DOCKETED	
Docket Number:	22-EVI-06
Project Title:	Vehicle-Grid Integration
TN #:	250623
Document Title:	ElaadNL - Technical solutions for PKI
Description:	N/A
Filer:	Jeffrey Lu
Organization:	California Energy Commission
Submitter Role:	Energy Commission
Submission Date:	6/13/2023 10:20:33 PM
Docketed Date:	6/14/2023

EVS36 Sacramento, June 14th 2023

Technical solutions for PKI interoperability

Elaadnl

Researching & testing
smart and sustainable charging

ElaadNL youtube video on the PKI for ISO 15118: https://www.youtube.com/watch?v=fBRc1bUL6Yw

Two publications

2018

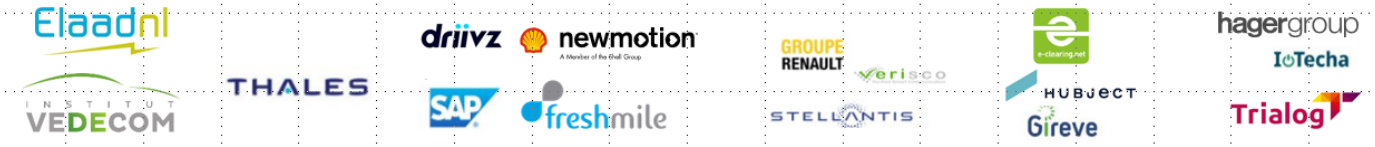
2022

Three PKI Interoperability demonstrations

Using Cross Certification

2020

Using a Certificate Trust List



2021

ISO 15118 Plug&Charge Ecosystem interop

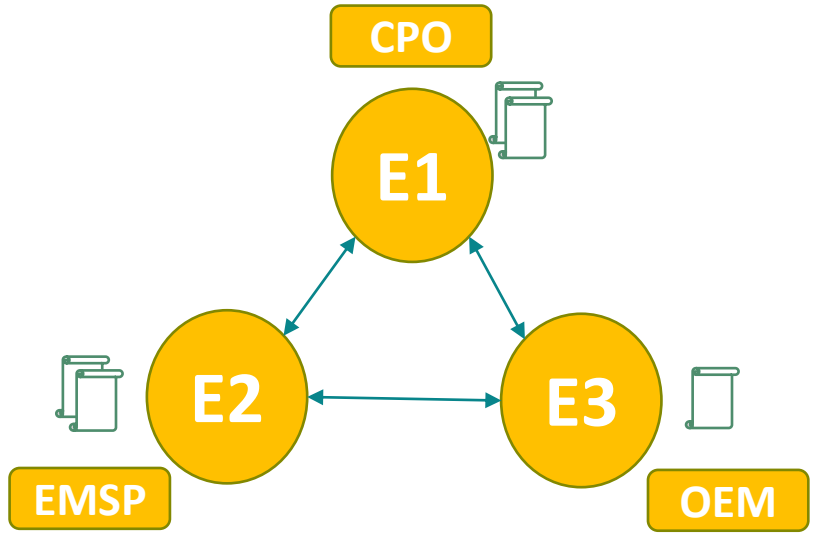
2022

Ecosystem / PKI Pool Interoperability

- Multiple Certificate Pools will exist in the market
- Prevent that all CPOs and EMSPs must join all Certificate Pools, or even PKI ecosystems
- This will make EV charging unnecessary expensive for end users
- Several options exist to handle multiple pools with multiple PKIs

Ecosystem / PKI Pool Interop. variants

- Parties provide certificates to all Certificate Pools
- Parties fetch certificates from all Certificate Pools
- Synchronization between pools
  - By request
  - Share all data between CPs
- Broker / directory service



Connecting PKI Pools

Some operations between Pools of different ecosystems are needed

- Fetching OEM Provisioning Certificate at external OEM Certificate Pool
- Signing Contract Bundles by external CPS
- Fetching Signed Contract Bundle at external Contract Certificate Pool
- Optional: Storing Contract Bundles at other Ecosystems (for telematics route)

PKI Pool Interoperability considerations

- Signing Contract Bundles
  - Depending on the V2G Root CA(s) in the EV
  - Pools are using CPSs from other ecosystems

- Storing Contract Bundles
  - If OEM Provisioning Certificates Pool and Contract Certificate Pool in different ecosystems: where to store contract bundle?
    - At “EMSP side”, i.e. the Contract Certificate Pool of the EMSP ecosystem
    - At “OEM side”, i.e. the Contract Certificate Pool of the OEM ecosystem

Assumptions & starting point

- Operating under several V2G Root CAs as seen in previous demonstrations
- Ecosystems cooperation
- Commercial / GDPR matters will be addressed before commercial implementations

Demo: OEM, eMSP and CPO are each using a different provider that interconnect

Demo step 1: The OEM stores its PC in e-clearing PCP

Demo step 2: The driver requests its eMSP to activate Plug&Charge.

2 The bundle needs to be signed by e-clearing (the OEM only trusts e-clearing PKI)

Demo step 3: The driver in Germany charges (for the first time) on a charging station whose CPO is connected to Hubject

3 The CC needs be installed in the vehicle before Plug&charge.

Final notes on ISO 15118 Plug&Charge Ecosystem interoperability

Benefits

- Technically it is feasible to **connect different certificate pools to provide** ISO 15118 Plug&Charge Ecosystem **interoperability**
- When taken care of, **it is not necessary for OEMs, CPOs and EMSPs** to join all Plug&Charge Ecosystems

Open Challenges:

- Due to the combined nature of the data (OEM Prov Cert & contract data), the topic of **sharing the data requires agreements between Plug&Charge Ecosystems**
- **Requires market definition** with accompanying rules for all market participants (commercial platforms, EMSPs, CPOs, OEMs)
- 5s rule could be violated via forwarded installationRequests

A successful PKI ecosystem needs

1. Technical Interoperability between PKIs
2. Quality Rules per PKI
3. Market Rules and Governance to ensure freedom for consumers and to ensure a fair and open market for all market parties
4. Inclusivity of ISO 15118

THANK YOU!!