# INNOVATION DEAL – ADDITIONAL ANSWERS TO THE COMMISSION QUESTIONS MEMORANDUM

## 1. An Analysis on the state of bi-directional charging:

*Technical/ interoperability barriers related to Bi-directional charging/ Discharging (both V2H/H2V and V2G/G2V): please provide a short description of the state of technical advancement of bi-directional charging, as this is missing.*

*What are the barriers? What are the missing elements- interoperability- for Home –charging? What is the expected time scale for this to happen?*
*What are the necessary protocols (including for bi-directional charging) so that smart charging is enabled et EU level? (not at OEM equipment level): that is entirely missing*

**Answer**:
The Technological Readiness Level of DC V2G, based on current pilots and research, is approximately at level 6 (technology demonstrated in relevant environment). This concerns DC V2G projects using the Chademo protocol. The TRL of AC V2G should be scaled in level 3 or 4.
One main interoperability barrier is the technology required to remotely control a V2G charger. Input signals coming from a third party (i.e. an aggregator) should be transferred to the V2G charger in order to make sure the connected vehicle is charging or discharging at the right time with the right amount of power. The dedicated protocol for transferring signals from a central system to a charging station is the Open Charge Point Protocol (OCPP) andOCPP ready for V2G is not yet ready. A task group has started to define relevant messages. However, since the communication protocol for AC V2G (ISO/IEC 15118 -20) is in the development stage till end of 2020 OCPP has to adapt accordingly. Lack of finished communication protocols between EV and EVSE and between EVSE and central system are one of the important barriers related to bi-directional charging.
To solve this, some initiatives exists:
ElaadNL aligned currently available requirements for production units on the grid, combined with general requirements for charging stations and some requirements derivated from the Dutch Grid Code to form a proposal for V2X systems. Implementation and use of these requirements should be done with notice to ElaadNL, since this is a greenfield and ElaadNL can provide tests whether the system is in conformance with the requirements in the ElaadNL Test Lab.
No rights can be derived from the V2X requirements. This document is the first appendix.

OEM's and chargepoint-providers are already starting to rollout AC V2G-ready chargers and test with first car-prototypes.
https://www.usi.nl/en/news/news/koning-willem-alexander-opent-bidirectioneel-ecosysteem-in-Utrecht

## 2. An analysis on the technical/ manufacturing barriers related to communication of the "state of charge" of Batteries in the EVs

For EV Battery- it is not clear- who is capable of performing "charging and discharging": if the OEM is the only party able to "read battery data"- b) transmit this information via a protocol to the Grid or from the Grid-- irrespective of who owns the battery- only the OEM/ undertaking will be able to perform balancing and flexibility.

The statement also appears on p.20- graph- "EV OEM manufacturer- determines if the EV is suitable for smart charging" and "unlocks data for smart charging"

Is there any analysis of the technical/ manufacturing barriers related to the reading of the "state of charge" of Batteries and transmitting this for purposes of smart charging?

- How does this affect other possible market players- such as aggregators- that are mandated by individual consumers to manage multiple loads?
- Or the DSOs- who could procure flexibility?
- How does it affect the right of individual consumers to become active consumers?

**Answer:**

The OEM should provide the technical enablers and customer authorization to communicate with an external body, whether it is the DSO, TSO, aggregators, to provide the SOC, and enable the control of the car. The OEM is responsible for the car and battery warranty and health of component, therefore this is to be strictly controlled. Which does not prevent all other actors to procure flexibility to the energy market. The right of individual consumers and their consent should be obtained by the one who provides the flex, and case by case.

**3. Analysis of barriers to deployment of Public Key Infrastructure and possible consequences- if that was not agreed or solved at EU wide level**

A short analysis would provide value added to the report, there is a reference on page 27 to an independent certification authority. For the sake of analysis, it should be explained, what are the possible consequences- for deployment of EV- if that PKI and certification authority roles are not properly addressed/ at EU level.
Answer:

To operate a cybersecure charging infrastructure the focus on of the physical devices of the charging infrastructure should at least be on five topics. To start, a future-proof design should be created with enough computational power and memory resources. These resources are needed to be able to handle future algorithms and protocols, and firmware updates. Second, the cryptographic algorithms and protocols of todays are well known and considered secure. However, it could be that a vulnerability is found which requires to switch to a different algorithm. The requirements, to follow the latest security advices, should be part of the requirements or regulation regarding roll out of charging infrastructure. Third, communication to and from the device(s) should be secured by encryption and digital signatures, for example by Transport Layer security (TLS). The fourth topic is creating norms and standards regarding resilience and system hardening. Charging stations should have unused interfaces disabled, and maintenance interfaces secured. The charging station should not crash when malicious messages are sent; the infrastructure should be able to detect a different format and handle it accordingly. Since the ability to charge is part of the vital infrastructure, the last topic regards the physical testing of the cyber security of devices in a certified laboratory.

Apart from the need for better cyber security on devices, consumers have a wish for choices and a seamless service. If the automotive and energy sectors are unable to agree on a common ground, we will lose interoperability. Losing interoperability is bad for both innovation in the sector and consumers. However, an agreement between players in the market is not yet in sight. How can we avoid quarrelling between market players and still have better cyber security of the infrastructure? This can be achieved with a public key infrastructure (PKI) with an open design. As mentioned, multiple designs for a PKI using ISO 15118 are possible. Models vary from a system managed by a single party or a consortium of parties, to an open PKI that allows everybody in the EV market to participate [2]. ElaadNL identified five options for a PKI: 1) a PKI consortium; 2) multiple PKIs; 3) a certificate trustlist; 4) walking chain of trust; 5) a European authority.

In an ideal world only one PKI is needed and possible for EV charging. Governance, technologic improvements and operations could be done by experts, favorably a qualified neutral third party. However, the PKI for smart charging is a global operation. Different countries on different continents have a different pace of roll out of electric mobility. Visions on governance might vary between countries, or within a sector. The PKI shall be a cross sector operation, with players in automotive, energy and possibly banking and internet. Therefore it must be clear that the root authority should themselves not be a player in the EV or automotive sector, because the authority cannot be an ally to a specific group of consumers. The world of EV is a too much fragmented platform for the top-down hierarchy needed for a one PKI consortium.

There can also be a single body that overlooks the ecosystem, but ownership is distributed among many, resulting in a federal scheme. A bridge PKI - a number of PKIs that each cross-sign each other – or a collaborative approach are examples of multiple PKI's of which there are already at use in different sectors, such as the internet. Key requirement is that the EV PKI must be as responsive as the web PKI. This is because the lifetime of the EV is long; a vehicle of today might still be there in twenty years' time. Therefore, it must be able to adapt to the technology of tomorrow.
To enable the transition towards multiple PKI's and their CA there can be worries about the scalability of the system. It might be impossible to be able to predict with any sort of inclusiveness what are the right root CA's that need to be installed in the cars. One root CA is enough. 5 maximum.

Large players may require multiple CAs in various geographic regions. Cross-certification allows different CA to deploy and maintain trusted relationships. For cross-certification two operations. First, a trusted relationship between two CAs has to be established. In the case of bilateral cross-certification, two CAs securely exchange their verification keys. These are the keys used to verify the CAs' signatures on certificates. To complete the operation, each CA signs the other CA's verification key in a certificate referred to as a "cross-certificate". Second, on the client-side software the trustworthiness of a user certificate signed by a cross-certified CA should be verified. The operation is often referred to as "walking a chain of trust". The "chain" refers to a list of cross-certificate validations that are "walked" (or traced) from the CA key of the verifying user to the CA key required to validate the other user's certificate. When walking a chain of cross-certificates, each cross-certificate be checked to ensure that it is still trusted. User certificates must be able to be revoked; so must cross-certificates. This requirement is frequently overlooked in discussions regarding cross-certification.

The question is not whether five PKIs are sufficient to serve the market, but what 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. To avoid scalability problems, or too long, uncontrollable chains of trust, there is a need for an open standard and a level playing field between different regions and sectors. Therefore there is a role for an European Authority to oversee the governance of the PKI.

From one PKI the architecture is evolving to multiple pki's. This allows competition and competition will reduce costs. However, at the stage of development of multiple PKIs interoperability is lost. Technical standards on quality and cyber security are needed before the architecture can grow to a next stage, where marketplaces start to trust each other: the certificate trustlist. Once marketplaces trust each other, cross-signing can take place. The walking chain of trust welcomes interoperability again and thus a cheap, seamless charging experience throughout Europe for EV drivers. An European authority should overlook the market.
So in the end, if not properly addressed, the plug and charge funtionnality will not be sustainable at EU level.

4. Pages 30-31- remuneration schemes for the DSOs and "net metering schemes":

Graph on p. 30 represents an example of 17 cents of savings- without “netting”. The analysis however does not further precise- if these “earnings from electricity to the grid” are to be considered as “network socialised benefits” for the network- i.e. network costs become less important. Statement on page 35 would indicate that “flex should be incorporated in the reimbursement by regulators- otherwise the DSOs will continue the expansion of the grid”.

# CHARGING STATIONS

## Requirements for bidirectional systems

**This document contains requirements for V2X systems. It is a draft from ElaadNL and contains general requirements as well as requirements derivated from the Dutch Grid Code.**
**Note: the grid code does not officially has V2X in scope. The requirements below form a proposal on current available requirements for production units on the grid, combined with general requirements for charging stations.**
**Implementation and use of these requirements is to be done with notice to ElaadNL.**
**ElaadNL also provides the possibility to test in conformance of the requirements below in the ElaadNL Test Lab.**
**No rights can be derived from the V2X requirements.**

## 1. General Requirements

| | |
|---|---|
| 1 | The responsible CPO reports the location of the V2X charger at the local DSO via the available platform www.energieleveren.nl<br>(Note: a new registration system called CEREX is being prepared by the DSO's. When CEREX is available, registration of bidirectional systems should be done there.<br><br>For more information https://www.netbeheernederland.nl/nieuws/nieuwe-zonnepanelen-na-27-april-voorlopig-verandert-er-niets--1285 |

## 2. Legislation and Standards

| | |
|---|---|
| 2a | NEN-EN 50549-1:2019<br><br>Requirements for generating plants to be connected in parallel with distribution networks<br><br>Part 1: Connection to a LV distribution network<br>Generating plants up to and including Type B |
| 2b | VDE-AR-N 4105 |