Data Privacy in Smart Electricity Networks

Slobodan Bojanić, Srdan Đorđević, and Octavio Nieto-Taladriz

***Abstract*—Smart Grids are amongst the most promising future developments to manage and control the energy consumption in the next decades. However, the integration and interdependencies that will evolve between the electricity power grid, telecommunication networks and ICT enable new threats and vulnerabilities to this critical infrastructure which must be addressed adequately with the right kind of security controls, balanced risk mitigation strategies and a continuous attention towards security, privacy and regulation aspects. It is an emerging area where new data privacy problems arise as mass rollout of smart meters is already happening.**

***Index Terms*—Smart Grid, Data Privacy, Smart Meter, Privacy by Design.**

I. Introduction

THE appearance of Smart Grids with intelligent meters alters the polling frequency of measurement and the coverage of the measurement at the consumer location. Namely up to now the measuring frequency is low and covers an area or larger number of energy users, the intelligent meter may change the frequency to minutes or real-time whereas the coverage is in the range of individual consumers or households. This implies that where up to now the operator has a large view of the energy behavior of a bigger set of consumers, this view will evolve to detailed information on the energy behavior of sole end consumers and most data from Smart Grids can be considered personal data [1]-[5].

Smart Grid applications are based on the advances the Electric Power System and increased integration with communications and information technology together with sensors and actuators for active monitoring and control. The potential benefits of the Smart Grids are far-reaching and significant like the opportunities for consumers to cut their bills by changing their habits, perhaps using energy at different times to take advantage of lower tariffs, as well as opportunities for industry to more accurately forecast demand, reducing expensive electricity storage costs and the realization of climate change targets. However they also have the potential to process increasing amounts of personal data, unprecedented in this industry, and to make that personal data more readily available to a wider circle of recipients than at present.

The implementation of Smart Grids potentially connects location information to specific data that holds information on the use of electrical energy, and in the future possibly more. The fingerprint or contents of this data provides information on what is going on at the location at a specific moment, and may show patterns over longer time which may have great impact on the privacy and security of the consumer [14].

Thus it is necessary to deploy adequate measures to protect the contents and nature of this data in order to safeguard the privacy of the consumer. Without such protection there is a risk not only that processing of personal data will be in breach of national laws but also that consumers will reject these programmes on the basis that the collection of personal data is unacceptable to them. Such rejection may arise even if there is no breach of the law. Therefore it is necessary that all parties involved in the deployment of smart meters and the development of the smart grid ensure that the fundamental rights of individuals are protected and respected.

These concerns are also reflected in Strategic Research Agenda for the year 2035 of the European Technology Platform on Smart Grids [15]. That is an update of the Strategic Research Agenda 2007 for the needs by the year 2035. Namely regarding changes between 2007 and 2011 with sensitivity towards better predicting today the needs for the year 2035, it is obvious that Data and Information is becoming much more important. The amount of data that is available but also to be handled has increased very much since 2007 and continues to increase exponentially. One reason is the already wide penetration of smart meters which will increase dramatically within next years. This allows new business models but also increases the need for data security. Here, consumers became much more aware of this topic and became very concerned about the privacy of their data. The increased amount of data also increased the need to use the grid for data transport.

II. Background

Privacy is normally assumed as the ability of an individual to be left alone, out of public view, free from surveillance or interference from others (individuals, organizations or the state) and in control of information about himself. Privacy is

Manuscript received 1May 2012. Accepted for publication 30 May 2012. Some results of this paper were presented at the 4th Small Systems Simulation Symposium, Niš, Serbia, February 12-14, 2012.

This research was partially funded by The Ministry of Education and Science of Republic of Serbia under contract No. TR32004.

Slobodan Bojanić and Octavio Nieto-Taladriz are with Universidad Politécnica de Madrid, ETSIT Avenida Complutense nº 30, 28040 Madrid, Spain, e-mail: {slobodan, octavio}@die.upm.es.

Srdan Đorđević is with the Department of Electronics, Faculty of Electronic Engineering, University of Niš, Aleksandra Medvedeva 14, 18000 Niš, Serbia, e-mail: srdjan.djordjevic@elfak.ni.ac.rs.

DOI: 10.7251/ELS1216092B

not a plainly delineated concept and is not simply the specifications provided within laws and regulations. Furthermore, privacy should not be confused, as it often is, with being the same as confidentiality; and personal information is not the same as confidential information. Confidential information is information for which access should be limited to only those with a business need to know and that could result in compromise to a system, data, application, or other business function if inappropriately shared.

Privacy was not of particular concern for many decades in the electricity networks which have provided the vital links between electricity producers and consumers with great success. The basic architecture of these networks was developed in most countries to meet the needs of large, predominantly carbon-based generation technologies. Since Europe is committed to the 20-20-20 targets to reduce carbon emissions and to secure energy supply, energy efficiency and renewable energy are seen as solution to attain this goal. Both measures call for changes in the energy supply system leading to smart grids as key enablers for the required innovation.

The Smart grid is usually defined as an intelligent electricity network that combines information from users of that grid in order to plan the supply of electricity more effectively and economically that was possible in the pre-smart environment. It is a challenge to efficiently integrate the behavior 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. A further step will be energy optimization crossing the domains of electricity, gas and heat.

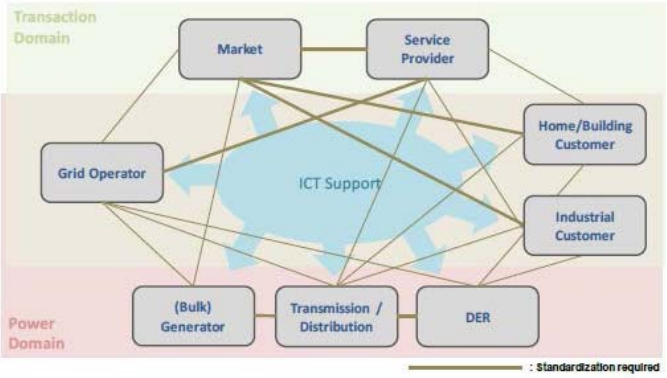

Fig 1. A conceptual model of the Smart Grid.

Key factors comprise the degree of decentralization of the system components and their interrelation with electricity networks, the variability of renewable generation, the increased distance between electricity generation and consumption, the intelligence level of the involved systems created by smart products and associated smart services, the legal framework, the associated regulation of market based product and service choices versus natural monopoly products and services and the business roles for actors involved in all aspects of networks and intelligent electric systems.

Furthermore the integration requires fast data transfer architectures between grid control areas and between distribution and transmission system operators' systems: a huge amount of data has to be exchanged as much as possible in real time and with a high reliability between areas in order to promptly react to any change in the grid operation parameters. To exploit economies of scale and to provide scalable solutions, the deployed field devices and systems have to be as much as possible interoperable and standardized.

The introduction of smart meters makes the process more complex in that the data subject will provide suppliers with insights into personal routines. There is a big difference in circumstances between countries, ranging from those where rollout is largely complete following government mandate to those where no meters have been installed. Furthermore high volumes of data coming from smart monitoring devices and smart meters must be managed efficiently. Such growth in data flow needs to be organized and structured to be relevant information ready for distribution and communication.

The new approach in energy systems should be based on role based data access. Namely, data must be owned by and located at the data "originator" from where will be utilized for all relevant purpose - but with restricted access to what is relevant for the owner of the data. This calls for enhanced activities for ensuring high level of cyber security and respect of the privacy issue. One important step in this process is data minimization in respect of purpose and time limitation and data quality. Namely data should be collected for specific, explicitly defined and legitimate purposes and not further processed in a way incompatible with those purposes. Data quality supposes that they are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed as well as accurate and, where necessary, kept up to date. Furthermore data needs to be retained only for as long as is necessary to fulfill that purpose.

III. Stakeholders

Smart Grids include a much wider area than smart metering which is an important first step towards a Smart Grid. Smart meters bring intelligence to the 'last mile' between the grid and the final customer. Without this key element, the full potential of a Smart Grid may not be realized. Being that only few countries in Europe have undertaken a full deployment of smart meters actors involved in the sector should draw from existing experiences and take account of best practices in place.

The smart metering brings with it the potential for numerous novel ways for processing data and delivering services to consumers. Whatever the processing, whether it is similar to that which existed in the pre-smart environment, or unprecedented, the data controller must be clearly identified, and be clear about obligations arising from data protection legislation including Privacy by Design, security and the

rights of the data subject. Data subjects must be properly informed about how their data is being processed, and be aware of the fundamental differences in the way that their data is being processed so that when they give their consent it is valid.

Therefore the following Smart Grid stakeholders are:

- 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.

It can also be viewed through various domains interconnected by secure communication flows and flows of electricity as presented in Fig. 2.

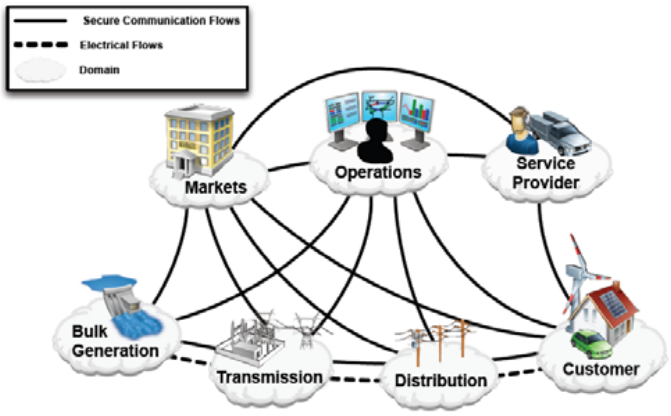

Fig. 2. Interaction among actors in Smart Grid.

Data processing service providers in provision of data processing services are in charge of respecting consumer privacy. Basically the smart meter takes a reading which reflects the energy usage at the property. At some point that reading, along with other information, can be transmitted outside the property. In some models it will be sent directly to a central communications hub where the smart meter data are managed. Once there, it can be accessed by DSOs, suppliers and ESCOs. It appears that the DSOs will have to face the greatest changes to make smart grids a reality. That is because of the growing distributed character (resulting in growing bidirectional power flow at all voltage levels) and variability of generation, customer privacy issues, system security, data and information processing for new applications and concepts such as Virtual Power Plants, etc.

Also multiple and complex methods of communication, with additional entry points and data paths creating complicated security challenges requiring solutions that encompass them all should be taken onto consideration. Given the complex and disparate landscape, the task of producing privacy solutions is quite challenging, and at this stage it seems that they can only be general, rather than specific.

The disparity of the current position does not allow presenting a comprehensive view on all specific aspects of smart metering programs across the countries. There is a huge variation in circumstances between countries, ranging from those where rollout is largely complete following government mandate to those where no meters have been installed. There is also much variation in the level of involvement from DPAs and in the nature of the market across member states, and where responsibility lies with installation of meters. In some countries, publicly owned utility companies are responsible. Elsewhere, there is a competitive supplier market. Distribution system operators have a more prominent role in some countries.

The smart grid brings a completely new and complex model of inter-relationships that poses challenges for the application of data protection. In this emerging area it is fully expected that new data protection problems and solutions will evolve as more smart meters and smart grid components are installed. It is obvious is that mass deployment of smart meters is already happening, so there is urgency to comprehend the way that smart meters process personal data, and the issues that this raises. The issues of general concern warrant serious consideration by all those involved in this area. Since data in Smart Grids might contain privacy sensitive information the principles such as privacy by design and default should be involved. The personal data is being processed by the meters, so data protection laws apply.

Data controller must be clearly identified, and be clear about obligations arising from data protection legislation, security and the rights of the data subject whatever the processing, whether it is similar to that which existed in the pre-smart environment. Data subjects must be properly informed about how their data is being processed, and be aware of the fundamental differences in the way that their data is being processed so that when they give their consent it is valid.

IV. Privacy Threats

The privacy implications are numerous for smart grid technology deployment centers on the collection, retention, sharing, or reuse of electricity consumption information on individuals, homes, or offices. Basically, smart grid systems will be multidirectional communications and energy transfer networks that enable electricity service providers, consumers, or third party energy management assistance programs to access consumption data. In addition, if plans for national or transnational electric utility smart grid systems proceed as currently proposed these far reaching networks will enable data collection and sharing across platforms and great distances [7]-[11].

As consumer privacy is a key factor in the change towards smart energy systems thus data access and ownership and the permission to gather data need to be very carefully considered. At the same time, consumers should be well informed about who deals with their data. It has to be emphasized that it is the consumer who owns his data, no one else, and therefore he is

entitled to appropriate rights and protections.

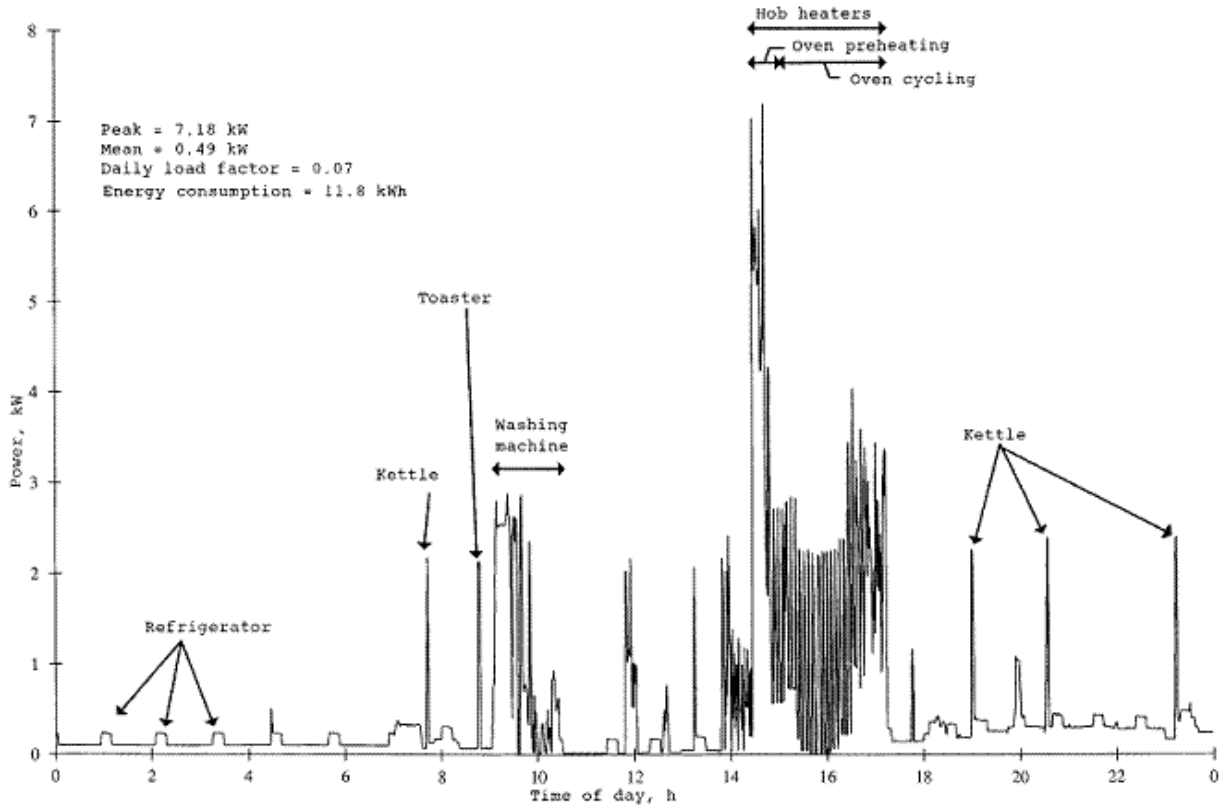

Fig. 3. Consumer profiling by energy.

A list of potential privacy concerns in Smart Grid systems include:

- Identity Theft
- Determine Personal Behavior Patterns
- Determine Specific Appliances Used
- Perform Real-Time Surveillance
- Reveal Activities Through Residual Data
- Targeted Home Invasions (latch key children, elderly, etc.)
- Provide Accidental Invasions
- Activity Censorship
- Decisions and Actions Based Upon Inaccurate Data Profiling
- Unwanted Publicity and Embarrassment
- Tracking Behavior of Renters/Leasers
- Behavior Tracking (possible combination with Personal Behavior Patterns)
- Public Aggregated Searches Revealing Individual Behavior.

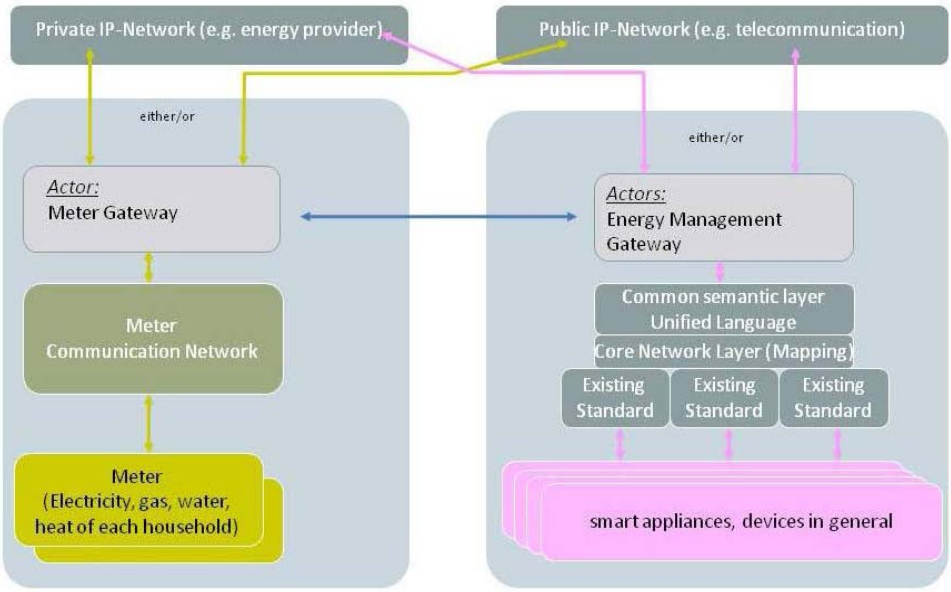

Fig. 4. Logical separation of metering and energy management.

Additionally, plans are underway to support smart grid system applications that will monitor any device transmitting a signal, which may include non-energy-consuming end use items that are only fitted with small radio frequency identification devices (RFID) tags may be possible. 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.

V. Privacy Principles

The increased amount of personal data being processed, the possibility of remote management of connection and the likelihood of energy profiling based on the detailed meter readings make it imperative that proper consideration is given to individuals' fundamental rights to privacy. The reference architecture for the home/building, pointing out the different logical blocks, and can be easily integrated in the whole system architecture is shown in Fig. 4. It is not related to a specific hardware design, but merely shows a logical separation of functions without predefining where and how those functions are implemented.

Privacy by Design (PbD) is a concept to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems [12]. The objectives of Privacy by Design — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following seven Foundational Principles:

1. Proactive not Reactive; Preventative not Remedial measures by anticipating and preventing privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before the-fact, not after.
2. Privacy as the Default Setting i.e. ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.
3. Privacy Embedded into design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.
4. Full Functionality — Positive-Sum, not Zero-Sum, *by* accommodating all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary tradeoffs are made such as privacy vs. security, demonstrating that it is possible to have both.
5. End-to-End Security — Full Lifecycle Protection extending securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion.
6. Visibility and Transparency — thus its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.
7. Respect for User Privacy — Keeping it User-Centric appropriate notice, and empowering user-friendly options.

Yet, privacy concerns still need to be transposed into specific, precise and non-ambiguous technical requirements if they are to allow the security industry to competitively design and develop privacy-compliant solutions and services. The Privacy by Design concept should, at its turn, be better detailed in order to allow for its practical implementation in concrete cases.

There are also OECD Privacy Guidelines:

1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, compete and kept up-to-date.
3. Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Principle 3 except — with the consent of the data subject; or by the authority of law.
5. Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual Participation Principle: An individual should have the right: a. To obtain from the data controller, or otherwise, confirmation of whether or not the data

controller has data relating to him; b. To have communicated to him, data relating to him.

8. Accountability Principle: A data controller should be accountable for complying with measures that give effect to the principles stated above. Data can be sent to the controller in real-time or be stored in the smart meter. In both cases however, under the Data Protection Directive, it is considered that the data have been collected by the controller.

As part of the Privacy by Design process, security and privacy risk assessments will identify the potential risks to data security. Given the novel and vast prospect that is in store with the smart grid and its associated technologies, the task of anticipating security requirements is a challenging one. In order to mitigate risk, the approach should be end-to-end, incorporating all parties and drawing on a broad range of expertise. Security should also be designed in at the early stage as part of the architecture of the network rather than added on later. Appropriately robust security safeguards must be in place that should apply to the whole process including the in-home elements of the network, the transmission of personal data across the network and the storage and processing of personal data by suppliers, networks and other data controllers. Security is a path, not a destination. Security is about risk management and implementing effective counter measures.

The technical and organizational safeguards should cover at least the following areas:

- The prevention of unauthorized disclosures of personal data;
- The maintenance of data integrity to ensure against unauthorized modification;
- The effective authentication of the identity of any recipient of personal data;
- The avoidance of important services being disrupted due to attacks on the security of personal data;
- The facility to conduct proper audits of personal data stored on or transmitted from a meter;
- Appropriate access controls and retention periods;
- The aggregation of data whenever individual level data is not required.

One of the aspects which can cause public trust to diminish is the retention of data. Namely data retention for the purposes of smart metering needs an in depth analysis. since smart metering, by collecting and processing data on all electricity flows within the grid, is capable of contributing to ubiquitous surveillance of the energy consumers by collection of facts and details arising from consumption of electricity i.e. profiling. Depending on the actual technical design of a particular electricity grid, smart metering can have a profound negative impact on privacy. A suggestion that privacy is jeopardized may cause public trust to diminish unless proper transparent strategies are in place to convince the people.

Data retention covers storing data (personal or any other type) for meeting various legal and business data archival requirements, as well as backup and historical purposes.

There are several reasons for the retention of personal and technical data within smart metering. Depending on future developments and desired functionality there can be even more of them.

1. Network Maintenance. The utilities need some data, both personal and technical in nature, that is required for standard network operation. For this kind of data, in many cases there is little reason for long term retention – if it had not been used within a week, the data usually provides little benefit. For some long term maintenance functions, utilities need to store information for a longer period of time. In this case, the information could be aggregated, either over several users as to be large enough to ensure privacy, or by deriving very coarse grained information about a single customer (e.g. assigning one of ten customer profiles). Some cases (e.g. local legislation) may warrant the retention of more detailed data for a specific purpose. Some operators will need detailed data and some might be satisfied on aggregated or anonymised data. Hence, special attention must be paid to those operators who process personal data (i.e. non-aggregated and not anonymised).

2. Billing and payments. Certain data must be retained in order to compute the electricity bill. An estimate on the retention time is around a year, but depends on payment intervals. There is a difference among the countries between the current practices on frequency when the customer is billed.

3. Taxation. Utilities need to maintain some financial data (i.e. on their income) for tax purposes for a specified time (tax records). It seems that tax record can sufficiently rely only on the top-line figures (e.g. the final sum of bills/invoices). This would not include detailed data on electricity consumption (e.g. the 15-min interval meter readings.).

4. Added Value Services. These are additional services, apart from energy supply, provided by the utility and/or third parties on a commercial basis. These are of high business-related importance for distributors and suppliers. They are capable of providing more benefits for all Smart Grids actors (e.g. energy savings), but also of too big an intrusion to private live. At present, we do not know much exact examples of such services. Yet nobody can predict what market value for third parties can have the detailed data on energy consumption. Two simple examples can be given as the optimisation of energy consumption (e.g. ‘join the savings programme’) and goods or services offered thy third parties: (e.g. ‘since it is known that you do not use much electricity after 8 pm, go to the cinema half price’).

5. Law enforcement. There are a number of points of interest for law enforcement (e.g. police, intelligence, tax and customs authorities) in smart metering’s data retention. Here we are touching criminal law and thus the rules on due process (fair trial) and presumption of innocence must be observed.

6. Policy-Making. The state itself (as a regulator) might be interested in data retention for the policy-making purposes. It is a matter of energy security and production planning, among others.

7. Profiling, red-lining and discrimination. The detailed data on electricity consumption might interest various commercial actors outside the electricity market, among others. The retained data are vital for making a customer's profile, as the creation of a profile highly depends on retained personal data. The 'profiling' means 'an automatic data processing technique that consists of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes.' A 'profile' is 'a set of data characterizing a category of individuals that is intended to be applied to an individual. Such profiling might lead to denial of services or increase their cost should a profile proves to be somehow dangerous or risky ('red-lining'). Furthermore, even a simple and non-detailed profile of energy consumption might facilitate commission of certain types of crimes.

VI. Technical Solutions

Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids [5] presents WAN interface to AMI subsystem & Head-End is used to connect the meter, a Local Network Access Point, or a Neighbourhood Network Access Point to a Central Data Collection system. Typical interface platforms for these interfaces are PSTN networks, public G2 (GPRS) and G3 (UMTS) networks, DSL or broadband TV communication lines, power line communications (PLC), either in narrowband or broadband.

The Head-End systems are the central Data Collection Systems for the Advanced Metering Subsystem. Head-end systems are typically part of an AMR (automatic meter reading) or AMM (automatic meter management) solution.

The interface towards the gateways and data concentrators (Network Access Points) is being standardized with Mandate M/441 whilst the interface from head-end systems towards central ERP and meter data management systems is covered by other IEC TCs, e.g. IEC TC 57 (61968-9).

Little work exists on the design of technical solutions to protect privacy in the smart grid [13]. Wagner et al. propose a privacy-aware framework for the smart grid based on semantic web technologies. Garcia and Jacobs design a multiparty computation to compute the sum of their consumption privately. The NIST privacy subgroup suggests anonymizing traces of readings, as proposed by Efthymiou et al., but also warns of the ease of reidentication. Molina et al. highlight the private information that current meters leak, and sketch a protocol that uses zero-knowledge proofs to achieve privacy in metering. Kumari et al. propose usage control mechanisms for data shared by smart meters connected to web based social networks.

It is equally important to make the principle of privacy by-design mandatory, including principles of data minimization and data deletion when using privacy enhancing technologies. As it is currently almost impossible to ensure the full anonymisation of personal data and it is often possible to 're-identify' or 'deanonymise' individuals hidden in anonymised data with astonishing ease, only aggregated data should be used to the maximum possible extend. Considering significant privacy threats, we ask for privacy impact assessment to be conducted prior to the smart meter roll out.

Usually in data retention, data that is anonymised is considered non-personal because the data subject can no longer be identified and thus is not affected by the data protection framework. However, it is almost impossible to ensure the full anonymisation of personal data and it is often possible to 're-identify' or 'deanonymise' individuals hidden in anonymised data easily by using e.g. advanced algorithms or conjunction with other data sets. Therefore in some cases the means likely reasonably used for identification would allow for the identification of the data subject and in consequence would lead to the processing of personal data which are subject to data protection principles.

In respect with the aggregation of personal data, it is not clear how many persons one needs to aggregate on to protect individual data. This is also very context- and data dependent. Some research indicates that the minimum number of users is around 7 to 8, but in many circumstances it will be more. In case a meter is 'adjacent' to a household (i.e. majority of situations) we cannot say that we have any kind of data aggregation. There are simply too few inhabitants in such a household.

On the other hand, it is possible to have a smart meter that is able to 'tell' which exact device was used at a particular time. It is easy to build in and there is actually a lot of research in de-aggregating the readings. It is certainly easy to identify big devices like a washing machine, tea kettle, etc. But even if data is aggregated over devices, it is critical – you can tell when one comes home in the evening, even if one does not know whether the device one uses then is light, the tea-cooker, or a computer. Hence, the concept of data aggregation is here obstructed. Moreover, technical standards and systems should be developed with a focus on upgradeability to safeguard end to- end security ensuring the overall intelligent metering system is future-proof and ready to cope with future challenges.

Standardization of smart grids is neither straightforward due to the huge number of stakeholders, the necessary speed, the many international activities and the still changing solutions make it a difficult task. Specific for the data privacy aspects, the 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.

Currently, there is no publically available reference architecture for Smart Grids with references to how privacy is designed into the core functionality, referring to all standards and principles for IT systems, business practices, and physical

designs and networked infrastructures.

Furthermore like in any other ICT-based infrastructure, cyber security has to be deeply analyzed. A single point of failure or back-door in the grid management system may be exploited to cut electrical supply to a country, resulting in enormous economic losses and endangering the whole community. Also, SmartGrids based ICT will transfer a lot of sensitive data that can be exploited to breach privacy, consequently, research has to ensure that state-of-the-art data-protection and data-privacy approaches are taken into account. To this end the communication systems and ICT should be upgraded to fast and diversified paths of data infrastructure.

Apart from consumer information handling in respect with security, privacy and data Protection, handling of huge amounts of data, the research issue is also the analysis of central versus decentral management.

Also Privacy Enhancing Technologies have to play significant role in the case of Smart Grids. While modern data mining technologies undermine classic protection, new advances in cryptographic techniques have become practical, and allow us to build systems that do not require the sharing of personal information. In a nutshell, it has become possible to compute almost arbitrary functions on encrypted data, i.e. the entity that handles the data never learns any input, only the result of the computation.

VII. Conclusion

Privacy and data protection challenge is arising in the move from the electricity grid towards the Smart Grid being unprecedented in terms of scale and complexity. This weighs even heavier dealing with critical infrastructure, in some cases unclear goals, some players moving into domains they have little experience in, a potentially huge privacy impact and an in-vivo implementation. An entirely new and complex model of inter-relationships poses challenges for the application of data protection. The wide ranging nature of the issues presented by smart metering hinders to encompass an exhaustive list of privacy and security points. In this emerging area, it is fully expected that new data protection problems and solutions will evolve as more smart meters are installed. The massive rollout of smart meters is already happening, so there is urgency to manage the way that smart meters process personal data, and the issues of general concern which warrant serious consideration by all those involved in this area.

References

[1] ANEC/BEUC POSITION ON ENERGY EFFICIENCY, Joint ANEC/BEUC position paper on the Commission's Communication "Energy Efficiency Plan 2011"

[2] Article 29 Data Protection Working Party, Opinion 12/2011 on smart metering, WP 183, 4.4.2011

[3] BEUC Response To CEER Public Consultation On Demand Response Programmes

[4] Cavoukian A., Privacy By Design …Take The Challenge, Book.

[5] CEN/CENELEC/ETSI Joint Working Group, Standards for Smart Grids, Final report, 4 May 2011.

[6] Elster's White Paper, Privacy Enhancing Technologies for the Smart Grid, 4.10.2011

[7] European Commission, COM(2010) 609, A comprehensive approach on personal data protection in the European Union Brussels, 4.11.2010

[8] European Commission, COM(2011) 202, Smart Grids: from innovation to deployment, Brussels, 12.4.2011

[9] European Technology Platform SmartGrids, Strategic Deployment Document for Europe's Electricity Networks of the Future

[10] Kursawe, K., Danezis, G. and Kohlweiss, M., Privacyfriendly Aggregation for the Smart-grid.

[11] NISTIR 7628, Guidelines for Smart Grid Cyber Security, September 2010

[12] PbD, SmartPrivacy for the Smart Grid, November 2009.

[13] Rial, R. and Danezis G., Privacy-Preserving Smart Metering, WPES11.

[14] The Task Force Smart Grids Expert Group 2 report on "Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection". 06 June 2011.

[15] European Technology Platform SmartGrids "Strategic Research Agenda for Europe's Electricity Networks of the Future - SmartGrids SRA 2035" March 2012.