws out specific learning points for Smart Grid development. A key conclusion from this review was that the Expert Group should recommend to the European Standards Organisations (ESOs) that they should mandate that Smart Grid products and solutions should be designed from the start with appropriate levels of data privacy and security at their core.

The data security section of the report, together with appropriate parts of the appendices focus on reviewing existing standards and where there might be gaps related to Smart Grid development. It also identifies appropriate responsible ESOs for each area to oversee any required standards development.

The Expert Group concluded that there was clearly a gap within EU standards relating to the handling and security of data within the area of Smart Grids. However, there are broader standards, guidelines and codes of practice in place within other industries such as the Banking and Payment Card Industries or the Payment Card Industry Data Security Standard PCI-DSS outlining the management of personal and credit card data by comparing the risks and related requirements, a judgment can be made to what level these solutions are applicable for the Smart Grid processes and ESOs can develop standards to fill identified gaps.

Summary of Recommendations

The recommendations made by this expert group are summarized below:

1. The Expert Group recommends that SG-EG2 is tasked with assessing how the privacy and data protection issues of Smart Metering and Smart Grids could be covered by and/or fit into the existing EU privacy and data protection framework or, if this is not possible in a sufficient manner, in detailing out the necessary additional legal framework to regulate those issues and in proposing particular privacy requirements for the stakeholders in Smart Grids to create a EU-wide, detailed privacy standard for Smart Metering and Smart Grids.
2. ESO’s should mandate that Smart Grid products and solutions are designed from the beginning with appropriate data privacy and security at their core.
3. Regarding security:
   - ESO’s should be tasked with updating, extending or developing new standards covering the security aspects of Smart Grid interfaces based on European requirements.
   - ESOs joint working group should review the Expert Group recommendations and list of relevant standards, and add the latest amendments, additions and future work required before starting any new standardisation work, based on still to be defined requirements.

- ESO's are tasked with evaluating the current state of cryptographic primitives through their relevant technical committees and make available the most appropriate technologies within the relevant standards framework. This should ensure
    - Not to preclude the initial adoption of symmetric key cryptography followed by smooth migration to asymmetric cryptography if required;
    - A business model is investigated to make the creation and maintenance of certification authorities (needed for asymmetric cryptography) possible;
    - A study is conducted on how to handle multi-national key management (e.g. one supra-national European certification authority certifying national certification authorities) and who should be in charge of performing this key management activity.
- One generic model is adopted by all European countries, for key management, and security and privacy principles, regardless of the communication technology or protocol, subject to appropriate and necessary allowances for different market models.
- These security and privacy principles should be relevant to not only Smart Meters, but also other devices or bodies in the Smart Grid if communicating consumption data.

4. With regard to data handling
    - Further pilots need to be done in the area of data handling[1], to propose a list of high level principles tuned to the Smart Grid environment, by which Smart Grid operators can design their systems and processes.
    - After the above has taken place a paper should be produced and presented to the CEN, CENELEC, ETSI joint working group, highlighting the additional detailed standardization required in this area.
5. With regard to data privacy
    - Distinguish between personal and non personal data;
        - Personal data is considered as specific data and can be traced back to the individual consumer whereas non personal data could be aggregated data and does not contain references to natural persons.
    - To ensure data safety and security within an intelligent network a clear division of roles and responsibilities regarding ownership, possession and access to data, read and change rights[2], etc. has to be defined.
        - This expert group (SG-EG2) should be tasked with providing the relevant detail necessary for Member States to identify the different data elements and define roles and responsibilities, including handling, possession and access to data.
        - Further work needs to be done around consent models – how consumers are able to control the use of their own data
        - Further work will be needed on potential monitoring and enforcement mechanisms around data protection and privacy rules.

[1] Consultation with the banking industry and payment card industry could be considered
[2] Used terms need to be validated against the EU data protection directive.

3 DEFINITIONS

Data Types
There are many data types already in existence and commonly recognised within the EU standards and legislative framework. However there are no common definitions relating to Smart Grid data. It would appear that in other areas of data protection, given data can have different classifications dependent on what it is to be used for (*ICO- Data Protection Technical Guidance determining what is personal data, 2007)*. Note that the definitions of data types are not exclusive, i.e., a data item can fall into several categories simultaneously. Some definitions are for purpose of explanation in this document, while others are externally defined and have a legal meaning.

Personal data
Source: Directive 95/46/EC European Union Directive on Data Protection:
Definition of personal data Article 2: For the purposes of this Directive: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Furthermore, references to the interpretation of personal data refer to the definition of the Directive 95/46 and the interpretation given by the Article 29 Working on the concept of personal data[3].

Location data
Absolute location is the actual spot on the planet where something is. A good example would be the latitude and longitude of a place. For instance, Lake Maracaibo of Venezuela is at 10°39' N latitude and 71°36' W longitude. In addition, an IP address is also a way to locate physical equipment. For Smart Grids the position of individual assets can be identified via a Global Information system (GIS). GIS is a system of hardware and software used for storage, retrieval, mapping, and analysis of geographic data. Spatial features are stored in a coordinate system (latitude/longitude, state plane[4], UTM[5], etc.), which references a particular place on the earth. Descriptive attributes in tabular form are associated with spatial features. Spatial data and associated attributes in the

[3] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf
[4] State Plane Coordinate System (SPCS). The SPCS is primarily used in engineering applications by utility companies and local governments for doing accurate surveys
[5] (UTM) Universal Transverse Mercator. A map projection system for global mapping. UTM divides the world into 60 zones each of 6 degrees longitude wide, extending from 80 degrees latitude south to 84 degrees latitude North.

same coordinate system can then be layered together for mapping and analysis.

Technical data (Smart grid)
Data that is gathered from metering, distribution, or transmission assets in order to assess the performance of the energy network, network problems, or potential future problems, security breaches and energy theft. The data is used for safety, revenue protection (i.e. fraud detection), and security of supply purposes. This data can be linked to individual supply points or aggregated data representing substation supply lines. In case of a DSO, aggregated date could be used to operate the network and to ensure that the network is not in a critical condition.
This data should not be able to be linked to individuals or households, as long as this data is not gathered on an individual supply point level (as in a household or a charging pole). When this data can be linked to a person it is also personal data and rules regarding personal data should apply.

Metering Ownership
In most European States the Distribution Network Operator provides and operates the relevant electrical infrastructure and they also own and provide the meter. Only in countries such as UK and Germany there are fundamental variants to this meter ownership model. The most disaggregated example of this is provided by the UK where competition has been introduced across the services provided by metering.

Key functions are:

- *Meter Operator* which can additionally be split into
    - *Meter Asset Provider (MAP)* – providing the funds and providing the meter
    - *Meter Asset Manager (MAM)* - bearing the responsibility for installation, commissioning, maintenance etc.
- Data Collection - collecting data from the meter responsible for measurement and communications equipment.
- Data Aggregation - aggregating all the meter readings for each Party to the Balancing and Settlement Code (BSC).

4 CURRENT EUROPEAN FRAMEWORK - PRIVACY

The legal base in Europe is founded on the “European data protection legal framework”. It has to be noted, that each country has the latitude to implement the directives in national laws, with national flavour. Therefore, a country has the possibility to be more protective. A common denominator of the regulations has to be defined to approach an EU wide Smart Grid.

The basic privacy and data protection issues that derive from the EU Privacy Directives and treaties and that need to be taken into account when discussing Smart Metering are:

a.) An assessment must take place to ascertain if the data processed in Smart Metering is personal related or not; meaning that the data can be related to a natural person or not. (For example: the meter ID is personal related data because the grid operator could link it to a customer). If it is personal related, there are privacy issues that need to be solved. If it is not personal related, there is no privacy issue. Therefore, one issue is to assess if and how Smart Metering technology could be designed to avoid the use of personal related data to avoid privacy issues from the beginning at the same time satisfying the needs and requirements of all stake holders involved.

b.)If personal related data is processed, there must be a legal basis for such processing which as to Smart Metering could be:

(i) a legal duty to install Smart Meters to be imposed by the EU or the member states (which would need to be in conformity with current law and regulations)

(ii) consumer consent

(iii) the necessity to use the data to fulfil the contract with the consumer

(iv) the prevailing interest for grid operation, which for example could be the need for grid operators and energy distributors to collect data to optimize the network, assure network functioning, optimize energy savings etc. Which data items qualify here is to be agreed by appropriate data protection authorities, conditions according to Directive 95/46 EC and similar European legislation need to be taken into account.

The privacy concept depends as well on a clear definition of the roles of the stakeholders in the Smart Grid. "Players" in privacy are the data subject, the data controller, the data processor and any third party that might get the data. Expert Group 2 is depending on the results of this "players" definition of the other Expert Groups.

It furthermore should not be overlooked that privacy does not only concern consumer privacy, but as well the privacy of the other stakeholders in the Smart Grid as some countries within the EU, like Austria, explicitly protects the data of companies (legal entities) as well. Therefore, access to data and exchange of data should not only be assessed from the consumer perspective, but as well from the perspective of DSOs (or energy suppliers in the case of the UK and Germany), which not only need to protect the personal data they store, but as well as their own (business) data.

c.) Directive 2002/58/EC[6] and 2006/24/EC[7]
Directive 2002/58 supplements Directive 95/46/EC regarding electronic communications services. Amongst others, the Directive lays down provisions regarding confidential communications, the processing of traffic data and location data.

The applicability of these specific data protection Directives in relation to Smart Metering needs to be assessed.

The purpose, design, functionalities and implementation of the Smart Metering system determines to a large extent whether or not it will comply with privacy and data protection legislation. Therefore, from the beginning, legislation on privacy and data protection must be taken into account as important requirements in the design of Smart Metering systems.

Recommendation 1:

The Expert Group recommends that SG-EG2 is tasked with assessing in how the privacy and data protection issues of Smart Metering and Smart Grids could be covered by and/or fit into the existing EU privacy and data protection framework or, if this is not possible in a sufficient manner, in detailing out the necessary additional legal framework to regulate those issues and in proposing particular privacy requirements for the stakeholders in Smart Grids to create a EU-wide, detailed privacy standard for Smart Metering and Smart Grids.

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.
[7] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.

5 STAKEHOLDER ANALYSIS

5.1 Smart Grid Stakeholders

- Grid users including/composed of grid operators, grid customers and meter operators
- End customer (domestic or commercial)
- Municipalities including energy retailers
- Politics
- Industries
- Consumer organizations
- Politics/society

Introducing Smart Grid/Meter functionalities as laid out in the 3rd Energy Package raises a number of issues and expectations from various stakeholders. Whilst there is a general consensus that Smart Grid/Meters are beneficial for all involved, certain concerns are raised. These can be summarized around security, privacy and data handling.

Specific for the data privacy aspects, the European consumer groups are asking for clear regulation around frequency of meter reading and usage of data. It is stressed that only data necessary to perform Smart Grid tasks should be collected and utilised. At the same time, whilst acknowledging benefits, Smart Grid/Meters should be designed for privacy and security.

5.2 Smart Grid and Smart Meter benefits – generic comments

The Smart Meter is key for the introduction of some services and functionalities of Smart Grids. Thus it has been agreed on dividing the benefits of Smart Meter and Smart Grid for each stakeholder group.

Smart Grid benefits for stakeholder	
Grid operator	• Distribution network stability & performance can be managed within the limits of an ever changing market • Cost savings due to an optimized facility utilization and enhanced efficiency • Predictive maintenance and “self-healing” responses to system disturbances • Automated maintenance and operation • New opportunities to improve grid security • Improved resilience to disruption

	• Increased lifespan of existing infrastructure • Reduction of technical losses
Grid user	• Expanded deployment of feed-in tariffs by renewable energy sources • Peak energy demand is met more efficiently and with less detriment to the environment • Increased sustainability • Effective support of transnational electricity markets by load-flow control to alleviate loop-flows and increased interconnection capacities • To enable new services still to be defined and developed
End customer	• Option to plug-in electric vehicles and new energy storage options • Increasing reliability of power supply (fewer and shorter outages) • Decentralized energy (micro generation) • Elimination of estimated bills • Advanced ability to feed-in decentralized Renewable Energy Sources • Better match energy consumption with production
Municipalities	• Advanced ability to feed-in decentralized Renewable Energy Sources • Positive image as an innovative community • Cost reduction through energy conservation and efficiency • Sustainability
Politics/society	• Increased market competition • New jobs • Achievement of climate targets • Securing the business location • Peak energy demand is met more efficiently and with less detriment to the environment
Industries	• New product opportunities • New Business areas

Smart Metering benefits for Stakeholder:

End customer	• Enable improved provision of energy consumption information for customers • Increased awareness of energy consumption • Control over energy usage and cost • More transparent pricing strategies • Increased consumer choice • Faster and more efficient switching • Flexible and more differentiated tariffs
Grid operator	• Information about changes in consumer consumption patterns

	• Increased possibility to control demand • Limiting fraud and reducing commercial losses • Flexibility to add metering for EV charging and Distributed Energy Resources (DER)
Municipalities	• Positive image as an innovative community • Cost reduction through energy conservation and efficiency
Politics/society	• Increased market competition • New jobs • Securing the business location • Reach the EU 20-20-20 goals and comply to related Directives
Industries	• New product opportunities • New Business areas

It should be noted that many of the consumer benefits will not be realised without adequate safeguards and a strategy to deliver these benefits. A systematic review of retail market protections will need to be carried out to ensure that they are fit for purpose in a smart world and action taken to ensure that customers can engage effectively in this new energy services market. This is particularly the case for low income and vulnerable consumers.

6 BENCHMARK OTHER INDUSTRIES AND INTERNATIONAL EXPERIENCE

6.1 Other Industries[8]

6.1.1 Banking

Electronic Banking and the Risks it posed for Banks

Banking sought to address the impact that wider introduction and integration of electronic banking would have on their existing risk management policies and processes. The integration of e-banking with their legacy systems meant they needed to reassess their integrated risk management approach to address this new risk.[9] This led to the development of a set of Risk Management Principles for Electronic Banking. These 14 principles were grouped under 3 broad headings of

A. Board and Management Oversight (Principles 1 to 3)
B. Security Controls (Principles 4 to 10)
C. Legal and Reputational Risk Management (Principles 11 to 14)

The key points to be noted from the banks experiences with the introduction of e-banking were to ensure that the security services Authentication, Access Control, Non-Repudiation, Confidentiality and Integrity and the availability were addressed appropriately.

Key findings for Smart Grid:

- *Security is a path, not a destination. Security is about risk management and implementing effective counter measures.*
- *Privacy needs to be considered at the design stage of Smart Grids, since the industry players in this development do not have the financial muscle of the Financial Sector, and they need to maintain consumers trust to deliver the assumed behaviour changes necessary to fully deliver the potential benefits of Smart Grids for all of society.*
- *The dilemma the energy sector needs to address up-front is how best to deliver appropriate levels of security and privacy, which are essential to facilitate the consumer's buy-in.*

[8] the solutions for the benchmarked industries will be considered having the differences in regulation, risks and related requirements in mind

[9] Basel Committee on Banking Supervision – Risk Management Principles for Electronic Banking.

- *For the particular use case of hybrid car charging in the Smart Grid, the privacy issues are similar: someone may know where someone is based on the identification of the location of a given car.*

6.1.2 Telecommunication

Whilst the advent of open systems interfaces has assisted in the acceptance and international deployment of networking technology (Communication and IT), it has also seen downsides in that it has become easier to intrude on networks designed with such open features. Many of the intruders were assisted in their endeavours by the openness and standardization that the telecommunication industry has undergone.

The following is a list of categories of threats to such networks that have influenced the development of security aspects over time:

1. Service denial or disruption - Typically, service disruptions caused by intruders have been brought about by accidental actions rather than malicious attempts. Nevertheless, with the attack in 2007 of Estonia's critical information infrastructure leading to a general denial of service of all internet based services, the need to adopt robust cyber security frameworks has increased.
2. Unauthorized monitoring and disclosure of sensitive information - The current approaches that intruders have used are eavesdropping techniques, network monitoring tools, and intrusions into network databases containing customer information.
3. Unauthorized modification of user or network information and network services - Intruders have changed user service profiles and affected billing and routing. This can result in unreliable service.
4. Fraud - The typical approach is to build upon the previous attacks and masquerade as a legitimate customer to commit fraud.

Key findings for Smart Grid:

- *Need to consider security features developed by telecommunication sector which developed out of threats they encountered and build appropriately into design for Smart Grids;*
- *Consumers position in Smart Meter / Smart Grid is very different from his/her position in the telecoms world, namely:*
    - *They have no choice regarding utility services since they are fundamental to their life and well-being.*
    - *They are the key enabler to delivering all of the policies linked to reducing energy consumption and dealing with climate change in each country. Consequently, alienate them at your peril.*

- *Although telecommunication provides insight, like potential tracking of movements, into some aspects of the personal world of a consumer, access to utility related data can provide detailed insight into a householder's behaviour in the privacy of their own home.*

This point reinforces the need to integrate consideration of privacy, together with security into the design phase of Smart Grids.

6.1.3 Automated fare collection

Automated fare collection for public transportation is an application domain where contactless technologies were introduced over the last few years and where privacy and data security became prominent.

The contactless smart card industry addressed the end user privacy issues explicitly by ensuring that the chips they provide will not be the weakest link in the privacy chain and in the data security chain[10]. It also shows that if privacy is addressed straight from the start when defining the chip, it is possible to define security architectures that are both satisfactory from the point of view of manufacturability and profitability while still providing the required level of protection for the various actors of the automated fare collection eco-system. One concrete example of such a design is the MIFARE(R) Plus technology.

GlobalPlatform has also published a white paper[11] that shows the prominent role of privacy and data security for automated fare collection for the public transportation industry.

Key findings for Smart Grid:

- *If privacy is addressed at the design phase of the Smart Grid ("privacy by design"), it is possible to derive user and business friendly solutions.*

6.1.4 Road pricing

Road pricing and other similar telematics services[12] are on the verge of being deployed in several parts of the world for several reasons: better traffic management, safety, environmental concerns (CO2 emissions); fairer charging for the use of the road infrastructures, better tuning of the insurance policies.

---

[10] [NXPCartes2009] Addressing end user privacy in contactless smart card systems, Henri Ardevol, NXP Semiconductors, CarteS, November 2009.

[11] GlobalPlatform's Value Proposition for the Public Transportation Industry: Seamless, Secure Travel Throughout Mulitple Transportation Networks, White Paper, November 2009, freely available on http://www.globalplatform.org in the white papers section.

[12] Telematics is the blending of computers and wireless telecommunications technologies, ostensibly with the goal of efficiently conveying information over vast networks to improve a host of business functions or government-related public services.

Road pricing although different from Smart Metering and Smart Grid presents several similarities with respect to

- the need to change consumers behaviour to achieve overall goals;
- the use of a meter (OnBoard Equipment – OBE for road pricing example);
- the transfer of data to a central system where further processing takes place;
- the privacy and data security concerns; having adequate solutions for end-user privacy preservation will be key to the acceptance of the concept.

Key findings for Smart Grid:

- *Issues around aggregating and anonymization of data will be as important for Smart Grids as it is for road pricing. There may be some lessons to learn from decisions taken with regard to road pricing options in the Netherlands.*
- *Road pricing shows that taking privacy into account straight from the start with innovative technological solutions helps in defining systems that are acceptable from both a business point of view and from an end-user privacy preservation point of view.*

6.2 Introduction to the Dutch privacy and security framework

In The Netherlands, the introduction of Smart Metering for consumers has not been without challenges. A growing awareness on privacy and security has fuelled a broad discussion on the collection and use of detailed metering data and on remote switching functionality in the meter. As laid down in the initial bill to implement Directive 2006/32/EC, consumers were obliged to accept a Smart Meter. Criticism from the political and scientific community and consumer groups led to the withdrawal of the initial bill in the Senate. An amended version is currently under discussion. This version gives consumers the right to refuse a Smart Meter and gives them control over the frequency with which metering data is collected.

Grid operators responded to these developments by jointly, and in dialog with all stakeholders, developing a set of guidelines (requirements and measures) to protect the privacy of consumers and the security of the (future) infrastructure. These guidelines will be public to convey to stakeholders that adequate measures are taken.

In the process of developing the guidelines, a methodology and framework for developing privacy and security guidelines were created. All stakeholders participated to foster transparency and trust. The aim of the framework is to establish a data privacy and data security regime that both protects and enables. This framework methodology is attached in the appendix.

Key findings applying the framework

During the process of developing the framework and the guidelines, a number of lessons were learned that may aid in the future development and updating of the guidelines:

- *Define explicitly how Smart Metering goals, tasks and data needs are linked, so reviewers have a basic understanding of the architecture and information flows.*
- *Be aware of future function creep and incorporate privacy and security considerations early on in the development by applying 'privacy (and security) by design' principles. This means that security & privacy architecture has to be researched and developed.*
- *Be also aware of 'data creep', i.e. gathering more and more data which can be linked to a person and thus is personal data.*
- *Make sure that guidelines are flexible enough to be applicable to current systems, legacy meters and future developments.*
- *Make sure that implementation of the guideline is flexible by clearly distinguishing requirements ('what to do'), measures ('how to do it'), and giving room for risk management, e.g. by allowing 'comply or explain'*
- *Make relevant privacy legislation part of the requirements and set up a code of conduct.*
- *Make sure that data is protected everywhere in the infrastructure, especially when you are not in control of the infrastructure (e.g. by applying encryption during wireless communications).*
- *Pay attention to organizational measures as well as technical ones, e.g. proper key management when dealing with encryption and limiting access to critical functionality with strong authorization.*
- *Involve stakeholders so they can explain their interests and to maintain support and trust.*
- *Involve experts and make sure that sufficient communication exists between groups dealing with privacy, security, functionality and business goals.*
- *The earlier privacy and security considerations are taken into account, the less expensive and complicated the solution will be.*
- *Define privacy and security guidelines 'top down', instead of defining measures right away.*

6.3 Non-EU Countries

U.S. – National Institute of Standards and Technology- Smart Grid Cyber Security Strategy and Requirements (NISTIR 7268)

The concern in the USA and the focus of NIST was initially firmly on security (e.g. malevolent attacks). Through the consultation process for the "Smart Grid Cyber Security Strategy and Requirements (NISTIR 7268)" document the weakness of the privacy aspects have been enhanced, but from what might be considered a low base point. This reinforces the view that "One can have security without privacy, but one cannot have privacy without security".
When first published this document was reviewed by the 'Electronic Privacy Information Centre (EPIC)' and they specifically commented on the NIST identified principles for the development of appropriate protection for 'personally identifiable information'. EPIC indicate that in their view several of the principles were flawed and they specifically criticised the heavy dependence of NIST on what they see as the discredited 'notice and consent' model of privacy protection. EPIC recommended that the NIST document could be strengthened (e.g. by the use of the OECD Privacy Principles). EPIC specifically recommended that NIST should:

- Adopt fair information practices: Information practices should adopt HEW report[13] and OECD Privacy Guidelines[14]
- Establish independent privacy oversight
  - recommend enforcement mechanisms
  - recommend that an independent Privacy Office with power over all entities
- Abandon the notice and consent model
  - Authorities and organizations must limit collection, use, retention and sharing of information in the first instance, rather than relying on consents
  - Establish a set of approved purposes for which collecting information is permitted
- Impose mandatory restrictions on use and retention of data
  - Set expiration dates so information can be retained only for a certain period of time
  - Implement role-based access control to Smart Grid data
  - Explicitly address law enforcement access to Smart Grid data
- Verify techniques for anonymization of data
  - Ensure that techniques for anonymization of data are robust, provable and transparent
- Establish robust cryptographic standards

[13] HEW Report – U.S. Department of Health, Education and Welfare's seminal 1973 report entitled "Records, Computers and the Rights of Citizens".
[14] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

- o Cryptography should be applied to secure all electronic communications
- o Cryptographic techniques do not rely upon hiding the cryptographic process

Key findings for Smart Grid:

- *U.S. has made considerable strides in addressing the security aspects of Smart Grids. For European implementation, this should be combined with an enhanced treatment for Privacy of personal data along the lines articulated above (which links to Netherlands approach).*

- *Whereas, in Europe energy theft and privacy are two important concerns related to Smart Grid implementation, in other parts of the world (e.g. in the US) it is energy theft and malevolent attacks that are the main concerns.*

Recommendation 2:

The Expert Group recommend that ESO's mandate that Smart Grid products and solutions should be designed[15] incorporating data privacy and security principles at their core[16].

[15] The implementation of a "privacy and data protection impact assessment" (PIA) should precede the implementation of a Smart Grid system. Taking into account Directive 95/46, an identification of each participant role within the system is important.

[16] Inclusion of IEC as one of the relevant standardization bodies should be evaluated.

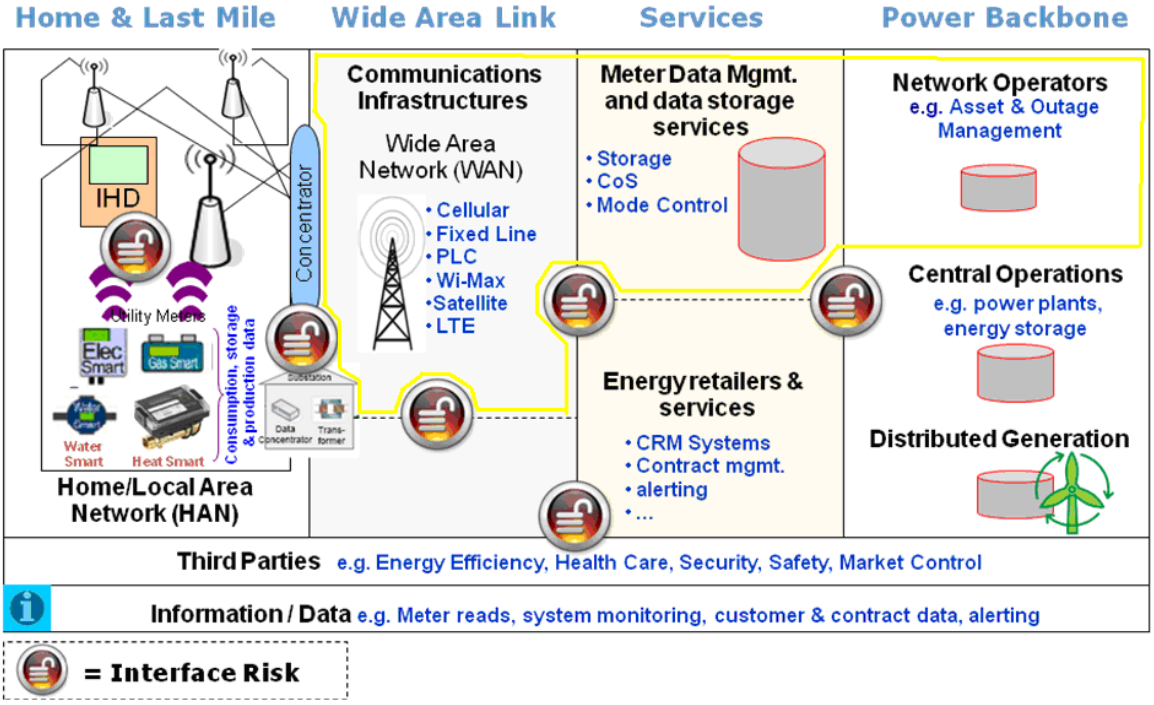
7 DATA SECURITY

7.1 Introduction

The scope of this section is to identify European Standardization Organizations (ESO) and current standards in existence related to security and privacy in the area of Smart Grids. The scope is further to identify areas where there are no standards in existence which may result in recommendations to ESOs to start new standardization work.

7.2 Architecture

The different functions today performed by most DSOs in the EU (Network Operation, Meter Data Management and Data Storage together with operating communication infrastructures) are (artificially) split up in order to provide the overview on the architecture of the market. Central operations belong to the non-regulated part of market structure, together with retail and (distributed) generation.
The yellow marked area comprises the functions that are currently performed by most DSOs in the EU (with an exception for UK and very recently Germany).



7.3 List of Interfaces

This Section attempts to define the interfaces in the diagram above and identifies which type of data is used and the associated risks which could be incurred. The types of data considered are Consumer (Con) and Technical (Tech). The table below also considers whether the interfaces mentioned are physical interfaces between devices within the Smart Grid (i.e. a meter communicating with an in home display), or data interfaces where data is moved from one legal entity to another (i.e. meter reading data bulk transported into settlements, or a data collection company allowing access to third parties such as Energy Service Companies).

Interface	Type	Notes	Data	Data Type
1) Meter to IHD	Physical interface between two devices	Security risk to personal data. Prepayment metering risk if network, interface or payment card is unsecured. Risk on firmware upgrade.	Meter Reads (Con) Pricing Info (Con) Tariff Info (Con)	Consumer data
2) HAN to LAN	Physical interface: consumers network and outside world	Used in PLC and long range RF mesh topology. Larger risk to security of data due to visibility of many meters. Risk on prepayment.	Meter Reads (Con) Load Profile (Con and Tech) Alarms (Con)	Consumer data for billing and technical for alarms
3) LAN to WAN	Physical interface: substation / regional data concentrator and central backhaul device i.e. PLC concentrator with IP bridge	Interface represents a higher lever of risk due to data moving out of the home and being combined with data from other consumers. In Smart Metering this could be an interface between a local data concentrator and the long range backhaul	Meter Reads (Con) Load Profile (Con) Alarms (Con) Meter Reads (Tec) Load Profile (Tec) Alarms (Tec)	Consumer data for billing and technical data for alarms and substation / comms efficiency data
4) WAN to Head Ends / DC businesses	Physical interface: link from backhaul data device to back end systems. Head end systems may communicate with meters directly.	Competitive model	Meter Reads (Con) Load Profile (Con) Alarms (Con)	Consumer data, and technical; data in the form of alarms
5) WAN to Central DC	Physical interface between meter or concentrator to central data collector.	Vertical Model	Meter Reads (Con) Load Profile (Con) Alarms (Con)	Consumer data for billing, technical data for network owners and meter ops
6) LAN/WAN/ DC to Dist. Network Operator	Data service interface from data collector	Substation monitoring	Meter Reads (Tec) Load Profile (Tec) Alarms (Tec)	Technical data for network monitoring
7) LAN/WAN /DC to Energy Retail	Data service interface	For billing and additional services	Meter Reads (Con) Load Profile (Con) Alarms (Con)	Consumer data for billing
8) Consumer Generation to distribution Network Operator	Physical interface into back haul network as supply metering.	For load management	Meter Reads (Con) Load Profile (Con) Alarms (Con)	Technical data for network monitoring
9) Consumer Generation to Energy Retail	Physical interface into back haul network as supply metering.	For billing purposes i.e. Feed In Tariffs (FITs)	Meter Reads (Con) Load Profile (Con) Alarms (Con)	Consumer data for billing purposes
10) Energy Retailer to Third Parties	For provision of outsourced service e.g. prepayment	For additional services	Meter Reads (Con) Load Profile (Con)	Consumer data
11) HAN to Third Parties	Data interface	For Energy Services	Meter Reads (Con) Load Profile (Con)	Consumer data
12)Consumer Generation to Third Parties	Data interface	Distributed generation aggregation services	Meter Reads (Con) Load Profile (Con)	Consumer data
13) Meter to Mop	Physical or data interface depending on topology	Installation data and downloading of tariffs on installation	Meter Reads (Con) Load Profile (Con) Tariff Data	Technical data to ensure meter is functioning

Note: Please note that the above table is not to be seen as a complete risk assessment. There will be e.g. updates to be performed during the life time of the physical equipments of the Smart Grid and these updates should happen securely. Upgradability is also to be foreseen with respect to the cryptography.

ESOs

For the scope of this report we have identified two categories of standards relevant to the Smart Grids field and technical standards. Technical standards are those that are chiefly concerned with the characteristics of the ICT systems, hardware and some communications protocols while the procedural standards are concerned with organisation, policies and management.

7.3.1 Technical Standard Organisations

IEC

The IEC 62351 series is focused on adding security mechanisms to the IEC suite of protocols developed within IEC TC57 and used for several purposes within Smart Grids, with the exception of meter reading. TC13 is currently defining the security mechanisms for Smart Metering

ISO

ISO/IEC joint standards in the 27000 series, especially notable is EN27002, previously ISO 17799 provides best practice recommendations on information security management.

CENELEC

CENELEC are the European Standardization Organisation for Electrotechnical standards within Europe. Many CENELEC committees monitor, feed into and parallel vote on International Standards produced in their corresponding committees in IEC. CENELEC are tasked under the Smart Metering Coordination Group (and Mandate 441) to identify, produce and maintain standards for electricity meters, communication protocols, home automation equipment, Electric Vehicles and other electrotechnical applications.

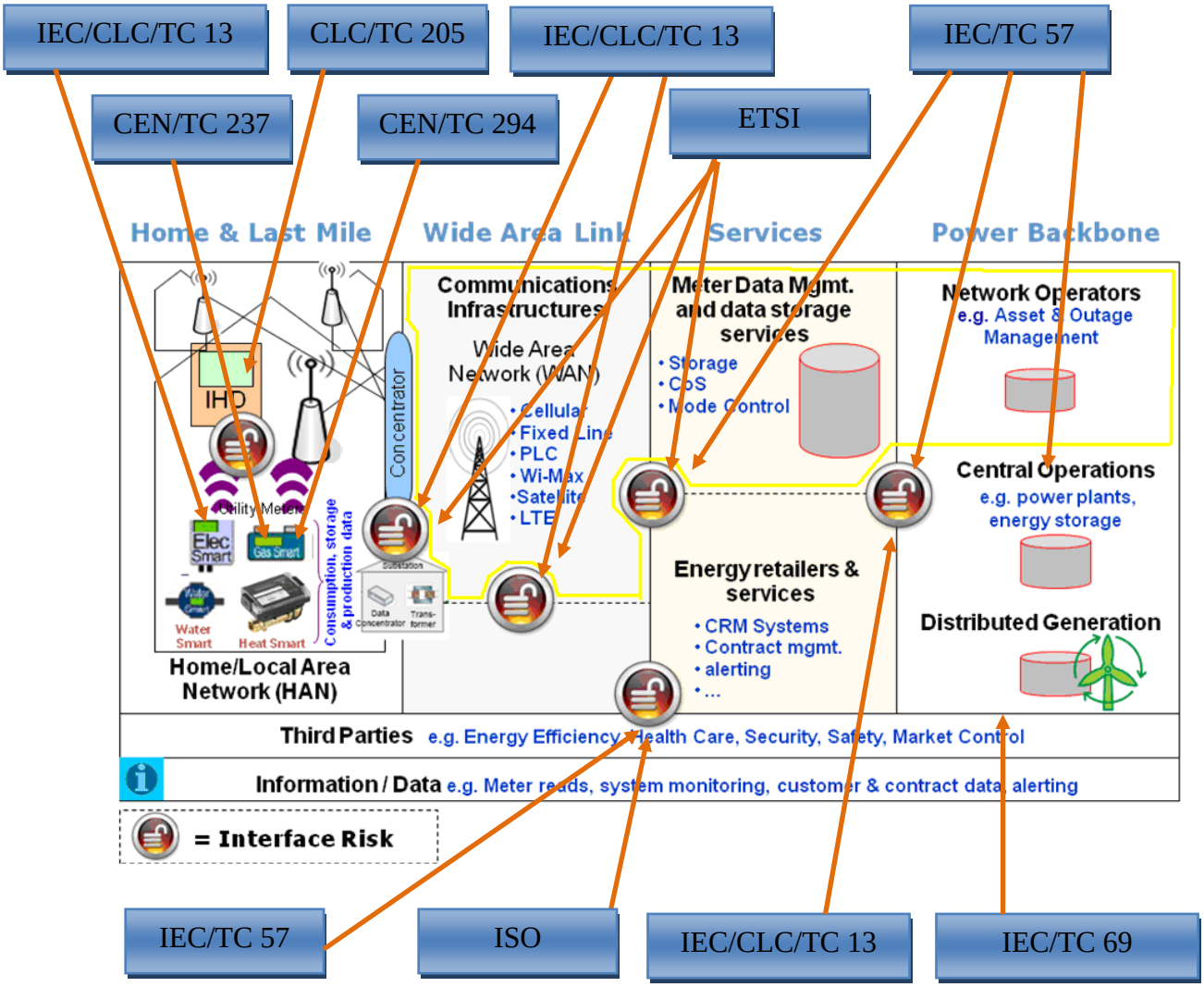
CEN

CEN is responsible for standards that are not Electrotechnical. The International equivalent of CEN is ISO, but there are some differences between the CEN/ISO relationship compared to the CENELEC/IEC relationship. CEN is also recognized by the Smart Metering Coordination group to identify, produce and maintain standards in the area of gas, water and heat meters, communications protocols for battery powered meters, and other non-electrotechnical applications.

ETSI
ETSI covers standards associated with telecommunications media, protocols and physical layers. ETSI are recognized by the Smart Metering Coordination Group for the delivery of standards in the area of telecommunications, as part of the ongoing work to fulfil the requirements of M441.

NERC
The North American Electric Reliability Council NERC is a self-regulatory, non-government organization which has statutory responsibility to regulate bulk power system users, owners, and operators through the adoption and enforcement of standards for fair, ethical and efficient practices. NERC has issued a series of standards NERC CIP 002 to NERC CIP 009 (http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html).

The diagram below is designed to highlight the responsible standards organizations and technical committees who either have standards now, have standards which need to be extended (most cases), or will need to develop new standards.



Standardization Committee / Organisation	**Area of responsibility**
IEC TC57	ERP systems interfaces and common information model
IEC TC13	Electricity meters and communications protocols
ISO	Business processes for data security
CEN TC 294	Battery Powered Meter communications
CEN/TC237	Gas Meters
ETSI M2M	Telecommunications
CLC/TC205	Home automation and communication protocols for associated equipment
IEC TC69	Electric Vehicles
PCI – DSS[17]	Payment Card Industry

7.4 Identified Gaps

Many standards (defacto or otherwise) are already available for sections of Smart Grid allowing communications between devices, and some such as ZigBee Smart Energy have very comprehensive security built into the protocol. Other EU and International standards are in the process of update to encompass higher levels of security such as DLMS COSEM (EN 62056-xx, MBus EN 13757-x). IEC 61968 goes some way to defining a common information model based on objects that are common from end to end in a Smart Grid system, but the emphasis is still security rather than privacy. There are other industries from which guidelines can be taken in this crucial area, such as the banking industry and payment card industry. The management of personal and credit card data is very well outlined in the PCI-DSS requirements, which could be used as a road map to define principles for responsible storage and use of data in back office systems in other contexts such as Smart Grids.

[17] Standard listed for informational purpose

Recommendation 3:

The Expert Group recommends that ESO's are tasked with either updating, extending or developing new standards covering on specifically or implicitly the security aspects of Smart Grid interfaces as outlined in section 7.3. (a detailed list of relevant standards are available in Appendix C "Existing Standards").

When designing the end-to-end security and privacy protection for the Smart Grid, it is clear that more work will need to be done to clearly assess the most appropriate cryptographic primitives to be used: for instance symmetric key cryptography (e.g. AES) or asymmetric cryptography (e.g. RSA or ECC cryptography). The choice of cryptographic privative has a deep impact on the trust provisioning, key generation, key distribution, key protection, key personalization, key revocation or retiring, key protection, key renewal.

We recommend that:

- **The CEN, CENELEC, ETSI joint working group review the EG2 recommendations and list of relevant standards, and add the latest amendments, additions and future works before starting any new standardization work.**
- **The 3 ESO's (CEN, CENELEC, and ETSI) are tasked to evaluate the current state of the art in cryptographic primitives through their relevant technical committees and make available the most appropriate technologies within the relevant standards framework.**
- **The CEN, CENELEC, ETSI, joint working group on Smart Grids should play a key role in this standardization work, and be responsible for ensuring continuity of all standardization work.**
- **the specification should not preclude the initial adoption of symmetric key cryptography followed by a further smooth migration to asymmetric cryptography if required.**
- **a business model is investigated to make the creation and maintenance of certification authorities (needed for asymmetric cryptography) possible**
- **a study is conducted on how to handle multi-national key management (e.g. one supra-national European certification authority certifying national certification authorities) and whom should be in charge of performing the key management.**
- **One generic model is adopted by all European countries, for key management, and security and privacy principles, regardless of the communication technology or protocol.**
- **Where appropriate, adequate protection profiles should be defined for security sensitive Smart Grid components according to ISO/IEC 15408**
- **These security and privacy principles should be relevant to not only Smart Meters, but also other devices in the Smart Grid if communicating consumption data.**

8 DATA HANDLING

There is clearly a gap within EU standards relating to the handling and security of data within the area of Smart Grids, however there are broader standards, guidelines and codes of practice in place within other industries such as the banking and Payment Card Industries. The management of personal and credit card data is very well outlined in the PCI-DSS[18] requirements, which could be used as a road map to define the principles for responsible storage and use of data in back office systems in other contexts such as Smart Grids.

It is the group's recommendation that a further package of work be carried out to develop a number of high level principles for Smart Grid data security and privacy based on already existing principles in other industries and referencing the Dutch Framework for Smart Metering. Guidance may also be taken from the EN 27000 series of standards and in particular EN 27002 (an Information Management Security standard)

Recommendation 4:

The Expert Group recommends that:

- **further pilot projects need to be done in the area of data handling, in consultation with the banking industry and payment card industry to propose a list of high level principles on EU level to be implemented, by which Smart Grid operators can design their systems and processes.**
- **After the above has taken place a paper should be produced and presented to the CEN, CENELEC, ETSI joint working group, highlighting the additional detailed standardization required in this area. An interaction with Art 29 Working Party could be useful.**
- **Security levels to be defined from minimum to advanced and the costs for the different security levels to be estimated.**

[18] Payment Card Industry Data Security Standard.

9 DATA PRIVACY

In the previous sections it has been discussed what regulations and laws that govern aspects of data security and privacy are to be implemented. Depending on whether the data relate to an identified or identifiable natural person, a data type can be defined as infringing the regulations and laws, thus it is recommended to differentiate between personal and non-personal data.
The DSO, in order to be compliant to its duties (network operation, stability and safety, detection and report to public authorities of frauds) generally needs to use both personal and non personal data.

The treatment of personal data, must comply with the relevant privacy regulation, and thus DSOs need to establish procedures in order to ensure protection of personal data.

The use of personal data for other purposes than the legal duties of the DSO requires freely given specific and informed consent from the customer.

A meter reading or load-profile is personal data if it can identify (directly or through inference, also taking into account combination with other data available) a natural person. In that case Directive 95/46/EC and other directives, legal frameworks are applicable (notification process, etc).

DSOs will adopt the definitions mentioned in Article 2 of the European Data Protection Directive 95/46/EC and implement the essential data processes of notification. This means that DSOs will establish the detailed purpose and process of the use of each personal data item and inform the Commissioner (Data Protection Authorities) accordingly.

Non-personal data:

Non personal data is all data that is not defined as personal by Directive 95/46/EC. Non-personal data can be gathered from metering, distribution, or transmission devices in order to allow the DSO to assess the performance of the energy network, (potential) network problems, security breaches, or energy theft and to resolve problems from remote or by sending technicians onsite. Examples for non-personal data are data items measured on a transmission station, such as voltage, current, phase angle and harmonic or signals that allow interaction with technical devices (actors).

Personal data:

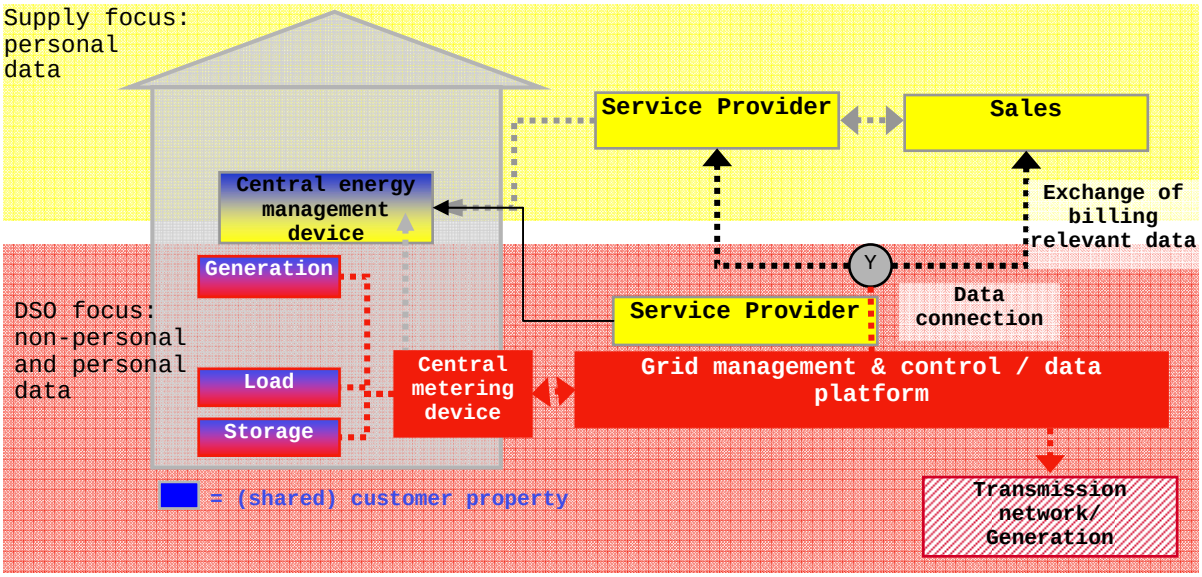
Personal data is all data defined as such be Directive 95/46/EC. Personal data is related to individual connection points and gathered from individual metering points with the intent to use this data. Here is a non exhaustive list:

- For network management by the DSO: connection; load management; DSM, fault restoration; fraud prevention and detection
- For the metering activity[19]: meter identification; personal consumption and generation information, in order to facilitate data exchange and data aggregation (through information hubs) ;
- For the supply of energy (by supplier)
- For essential energy services such as billing
- For provision of value added services to consumers, with their specific and informed consent.

Personal data can be traced back to households or the individual consumer, here defined as point of consumption or generation, and is considered as specific information about an identified or identifiable natural person.

The above concept of using personal data for DSOs also applies to all roles and responsibilities in the Smart Grids value chain.

The smooth operation of an intelligent network requires a clear division of roles and responsibilities - the central question to assess the risk especially for personal data is: which data is used by whom and for what purpose, and is the use of that data really necessary for the given purpose?



[19] Operated by the DSO in all Member States except UK and (partially) Germany

Recommendation 5:

The Expert Group's recommendation is to distinguish between personal and non-personal data to minimize the exposure of personal data.

Personal data is considered as specific data and can be traced back to the individual consumer whereas non personal data could be aggregated data. To ensure data safety and security within an intelligent network a clear division of roles and responsibilities of all parties involved (with their respective functions in the energy market) regarding ownership, possession and access to data, read and change rights, etc. has to be defined.

The Expert Group recommends that the SG-EG2 is tasked with detailing out the different personal data elements and define the corresponding data usage and necessity, including handling, possession and access to data under the current legal framework.

APPENDIX

A. Terms and Definitions

The following table provides a summary of definitions additional to chapter 2 that are important to the work of Expert Group 2. Alignment is to be reached with other expert groups and SM-CG.

Term	Original Source	Suggested Definition
Smart Grid	Task Force Expert Group 1 report	Smart Grid is an electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety.
Smart Metering	European Smart Metering Alliance (Updated)	Smart metering is designed to provide utility customers with information about their domestic consumption. This information includes data on how much of a specific product (electricity, gas water or heat) they are consuming, how much it is costing them and what impact their consumption is having on greenhouse gas emissions. When triggered by a grid signal the Smart Meter will additionally act as a load balancer/mediator between decentralized product providers and the grid.
Data Security	ISO 7498-2 Information processing systems – OSI –Basis Reference Model Part 2: Security Architecture	The term 'security' is used of minimizing the vulnerabilities of assets and resources. An asset is anything of value. A vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential violation of security (A.2.1). To achieve security basic security services and mechanisms and their appropriate placement are needed. Basic security services are: **Authentication**, **Access control, Data confidentiality, Data integrity, Non-repudiation** Security mechanisms are**:** Encipherment, Digital signature mechanisms, Access control mechanisms, Data integrity mechanisms, Authentication exchange mechanisms, Traffic padding mechanisms, Routing control mechanisms, Notarization mechanisms **The terms mean:** **Authentication**, The corroboration that the source of data received is as claimed (data origin authentication) or that a peer entity in an association is the one claimed (peer-entity authentication) Data access requires the identification of the party performing the access **Access control**, The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized

		manner. **Data confidentiality**, The property that information is not made available or disclosed to unauthorized individuals, entities or processes **Data integrity**, The property that data has not been altered or destroyed in an unauthorized manner **Repudiation**, Denial by one of the entities involved in a communication of having participated in all part of the communication
Data Controller	Based on [20]Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data	'Controller' – shall mean the natural or legal person, public authority, agency or any body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations the controller or the specific criteria for his nomination may be designated by national or Community law.
Data Processor		'Processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
Data Handling		The process of ensuring that data is stored, archived or disposed off in a safe and secure manner during and after the conclusion of a process.
Data Protection	Based on Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data	The data protection Directive applies to 'any operation or set of operations which is performed upon personal data,' called 'processing' of data. Such operations include the collection of personal data, its storage, disclosure, etc. The Directive applies to data processed by automated means (e.g. a computer database of customers) and to data that are part of or intended to be part of non automated 'filing systems' in which they are accessible according to specific criteria. (For example, the traditional paper files, such as a card file with details of clients ordered according to the alphabetic order of the names). The eight data protection principles stated by the Information Commissioner's Office enshrine how data should be protected: 1. Fair and lawful processing 2. Processed for limited and specified purposes 3. Adequate, relevant and not excessive 4. Accurate and up to date 5. Not kept for longer than necessary 6. Processed in line with individuals' rights 7. Kept secure 8. Not transferred outside the EEA without adequate protection

[20] The concept of data controller and its interaction with the concept of data processor play a crucial role in the application of Directive 95/46/EC, since they determine who shall be responsible for compliance with data protection rules, how data subjects can exercise their rights, which is the applicable national law and how effective Data Protection Authorities can be.

Data Privacy	Based on Articles 7 & 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01)	All EU citizens have the following data privacy rights linked to the Charter of Fundamental Rights: Article 7: Everyone has the right to respect for his or her private and family life, home and communications. Article 8 - Protection of personal data 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.
Integrity	NIST IR 298 Glossary of Key Information Security Terms	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. SOURCE: SP 800-53; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542 The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. SOURCE: FIPS 140-2
Authentication	NIST IR 298 Glossary of Key Information Security Terms	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. SOURCE: SP 800-53; FIPS 200 The process of establishing confidence of authenticity. SOURCE: FIPS 201 Encompasses identity verification, message origin authentication, and message content authentication. SOURCE: FIPS 190 A process that establishes the origin of information or determines an entity's identity. SOURCE: SP 800-21 [2nd Ed]
Non-repudiation	NIST IR 298 Glossary of Key Information Security Terms	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. SOURCE: SP 800-53; CNSSI-4009 Is the security service by which the entities involved in a communication cannot deny having participated. Specifically the sending entity cannot deny having sent a message (non-repudiation with proof of origin) and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery). SOURCE: FIPS 191

B. Dutch Framework Privacy & Security

Introduction to the Dutch privacy and security framework

Scope and objectives of privacy and security guidelines in The Netherlands

In the Dutch architecture, smart energy meters collect and transmit detailed usage data and have the ability to switch energy flows. Large scale rollout introduces a number of specific privacy and security risks. These risks include blackouts by accident, system error or on purpose (malevolent

attackers) and the disclosure of personal data. In more general terms, confidentiality, integrity and availability of information and (switching) commands must be protected. The main objectives of the guidelines are to achieve a sufficient level of protection across Smart Metering infrastructures in The Netherlands and to minimize the damage should an incident occur.

Authorship and review of the guidelines

The framework and the guidelines have been created by the Dutch Association of Grid Operators: 'Netbeheer Nederland'. This organisation is the industry association of all Dutch regional grid operators since 2007. Netbeheer Nederland has taken the initiative to establish a working group to design the guidelines. In this working group all Dutch grid operators have been given the opportunity to contribute.

During the development, the guidelines have been reviewed by experts in the field of privacy and security from within and from outside the industry. The Netherlands Organisation for Applied Scientific Research (TNO) as well as the Radboud University Nijmegen (RUN) have provided valuable feedback. PricewaterhouseCoopers (PWC) has contributed on various aspects of the framework. Stakeholders were identified and then consulted in three informal 'round-table sessions' to listen to their expectations and demands. This included interest groups and government representatives.

Structure of the framework and its use for developing guidelines

Together with stakeholders and experts, the workgroup has come up with a practical and 'easy to fill' framework for developing privacy and security guidelines. This framework helps ensure completeness and correctness of the guidelines, ensures transparency, and makes it easy for third parties to review guidelines (requirements and measures) and understand their background and rationale.

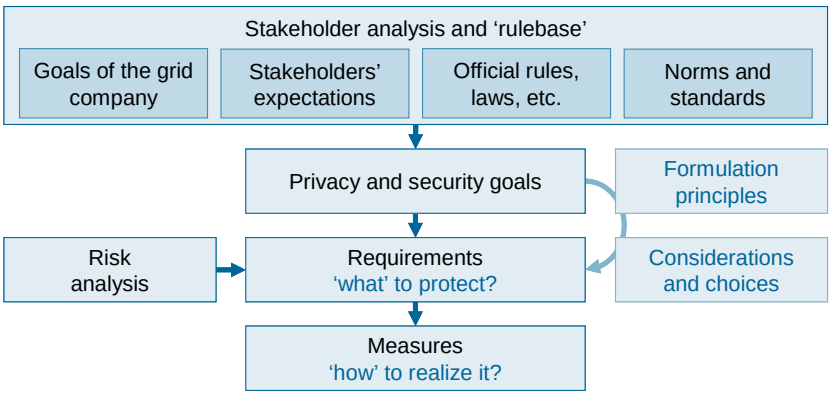


Figure 1: Dutch framework for developing privacy and security requirements and measures

The framework defines the steps to get to a complete and correct set of privacy and security guidelines (see figure 1 above):

1. **Stakeholder analysis and rulebase** - The stakeholder analysis consists of an overview of all relevant stakeholders and their demands and expectations with

regards to Smart Meters. This includes both formal expectations (e.g. legislation) and informal expectations (e.g. opinions expressed in the media). Stakeholders' demands and expectations have been condensed to approximately 30 'rules' as listed in a high level 'rule base'.

2. **Privacy and security goals** - Based on this rulebase, a number of high level goals for the privacy and security requirements have been defined. Approximately ten high-level objectives explain the intended level of security and privacy protection that should be achieved with the set of guidelines.

3. **Risk analysis** - In a parallel process, risks were identified rated on probability and impact. About 60 risks form the basis for the definition of requirements and measures. Since risks depend on available functionality in the infrastructure, a risks classification has been devised. The higher the risk class, the more requirements apply.

4. **Formulation principles -** Four principles are applied drafting the requirements based on the risks and goals:
   - Minimization of information to be secured by limiting communication, storage, retention and locations.
   - Layering of security measures in prevention, detection and resolution.
   - Minimization of impact of incidents by restriction of privileges and influences.
   - Centralization of security for control and maintenance purposes.

5. **Considerations and choices.** In order to track considerations, choices, rationale and evolution of the guidelines all considerations and choices are logged. This is done to provide accountability for these choices.

6. **Requirements** - based on risks and high level goals, requirements have been developed using the formulation principles. These requirements define what has to be done and about 100 are defined.

7. **Measures**. For a number of requirements specific measures are designed in order to aid with implementation choices and to provide consistency over the operators. These define *how* the requirements can be implemented.

By following the steps of the framework, a top-down, risk-based approach is realized during development of the guidelines. In the Dutch case, this resulted in three documents: a main document introducing, explaining and listing the guidelines (requirements and measures), a second document containing the risk analysis, and (third) the stakeholder analysis. A separate database logs all considerations and choices provide transparency and accountability.

C. Existing Standards

This section highlights all identified EU and international standards identified in the IEC, NIST and ESMIG reports related to Smart Grid and Smart Metering. Each standard is marked with the interface, if any that relates to the standard with reference to the interface model in section 6.3 of this document. Standards

listed are considered to be particularly related or affect by requirements for security and privacy.

European Standards

	Description	Interface Reference
EN 61334-3-22:2001	Distribution automation using distribution line carrier systems -- Part 3-22: Mains signaling requirements - MV phase-to-earth and screen-to-earth intrusive coupling devices	6
EN 61334-4-1:1996	Distribution automation using distribution line carrier systems -- Part 4: Data communication protocols -- Section 1: Reference model of the communication system	6
EN 61334-4-33:1998	Distribution automation using distribution line carrier systems -- Part 4-33: Data communication protocols - Data link layer - Connection oriented protocol	6,8
EN 61334-4-42:1996	Distribution automation using distribution line carrier systems -- Part 4: Data communication protocols -- Section 42: Application protocols - Application layer	6
EN 61334-4-32:1996	Distribution automation using distribution line carrier systems -- Part 4: Data communication protocols -- Section 32: Data link layer - Logical link control (LLC)	6,8
EN 61334-4-41:1996	Distribution automation using distribution line carrier systems -- Part 4: Data communication protocols -- Section 41: Application protocols - Distribution line message specification	6
EN 61334-4-61:1998	Distribution automation using distribution line carrier systems -- Part 4-61: Data communication protocols - Network layer - Connectionless protocol	6
EN 61334-4-511:2000	Distribution automation using distribution line carrier systems -- Part 4-511: Data communication protocols - Systems management - CIASE protocol	6,8
EN 61334-4-512:2002	Distribution automation using distribution line carrier systems -- Part 4-512: Data communication protocols - System management using profile 61334-5-1 - Management Information Base (MIB)	6,8
EN 62056-21	Electricity metering – Data exchange for meter reading, tariff and load control – Part 21: Direct local data exchange	13
EN 62056-31	Electricity metering – Data exchange for meter reading, tariff and load control – Part 31: Use of local area network on twisted pair with carrier signalling	1
EN 62056-42	Electricity metering – Data exchange for meter reading, tariff and load control – Part 42: Physical layer services and procedures for connection-oriented asynchronous data exchange	2,3,4,5,6,8,9,11,12
EN 62056-46+am1	Electricity metering – Data exchange for meter reading, tariff and load control – Part 46: Data link layer using HDLC protocol	2,3,4,5,6,8,9,11,12
EN 62056-47	Electricity metering – Data exchange for meter reading, tariff and load control – Part 47: COSEM transport layers for IPv4 networks	2,3,4,5,6,8,9,11,12
EN 62056-53	Electricity metering – Data exchange for meter reading, tariff and load control – Part 53: COSEM application layer	2,3,4,5,6,8,9,11,12
FprEN 61968-9:2008	Application integration at electric utilities - System interfaces for distribution management -- Part 9: Interface standard for meter reading and control	5,6,7,10

	Description	Interface Reference
Communications		
EN 13757-1:2003 Part 1	Developed by CEN. Communication system for meters and remote reading of meters. Include such communication systems as M-Bus and PLC. Part 1: Data exchange includes Obis and DLMS/COSEM)	1
EN 13757-2:2004 Part 2	Developed by CEN. Communication system for meters and remote reading of meters. Include such communication systems as M-Bus and PLC. Part2: Physical and link layer.	1
EN 13757-3:2004 Part 3	Developed by CEN. Communication system for meters and remote reading of meters. Include such communication systems as M-Bus and PLC. Part 3: Dedicated application layer.	1
EN 13757-4:2005 Part 4	Developed by CEN. Communication system for meters and remote reading of meters. Include such communication systems as M-Bus and PLC. Part 4: Wireless meter read-out (electricity meters are not covered by this standard, as the standardization of remote readout of electricity meters is a task for IEC/CENELEC.	1
EN 13757-5:2008 Part 5	Developed by CEN. Communication system for meters and remote reading of meters. Include such communication systems as M-Bus and PLC. Part 5: Wireless relay.	1
EN 13757-6 Part 6	Developed by CEN. Communication system for meters and remote reading of meters. Include such communication systems as M-Bus and PLC. Part 6: Local Bus.	1
EN 50090-4-1:2004	Home and Building Electronic Systems (HBES) -- Part 4-1: Media independent layers - Application layer for HBES Class 1	1
EN 50090-4-3:2007	Home and Building Electronic Systems (HBES) -- Part 4-3: Media independent layers - Communication over IP	1,2 ?
EN 50090-5-1:2005	Home and Building Electronic Systems (HBES) -- Part 5-1: Media and media dependent layers - Power line for HBES Class 1	1,2 ?
EN 50090-5-2:2004	Home and Building Electronic Systems (HBES) -- Part 5-2: Media and media dependent layers - Network based on HBES Class 1, Twisted Pair	1,2, ?
EN 50090-5-3:2006	Home and Building Electronic Systems (HBES) -- Part 5-3: Media and media dependent layers - Radio frequency	1,2, ?
CLC/prTS 50090-6-4	Home and Building Electronic Systems (HBES) -- Part 6-4: Interfaces - Residential gateway model for a home and building electronic system	3,4 ?
EN 60870-5-1:1993	Telecontrol equipment and systems -- Part 5: Transmission protocols - Section 1: Transmission frame formats	3, 4 ?
EN 60870-5-2:1993	Telecontrol equipment and systems -- Part 5: Transmission protocols - Section 2: Link transmission procedures	3, 4 ?
EN 60870-5-3:1992	Telecontrol equipment and systems -- Part 5: Transmission protocols - Section 3: General structure of application data	??
EN 61850	Communication networks and systems in substations -- Part 3: General requirements	3,6
EN 61850-4:2002	Communication networks and systems in substations -- Part 4: System and project management	3,6
EN 61850-5:2003	Communication networks and systems in substations -- Part 5: Communication requirements for functions and device models	3,6

	Description	Interface Reference
EN 61850-6:2004	Communication networks and systems in substations -- Part 6: Configuration description language for communication in electrical substations related to IEDs	3,6
FprEN 61850-7-3:2008	Communication networks and systems for power utility automation -- Part 7-3: Basic communication structure - Common data classes	3,6
EN 61850-7-3:2003	Communication networks and systems in substations -- Part 7-3: Basic communication structure for substation and feeder equipment - Common data classes	3,6
FprEN 61850-7-4:2008	Communication networks and systems for power utility automation -- Part 7-4: Basic communication structure - Compatible logical node classes and data classes	3,6
EN 61850-7-4:2003	Communication networks and systems in substations -- Part 7-4: Basic communication structure for substation and feeder equipment - Compatible logical node classes and data classes	3,6
CLC/prTS 61850-80-1	Communication networks and systems for power utility automation - Part 80-1: Guideline to exchanging information from a CDC-based data model using IEC 60870-5-101 or IEC 60870-5-104	3,6
Interface		
EN 61970-403:2008	Energy management system application program interface (EMS-API) Part 403: Generic data access	3,6
EN 61970-404:2007	Energy management system application program interface (EMS-API) Part 404: High speed data access (HSDA)	3,6
EN 61970-407:2007	Energy management system application program interface (EMS-API) Part 407: Time series data access (TSDA)	3,6
EN 61968-1:2004	Application integration at electric utilities - system interfaces for distribution management Part 1: Interface architecture and general requirements	6, 11 ?
EN 300 220	Electromagnetic Compatibility and Radio Spectrum Matters; Short Range Devices (SRD)	2
EN 300 228	Electromagnetic Compatibility and Radio Spectrum Matters; Wideband Transmission Systems	2
EN 300 356-1	Integrated Services Digital Network (ISDN); Signaling System no. 7 (SS7)	
EN 300 403-1	Integrated Services Digital Network (ISDN); Digital Subscriber Signaling System no. 1 (DSS1) protocol	
EN 300 440-2	Electromagnetic Compatibility and Radio Spectrum Matters; Short Range Devices; Radio Equipments to be used in the 1GHz to 40 GHz frequency range	2
EN 300 328	Electromagnetic Compatibility and Radio Spectrum Matters; Wideband Transmission Systems; Data transmission equipments operating in the 2.4GHz ISM band and using Wide Band Modulation techniques	2

	Description	Interface Reference
EN 302 065	Electromagnetic Compatibility and Radio Spectrum Matters; Ultra Wide Band (UWB) technologies for communication purposes	2
EN 302 500	Electromagnetic Compatibility and Radio Spectrum Matters; Short Range Devices (SRD) using UWB technology; Location tracking equipment in the frequency range from 6GHz to 8.5GHz	2
ES 202 630	SRD Technical Characteristics and Test methods	

International

IEC/TR 61334-1-4 (1995-11)	Distribution automation using distribution line carrier systems - Part 1: General considerations - Section 4: Identification of data transmission parameters concerning medium and low-voltage distribution mains	
IEC 61334-4-32 (1996-09)	Distribution automation using distribution line carrier systems - Part 4: Data communication protocols - Section 32: Data link layer - Logical link control (LLC)	
IEC 61334-4-33 (1998-07)	Distribution automation using distribution line carrier systems - Part 4-33: Data communication protocols - Data link layer - Connection oriented protocol	
IEC 62056-21	Electricity metering – Data exchange for meter reading, tariff and load control – Part 21: Direct local data exchange	
IEC/TS 62056-41	Electricity metering – Data exchange for meter reading, tariff and load control – Part 41: Data exchange using wide area networks: Public switched telephone network (PSTN) with LINK + protocol	
IEC 62056-42	Electricity metering – Data exchange for meter reading, tariff and load control – Part 42: Physical layer services and procedures for connection-oriented asynchronous data exchange	
IEC 62056-46+am1	Electricity metering – Data exchange for meter reading, tariff and load control – Part 46: Data link layer using HDLC protocol	
IEEE 802	Standards for Local Area Network and Metropolitan Area Network. The most widely used standards are: Ethernet, Token Ring, Wireless LAN, Wireless PAN (Personal Area Network), Wireless MAN, Bridging and Virtual Bridged LANs.	
IEC 61850-6 Ed. 1.0	Communication networks and systems in substations - Part 6: Configuration description language for communication in electrical substations related to IEDs	
IEC 61850-7-3 Ed. 1.0	Communication networks and systems in substations - Part 7-3: Basic communication structure for substation and feeder equipment - Common data classes	
IEC 61850-7-4 Ed. 1.0	Communication networks and systems in substations - Part 7-4: Basic communication structure for substation and feeder equipment - Compatible logical node classes and data classes	
IEC/TS 61850-80-1 Ed. 1.0	Communication networks and systems for power utility automation - Part 80-1: Guideline to exchanging information from a CDC-based data model using IEC 60870-5-101 or IEC 60870-5-104	3,6
Interface		
IEC 61970-407	Energy management system application program interface (EMS-API) Part 407: Time series data access (TSDA)	3,6
ETSI TS 102 887-1	Smart Metering wireless access protocol; part 1: Physical layer	2

ETSI TS 102 887-2	Smart Metering wireless access protocol; part 2: Data Link Layer (MAC)	2
ETSI TR 102 886	Performance requirements for Smart Metering Wireless Access Protocol	2
Data exchange security		
IEC/TS 62351-1:2007	Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues	3,6
IEC/TS 62351-2	Application integration at electric utilities - System interfaces for distribution management - Part 2: Glossary	3,6
IEC/TS 62351-3:2007	Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP	3,6
IEC/TS 62351-4:2007	Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS	3,6
IEC/TS 62351-6:2007	Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850	3,6
ETSI TS 102 689	M2M Service requirements	
ETSI TS 102 221	Smart Cards; UICC-Terminal Interface; Physical and Logical characteristics	1
ETSI TS 102 671	Smart Cards; Machine to Machine UICC; Physical and Logical characteristics	1, 2
ETSI TS 102 223	Smart Cards; Card Application Toolkit (CAT)	1, 2
ETSI TS 102 225	Smart Cards; Secured Packet structure for UICC based applications	2, 7
ETSI TS 102 226	Smart Cards; Remote APDU structure for UICC based applications	2, 7
ETSI TS 102 484	Smart Cards; Secure channel between a UICC and an endpoint terminal	1, 2
ETSI TS 184 002	Identifiers (IDs) for Next Generation Networks (NGN)	2, 7
ETSI TR 187 010	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity management and their resolution in the NGN	2, 7
ETSI TS 185 005	Services Requirements and Capabilities for customer networks connected to TISPAN NGN	2, 7
Draft ETSI TS 185 003	TISPAN Customer Network Gateway (CNG) Architecture and Reference Points	2
ETSI TS 185 006	TISPAN Customer Devices Architecture and Reference Points	1, 2
ETSI TS 181 005	TISPAN Service and Capability Requirements	
ETSI TS 122 228	IMS Service Requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1	
ETSI TS 122 173	IMS Multimedia Telephony Service and Supplementary Services; Stage 1	

ETSI TR 187 002	TISPAN NGN Security (NGN SEC); Threat Vulnerability and Risk Analysis	
ETSI TS 187 001	TISPAN NGN Security (NGN SEC); Security Requirements	
ETSI TS 187 003	TISPAN NGN Security (NGN SEC); Security Architecture	

Other Defacto standards, TRs, FDIS, CDs

Standard	**Description**	**Interface Reference**
ZigBee Smart Energy Profile	HAN protocol based on IEEE 802.15.4 MAC and PHY.	1
PCI – DSS	Code of practice for payment card Industry for the holding of Credit and Debit Card details and persona data.	4,5,6,7,10,11