EVS30 Symposium
Stuttgart, Germany, October 9 - 11, 2017

The need for cybersecurity within the electric vehicle infrastructure

A study on the use of digital signatures in the electric vehicle infrastructure

Harm van den Brink[1]

[1]*ElaadNL / Enexis, harm.van.den.brink@enexis.nl – NL*

Executive Summary

As the electric vehicle (EV) charging infrastructure grows exponentially, the need for better security grows with it as well. The next step will make electric cars and Smart Charging a crucial part of the electricity system in the near future. Smart Charging is using innovative techniques to charge EVs at moments when there is abundant power available in combination with low demand. Since these techniques rely on measurements and data, the integrity and authenticity of this data is crucial. In this paper, a study of the use and need of digital signatures in the EV infrastructure is discussed. This study aims to give more insight in how the implementation of digital signatures could technically work, what risks are mitigated and how the organizational process could work. To be able to answer these questions this study will identify the current situation in the EV charging infrastructure and why digital signatures should be implemented.

Keywords: *Electric vehicles, cyber security, digital signatures, public key infrastructure*

1 Overview

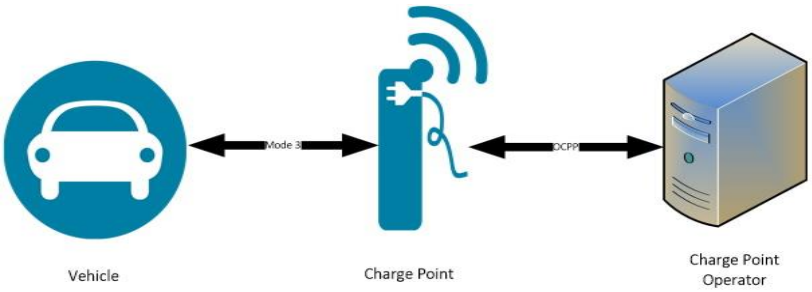
1.1 Introduction

As the EV infrastructure grows exponentially, the need for better security grows with it as well. The current developments are comparable with the situation when the first gasoline cars were introduced on the market. In the beginning there were not many cars on the roads , so the urgency for proper signs, guardrails and regulation was low. Once more cars were on the road, the need for proper signs, guardrails and regulation grew to keep the traffic manageable and to omit accident risks. In a way the same phenomenon is happing now with the EV infrastructure.

In 2009 when the first charge points and related IT infrastructure were deployed by ElaadNL, the focus was to have it functionally working. Byate 2016 more than 11,700 public and over 14,300 semi-public charge

points (installed on private terrain, but with (limited) public access) were deployed in the Netherlands and the number is still growing. Furthermore, the number of private charge points in the Netherlands is estimated at 72,000 [3].

With these continuously growing numbers, the necessity for privacy and security within the EV charging infrastructure became more and more clear. This means that the metering data, which consists of the energy consumed, must be reliable and the integrity of this data must be guaranteed. Within the current infrastructure in place, there is room for improvement regarding cybersecurity.



The up-coming developments within the electric vehicle infrastructure will make electric cars and Smart Charging [1] a crucial part of the electricity system in the near future. Smart Charging is using innovative techniques to charge cars at moments when there is abundant volume of power available on the grid while the power demand is low.

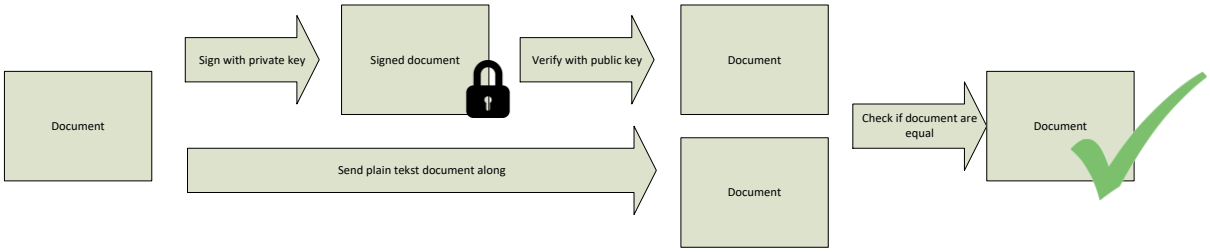
2 Digital signatures

2.1 What is a digital signature?

A digital signature is a mathematical scheme for demonstrating the authenticity of a (digital) message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity). Digital signatures are commonly used in software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.[1]

Digital signatures rely on the use of asymmetric cryptography, or often called Public-key cryptography. A user, or computer system, can generate a private and public key-pair. The private one has to, of course, remain private and the public one can be spread to others. If the user wants to sign a document, it uses its private key for the signature. By sending the actual document, along with the signature created with the private key, others can verify, using the public key, if it was actually that specific user (because it is the only one who knows the private key), who signed the document and that the document is not tampered with.

If the document or the signature is tampered with along the way, the user who verifies the signature will detect this. Because there will be a mismatch between the signature and the document. Nobody except the owner of the private key can generate the signature.



[1] https://en.wikipedia.org/wiki/Digital_signature

2.2 Why digital signatures in EV?

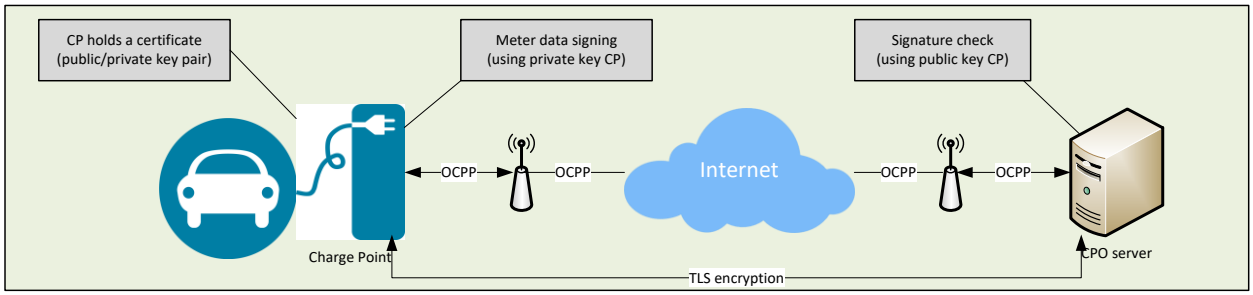
Data exchange between charge point and charge point operator

The data from and to the charge point, which includes information on the energy consumed by the car, is sent from the Charge Point (CPO) via the Open Charge Point Protocol (OCPP) protocol to the server of the charge point operator (CPO).

OCPP is the accepted protocol of choice in 50 countries and used by over 50,000 charging stations, providing accessibility, compliance and uniform communications between charging stations and management systems. The CPO can control its charge points using OCPP. The protocol is co-developed by ElaadNL and can be downloaded for free (www.openchargealliance.org).

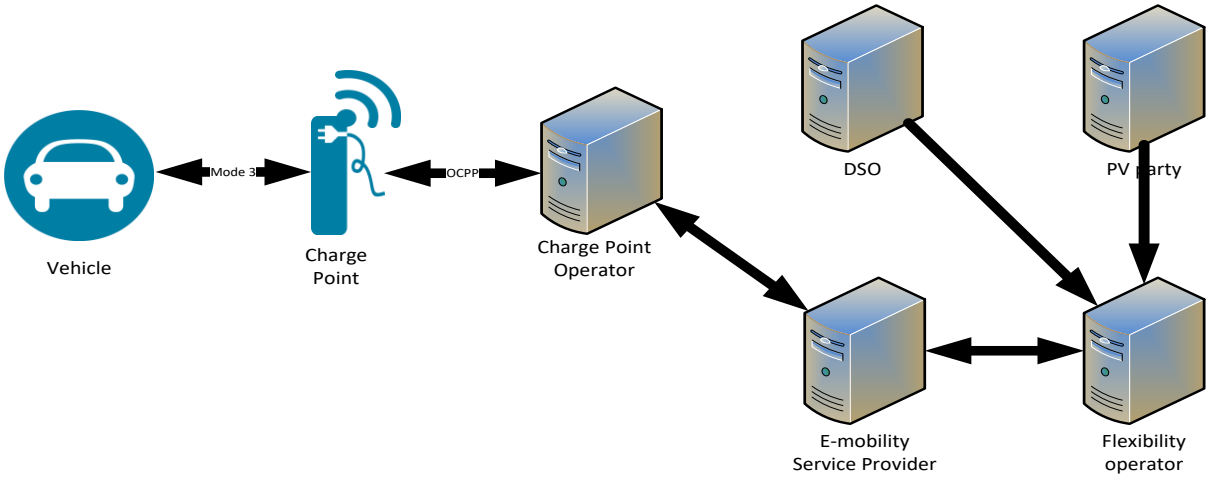
Data shared with multiple parties

The EV eco-system is growing rapidly (in the Netherlands). New companies try to make business out of the EV infrastructure. In the beginning the focus was only on selling energy, nowadays they are moving to sell capacity or (grid)balancing algorithms. The battery of the car is used to balance the grid, balance a program responsible party's portfolio and to make optimum use of solar and wind energy. This means the charging behavior (energy consumed, maximum charging power etc.) of cars will be shared with multiple parties in the EV infrastructure.



Sharing the meter values with digital signatures to others parties, also gives the other parties the possibility to check the validity and integrity of the actual meter reading. Digital signatures adds the possibility for integrity checks in the whole chain of the EV infrastructure, and could even be used without TLS *if there is no privacy related information shared*.

With the use of digital signatures, created by the charge point, it doesn't matter how many parties are in between the chain. Each partner involved can verify and check the integrity of the message using the public key of the corresponding charge point.



Example of the information flow

Example: A flexibility operator wants to calculate the best charging profile (price oriented) for a specific user (car). Therefor it needs input from the balance responsible party, the e-mobility service provider, the DSO and of course the current charge rate of the actual car. Since the actual meter values of the charge rate of the car are sent via the charge point operator and the e-mobility service provider, the flexibility provider needs something to be sure that the integrity of the meter values are guaranteed. After all, the flexibility operator is the one which is generating a charging profile which takes into account the different variables like grid capacity, sustainable production forecast, EV driver preferences etc. He has to rely on accurate data. To achieve this, the charge point generates a digital signature according to the meterValues message. In transit from the charge point all the way to the flexibility provider the integrity is guaranteed via the digital signatures. If something changes to the meter values, or the signatures, they would not match anymore and will not be valid. The flexibility operator can verify if the actual meter values and the signature are still valid.

Why TLS alone is not sufficient

Although the communication between the charge point and the charge point operator is secured with TLS 1.2, securing the communication only assures that the information was correctly, and privately, sent from the charge point to the charge point operator. Usually information is also shared with other parties in the EV infrastructure, TLS alone does not give any additions to integrity check once it is stored at and shared from the charge point operator.

3 Pilot implementation

3.1 Hardware changes to the charge point

In our pilot we used a charge point which has a controller running on embedded Linux. By default Linux is able to create digital signatures via the OpenSSL library. The problem with charge points is that they are out in the open. Like explained before, the private key needs to be private. Because the charge points are relatively easily accessible, keeping the private key private was one of the major issues we had to deal with.

If we store the private key just in the memory of the controller, one would be able to copy the SD card and steal the private key without us knowing it was stolen. Or hack the charge point somehow remotely and copy the private key. So we had to implement something which would secure the private key, even if the charge point got physically 'hacked'.

The solution in our case was the use of a smart card. A smart card is similar to a SIM card used in mobile phones. The advantage of a smart card is that you can upload a private key to it, which cannot be extracted from the chip. You can only talk to the chip for doing operations like signing, but the private key never leaves the chip.

A smart card includes an embedded secure chip that can be either a secure microcontroller with internal memory or a secure memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency (RF) interface, in our case it was a physical contact by using a smart card reader.

With an embedded microcontroller, smart cards have built-in tamper resistance and have the unique ability to securely store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures), and interact intelligently with a smart card reader.[2]

Every time a signature needs to be generated the charge point controller asks the smart card to perform the signing process on the data which the controllers supplies. The smart card outputs the signature in response.

If the charge point gets hacked, or opened, one is only able to use or extract the smart card. However, extracting the smart card would be noticed by the charge point. The charge point will notify the charge point operator server. The charge point server can than revoke the certificate for the charge point, which makes sure that the data from the charge point won't be trusted anymore.

3.2 Software changes to the charge point

OCPP needs to be able to handle the signature that is going to be transferred from the charge point to the charge point operator server. The OCPP 1.5 (and 1.6) specification already anticipated on signed data (page 23 of the specification), by adding an experimental value element 'format' to MeterValues. The attribute 'format' could be used to specify if the data is Raw or for example SignedData.

The EXPERIMENTAL optional format attribute specifies whether the data is represented in the normal (default) form as a simple numeric value ("Raw"), or as "SignedData", an opaque digitally signed binary data block, represented as hex data. This experimental attribute may be deprecated and subsequently removed in later versions of OCPP, when a more mature solution alternative is provided.

Signing the StartTransaction and StopTransaction is not able in OCPP 1.5, this means we need to change the OCPP specification. We added a field called 'signedData' to both the StartTransaction.req and StopTransaction.req. This also means the WSDL files had to be changed to support the new added fields.

[2] http://www.smartcardalliance.org/publications-smart-card-security/

This resulted in the following addition for the startTransaction:

```
<startTransactionRequest xmlns="urn://Ocpp/Cs/2015/07/signed/">
      <connectorId>1</connectorId>
      <idTag>test</idTag>
      <timestamp>2015-09-02T11:26:03.000Z</timestamp>
      <meterStart>51190</meterStart>

<signedData>YYJ2xhpK8XuqI82KbKEp5AJvHQb/SNuII62Ah64hWPvAvkSLe39GcKZkY/+gwa+GsebcIIbemA93
nnmzxJMKACzh2kZNwPhwguLHmKn7akl4IH85pQy66mAUYHp3EGlo/0G8BOKb1fuPsnNj7z02C1Qp
euVmPBmBK5L+UA7k5m4g+WUCypt1VdUcQk1UevTx0I467HcOSsvnc1jVZ+AXMGmqQg8q1uFXJcyj
wOjaCRxMbKxPEtRPv0pFC4F3TMXFOmwcA6Ocj3NntuzGjd9CRjKbtKCVFjXyXoPnnxtZ/7agI1HH
7AMDizfctmxVkG2IAN/FkBf0b8Ja7zRnWjQSqg==</signedData>

 </startTransactionRequest>
```

This resulted in the following addition for the stopTransaction:

```
<stopTransactionRequest xmlns="urn://Ocpp/Cs/2015/07/signed/">
      <transactionId>6417</transactionId>
      <idTag>test</idTag>
      <timestamp>2015-09-02T11:29:11.000Z</timestamp>
      <meterStop>51210</meterStop>

<signedData>PiXok51SI/gOy/T6A83jhgauXXSvmJdwFp/7ARsh7b8CQBCzAyzQpkflhLXwpSBtpc6NSjNRglwl
Dwi0Yj/2opJWe8A8r90kyCjn4B+9EJJJC0lD0GlgQaj2LLukGU4E1p45NEZy/DhbGON86Pj5iI8g
4WHMEHG0DG6VHfcZ6Lc5gEUnImtmDIH4ieY2oDYa16LAVYJN1qIXM8I6mHNm+o0jt5T9LH4jzEo1
g01ewmdh2u37xU6dKnFY0r17F85CYowaF5Yztw/DOMeGNijb+KuA96tXvqO41MP45fnD+ljntjtU
3NfBFnQEixTvfZz2eggTNkyrl2z0RoAA6vVYdw==</signedData>

</stopTransactionRequest>
```

This resulted in the following addition for meterValues:

```
<meterValuesRequest xmlns="urn://Ocpp/Cs/2015/07/signed/">
      <connectorId>1</connectorId>
      <values>
        <timestamp>2015-09-02T11:25:07.000Z</timestamp>
        <value format="Raw" measurand="Energy.Active.Import.Register" unit="Wh">51190</value>

<value format="SignedData" measurand="Energy.Active.Import.Register"
unit="Wh">DWWwityLHx/Xx6QaiVLiZolDRlUDah0M/GC9RiflVpKrFe4d93TGvrbmgEI0zJEuIp611Ezc5eIXHfGyYE
hdzclXmM8+eN1ayb1YpXwfVStRdgSlSvvFSpr9fhswh8IdcltSyc1w+lnADI81NN79WfsW
aVTYK90KSCjh0cOMOPpUsQoUYitkc/rpwMzhhiy/C9LrD97Y0i1u8ooaNwAMSm3XKrEBaL+ynw/h
D/Kz0csYH8/d5KmP+37zldJzy5jqoNIr3/hQCDegFnD5/X39VGYIlHRGMSByPJ4YSrLx1EKEKmeJ
qIyKThQwWA618Gl72ow7CF4jAYkPR7W7OugXNA==</value>

      </values>
 </meterValuesRequest>
```

3.3 Changes to the charge point operator server

The charge point operator server needs to be able to verify the signature send along with the actual message. The server needs to know the public key (certificate) which belongs to the charge point. So we supplied the server with the right public key.

We implemented the verification process, to allow the verification of the signatures being sent. Each transaction will show up in the management graphical interface of the charge point operator. If one of the verifications of the signatures went wrong, a red checkmark was shown. If everything went well, and all signatures were verified as being good it shows a green checkmark.

Card Start	Start Source	Card Stop	Stop Source	Start Date	End Date	Total duration	Start kWh	End kWh	Total kWh	Manually Updated	Smart Charging	Signature Valid
F2F7713A		F2F7713A		19/08/2015 10:51:19.000	19/08/2015 10:58:16.000	0d, 0h, 6m, 57s	20.870	20.880	0.010			✗
F2F7713A		F2F7713A		19/08/2015 10:42:39.000	19/08/2015 10:46:48.000	0d, 0h, 4m, 9s	20.860	20.870	0.010			✓

4 Results and future work

4.1 Summary of results

Implementation (hard- and software)

Using digital signatures is [2], once implemented, very easy to use. It does not involve high costs in hardware or software, since most of the technology is already in place. The use of embedded Linux facilitates the use of digital signatures. At the same time we need to keep in mind that some charge points make use of microcontrollers, which are needed for specially programmed software. These microcontrollers probably require more effort in order to integrate digital signatures.

The management system of the charge point operator requires validation of digital signatures in the Open Charge Point Protocol (OCPP) [4] messages. The validation of the signatures is relatively simple to , but it is strongly related to proper key management.

Length of messages

The signatures, using RSA, shown in the examples are quite large compared to the actual message. With the use of GPRS, the length of these messages is important and should not be too high since this would increase the use of mobile data. EVNetNL, for example, has 3.000 charge points in the field. The digital signature shown in the example is 380 bytes. If this value needs to be transmitted with every meterValue (every 15 minutes), and every transaction, this would mean it needs to be sent 96 times a day. Switching to another cryptography algorithm which requires smaller keys, such as elliptic curve cryptography, would decrease the digital signatures.

Requirements for OCPP

OCPP had an experimental field for addition of digital signatures, but it was not even sufficient for this small scale pilot. Adding extra fields to the OCPP protocol was reasonably simple, and it did not require much additional effort. However, the addition of fields for digital signatures or extra security features should be aligned with the Open Charge Alliance to create a common agreement for the use of security features.

4.2 Recommendations

Extending OCPP with digital signatures

In the proof of concept discussed in this paper we added digital signatures to just a few OCPP messages, from the charge point to the charge point operator server. In the near future we would probably want to have digital signatures added to all messages, from the charge point to the charge point operator and vice-versa.

When we add Smart Charging functionalities on a broader scale, the charge point should be able to verify the authenticity and integrity of the Smart Charging message (i.e. high or lower current). This would only be necessary if the charge point operator acts as a proxy to the charge point. The current situation is that the communication from the charge point to the charge point operator is secured via TLS, and charge profiles are sent directly from the operator to the charge point. Once the operator acts as a proxy, for example to allow a third party to send charge profiles directly, the need for digital signatures to assure integrity and authenticity becomes relevant again.

Cryptography algorithms

More research should be done regarding proper cryptography algorithms for the EV infrastructure. The length of the keys, hardware requirements like computing power and memory is very important. Charge points are usually very limited devices, extending it with cryptography should not lead to delays in the interaction with the user or the charge point operator server and should not lead to a disproportional amount of additional costs.

Public-key Infrastructure (PKI)

Initiating and maintaining a PKI is important with the use of digital signatures and certificates. The management of these certificates is not trivial, as we have seen with DigiNotar[3]. PKIs require more effort and responsibility by the charge point operator, since they need to manage the certificates. We should also think of a national or even an international PKI infrastructure concept. In addition, several key choices needs to be made such as who is going to be root? Who is going to be subordinate? Will there be an European root or anational root?

[3] https://en.wikipedia.org/wiki/DigiNotar

References

[1] Deilami, S., & Masoum, A. et al. (2011). Real-Time Coordination of Plug-In Electric Vehicle Charging in Smart Grids to Minimize Power Losses and Improve Voltage Profile. IEEE Transactions on Smart Grid, 2(3), 456-467.

[2] Rogers, K. M., & Klump, R. et al. (2010). An Authenticated Control Framework for Distributed Voltage Support on the Smart Grid. IEEE Transactions on Smart Grid, 1(1)

[3] Rijksdienst voor Ondernemend Nederland, Cijfers elektrisch vervoer (2017, January 4). Retrieved from http://www.rvo.nl/onderwerpen/duurzaam-ondernemen/energie-en-milieu-innovaties/elektrisch-rijden/stand-van-zaken/cijfers

[4] Rodriguez-Serrano, A., & Torralba, A. et al. (2013). A communication system from EV to EV Service Provider based on OCPP over a wireless network. IECON 2013 - 39th Annual Conference of the IEEE Industrial Electronics Society.

Authors

Harm van den Brink received a MSc degree in 2013 from the Radboud University of Nijmegen, Netherlands. Currently he is employed as IT Architect Smart Grids & Electric Vehicles at ElaadNL and Enexis. Van den Brink is a specialist in IT and security and is responsible for the IT architectures of smart grids and electric mobility. The main focus is on requirements for IT security, the implementation of IT security and the development of innovative Smart Charging features within the EV infrastructure, the smart grid and between all parties involved in the smart grid system.