Comments on CPUC VGI Working Group "Draft Proposal for Next Steps" from 2017-10-27

oxygen
INITIATIVE

Oxygen Initiative
2017-11-08

Northbound: Grid integrated charging

- For grid-friendly charging it is necessary that distribution system operators provide data (e.g. Time-of-Use tariffs or information about available power) and that this information is transferred to the charging controller (in the sense of ISO 15118 this is the EV, in the sense of SAE J1772 it is the EVSE). We recommend that CPUC-ARB add to the proposal:
  - Which interface should be used to get utility information (e.g. Time-of-Use tariffs over OpenADR)?
  - This information should be offered to an EVSE/EV for optimizing the charging strategy or profile.

Southbound communications

- We recommend to add to the proposal:
  - For AC level 2 and DC level 1 to 3 also the control pilot signal and its corresponding pin is a required hardware specified by SAE J1772 / IEC 61851-1.
- For an economical interoperability of communication between EV and EVSE a well-defined, market ready, highly accepted international standard at a high level of maturity should be proposed. Charging session management should be done automatically. We recommend to add to the proposal:
  - EV and EVSE should support ISO 15118 with External Identification Means (EIM) and Plug-’nd-Charge (PnC).

Cyber Security (EVSE and EV requirements)

- To ensure cyber (or information) security (see basic concepts at https://en.wikipedia.org/wiki/Information_security#Key_concepts) it is well known practice to use digital certificates together with algorithms (like Elliptic Curve Cryptography, AES, SHA-1, random number generator). While EVSE are normally not operated in a controlled and secured environment (e.g. a computing center), a secure storage for certificates and secure implementation of algorithms should be available. A popular way is using a Hardware Security Module (HSM, https://en.wikipedia.org/wiki/Hardware_security_module). A kind of small built-in HSM is a Trusted Platform Module (TPM) as a secure cryptoprocessor, specified as international standard ISO/IEC 11889 (https://en.wikipedia.org/wiki/Trusted_Platform_Module). A TPM is built-in nearly in all laptops and a lot of desktop computers.
- We recommend to build in a TPM in each EVSE controller.