A FLEXIBLE, PRIVACY ENHANCED AND SECURED ICT ARCHITECTURE FOR A SMART GRID PROJECT WITH ACTIVE CONSUMERS IN THE CITY OF ZWOLLE - NL

Carlos MONTES PORTELA
Enexis / Open University - NL
carlos.montes-portela@enexis.nl

Hans ROODEN
CGI - NL
hans.rooden@cgi.com

Jaap KOHLMANN
Enexis - NL
jaap.kohlmann@enexis.nl

Denny VAN LEERSUM
Flexicontrol - NL
denny.van.leersum@ibb.nl

Danny GELDTMEIJER
Enexis / Avans University of Applied Sciences - NL
danny.geldtmeijer@enexis.nl

Han SLOOTWEG
Enexis / Eindhoven University of Technology – NL
han.slootweg@enexis.nl

Marko VAN EEKELEN
Open University – NL / Radboud University Nijmegen – NL
marko.vaneekelen@ou.nl

ABSTRACT

This paper presents the ICT architecture for a Smart Grid project with consumer interaction in the city of Zwolle, the Netherlands. It describes the privacy and security enhancing measures applied to ensure a positive sum of necessary functionality and respect for consumer's privacy and secure business operation. The project was executed by Enexis (a Dutch DSO), in cooperation with CGI (IT services), Flexicontrol (In-Home automation), DONG Energy (Electricity Supplier), Eindhoven University of Technology (TU/e) and SWZ (Housing Corporation in Zwolle). The implemented system facilitates Demand Side Management (DSM) for 250 households in a residential area. It aims at investigating to what extent the households' flexibility in demand can be made available. The obtained knowledge is to be used for optimizing the use of locally produced sustainable energy and the local grid capacity. The idea is to realize this using a combination of technology, incentives, interaction and communication instruments as presented at CIRED 2011 [1].

INTRODUCTION

An increased usage of sustainable energy sources leads to more distributed generation. By its nature this type of power generation is less predictable than centrally generated electricity from e.g. coal or nuclear power plants. To deal with the resulting challenge to match production and demand, flexibility at the demand side could be used advantageously. Demand Side Management (DSM) is considered to be a promising approach to unlock the potential of flexibility in electricity demand at the houses of consumers [1]. With DSM one can control demand with a non-critical time constraint, like washing clothes with a smart washing machine based on user wishes.

To explore the possibilities of DSM in real life, Dutch DSO Enexis initiated a Smart Grid project with consumer interaction in the city of Zwolle, the Netherlands. It aims at investigating to what extent the households' flexibility in demand can be mobilized. The project has been executed in a consortium consisting of CGI (IT services), Flexicontrol (In-Home automation), DONG Energy (Electricity Supplier), Eindhoven University of Technology (TU/e) and SWZ (Housing Corporation). The consortium implemented a system that facilitates DSM up to 250 households in a residential area. The project was inaugurated officially on the 30th of November 2012 where the first 100 households were connected to the DSM system [2]. The project will run from the end of 2012 till 2015 and gradually additional households will be added. The obtained knowledge is to be used for optimizing the use of locally produced sustainable energy and the local grid capacity. *Figure 1* illustrates a Smart Home in a DSM setting.

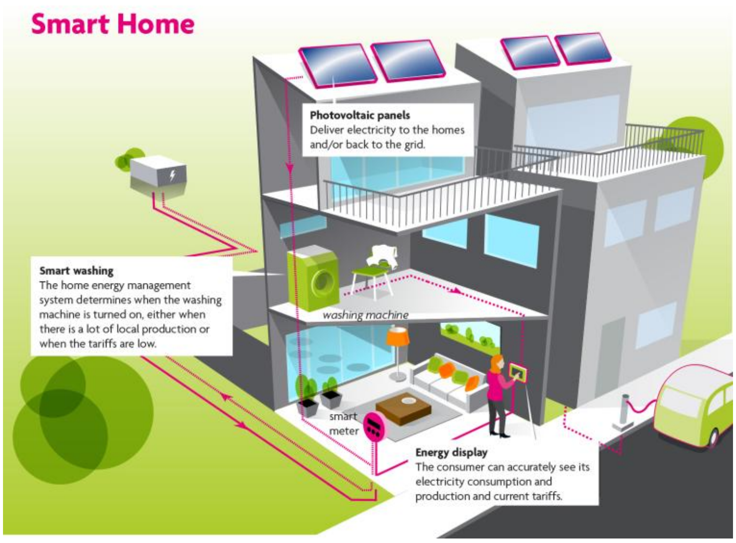

Fig. 1 – Artist impression of a Smart Home in a DSM setting

DSM solutions involve interaction between multiple parties. For this project it concerns consumers, DSO Enexis, Electricity Supplier DONG, PV production forecast company MeteoConsult and EDSN (the national clearing house of the Dutch energy sector). Furthermore, within the consumer's house multiple components interact as well: Home Energy Management System (HEMS), touch screen display for user interaction, Smart Meter, Smart Appliances and a gateway to the Central Energy Management System (CEMS). The resulting information flows need to be handled appropriately, as without protection measures, unauthorized third parties could obtain information regarding electricity consumption, use of Smart Appliances, amount of PV production, etc. This information is privacy sensitive as it can reveal the whereabouts and behaviour of the consumers. Based on the negative experiences with privacy discussions regarding the Smart Meter in the Netherlands, this could become a problem for DSM initiatives as well. The next sections show how DSO Enexis and its consortium partners achieved a flexible, privacy enhanced and secured ICT architecture to ensure a positive sum of necessary functionality and respect for consumer's privacy and secure business operation.

THE ROAD TO A FLEXIBLE, PRIVACY ENHANCED AND SECURED ICT ARCHITECTURE FOR THE CONSUMERS IN ZWOLLE

This section explains the main characteristics of the DSM use case in the city of Zwolle. Furthermore, it clarifies which methods were used to implement an ICT architecture that takes into account the flexibility, privacy and security requirements of the use case.

How does the use case look like?

The main DSM use case consists of interactions between several actors. *Figure 2* shows these interactions in a use case diagram. In the use case APX stands for the Dutch electricity market; the project uses day-ahead prices.

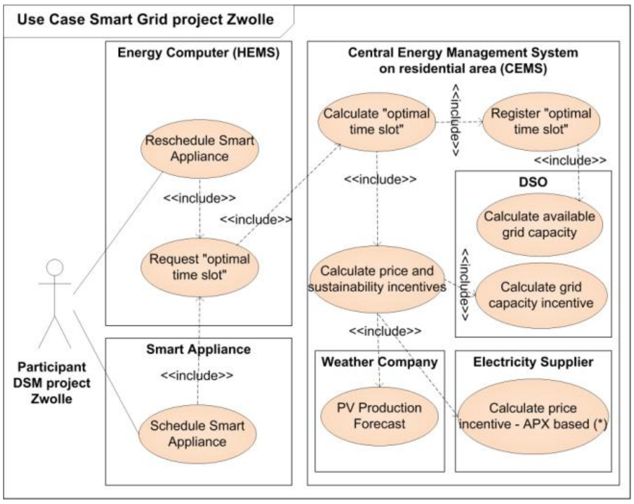

Fig. 2 – Simplified use case DSM project in the city of Zwolle

In this project the participating consumers are equipped with controllable Smart Appliances (laundry washer and optionally dish washer or dryer). The consumers can express their wishes to the appliance e.g. "laundry should be washed before 6 P.M.". An energy computer in their homes will then help them in planning these appliances in timeslots that will use as much locally produced sustainable energy (PV panels at residential area) or the lowest price for electricity, depending on the predefined profiles of each consumer. In order to find appropriate time slots and to optimize the usage of locally produced electricity, the energy computers of each household interact with a central ICT system at residential area level (CEMS). Besides helping the households in meeting their wishes, the solution provides certain flexibility to the DSO in scheduling these Smart Appliances. This flexibility could be used advantageously to distribute the loads of the households in time, whilst respecting the consumers' wishes (i.e. wash should be finished at 6 P.M.). Furthermore, the participants will receive incentives that stimulate them to shift their non controllable loads in time to save money or to optimize usage of locally produced renewable energy.

The main actors of the use case are:

- The users of the demand-side management system, being it the consumers participating in the project
- The Electricity Supplier, buying electricity on the wholesale market and selling it to its customers
- The DSO, responsible for the electricity grid
- The weather company, responsible for household specific PV production forecasts

The main technical components that are used are:

- CEMS, a central ICT system at residential area
- Smart Appliances, at least a laundry washer and optionally a dish washer and dryer
- Energy Computers, being the HEMS of the consumers.
- Energy displays, wall mounted touch screens in the houses of the consumers used for interaction
- Smart Meters, register detailed energy measurements
- PV installation installed on each house

Flexibility requirements and applied methods

An initial period of three months was used to elicit the main high-level requirements for the CEMS, the Energy Computer, the touch screens and all other components involved. The requirements elicitation process was realized via a series of semi structured brainstorm sessions where the main characteristics and rationales of the use case were grasped and documented. The resulting document "Business Requirements – Smart Grid pilot with user interaction in the city of Zwolle" was discussed with and accorded by the main stakeholders of the project. Although the DSM use case in the city of Zwolle focuses on the 250 participating households, the consortium has used it to explore the requirements that would need to be implemented in case of a larger roll-out.

The main high-level requirements regarding flexibility that were defined are interoperability, scalability and loose coupling (each component has, or makes use of, little or no knowledge of the implementation of other components). In order to explore these requirements in more detail and foster a timely delivery of the project within budget constraints, an agile approach was chosen. An agile approach uses short iterations to step-by-step discover more and more detailed requirements and implement them as the project moves on. This differs from traditional waterfall approaches where all requirements are analysed before actually starting the implementation phase [3]. The agile approach comes with the advantage of more flexibility, customer collaboration and the main risks of the project are tackled as soon as possible. In the agile manifesto the approach is characterized by [4]:

1. Individuals and interactions over processes and tools
2. Working software over comprehensive documentation
3. Customer collaboration over contract negotiation
4. Responding to change over following a plan

As the DSM project in Zwolle uses a completely novel approach in facilitating a residential area with Smart Grid technologies, the agile approach was chosen to tackle the different technical and functional challenges that came along. *Figure 3* illustrates this approach.

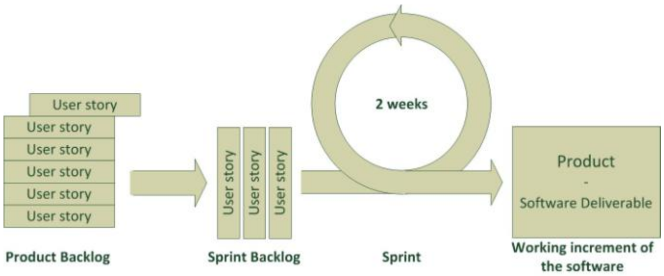

Fig. 3 – Applied agile project lifecycle

To achieve interoperability and loosely coupling, a set of Web services was designed and implemented between the Energy Computers and the CEMS. Basically Web services enable a technology agnostic approach for information exchange via the Internet. They can be described via so called WSDLs. WSDL (Web Service Description Language) makes it possible to define a 'contract' between all participants involved which defines what information needs to be send and what information is to be received back afterwards.

If one would standardize these Web services, Energy Computers from different vendors could be used to connect to the same CEMS and each CEMS in a residential area could be provided by its own IT Services / Energy Services provider. Scalability was achieved by using a cloud based solution for the CEMS. It offers software and hardware over the Internet and can be scaled up or down based on demand. E.g. if more participants are added to the project in the same residential area extra cloud resources like database or Web service containers can be added. Furthermore the cloud solution can be replicated to serve other residential areas in case of a large scale roll-out.

Privacy and security requirements and applied methods

Although the main goals of the project were not related to privacy and security, Enexis has taken the opportunity to use it to obtain hands-on experience with privacy and security in the Smart Grid with consumer interaction domain. For Enexis, DSM with consumer interaction is a promising use case within the future Smart Grid. In order to make it successful, it is necessary to obtain a positive sum of functionality, privacy and security. Privacy and security were taken into account from the start, by applying so called privacy and security *by design* principles applicable to this type of ICT architectures. Herewith, privacy and security are embedded in the design.

To have a better understanding of the privacy and security risks involved in the use case, several privacy and security workshops were conducted by internal and external subject matter experts. As a result the following privacy and security risks were identified: (R1) Reputation damage for non compliancy with privacy laws, (R2) Unsatisfied participants due to low availability of ICT components, (R3) Unsuccessful results for research purposes and therefore unsuccessful project and (R4) Reputation damage as a result of a hacked ICT component. R1is privacy related, R2 and R3 are security related and R4 is privacy and security related.

According to Spiekermann and Cranor [5] basically two strategies can be applied to engineer privacy into a solution: privacy-by-policy and privacy-by-architecture (currently known as privacy *by design*). As a system that is engineered applying privacy *by design* processes less or no privacy sensitive data at all and the consortium was in full control of the design and implementation aspects, the privacy *by design* approach was chosen. Privacy sensitive data in the DSM use case are: detailed energy measurements per house, participants' choices regarding Smart Appliances, detailed information regarding energy delivered to the grid by the participants (15 minute values) and participants' choices regarding the incentives they receive. By applying privacy design strategies one can increase the privacy friendliness of the end result. During the design phase of the demonstration project the following were applied: MINIMIZE, SEPARATE, AGGREGATE and HIDE [6]. MINIMIZE is achieved by minimizing or even avoiding the processing and storage of privacy sensitive data, SEPARATE is achieved by partitioning information processing and storage between the different participants so that each and one only knows what it needs to know, AGGREGATE is achieved by aggregating data and using it in its least detailed level whilst still being useful and HIDE is achieved by protecting data in order to avoid unauthorized access.

RESULTS

To deal with risk R1 a set of privacy enhancing measures were taken. E.g. the CEMS knows only the energy requests of the different houses and to which electrical cable(s) of the LV-MV transformer they are connected. It doesn't know to which consumer or home address a scheduled Smart Appliance belongs. The Energy Computer is implemented in a consumer agnostic manner and therefore protects the consumer's privacy even if it would be stolen during a burglary. *Figure 4* shows the measures found by applying the earlier mentioned strategies during privacy and security workshops.

Strategy / Role	HIDE	SEPARATE	MINIMIZE	AGGREGATE
Consumer	Smart Appliances planned consumer agnostically	Consumer related tasks are processed in home	Maximum of data handled in home by Energy Computer	
DSO	Data protection (access control and encryption) from/to CEMS		No personal data is processed by the DSO functionality	Incentive driven demand control at *residential area* level
Electricity Supplier	Idem DSO	Choices consumer on Smart Appliances separated from Supplier	Only data necessary for billing purposes (incentives + meter data) is handled	

Fig. 4 - Applied privacy design strategies per role

To deal with risk R2 extra attention was given to the availability of the system. As a result, the ICT inside the houses can operate in island-mode with most features available for 12 up to 36 hours. All in home energy-measurements remain visible to the consumer, whenever communication with the CEMS is unavailable. Additionally, thorough tests have been executed both on the components inside the homes and the CEMS at residential area level.

R3 and R4 were dealt with by implementing a set of security enhancing measures. An example of such a measure is that the Energy Computers inside the houses always initiate the communication to the CEMS and never the other way around. Furthermore, this communication is secured by encryption (client and server side PKI), where every Energy Computer has its own digital identity. This way if a hacker would be able to compromise one Energy Computer, it would not automatically mean all others are compromised. To obtain the necessary flexibility, a decoupled and scalable cloud-based Service Oriented Architecture was implemented. Furthermore the ICT inside the houses can operate in island-mode, whenever communication with the CEMS is unavailable. *Figure 5* reflects the final picture.

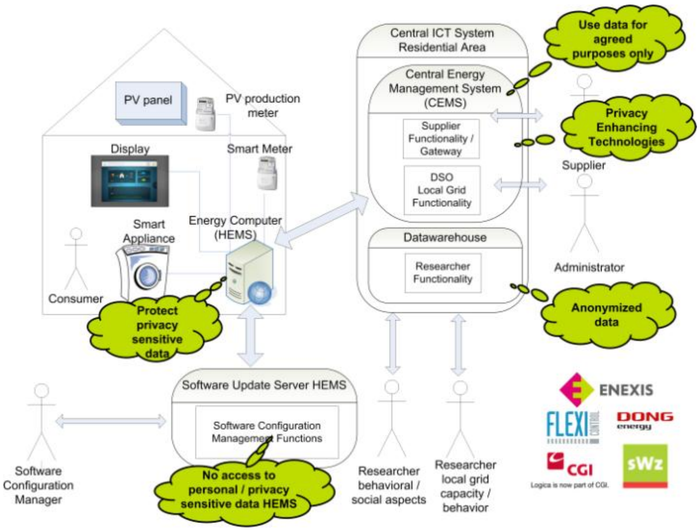

Fig 5. - Depiction of the ICT architecture for a Smart Grid project with active consumers in the city of Zwolle

As a result of the privacy and security workshops of the project, a set of generic privacy and security *by design* principles for future use by Enexis has been defined. They are listed below and not explained further in this paper.

Principle 1	Avoid (centralized) storage
Principle 2	Access on need to know basis
Principle 3	Run in least privilege
Principle 4	Purpose of data processing explainable
Principle 5	Consumer must be informed
Principle 6	Data is used for agreed purposes only
Principle 7	Anonymize data where possible
Principle 8	Research goals may lead to exceptions

CONCLUSION

Implementing a DSM solution leads to both challenges and opportunities. We show that it is possible to implement an ICT architecture that is flexible enough to deal with the interactions between the different actors. Furthermore, it is scalable to handle an increasing number of residential areas in the future and fosters interoperability between the participants whilst leaving freedom of choice regarding the internal ICT implementations. By applying privacy and security *by design* a positive sum of functionality, privacy and security was achieved for the use case of DSM driven Smart Grid with consumer interaction.

DISCUSSION

Although much effort and attention has been put into the design of the ICT architecture for the project, a large scale roll-out of the DSM solution would require additional measures. Especially on security an even more thorough risk analysis should be conducted, in order to weigh the different security risks and take appropriate measures as for example the internet connection of the consumer is used as a gateway between the Energy Computer and the CEMS. A large scale roll-out would furthermore request for a better insight of the costs involved in all necessary ICT for the DSM solution (purchase, installation, maintenance, etc.).

All participants of the project have initially signed for their participation and usage of relevant data for research purposes during and after the project. Although there is a goal binding for the use of this data, DSO Enexis has decided to implement the data warehouse for research purposes, so that it stores anonymized data only. Herewith, participants' privacy is protected even further than previously discussed and participation is on a voluntary basis.

Currently extra functionality for smart phones, tablets and a social incentive is being designed. This calls for an ongoing effort in finding a positive sum between privacy, security and functionality. Privacy and security *by design* should take place throughout the entire software-lifecycle of the system.

REFERENCES

[1] Kobus, C.B.A., Jonge, B., Knigge, J.D. & Slootweg, J.G., 2011, user centric design of a Smart Grid – A social and economical approach, Proceedings of the 21st International Conference on Electricity Distribution, 6-9 June 2011, CIRED - Frankfurt - pp. 1-4 paper 0098

[2] Dutch DSO Enexis, 2012, Official inauguration of the Smart Grid pilot with consumer interaction in the city of Zwolle on the 30th of November 2012, website Enexis https://www.enexis.nl/over-enexis/nieuws/urgenda-directeur-minnesma-geeft-startsein-eerste-slimme-wijk-van-nederland *(in Dutch)*

[3] Cohen, David, Lindvall, Mikael & Costa, Patrich, 2004, An Introduction to Agile Methods, Advances in Computers, Vol. 62

[4] Beck, K., Cockburn, A., Jeffries, R. & Highsmith, J., 2001, The agile manifesto, website http://www.agilemanifesto.org/

[5] Spiekermann, Sarah and Cranor, Lorrie Faith, 2009, Engineering privacy, IEEE Transaction on Software Eng., 35(1):67–82

[6] Hoepman, Jaap-Henk, 2012, Privacy Design Strategies, Computers and Society / Cryptography and Security, Cornell University - http://arxiv.org/pdf/1210.6621.pdf