PKI

Craig Rodine
Principal Investigator
Sandia National Laboratories

Sandia National Laboratories

Exceptional service in the national interest

PUBLIC KEY INFRASTRUCTURE (PKI) IN EV CHARGING

Enhancing the cybersecurity posture of EVSE-CSMS (OCPP) communications

Craig Rodine

PMTS, Science and Engineering – Cybersecurity R&D
Electric Grid Security and Communications

Open Charge Alliance – Cyber Security Event US
12 May 2026, Dekra Test Laboratory, Plymouth, MI

U.S. DEPARTMENT of ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

AGENDA

- Background and context
- Framing this investigation
- OCPP Security Profiles
- Certificate Policy and Certification Practice
- CNO-serving Roots in a Certificate Trust List

BACKGROUND AND CONTEXT

Sandia's prior R&D on PKI for EV Charging Infrastructure

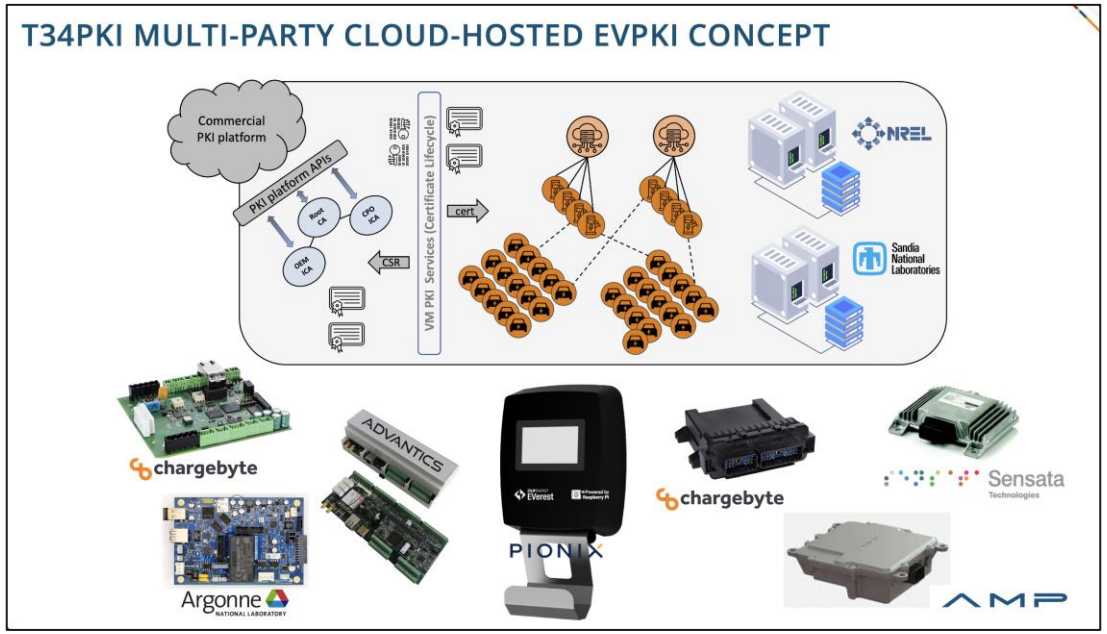
- Testing PKI for secure EV-EVSE-CSMS comms (SiL) within a large-scale cyber range
- Analysis and assessment: "Cybersecurity Risks in Standards-based EVCI Deployment"
- Table-Top (Hardware-in-Loop) PKI test bench for EV and EVSE communications controllers

Sandia's lab facilities for EVCI cybersecurity R&D

- Situated in our Distributed Energy Technology Laboratory (part of our focus on the 'energy edge')
- COTS hardware and FOSS software (Everest, CitrineOS)

Cybersecurity provisions for public cloud-based CSMS

- Hosting an exemplary CSMS on public cloud (AWS)
- Goal: help industry develop an authoritative, automated, comprehensive online PKI testing capability



FRAMING THIS INVESTIGATION

- OCPP v2.x enables the use of best-in-class cybersecurity [building on LaQuSo, 2014]
  - TLS v1.2 or above, thoughtfully selected cipher suites, clear requirements
  - Suitably robust e2e for EVSE-CSMS communication over the public Internet
- Actual practice differs and varies, for example:
  - CNOs may use VPNs and/or M2M carrier-provided security
  - Public cloud-hosted CSMS could use CSP-native PKI
- Managing security data (passwords, certificates, keys) would be a major challenge
  - Each CNO has to implement their own credentials management
  - PKI tools and systems made for WebPKI (not M2M) might not be suitable
- R&D task: explore how OCPP could be supported by an ecosystem-wide PKI and CTL
  - Design the exact PKI capabilities needed for EVSE-CSMS communications
  - Provide OCPP certificate management (PKI operations) for the whole ecosystem
  - Establish common, transparent governance to improve cybersecurity posture

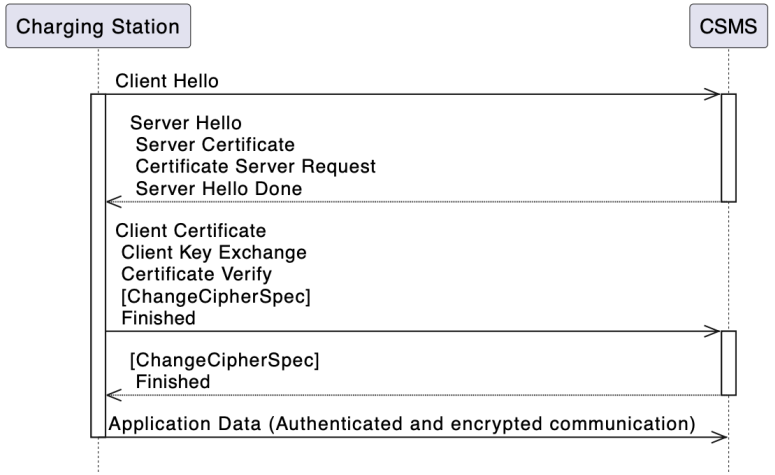
OCPP SECURITY PROFILES

1.3. Security Profiles

This section defines the different OCPP security profiles and their requirement. OCPP 2.1 supports three security profiles:
The table below shows which security measures are used by which profile.

Table 12. Overview of OCPP security profiles

Profile	Charging Station Authentication	CSMS Authentication	Communication Security
1. Unsecured Transport with Basic Authentication	HTTP Basic Authentication	-	-
2. TLS with Basic Authentication	HTTP Basic Authentication	TLS authentication using certificate	Transport Layer Security (TLS)
3. TLS with Client Side Certificates	TLS authentication using certificate	TLS authentication using certificate	Transport Layer Security (TLS)



ID	Requirement definition
A00.FR.421	The CSMS SHALL support at least the following four cipher suites: **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** **TLS_RSA_WITH_AES_128_GCM_SHA256** **TLS_RSA_WITH_AES_256_GCM_SHA384** (Same as A00.FR.318) Note: The CSMS will have to provide 2 different certificates to support both cipher suites. Also when using security profile 3, the CSMS should be capable of generating client side certificates for both cipher suites.
A00.FR.422	The Charging Station SHALL support at least the cipher suites: (**TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** AND **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**) OR (**TLS_RSA_WITH_AES_128_GCM_SHA256** AND **TLS_RSA_WITH_AES_256_GCM_SHA384**) (Same as A00.FR.319)

CERTIFICATE POLICY AND CERTIFICATION PRACTICE

OCPP specifications lack Certificate Profiles (CPs)

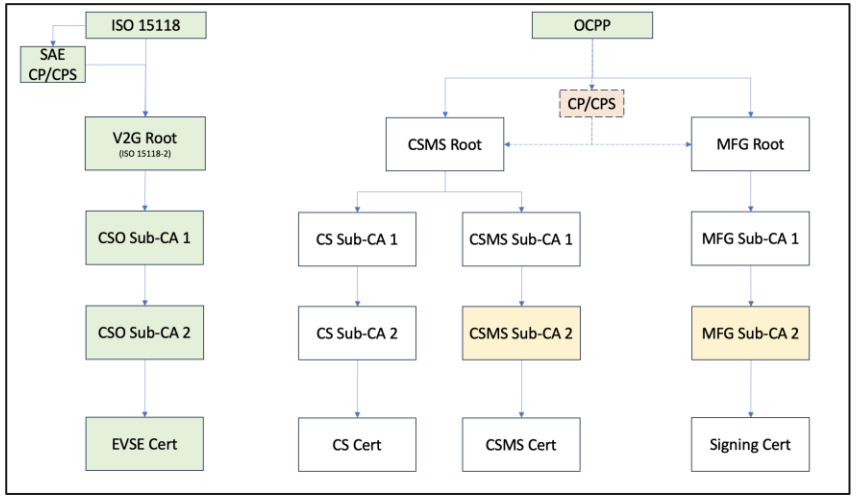
- PKI providers need these to provide OCPP certificates
- And to develop Certificate Practice Statements explaining how they support the CPs

CPs would also be useful for defining cloud PKI configuration needed to support CSMS (e.g. OCPP server, firmware signing)

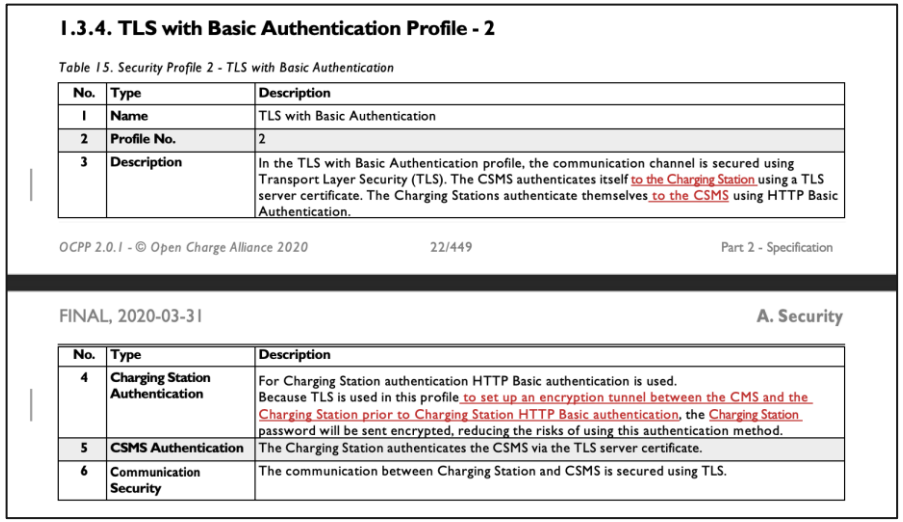
- Replicated for each CNO using the public cloud? or shared across CNOs using that public cloud? or across clouds?
- Would governance and operations remain proprietary?

Sandia would be glad to contribute to the OCA community:

- Our draft CP covering all needed OCPP 2.x certificates
- Redline comments to Security chapters of OCPP v2.0.1 and v2.1 specifications (reflecting best PKI practices)



Draft PKI hierarchy for OCPP (basis for CPs)



1.3.4. TLS with Basic Authentication Profile - 2

Table 15. Security Profile 2 - TLS with Basic Authentication

No.	Type	Description
1	Name	TLS with Basic Authentication
2	Profile No.	2
3	Description	In the TLS with Basic Authentication profile, the communication channel is secured using Transport Layer Security (TLS). The CSMS authenticates itself to the Charging Station using a TLS server certificate. The Charging Stations authenticate themselves to the CSMS using HTTP Basic Authentication.

No.	Type	Description
4	Charging Station Authentication	For Charging Station authentication HTTP Basic authentication is used. Because TLS is used in this profile to set up an encryption tunnel between the CMS and the Charging Station prior to Charging Station HTTP Basic authentication, the Charging Station password will be sent encrypted, reducing the risks of using this authentication method.
5	CSMS Authentication	The Charging Station authenticates the CSMS via the TLS server certificate.
6	Communication Security	The communication between Charging Station and CSMS is secured using TLS.

Example Mark-up of Security Section (OCPP 2.0.1)

CNO-SERVING ROOTS IN A CERTIFICATE TRUST LIST

An ecosystem Certificate Trust List enables an open, competitive market for EVCI PKI (Root CAs)

digicert®

Won competitive bid for CTL Root CA role

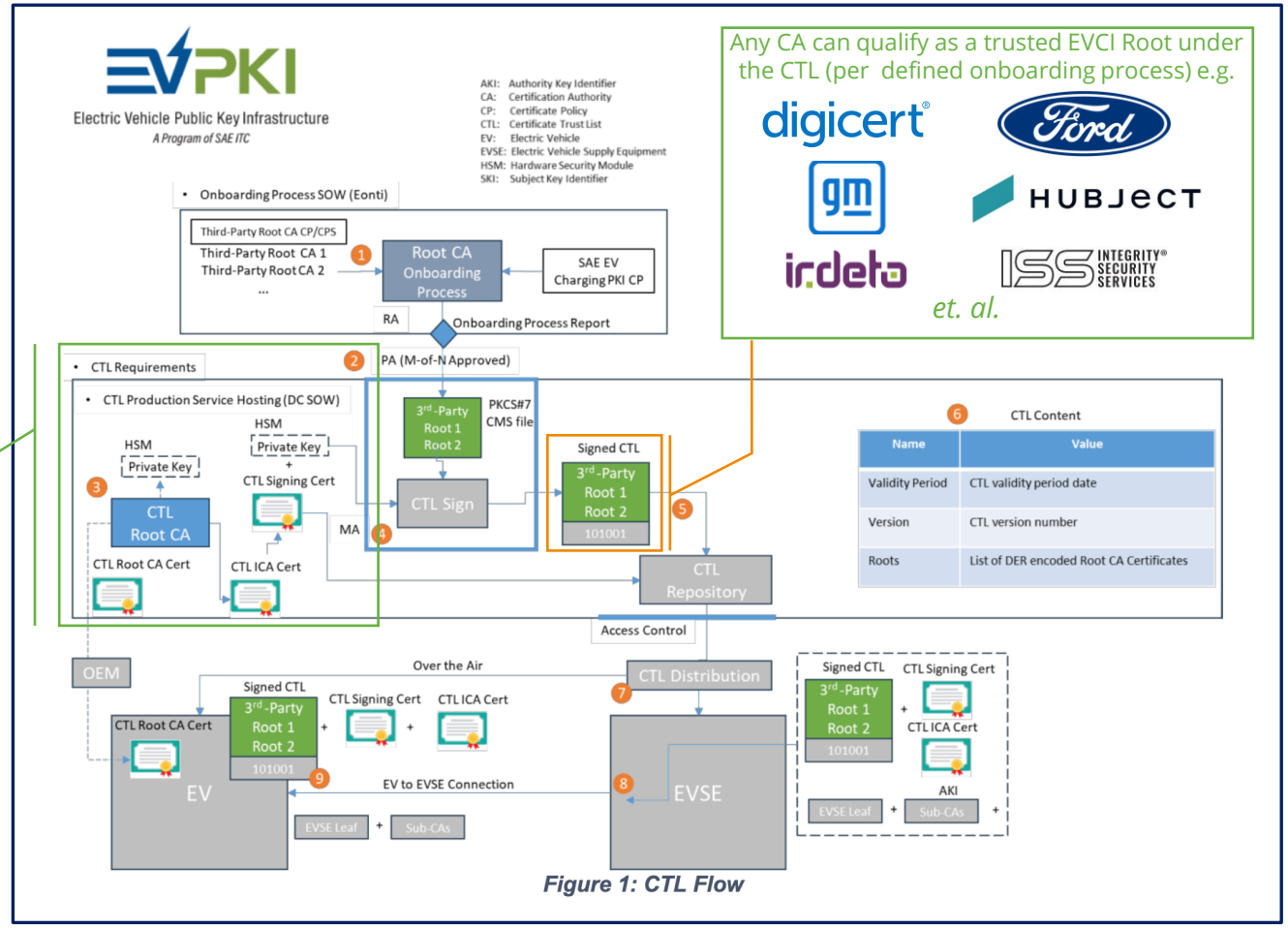


Figure 1: CTL Flow

CNOs should ensure that V2G Roots serve their needs and interests, or perhaps create dedicated Roots providing certificates for OCPP endpoints (CSMS, EVSE) and code signing?

Source: https://www.sae-itc.com/programs/evpki/pub/certificate-trust-list-requirements

THANKS FOR YOUR ATTENTION AND INTEREST TODAY!

crrodin@sandia.gov