23 February 2012

Work Package 2.2

Inclusion of effective security measures for smart grid security and resilience

Programme of Work

Expert Group on the security and resilience of Communication networks and Information systems for Smart Grids

Version 0.5

Table of contents

1. Introduction

Work Package 1 investigates the "Risks, Threats and Vulnerabilities" linked with the Information and Communication Technologies (ICT) part of a Smart Grid Infrastructure. Work Package 2 aims at identifying "Requirements and Technology" that can be used to address the vulnerabilities identified within Work Package 1.

In this context, Work Package 2.1 considers the phases and stages for risk mitigation to establish categories of security requirements and attributes of security measures. The present work package (2.2) intends to extend the high level security requirements identified previously to include effective security measures.

In this work, we distinguish "security requirements" from "security measures" according to the definition of the "Privacy and security of the Advanced Metering Infrastructure" study made by Netbeheer Netherlands [NL AMI], i.e.:

- Security requirements are setting the security goals, by answering the question "What do we want to achieve?" As such they are supposed to be technology agnostic.

- Security Measures provide a way, or at least guidance for satisfying a security requirement, by answering the question "How do we achieve this?" They may typically be technology related.

1.1. Mission, vision and goals

There are currently several Smart Grid standard initiatives that are useful in harmonising the design and operation of Smart Grids. This includes in particular the NIST work in the USA, [NIST Framework] with the 3 volumes of NIST IR 7628 [NIST 7628] on the security side in particular, and the work under the EC M/490 mandate conducted by the Smart Grid Coordination Group of ETSI/CEN/CENELEC in the European Union, with the Smart Grid Information Security (SGIS) group report [SGIS] on security.

In order to effectively secure Smart Grid communications, the considered standards can be extended to include security measures. Standards need to be based on a threat and risk-based approach.

1.2. Strategy

The approach is to first analyse existing documents and build upon that to reach an integral overview of effective security measures. These documents include on the smart grid specific side:

- the NISTIR Guidelines for Smart Grid Cyber Security [NIST 7628 V1], [NIST 7628 V2] and [NIST 7628 V3]. Volume 1 in particular includes 197 high level Security "Requirements", generally with technical enhancements which are actually security measures. Volume 2 focuses on Privacy and Volume 3 contains supportive analysis and references justifying the security requirements and proposed measures. New Research and Development themes for Smart Grid Cybersecurity are identified in Chapter 8 of Volume 3.
- the SGIS draft report [SGIS] developed by the SGIS subgroup of the ETSI/CEN/CENELEC SGCG
- the work in other Work packages of the Expert Group on Smart Grids ICT Security, as listed in the introduction
- the Reports of Expert Group 2 of the EC Smart Grid Task Force, i.e. the report on Regulatory Recommendations for Data Safety, Data Handling, and Data Protection [EG2 Report] and "Recommendations to the European Commission for Essential Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection" [EG2 REQ]

This list is further refined in Section 2.1 of the present report. The rest of Section 2 then focuses on adapting the already extensive list of security measures provided by NIST to the European framework and completing them in specific areas, based on the other documents identified.

1.3. Scope

In line with the scope of the expert group, we only consider security measures for ensuring the security and resilience of the ICT part of smart grid infrastructures. As such, power protection measures that can be implemented on the energy plane independently of ICT components are not considered.

Best efforts are made to effectively cover all the domains of a smart grid infrastructure, especially in the context of the European framework which integrates issues left aside by the US work, such as the preservation of individual privacy and the integrated management of Distributed Energy Resources and Electric Vehicles connecting infrastructures.

Results: Inclusion of effective security measures through smart grid requirements related to security
Deliverables: List of smart grid requirements related to security, put in relation with effective security measures.

1.4. Team

Team leader:

- Francois Ennesser, Standardization & Technology Technical Marketing at Gemalto. In charge of M2M standardization activities for Gemalto, Francois chairs the Security Working Group of the ETSI Technical Committee M2M (Machine to Machine) and is involved as ETSI representative for the security aspects of EC standardization mandates M/441 (Smart Metering), M/468 (Electro Mobility) and M/490 (Smart Grids). He represented ETSI in Expert Group 2 of the Smart Grid Task Force and is now active in the SGIS Working Group for M/490. He holds a joint Diplome d'Ingenieur with honours from Ecole Superieure d'Ingenieurs en Electrotechnique et Electronique (Paris) and a Master of Science in Electrical Engineering from the University of Southern California (Los Angeles).

Team members:

- Monika Josi, Chief Security Advisor EMEA at Microsoft Corporation.

- Elyoenai Egozcue, Security Researcher at S21SEC.

- Hani Banayoti, Executive consultant at ATOS. Information Security consultant who has been working in the consulting profession since the late 90's. Hani has extensive knowledge and application of security standards and risk management principles applied across numerous industry sectors with special focus on SmartGrid/Metering applications.

2. Review of existing work

2.1. Relevant International standards

In addition to the high-level work listed in section 1.2, and as noted in the SGIS report [SGIS], there are already established standards in specific industries that contain security requirements and measures applicable to Smart Grids, even though these standards are not smart grid specific.

- Within the ISO 27000 series, which addresses high level operational and technical requirements for Cybersecurity as considered in WP 2.1, the ISO 27001 [ISO 27001] and ISO 27002 [ISO 27002] are especially relevant. Note that a new revision of ISO 27002 is currently under review. Considering the wide overlap with the NIST IR 7628 requirements for Smart Grids, the M/490 SGIS group is recommending the development of a smart grid sector specific standard within the ISO 27000 series to cover the operational aspects of smart grid cyber security. One important aspect is that organizational security recommendations should not only target the actors directly involved in grid operation, but also the organizations involved in product development and manufacturing, the integrators, and any third party involved in configuring the product and bringing them into operation. Extension of the standards in this direction are also addressed by the M/490 SGIS Working Group.

- IEC 62351 [IEC 62351] is a recognized series of standards in the field of Supervisory Control and Data acquisition in the power systems domain. It was developed for handling the security of the large series of protocols developed by IEC TC 57 such as the IEC 61850 series. Its security objectives focus around intrusion detection, authentication of data transfers through digital signatures and prevention of unauthenticated access, eavesdropping, playback and spoofing. The SGIS group of M/490 foresees that it could be extended to cover more technical/products related aspects of smart grid cyber-security. It also partially overlaps with the NIST IR 7628 and ISO 27001/27002 requirements.

Annex B of the SGIS draft report includes a detailed gap analysis between these existing security standards and NIST IR 7628 Volume 1.

2.2. Completeness of NIST IR 7628 for Smart Grid Security and Resilience

Assuming the above extensions foreseen by the M/490 SGIS Group would provide a complete coverage of the 197 Smart Grid security requirements identified by NIST by international or European standards, we still have to consider that the NIST framework does not fully address some specific parts within our scope:

- Aspects related to the resilience of ICT infrastructures for smart grids were not directly addressed by NIST. This is addressed in section 3.2 of this report.

- The integration of Distributed Energy Resources and the infrastructures for handling electric vehicles (with the ability to charge batteries but also to exploit their available capacity to smooth production) was not addressed by the NIST work, while these aspects appear fundamental for the fulfilment of the 20/20/20 objective set by the European Union. These aspects are addressed in section 3.3.

- Some issues impacted by national legislation and regulation such as Privacy and certification/accreditation schemes were written within the US context and need to adapted to the European Union regulatory framework, also taking into account variations of national legislations within EEC countries. Privacy considerations, certification schemes, and the establishment of a trusted network for sharing security incidents and good practices are the object of sections 3.4, 3.5 and 3.6 respectively.

2.3. Lessons from the AMI domain

On the other hand some aspects of the NIST work have already been largely completed, adapted or duplicated, noticeably within the context of several European Union countries, when it comes to the Automated Metering Infrastructure domain:

- The US Advanced Security Acceleration Project- Smart Grids (ASAP-SG) published a "Security Profile for Advanced Metering Infrastructure" [ASAP-SG AMI].

- In the Netherlands, a study report on AMI Security and Privacy was published by Netbeheer Netherland [NL AMI], clarifying the regulatory framework and deriving Security Requirements and Measures.

- In the UK, a public consultation was conducted in 2011 on the "Draft Smart Metering Security Requirements" [UK Meter] published by the Department of Energy and Climate Control. Apart from differences resulting from the centralized model for the metering infrastructure developed in the UK, the proposed security certification relies on US NIST standard FIPS 140-2 which was intended for cryptographic modules and therefore leaves aside aspects relevant to complete, more open systems such as meters or communication hubs. Therefore, such certification can typically be reached without relying on specific tamper resistant security hardware.

- In Germany, the BSI took the initiative to define a Common Criteria (ISO 15408) "Protection Profile for the Gateway of a Smart Metering System" [BSI GPP], as it identified the Communication Gateway (bridge between the local and WAN communication infrastructures) as the critical entity in the AMI architecture to ensure security and privacy. This relies on a secure element also certified according to "Protection Profile for a Security Module for Smart Metering Systems". The intention is to require security certification according to these protection profiles for such products to be deployed in Germany. The required Evaluation Assurance Level is EAL 4+, one of the highest levels, which typically requires specific security hardware and strong security software design for resistance to tampering attempts. In the future, this scheme may lead to the emergence of independent gateways addressing unregulated smart grid functions, allowing flexibility of evolution, which would co-exist with the regulated gateway.

It is important to realize that there are aspects of national laws that may impact the security requirements of the Smart Grid Infrastructure. For example in the AMI domain, the ownership of the smart meter (is it e.g. considered part of the distribution domain governed by the DSO, or part of the house and owned by the consumer?), and the possible presence of a centralizing entity as in the UK model, may imply regulatory impact affecting the security recommendations. The risk is that the lack of harmonization on such aspects within the EEC prevents the development of a single European market in the energy domain: The lack of a single market may have negative impact on innovation and price and reduce the competitiveness of European players in this market.

3. Development of European Smart Grid ICT security measures

3.1. European coverage of Security measures from NIST IR 7628

In this section, we review by category the security measures from NIST IR 7628 Volume 1 [NIST 7628 V1] that are not already covered by requirements of standards applicable in Europe. A wide coverage of the NIST Smart Grid Security requirements is fortunately provided by the ISO 27001, ISO 27002 and IEC 62351 international standards, according to the analysis of Annex B in SGIS report [SGIS]. Appendix A of the US Department of Homeland Security "Catalog of Control System Security Recommendations" [DHS CS], which overlaps at about 90% with NIST IR 7628 Part 1, further contains a wider cross reference of its security measures with those of ISO 27001, ISO 27002, IEC 62351, FIPS 140-2, NERC CIP, ISO 17799 (Code of Practice for Information Security Management), IEEE 1402 (Guide for Electric Power Substation Physical and Electronic Security) and some more specific documents.

The result of this analysis highlights the categories of smart grid security measures which deserve particular focus, due to deficiencies in prior work.

The following categories seem to be well covered by the mentioned existing International Standards:

- Security Assessment and Authorization (SG.CA)
- Identification and Authentication (SG.IA)
- Media Protection (SG.MP)
- Program Management (SG.PM)
- Personnel Security (SG.PS)
- Risk Management & Assessment (SG.RA)

The following NIST requirements in the below categories are either not covered, or only partly covered, or covered but not satisfied by international standards:

NIST IR 7628-1 Requirement	Covered but not met	Covered in part	Not covered
Info system & Comm. protection(SG.SC)	10,13,23	4,17,21,25,26	24,25,27,28
System & Service acquisition (SG.SA)	1	3,4,8,10,11	
Access Control (SG.AC)	11, 16, 18, 20	9	
Physical & Environmental sec. (SG.PE)	7	6,10	8
Planning (SG.PL)	2,4	5	1
Configuration Management (SG.CM)		1,7,11	10
Continuity of Operations (SG.CP)	8		11
Incident Response (SG.IR)		4	8
Development & Maintenance (SG.MA)	2	1	
Information and doc. Mgmt. (SG.ID)		5	
Awareness and Training (SG.AT)	7		
Audit and Accountability (SG.AU)	7		
Info system & Info. integrity (SG.SI)		2	

From this analysis, we can draw the following conclusions:

- ***Generally, measures related to organizational security are already well covered by international standards, but they have not been adapted to fit the smart grid ecosystem which will involve a multitude of actors, each bearing their own security risks.***

- ***Technical measures related to the protection of the information and communication system, including issues related to acquisition and access control, require significant extension to address smart grid security risks.***

It has to be noted however that this analysis did not consider standards related to specific information and communication technologies that may support a smart grid ICT backbone. An extensive list of applicable security specifications for several mainstream communication technologies was provided in Appendix C of the SGTF EG2 initial Report [EG2 Report]. While some ICT technologies, such as wireless WAN, already implement strong security measures, other technologies may require significant security enhancements to meet the smart grid security requirements. Selection of particular ICT technology however remains subject to other constraints (latency and availability constraints, resilience, etc.) that are likely to be predominant over security considerations. The focus on process security should not leave aside product security. Especially in equipment markets like smart metering, security not only needs to be designed in, but also priced in.

3.2. Extending NIST security measures toward Smart Grid Resilience considerations

The purpose of this section is to identify directions for further extensions of the requirements in NIST IR 7628 Volume 1 [NIST 7628 V1] to reinforce the resilience of the Information & Communication Infrastructure of the Smart Grid.

The following high level requirements have been identified in previous work of the SGTF Expert Group 2 [EG2 REQ] (Recommendation EG2.S.2) and the present Expert Group regarding resilience of ICT infrastructures for smart grids:

- The Smart Grid ICT Infrastructure should have Black Start capability, even after long periods of blackout.

- It should provide graceful degradation, always maintaining as much of its core functionality as possible. Dependencies on other information & communication infrastructures should be minimized. Critical functionalities should not be endangered by less critical ones (e.g. processes that do not have strong latency requirements could be interrupted in emergency situations).

- It should provide uninterrupted services, even in crisis situations (natural, e.g. earthquake, or human generated, e.g. massive IT attack). Following disturbances or interruptions, all processes and functionalities should be able to resume normal operations.

- Problems affecting the ICT infrastructure should not compromise safe operation of power equipments. The energy infrastructure should be able to operate independently of ICT in a safe manner, though without optimization, as a fall-back mode in case of failure of the ICT infrastructure. Impact of ICT incidents in the power domain should always be minimized.

- Furthermore the differences of expected lifetime between ICT components and power equipments, which can reach a factor of 10, should not endanger the level of reliability reached by traditional power grids.

Going further, the following general measures can be recommended for the robustness and resilience of Smart Grid ICT infrastructures:

- ***All architectural layers of the smart grid, taken independently (power layer, communication layer, information layer…), should be as robust and resilient as possible with regard to delivering its services toward other layers.***

- ***Power devices should be able to overrule ICT-issued commands whenever they are seen as not electrically appropriate (i.e. they may compromise electric safety), even when the addressed asset is owned by a prosumer (e.g. Distributed Generation).***

- ***The smart grid ICT infrastructure should be able to switch to independent back-up power in case of outage of their main power source.***

- ***The information architecture for communication and processing should be distributed, to minimize the risk that attacks on a critical node could lead to global compromission.***

- ***Smart Grid ICT infrastructures should be deployed with sufficient redundancy to provide the intended level of availability, also taking into account the shorter lifetime of ICT equipments compared to power elements. Ideally, deployment should be planned so that redundancy is ensured between equipment with different expected lifespan, to limit the risks of redundant equipments failing simultaneously. Redundancy between equipments in different geographic locations should be preferred to limit the risk of disruptions, and required for critical elements (this requires that all the information required for operation is available in all places to enable service take over).***

- ***The large amount of information acquired from sensors and processes within the smart grid ICT infrastructure should be exploited for predictive rather than reactive maintenance of ICT equipments as well as power elements.***

- ***The amount of traffic exchanged on the smart grid ICT infrastructure should be minimized, by promoting local processing of the information within a node and communicating only the minimum required information to other nodes.***

- ***The communication links of the smart grid ICT infrastructures should be dimensioned to withstand surges in traffic that may occur even as a result of emergency situations. Extensibility and flexibility should be promoted to facilitate adaptation to evolving traffic conditions.***

- ***It should be possible to isolate affected ICT components, where such precaution is necessary to prevent extension of damages to other elements (e.g. cascading effects).***

Regarding the involvement of Distributed Energy Resource and Storage within the grid, grid resilience will benefit from requiring the support of islanding, especially forced islanding imposed by grid outages. The main impact for supporting islanding will be more on power equipment than on ICT infrastructures. However possible disruptions of the grid ICT backbone in emergency situations should not prevent fall-back to islanding mode, and may even be used as a trigger for switching into islanding mode.

Standards for DER and Storage integration in transmission and distribution systems that properly address the power disturbance they may generate when switched on and off (avoiding possible cascading effects on triggering conditions) will be essential to ensure smart grid stability and resilience. This requires proper standards for modelling such resources.

3.3. Additional Security measures to address the Distributed Energy Resources and Storage, including Electric Vehicles Infrastructures

As noted previously, the domains related to the integration of Distributed Energy Resources (DER) and storage as well as electric vehicles charging infrastructures within the smart grid has not been considered in the previous studies identified above. Intermittent generation from renewable source combines advantageously with Vehicle-to-grid technology to exploit the transient storage capacity of electric vehicles batteries connected to a charging facility. In this context locally plugged Electric Vehicles can be integrated in the grid as a DER, even while they are seen as a load at other time. This requires transmission of proper tariff incentive to the customers and easy-to-use interfaces for configuration of customers choices upon plug-in.

The purpose of this section is to address the additional ICT security requirements and associated measures that arise from the integration of these domains. The term "Prosumer" has been used in reference to the resulting need to measure and bill customers based on the (positive or negative) difference between the energy generated from their facilities (wind power generators, solar panels, or local, e.g. electric vehicle, storage drawn from local charging station at time of peak) and the energy consumed locally: A positive difference corresponds to energy that can be redistributed to the network from the consumption point, while a negative difference represents an actual energy consumption from the network as in the traditional model. Such "prosumer nodes" may be aggregated by specific market actors to be seen as Virtual Power Generation facilities. The consumption of on-site generated electricity (e.g. by tenants) needs to be subject to efficient and reliable commercial process, though not necessarily managed via existing market communication processes. These measures might increase trust and participation of the end consumer.

On the power side, DER integration requires the support of bi-directional energy flows in the Distribution domain, which is a change of paradigm from traditional energy grids and introduces new risks with potential

hazardous physical impact on expansive power elements (transformers etc.). Safe connection of local (low or medium voltage) generators to the network requires proper control of the generated power (active and reactive), to ensure good synchronisation in terms of phase, frequency and voltage. Therefore, the security of the ICT control infrastructure for managing DER is not less sensitive than for other parts of the distribution domain, while it is potentially more exposed to attacks due to proximity to network access points on the customer side (communication gateway with access to metering units for consumed and generated power) and risk of frauds impacting the payment and settlement system for DER generation.

In principle, the measurement of DER-generated energy transferred to the network will be subject to similar risks (tampering for fraud) as identified for other metering equipments (cf. Recommendation EG2.M.1 from SGTF EG2 [EG2 REQ] regarding conformity with the measuring instrument directive). This assumes that the measurement takes place after the DER-generated energy (e.g. continuous current) has been converted and synchronized to fit the local grid energy waveform. Such measurements typically take place at the point of entry to the grid. The owner of the DER resources connected to the entry point, however, cannot always be identified unambiguously, and in the future, flexibility will require accommodation of displaceable resources such as electric vehicles allowing the energy network to draw energy from their battery during hours of high demand. Such scenarios will require the capability to uniquely identify the locally plugged resource to handle the billing properly. Low-cost identification and authentication techniques similar to those deployed today in mobile telecommunication or credit card systems can be reused for this purpose.

Unfortunately there is still a lack of standards in this domain regarding electric equipment safety and information protocols (e.g. for reporting conditions and triggering action), which needs to be quickly addressed under M/490 to allow timely development of this important area of benefits for smart grids. However the considerations above lead to the following specific additional security measure:

- ***The reporting of power generated locally by distributed energy resources or storage requires proper identification and authentication of the involved resource and its asset owner.***

Technically, this could be met by implementing within the distributed generation equipment (e.g. Photovoltaic panel, wind power generator or electric car battery) a "thin client" (as defined by NIST) with a communication unit and a secure processor providing tamper-resistant storage of local identification and authentication credentials, which would authenticate to a network server (part of a central management platform) in charge of aggregating renewable reports for billing and settlement purposes, and provide certified reports of the locally generated power. This also enables performance monitoring of locally distributed resources for efficient maintenance of the equipment as well as services delivered by third parties such as carbon credit aggregation or electricity donation to Non-Governmental Organizations (e.g. schools).

3.4. Adapting NIST security measures for the European Privacy context

In this section, we attempt to adapt and complete the considerations from NIST IR 7628 Volume 2 [NIST 7628 V2] in the area of Privacy for the context of European privacy legislation and cultural sensitivity, by building on the recommendations from SGTF EG2 and the Dutch experience in this area.

First of all, it is important to remind that risks related to privacy exposure should not be considered solely within field-specific contexts such as Smart Grids: Instead, privacy risk assessment must take into account all the potential exposures of an individual throughout his daily life, whether they are related to individual communication transactions, energy management and billing, banking, use of automobile (tolling for road usage), ticketing for public transport or entertainment, or health monitoring. This is because modern profiling techniques allow retrieval of an individual's identity from a combination of different exposures, even when each exposure is properly anonymized when considered separately. Only by minimizing exposure at the root level in each individuals private interactions can privacy be properly ensured. Any dissemination of even properly

anonymized information about an individual's private life, if multiplied across several domains, will eventually expose his/her privacy all the same.

The importance to address privacy issues in the smart grid security context was already acknowledged by NIST and lead to the development of NIST IR 7628-2. Though this was developed in the context of the North American privacy legislations, high level requirements remain generally applicable, and especially:

- The design of Smart Grid Applications and devices should allow consumers to have control of their personal information to the greatest extent possible. In particular, all usage details records should be seen as user-generated content owned and controlled by the consumer.

Following the consumers concerns about privacy which blocked an initial attempt to roll out smart meters in the Netherlands, Expert Group 2 of the SGTF conducted an extensive review of the European legislative framework around privacy which resulted in 11 Privacy-related recommendations to the European Commission [EG2 REQ]. Most of these recommendations such as the use of Privacy certification schemes to re-establish customers trust or the need to clarify the notion of personal data do not impact smart grid security measures.

However, in line with the privacy analysis above and high level requirement expressed by NIST, the guiding principle of Privacy by Design and by Default expressed in Recommendation EG2.P.3 easily translates into a general security measures on the ICT infrastructure to protect privacy in the smart grid. Indeed:

1. The different smart grid actors requiring access to consumers personal information and devices (such as the energy retailer for billing, the DSO for line quality monitoring, a settlement authority, or a privately contracted third party processing customer information) each only need to receive those specific extracts of the private data that are enabled by their specific roles according to applicable legislations.

2. There is always be some (even if limited) secure information processing and storage capability at the point where consumers private data (typically fine scale energy consumption readings) are generated (typically in a smart meter) or exposed outside of the private consumers environment (metering gateway, as access point to the Home Area Network).

As a consequence, the most efficient measure to ensure "Privacy by Design" is to:

- ***perform locally, within the private environment of the customer whose personal information are at stake, all the processing of personal data required to extract the pieces of information needed by smart grid actors.*** Locally distributed processing saves the cost of exporting raw data to a central database and processing them centrally. Distributing the processing over multiple local nodes further increases resilience by reducing the risk that a security compromise at a single central point could give an attacker extensive control of the system and the customers data.

- ***send only the processed data externally, via a secure communication link established with the service provider entitled to receive those data.*** This has the further advantage of minimizing the amount of data exchanged over the communication infrastructure. Note that such processed data may still contain personal information, but the fact that it contains no more personal information than necessary to deliver an intended service should promote customer's trust. It is of course assumed that the receiving entity has obtained legal permission to manipulate such (potentially personal) information for its business, and will meet its responsibility to protect such data if they are indeed personal.

With this principle, consumption data could be acquired at much finer time interval than currently considered (e.g. every minutes) without compromising privacy (since the raw data are not sent outside), nor increasing the amount of data transfer over the communication infrastructure. Yet the information contained in the acquired data could be extracted by relevant actors, e.g. the meter or gateway could be instructed to immediately notify the energy distribution organization when an important change of consumption load occurs locally (thus minimizing latency and facilitating correlation of customer actions with market signals rewarding reduction of

consumption during peak demand). The risks of frauds are not affected as long as proper security is implemented locally to prevent compromission of code and data, which is anyway required in all cases. An example of technical implementation of Privacy by design through local processing is described in Annex A.

Such local processing is definitely the best way to provide the consumer full control over his private data and create trust, compared to schemes where personal data are first accumulated in a central database over which the consumer has only indirect control through an entity he may not trust.

Even with these techniques, a privacy risk remains when personal data are exchanged within the private environment of the consumer using network technologies (local or home area network) that can expose unprotected data outside of his premises (this is the case e.g. with some powerline technologies). Such risks can be prevented by encrypting the data securely even for local exchange of the data between a meter and a communication hub.

3.5. Smart Grid Security conformity, product certification and organizational accreditations in the European context

In this section, we consider how the security measures involving certification of products or accreditation of people or organizations can be accommodated within the European legislative framework. Special attention is given to the already diverging directions taken in several EC countries regarding AMI deployments, as a result of unaligned national business models, legislations and accreditation organizations.

The NIST Framework and Roadmap for Smart Grid Interoperability Standards recognize the need to develop a conformity assessment program for security requirements: This is because standards cannot ensure proper implementation of security functionalities. Even when a product or system demonstrates compliance with a highly secure functionality specification, it does not guarantee that there is no implementation breach in the system. There are countless examples of proven security algorithms that have been subject to breaches in specific environments because of poor implementation (e.g. faulty Random Number Generator used in key generation). Even when relying on a tamper-resistant hardware, straightforward implementations of cryptographic algorithms may lead to the exposure of sensitive information through side channel attacks such as Simple or Differential Power Analysis.

The experience gained from other industries shows that ***regulatory obligations combined with a certification scheme is the most reliable option to ensure the security level of deployed equipments***. The importance of a ***unified certification framework for European smart grid deployments*** was also highlighted by the SGTF EG2 [EG2 REQ] in their recommendation EG2.S.4.

The most proven scheme for security certification is the Common Criteria methodology standardized by ISO [ISO 15408]. NIST standard FIPS 140-2 is also used in the US but tackles only part of the problem by testing only cryptography and is mostly appropriate for cryptographic modules rather than complete systems such as smart meters or communication hubs. Several industry-specific certification schemes also exist, such as EMVCO and PCI in the payment card industry, or GSMA SAS in the wireless telecommunication industry.

Examples of successful certification schemes in Europe include:

- Secure Signature Creation Devices
- Electronic passports
- Payment cards
- Wireless network cards (aka SIM)

- Tachograph devices
- Point of Sale terminals accepting payment cards

This large number of certifications established since several years has resulted in a network of mature evaluation laboratories that can perform reliable and affordable security testing.

It should be noted that ***reaching a European agreement on certification would allow the industry to address a wider market with similar products and significantly reduce the design costs***.

The EC should consider either to rely on an existing certification scheme (for example Common Criteria) or to jointly create a more suitable one in cooperation with the industry (which could lower certification costs if properly tailored to industry practices). In any case a work stream should be created on that subject in order to work on evaluation scheme, security testing level and scope, laboratories accreditation, etc.

3.6. Further considerations for the European context

The smart metering experience reported in section 2.3 highlights the ***importance of coordinating smart grid security aspects at the European level to ensure the compatibility of specific national frameworks and consistent interpretation of applicable directives***, if the final target for a more integrated European energy network requiring cross-border interoperability is to be reached. This aspect was already highlighted by EG2 in their recommendation EG2.G.3 [EG2 REQ].

The other recommendations to further complete the European security framework for smart grids that were identified by SGTF EG2 highlight the need to ***establish a trusted network of public and private organizations to encourage the sharing of experiences about incidents, threats, vulnerabilities and good practices*** (see [EG2 REQ], Recommendation EG2.s.1). ***Such a network would provide a good place to further develop and maintain a European catalog of effective Smart Grid security measures as well as security certification of products and organizations and conformity testing***, as was already highlighted in the EG2 recommendation EG2.S.5 [EG2 REQ]. Given potential synergies in addressing ICT issues affecting smart grids and other systems (industrial control, financial transactions, telecommunication systems etc.), this smart grid security sharing network could beneficially be integrated within European or wider networks for sharing cybersecurity incidents and practices, already in discussion in the wider cybersecurity context.

4. Conclusion

It is clear that an extensive set of security measures needs to be applied to ensure the security and resilience of smart grid ICT infrastructures, be it at the technical level (for products and services) or at the organizational level (for involved organizations and processes). But in the end, Smart Grids are very complex systems which involve a large number of actors, some of which may be subject to different requirements and regulatory frameworks (e.g. Energy distribution companies and telecommunication operators). Assuming that each actor masters its own domain, we can hope that proper security and resilience will be implemented sustainably, but for this to happen, the biggest challenges of the smart grid environment still need to be overcome:

- Actors of different domain (e.g. utilities and telecommunication companies) need to be able to cooperate, despite their differences in culture, business practice and professional languages.

- But most of all, despite the complexity of the ecosystem, the legal and regulatory framework must clearly establish the responsibilities of all actors, be it in terms of reliability or security incidents, so that each involved stakeholder is aware of its potential liability in case of incidents and takes due diligence to address the risks in its own domain. Special focus should be given to privacy issues and commercialization of micro-generation in order to reach the engagement of the prosumer / European Citizen.

References

[EG2 Report] Task Force Smart Grids, Expert Group 2: Regulatory recommendations for Data safety, Data handling and Data protection, Report, issued December 10 2010

[EG2 REQ] Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection, Recommendation to the European Commission

[SGIS] ETSI/CEN/CENELEC Smart Grid Coordination Group for the M/490 mandate, Smart Grid Information Security (SGIS) Working Group draft report, version 0.441, January 2012

[NIST 7628 V1] NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, SGIP-CSWG, August 2010

[NIST 7628 V2] NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, SGIP-CSWG, August 2010

[NIST 7628 V3] NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References, SGIP-CSWG, August 2010

[NIST Framework] NIST Special Publication 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, Office of the National Coordinator for Smart Grid Interoperability, January 2010

[ASAP-SG AMI]Security Profile for Advanced Metering Infrastructure, The Advanced Security Acceleration Project (ASAP-SG), Version 2.0, June 2010

[NL AMI] Privacy and Security of the Advanced Metering Infrastructure, Main document, Netbeheer Nederland Privacy & Security Working Group, July 2010

[UK Meter] Draft Smart Metering Security Requirements, U.K. Department of Energy & Climate Change, V0.3, April 2011

[BSI GPP] Protection Profile for the Gateway of a Smart Metering System, v1.1.1 (final draft), Bundesamt fur Sicherheit in der Informationstechnik, 2011

[ISO 27001] Information Technology - Security techniques - Information Security Management Systems - Requirements, ISO/IEC JTC1 SC27, 2005

[ISO 27002] Information Technology - Security techniques - Code of Practice for Information Security Management, ISO/IEC JTC 1/SC27

[IEC 62351] IEC 62351 (parts 1-8), Power System Control and Associated Communications - Data and Communication Security, IEC TC 57 WG15

[DHS CS] Catalog of Control Systems Security: Recommendations for Standards Developers, U.S. Department of Homeland Security, Control Systems Security Program, National Cyber Security Division, September 2009

[ISO 15408] Evaluation Criteria for IT Security (also known as

"Common Criteria")Annex A- Technical example of "Privacy by Design" through local processing

The technical requirements to enable the "privacy by design" vision presented in Section 3.4 are the following:

- The local processing environment (in the meter or communication gateway) has to support an interoperable (standardized) programming capability enabling secure download/replacement/upgrade of applications. This enables contracted service providers to provision their data processing algorithm in the local environment of the consumer using the same infrastructure and technologies as regulated entities (e.g. DNOs).

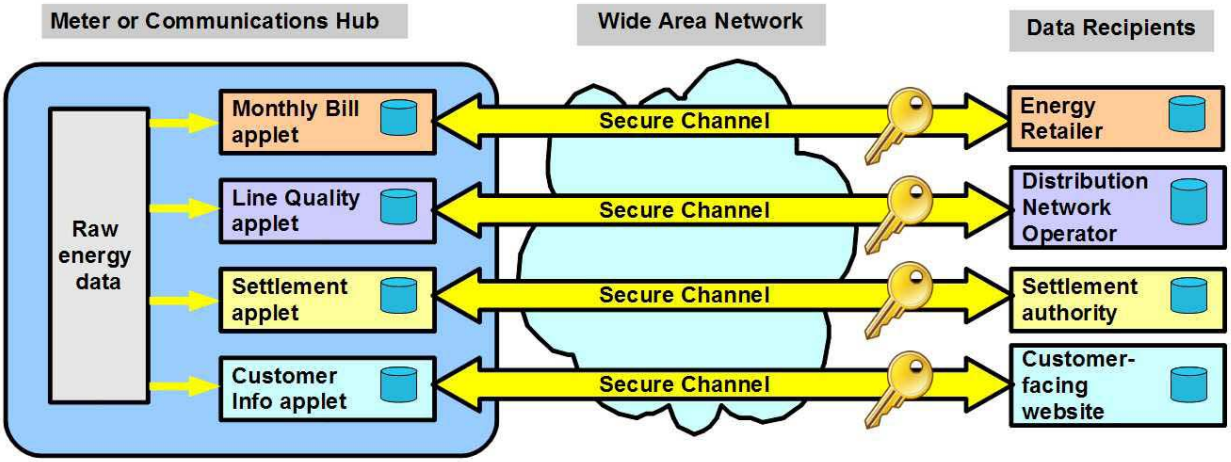
- It shall be possible to remotely administer the local processing environment in a secure manner (addition/deletion/upgrade of applications)

- This programming environment has to provide firewalling to prevent the data related to one application (i.e. one service provider) to be accessed by other applications (i.e. other service providers not entitled to get those data).

- An application shall have the capability, thanks to securely stored credentials, to establish a secure communication channel with a server associated with its service provider. Digital signatures may be used to prove that messages received from an application have really originated from within that application and could not have been fabricated elsewhere.

The need for such technologies had already emerged years ago in other industries such as payment systems and mobile communication networks. Therefore they have become mainstream today in the smart card industry, making them available at affordable cost, and are supported by ETSI standards (e.g. ETSI TS 102 225 and TS 102 226) based on established specifications from GlobalPlatform (www.globalplatform.org) for secure remote application management and from the JavaCard Forum (www.javacardforum.org) for the interoperable programming environment.

The example below illustrates this "privacy by design" concept:



In this example:

- The monthly bill applet simply calculates the monthly consumption from the raw data and rate information, and send the resulting bill amount to the customer. Thus the energy retailer gets the information he needs, but no more.

- Information of interest to the energy distribution network, such as voltage levels, are sent to the distribution network on occurrence of specific events or upon request. Again the DNO receives all the information he needs to smooth network operation, but no more.

- The settlement applet generates time of use profile information that are sent to a settlement authority, who can use this to improve the settlement process. Here again the raw data are not transmitted as they are not needed.

- The customer information applet could process and display consumption analysis locally or offer a comparison service interactively via a website, if the customer accepts to share her data this way. The customer who installs such an applet on his system expresses his informed consent.

The secure remote management functionalities enable the customer to change service providers by replacing applets from a previous service provider with those of the chosen service provider. The customer fully controls the loading and execution of applications. The interoperable local programming environments enable to write such applets once for all and run them on any compliant processing node.