Smart charging

Baerte de Brey
5 juni 2020
Founded in 2009 by Dutch grid operators
Three phases of ElaadNL

2009–2013
BASISNETWERK VAN PUBLIEKE LAADPUNTEN

2014–2018
SMART CHARGING OP DE KAART

2019–2023
NETBEHEER VIA SMART CHARGING
EV in the Netherlands

*Vehicles*

- **Battery Electric Vehicle (BEV)**
- **Plug-in Hybrid Electric Vehicle (PHEV)**

<table>
<thead>
<tr>
<th>Type</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEV</td>
<td>117,756</td>
</tr>
<tr>
<td>PHEV</td>
<td>98,089</td>
</tr>
</tbody>
</table>
EV in the Netherlands

Charging stations
Effect of Smart Charging

No balance in the grid

SMART CHARGING
Total (semi-)public EV charging infrastructure in the Netherlands will reach a threshold where it can have serious impact on the grid.

Growth extrapolated at 40% based on historical data.
Charging station load estimated at 3.7 kW (low), 7.4 kW (medium), or 11 kW (high).
Assessment: Impact of total EV infrastructure NL

• Attackers can cause problems in balancing electricity supply and demand by strategically turning on and off charging stations on a larger scale.

• Turning a lot of power on and off repeatedly can also cause damage to the distribution network.

• The financial impact of this is estimated to be considerable; 20M euros.
Status of CS-requirement implementations

Public
- 30,000 existing public chargepoints without CS-requirements
- 6,000 to be installed from tenders with CS-requirements
  - ~2,500 installed with CS-requirements
    - Partly CS-requirements to be added after installation
- All existing tenders, except MRA-E, contain CS-requirements
  - MRA-E tender consists of 20,000 points

Private
- ~180,000 existing private charge points
- Only the tender Rijksvastgoed contains CS-requirements
  - (most private points are not tendered)
Cyber security on devices

To make charging infrastructure secure we should at least address five issues:

1. A future-proof design with enough computational power and memory resources
2. Have requirements or regulation regarding roll out of charging infrastructure to follow the latest security advices and apply cryptographic agility
3. Communication to and from the device(s) should be secured by encryption and digital signatures
4. Create norms and standards regarding resilience and system hardening.
5. Physical testing of the cyber security of devices in a certified laboratory.
ElaadNL identified five options for a PKI:
1. a PKI consortium
2. multiple PKIs
3. a certificate trust list-based PKI
4. walking chain of trust
5. a European authority PKI.
One PKI consortium

• The most basic option; to let all parties reside under one root Certificate Authority (CA).
Multiple PKI’s

• Market parties will join as many PKIs as possible. Original equipment manufacturers (OEM) adopt multiple root certificates into their EVs. Charge Point Operators (CPO) will also adopt multiple root certificates into their charging stations.

• At a certain stage, multiple PKIs exist independently next to each other, not trusting each other.
Certificate trustlist

- PKIs can express their trust in each other.
- An administrative authority might evolve with a mission to create a unique trust list.
- Worries about the scalability of the system
- Given these ISO 15118 specifications, OEM’s might limit the number of CA’s in the EV, thus frustrating interoperability and the scale up of the system.
Walking chain of trust

• Large players may require multiple CAs in various geographic regions.
• Cross-certification allows different CAs to deploy and maintain trusted relationships.
European authority

• Our starting point is to develop a transparent, trusted, safe, simple, fast, cost-efficient and legal PKI that supports the level playing field in e-mobility.
• There is a need for an open standard and a level playing field between different regions and sectors.
• A neutral and independent referee in case of disputes.
• Therefore there is a role for an European Authority to oversee the governance of the PKI.
Situation, and expected market pathway

One PKI consortium

current situation

We are here

multiple PKI's

EVs only allow for 5 V2G roots!

Certificate trustlist based PKI

European Authority

Walking chain of trust

The current situation seems to mirror the early days of the telecoms industry
Towards an open market

Apart from quality requirements initiated, market rules should be deployed:

• Balance in the market
• Create fair and reasonable conditions
• Clear rules stimulate the needed innovation, improvement of service and price pressure.
• Market rules prevent a lock out of small companies and start ups, or a lock in of consumers
Market rules

For the specific design of a PKI, it should in our opinion be drawn along some indicators which should:

1. be trusted by all market parties,
2. be simple, can be set up quickly, fast in implementation of upgrades,
3. cost not too much to set up and maintain,
4. respect all the legal requirements and creates a level playing field
5. have clear, non-discriminatory rules for participation and a neutral authority to guard these 5 indicators
Conclusion 1: open market
Conclusion 2: Security in the new energy system