A FLEXIBLE AND PRIVACY FRIENDLY ICT ARCHITECTURE FOR SMART CHARGING OF EVS

Carlos MONTES PORTELA
Enexis / Open University of
The Netherlands - NL
carlos.montes-portela@enexis.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 of
The Netherlands / Radboud
University Nijmegen – NL
marko.vaneekelen@ou.nl

ABSTRACT

This paper presents a flexible and privacy friendly ICT architecture for Smart Charging of EVs. It has been implemented for demonstration purposes at Enexis (Dutch DSO), in cooperation with EV market parties. The architecture aims at the proposed market model for public EV charging infrastructures, to be embedded in the Dutch liberalized electricity market as presented at CIRED 2011 [1].

INTRODUCTION

Implementing infrastructures for charging EVs is a complex task, optimizing counteracting goals. The main aim is maximizing EV driver's convenience, by using the available charging infrastructure and local grid capacity as efficiently as possible. *Figure 1* shows the technical problems that charging EVs (on a large scale) in an uncontrolled fashion could cause. First of all the MV/LV transformer could be overloaded if the total demand for electricity exceeds its capacity, secondly a single feeder could be overloaded (e.g. if many EVs are charged in the same street) and lastly the last houses connected to the cable could be confronted with voltage level problems due to the heavy loads related to the EVs being charged. By controlling the charging process, the DSO could avoid these technical problems optimizing the grid usage and facilitating the integration of RES. Herewith additional investments necessary for (large scale) EV charging could be avoided or at least minimized. This is coined as 'Smart Charging' by Eurelectric [2].

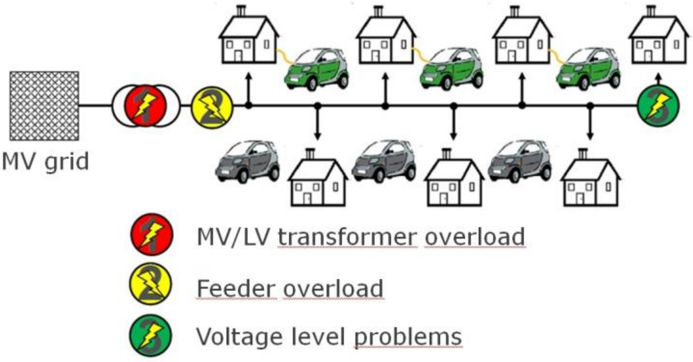

Fig 1: Technical problems related to (large scale) uncontrolled EV charging [3]

To deal with these technical issues in an efficient way Smart Charging is a promising strategy (i.e. by limiting the investments related to extra grid capacity). However, implementing Smart Charging in a liberalized context calls for an interaction and corresponding information exchange between DSOs, Charge Spots, EVs, EV drivers, energy suppliers and possibly new market participants / roles. Amongst the latter, one could count a Charge Service Provider (CSP) which deals with fulfilling the charge wish of the EV driver and a Charge Spot Operator (CSO), which deals with the operation of the Charge Spots. Without measures, one could derive the charge locations of EVs throughout time. If this could be coupled to EV drivers, it would then become privacy sensitive data as it reveals the whereabouts of the latter. Based on the negative experiences with privacy during the roll-out of Smart Meters in the Netherlands, this could become a problem for the concept of Smart Charging. Furthermore, the interest of hackers and commercial parties for privacy sensitive data increases the likelihood of disclosure. To deal with these issues, privacy and security should be taken into account from the start, also known as privacy and security *by design*. This paper will focus mainly on the privacy aspects. Lastly, the fact that the proposed marked model for public EV charging is still evolving into its full maturity, calls for an ICT architecture that is flexible enough to deal with future changes.

To increase the readability of this paper *Figure 2* shows the proposed market model for public EV charging as presented at CIRED 2011 [1].

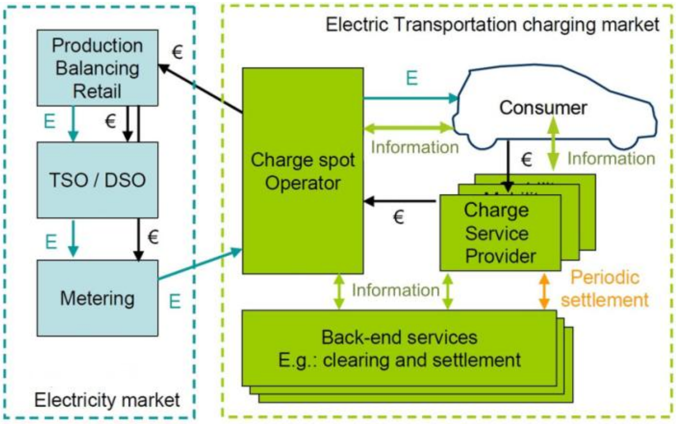

Fig 2: proposed market model [1]

It shows an interaction between different existing (in light blue) and possible new (in green) market roles. Note that the Mobility Service Provider has been renamed to Charge Service Provider to align with the European standardization efforts regarding EV charging and more specifically the generic use case on Smart (re-/de-) Charging of EVs [4]. The Enexis Smart Charging demonstration project has been used as input for the latter.

THE ROAD TO A FLEXIBLE AND PRIVACY FRIENDLY ICT ARCHITECTURE FOR SMART CHARGING EVS

This section explains the main characteristics of the Smart Charging for EVs use case. Furthermore, it clarifies which methods were used in the demonstration project at Enexis to implement an ICT architecture that takes into account both the flexibility and privacy related requirements of the Smart Charging use case.

How does the Smart Charging use case look like?

The Smart Charging for EVs use case consists of interactions between several actors. *Figure 3* shows these interactions in a UML use case diagram.

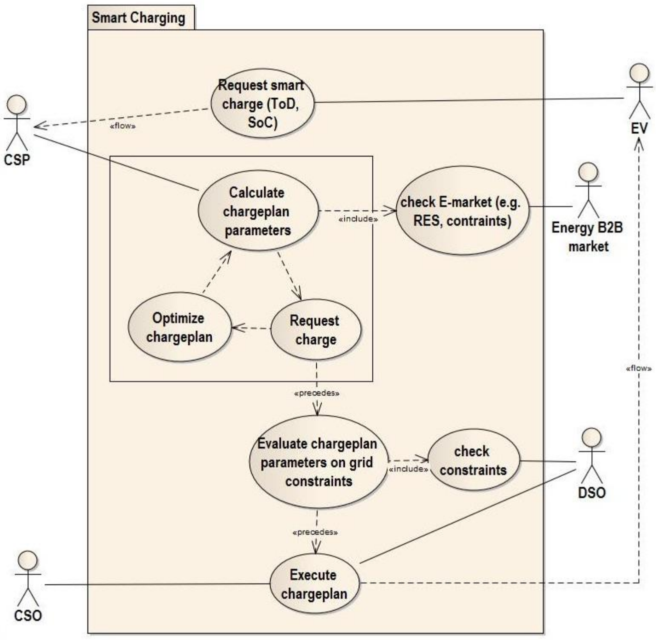

Fig 3: Smart Charging UML use case diagram

In the demonstration project each EV / EV driver has a CSP. When the EV arrives at a charge spot it expresses its charging wishes to its CSP, consisting of information like the battery state of charge (SoC), the requested amount of kilometres / energy and the time of departure (ToD). Based on this information the CSP creates a charge plan for the EV and submits it to the CSO. The CSO forwards the request to the DSO for approval, where the DSO shares available capacity in a Fair, Reasonable And Non-Discriminatory (FRAND) manner. If the charge plan fits within the local grid constraints the charge plan is executed and the EV is charged according to this plan. If not, the charge plan can be recalculated based on a forecast of the local grid capacity that is returned. The CSP can then create a new charge plan, based on negotiations with the requesting EV driver and / or other EV drivers in the same grid area. The CSP can thereafter alter the charge plan, or a set of active charge plans at the site in consent with the respective EV drivers.

Flexibility requirements and applied methods

Flexibility in the Smart Charging domain is necessary because of the evolving EV charging market model. In the proposed market model an EV driver will be able to choose its CSP. In order to foster a free and flexible market where new market parties can enter easily, the information flows that facilitate Smart Charging of EVs have to be designed in a participant independent manner. These so-called information interfaces must not impose any barriers for (new coming) market participants. Furthermore, they must not imply (technological) design choices for the internal ICT systems of the market participants. Moreover, manufacturers of Smart Charging components and their corresponding software need to know how to interact with the different participants. Examples of these components are: charge spots, EVs, EV user interaction devices and ICT devices that reside inside the MV/LV substations of the DSO. In this way the manufacturers have the flexibility to make their own ICT choices (e.g. Java –vs- .Net, what type of relational database, centralized or less centralized architectures, self owned data centers or cloud solutions, etc.) without the fear of not being able to connect to other market participants.

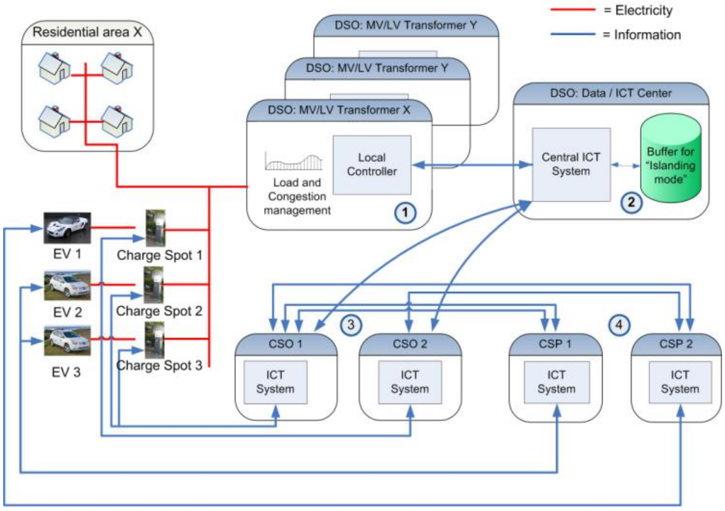

Fig 4: Smart Charging participants and information flows

As the number of market participants like CSPs, CSOs and EV drivers is expected to increase in the future the ICT architecture for Smart Charging has to facilitate this. The blue arrows in *Figure 4* show the information flows between the participants and clarifies the fact that the interfaces between the participants must be generic. Otherwise CSP 1 would for example need to implement different ICT solutions for its interaction with CSO 1 and CSO 2. CSO 3 entering the market could lead to changes at all existing

CPSs. To achieve this, a set of Web services was designed and implemented. Basically, Web services enable a technology agnostic approach for information exchange via the Internet. It does so via so-called SOAP messages that contain the functional information that needs to be send back and forth. The following Web services were designed: *createEVChargePlan* - between CSP and CSO to execute the appropriate Charge Plan, *executeEVChargePlans* - between CSO and DSO to execute all Charge Plans belonging to a CSP and *expressChargeWish* - between EV driver and CSP to exchange the charge wish of the EV driver. Web services can be described via so-called WSDLs. WSDL (Web Services Description Language) makes it possible to define a 'contract' between all participants involved. It defines what information needs to be sent and what information is to be received back afterwards. However, it does not imply the usage of a specific technology for the participant (i.e. CSP 1 can implement its ICT with programming language Java and CSO 2 with C# in .Net and still interact with each other). One could say that just like electricity has proven to be handy for transmission and distribution of energy this also holds for Web services when it concerns the exchange of information. Currently Web services are gaining momentum in the energy world, as is for example reflected in the wind power craft related standard IEC 61400-25 and other initiatives [5].

Functionally the Web services have been designed to enable the CSO execute its tasks, without knowing to which MV/LV transformer substation and feeder its Charge Spots are connected. Herewith the roles of the CSO and the DSO are clearly separated: the CSO can focus on managing the Charge Spots and the DSO on managing the grid without the need of disclosing its topology.

Privacy requirements and applied methods

Although the main goals of the Smart Charging demonstration project were not related to privacy, DSO Enexis has taken the opportunity to use the demonstration project to obtain hands-on experience with privacy in the EV domain. For DSO Enexis Smart Charging of EVs is a promising use case within the future Smart Grid and in order to make it successful, it is necessary to obtain a positive sum of functionality, privacy and security. According to the inspiring paper of Spiekermann and Cranor [6] basically two strategies can be applied to engineer privacy into a solution: privacy-by-policy and privacy-by-architecture (currently referred to as privacy *by design)*. As a system that is engineered applying privacy *by design* processes less or no privacy sensitive data at all, the privacy *by design* approach was chosen. Furthermore it concerned a demonstration project and therefore an excellent opportunity to engineer privacy preserving measures into the design of the solution. Privacy sensitive data that can be found in the Smart Charging use case are: information regarding the charge wishes of EV drivers, charge locations of EVs throughout time, charge plans executed in combination with the EVs they relate to and detailed energy measurements on Charge Spots in combination with the EVs they relate to. By applying privacy design strategies one can increase the privacy friendliness of the end result. During the design phase of the demonstration project the MINIMIZE, SEPARATE, AGGREGATE and HIDE privacy design strategies were applied [7]. MINIMIZE is achieved by minimizing or even avoiding the processing and storage of privacy sensitive data, SEPARATE is achieved by separating 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

As a result of the applied methods a privacy friendly solution for the Smart Charging demonstration project was designed: CSPs know only the charge wish of their customers (EV drivers) but not their locations, CSOs know that an EV needs to be charged for a certain CSP at a certain Charge Spot but not which EV / EV driver it concerns, the DSO handles the charge request safeguarding the local grid for congestions without knowing which EV / EV driver it concerns and last but not least the Charge Spots execute charge requests and forget about it afterwards. *Figure 5* reflects the different strategies that were applied per market role.

Strategy / Role	**HIDE**	**SEPARATE**	**MINIMIZE**	**AGGREGATE**
EV / EV driver	No id is sent to Charge Spot	n/a	Only necessary data sent to CSP	n/a
CSP	Processed and stored data is protected (access control and encryption)	Authorizes and fulfils charge wishes EV driver location agnostically	Only necessary personal data stored and processed (billing and charging)	
CSO	Processed and stored data is protected (access control and encryption)	Charges EV based on CSP's approval without knowing EV (driver)	No personal data handled. EV (driver) agnostic implementation	
DSO	Data protected (access control and encryption)	Safeguards grid constraints EV (driver) agnostically	Idem CSO	Charge plans of a CSP are aggregated.
Charge Spot	Communication is protected	No data is stored	Idem CSO	n/a

Fig 5: Applied privacy design strategies per role

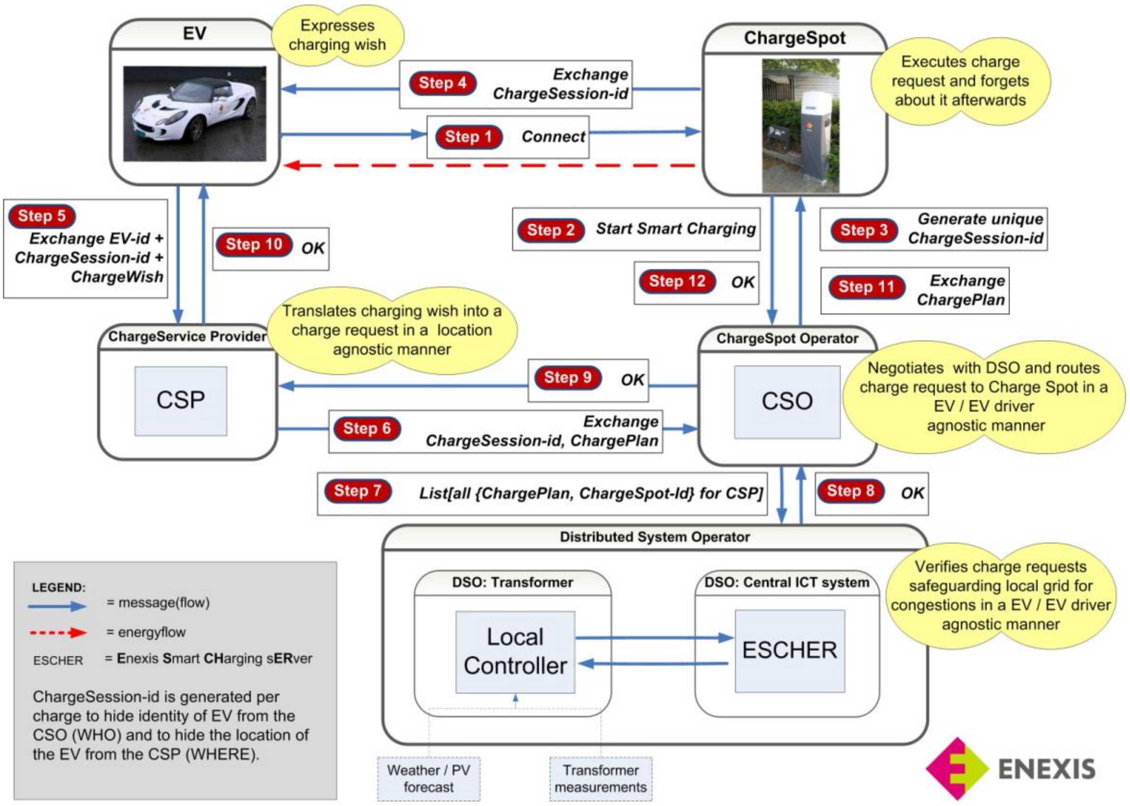
EV
Expresses charging wish
ChargeSpot
Executes charge request and forgets about it afterwards
Step 4 Exchange ChargeSession-id
Step 1 Connect
Step 5 Exchange EV-id + ChargeSession-id + ChargeWish
Step 10 OK
Step 2 Start Smart Charging
Step 3 Generate unique ChargeSession-id
Step 12 OK
Step 11 Exchange ChargePlan
ChargeService Provider
Translates charging wish into a charge request in a location agnostic manner
CSP
ChargeSpot Operator
CSO
Negotiates with DSO and routes charge request to Charge Spot in a EV / EV driver agnostic manner
Step 9 OK
Step 6 Exchange ChargeSession-id, ChargePlan
Step 7 List[all {ChargePlan, ChargeSpot-Id} for CSP]
Step 8 OK
Distributed System Operator
DSO: Transformer
Local Controller
DSO: Central ICT system
ESCHER
Verifies charge requests safeguarding local grid for congestions in a EV / EV driver agnostic manner
Weather / PV forecast
Transformer measurements
ENEXIS
LEGEND:
= message(flow)
= energyflow
ESCHER = Enexis Smart CHarging sERver
ChargeSession-id is generated per charge to hide identity of EV from the CSO (WHO) and to hide the location of the EV from the CSP (WHERE).

Fig 6: Depiction of the privacy friendly Smart Charging solution

Besides the privacy enhancing measures, a decoupled and partly cloud-based Service Oriented Architecture has been implemented to obtain the necessary flexibility. The end result is reflected in *Figure 6*.

CONCLUSION

The introduction of EVs 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 participants in the Smart Charging domain. Furthermore, it is scalable in order to deal with an increasing number of EVs, CSOs and CSPs and fosters interoperability between the participants whilst leaving freedom of choice regarding the internal ICT implementations. By applying privacy *by design* a positive sum of functionality and privacy was achieved for the use case of Smart Charging. Despite all the applied ICT, Smart Charging of EVs remains as privacy friendly as conventional fueling for combustion engine vehicles.

DISCUSSION

Technical restrictions have lead to differences between the design and the actual implementation for the demonstration project. For example the current Charge Spots in the Netherlands ask for the EVs to send their IDs to the Charge Spot instead of the suggested privacy enhancing ChargeSession-Id generated by the CSO.

Furthermore, restrictions on the production system of the CSP lead to changes in the final implementation. Nevertheless, we think that this doesn't affect the outlined concept of a privacy friendly and flexible ICT architecture for Smart Charging of EVs, as the restrictions can be tackled in a large scale roll out of Smart Charging.

REFERENCES

[1] Geldtmeijer, Danny, Hommes, Klaas, Postma, André, 2011, Charging EVs in a liberalized electricity market, Procedings Cired Conference, paper 0889

[2] Eurelectric, 2011, European electricity industry views on charging Electric Vehicles, A EURELECTRIC position paper, http://www.eurelectric.org/media/26100/2011-04-18_final_charging_statement-2011-030-0288-01-e.pdf, chapter 2

[3] Rehtanz, Christian and Wietfeld, Christian, 2011, Presentation Interoperabilität als Schlüssel zur Integration der Elektromobilität in die Netzsysteme der Zukunft, Technische Universität Dortmund and IKT

[4] Postma, André, Klapwijk, Paul, Montes Portela, Carlos, Wollersheim, Maurice, 2012, Report Workgroup Sustainable Processes under mandate M/490, Generic Use case WGSP-1300 Smart (re-/de-) Charging of EVs

[5] Fries, Stefan, Hof, Hans-Joachim, 2012, Smart Grid Applications - Wiley, Communications and Security, Chapter 12 - Smart Grid Security Standardization

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

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