DOCKETED

Docket Number:	22-EVI-06
Project Title:	Vehicle-Grid Integration
TN #:	250624
Document Title:	CharIN - Workshop on PKI Governance and Solutions, Part B
Description:	N/A
Filer:	Jeffrey Lu
Organization:	California Energy Commission
Submitter Role:	Energy Commission
Submission Date:	6/13/2023 10:21:33 PM
Docketed Date:	6/14/2023

Empowering the **next level** of e-mobility

CharIN – Charging Interface Initiative e. V.

CEC-ElaadNL Workshop on PKI Governance and Solutions

Wednesday June 14, 9:00 am - 12:00 pm PT | 12:00 pm – 3:00 pm ET

CHARIN

CharIN North America

Antitrust Statement

Antitrust Statement: In discharging their responsibilities, members of CharIN e. V. (association) function as individuals and not as agents or representatives of any organization with which they may be associated.

In the course of all CharIN activities, members must avoid discussion about pricing, sales and marketing programs, territories, customers, production capacity and other competitively sensitive topics. In the event any member ever feels that the course of association activities or statement or actions in association meetings is headed into such an area, members should raise the issue immediately so that further discussion of such matters can be suspended pending receipt of advice satisfactory to the members that the topics addressed to not give rise to antitrust problems.

Patent Disclosure: Each CharIN member would be required to disclose at specified times during a development process all patents and patent applications that are owned, controlled or licensed by the member, member's employer or third party and that the member believes may become essential to the draft specification under development. The member would make this disclosure based on the member's good faith and reasonable inquiry. If CharIN e. V. receives a notice that a proposed CharIN standards recommendation may require the use of an invention claimed in a patent, the respective part of the CharIN Board Policy will be followed.

Transparency Statement: The CharIN e. V. is committed to transparency at the highest level. All topics are discussed in open meetings and decisions are consensus based (not unanimous). CharIN members are required to be vigilant in their efforts to monitor CharIN association`s activities and decisions by actively participating in the meetings and calls. Any issues with the transparency of the CharIN e. V. should be brought to the attention of the CharIN Executive Board for resolution.

Reference: CharIN Compliance Guideline

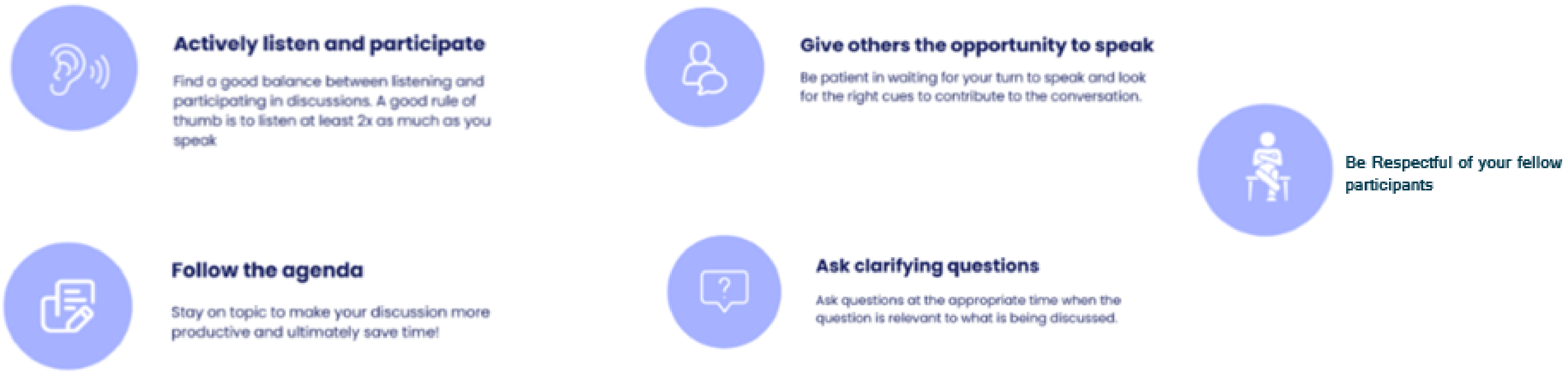
CEC-ElaadNL Workshop on PKI Governance and Solutions

subtitle

Agreement for Royalty Free Use

Participants agree to offer their technical proposals with no patent claims or in case of pending patent, be willing to grant royalty-free licenses for such proposals and its derivatives.

Further, Participants agree to abide by CharIN's antitrust policy in developing an industry solution and accept all the CharIN convening rules.



Actively listen and participate

Find a good balance between listening and participating in discussions. A good rule of thumb is to listen at least 2x as much as you speak

Give others the opportunity to speak

Be patient in waiting for your turn to speak and look for the right cues to contribute to the conversation.

Be Respectful of your fellow participants

Follow the agenda

Stay on topic to make your discussion more productive and ultimately save time!

Ask clarifying questions

Ask questions at the appropriate time when the question is relevant to what is being discussed.

Part B - Agenda

Part B: **Determining a path for North America** (120+ minutes)
Discussion led by CharIN North America
Near term objectives: Review near term objectives and outcomes from the VOLTS PKI Workshop.

a. Review Status of Joint Working Group
b. Discussion of (immediate/medium term) solutions for PnC enablement in North America
c. Other immediate solutions to be deployed within the next 12mos while discussions about longer term rules are pending

Discuss framework for determining PKI governance and rules in North America:

a) CharIN's process for commonly developing PKI governance and Market guidelines in NA.
b) Agree upon appropriate forum going forward for determining governance and market guidelines

Discuss longer term solutions for PKI interoperability and governance: This discussion will be transferred to the above forum when that forum is established.

Follow -up meeting [PKI workshop #1]: Develop short-term solutions for multiple PKI’s

Discussion: Review Near-term tasks

Review Near-term tasks outlined during Workshop #1

- How to handle multiple roots for TLS
- How the vehicles select the right contract certificate to present
- How the contract can be authenticated in the charger
- Define fallback solutions when TLS establishment fails

Determining a Path for North America

Near term objectives: Review near term objectives and outcomes from the VOLTS PKI Workshop

a. Review Status of Joint Working Group

b. Discussion of (immediate/medium term) solutions for PnC enablement in NA

c. Other immediate solutions to be deployed within the next 12mos while discussions about longer term rules are pending

A) Update from 15118-2 User Group

A Proposal to help EVs deal with multiple contracts, Peter Thompson

15118-2 User Group Proposal to help EVs deal with multiple contracts

Peter Thompson, Standards Engineer

June 14, 2023

Agenda

1. The current situation
2. MO identifier definition
3. Delivery methods of MO identifiers
4. Discussion

Please wait until the end to ask questions.

Overview

- EVs with multiple contract certificates from different MOs have no hints to help decide which contracts to use for PnC. With ISO 15118-2, upon failure, the EV will have to restart the entire session – including the TLS connection.
- This proposal provides 2 solutions to provide sufficient hints to the EV. In addition, a technical proposal is given in the extra slides.
- The ISO 15118-2 User Group has discussed this proposal in great depth, and agrees that the 2 solutions solve the problem.

The current situation

- We need a solution to allow an EV to choose an appropriate contract certificate for PnC.
- ISO 15118-2 does not deal with the possibility of an EV having multiple contract certificates.
    - The standard does attempt to provide enough hints, but these hints are for TLS, not indicating which MO are supported on the station.
- By the end of 2023:
    - There will be at least 3 V2G Root CAs in operation.
    - There will be over 100 MOs in operation.
- TLS only provides hints about which trust chains can be used to set up the TLS channel – nothing about which MO are supported.
- Once PnC fails, ISO 15118-2 requires terminating the session, after which the EV can try again with a different certificate.

The current situation (continued)

- Note that there are several trust chains in ISO 15118-2 – we need to be clear that for TLS, the CPO trust chain is used. For PnC, the MO trust chain is used.
- During the TLS handshake, hints are provided to allow TLS to work. However, the hints are for the CPO trust chain.
- In order to choose a contract certificate that will work, there needs to be a mechanism where the EVSE and the EV can communicate which MOs are supported on the EVSE (which MO the EVSE has roaming agreements with – if there is no roaming agreement, the PnC will fail).
    - Naturally, if the station is owned by the MO, then the PnC will work – provided the EV knows this. The EV could guess that by the TLS certificate, but even then, that is not guaranteed to work.

MOIdentifier definition

- ISO 15118-20 uses a phrase “ProviderID” but does not give any definition for this. This is also not defined in ISO 15118-2.
- In order for the EV to be able to select a contract certificate, it will need to be able search through its contract certicates for a specific string. This string will be called the MO Identifier.
- We can create the MO Identifier by taking parts of the EMAID (in every contract certificate) – the country code (2 letters), and the provider ID (3 letters).
  - Examples: USEVG, NLCPI, USEAI
- The MO Identifier is something that all contract certificates have, and while having no clear authority for the provider ID, seems to be adequate.

Supported MO identifier delivery

- There are two possibilities for delivery of the EVSE’s supported MOs to the EV:
  - Creating a new SDP service (similar to what was done in ISO 15118-20),
  - Creating a new Value-Added Service.
- Both will aid in the selection of a mutually supported MO.

SDP query of supported MO identifiers

- Since there will hundreds if not thousands of MO Identifiers, we need to be able to quickly reduce the set of mutually supported MOs.
- The EV would send a SDP query with a list of the MO Identifiers from the contract certificates on the EV. The SDP Server (EVSE) would then take that list, remove the non-supported MOs, and send that along with the IP address and Port to the EV.
  - The EV doesn’t need to ask for TLS nor TCP, since this is implied already.
- In order to re-use as much code as possible, the first part of the SDP response would look identical to the current SDP response (with IP address, Port, and Security bit). The second part of the response would be the list of mutually supported MO Identifiers.
  - If there are no mutually supported MO Identifiers, the list will be empty.

SDP query of supported MO identifiers

- The flow would look like:
  - The EV sends the UDP broadcast with a payload type value of 0x9004, with a comma separated list of MO Identifiers taken from the EV's contract certificates.
  - The SDP server would respond with a payload type value of 0x9005, with:
    - IP address and port for the EV to use for ISO 15118-2/20,
    - List of mutually supported MO Identifiers (comma separated) (empty if no matches).
- The EV would then start the ISO 15118-2 or -20 messaging, and would then be able to use a mutually supported contract, or only use EIM.

VAS delivery of Supported MO Identifiers

- For the VAS delivery, the EVSE would add in a new service – “SupportedMO”
    - Suggestion is to use ServiceID 64 – this is unused in both -2 and -20.
- The EV would then use ServiceDetailReq to request the supported MO identifiers.
- The EVSE would respond with ServiceDetailRes with the list of MO identifiers in the ServiceParameterList.
- The problem with this approach is that ServiceDetailRes can only transmit up to 255 MO Identifiers, and there is nothing in ISO 15118-2 / -20 that allows data to be sent as part of the ServiceDetailReq.

TLS is not appropriate for communicating MO identifiers

+ TLS allows for exchange of authorities, but this is for the communication channel, not for the charge authentication.
+ There are two sets of certificates that we are concerned with:
  - One for the communication channel,
  - One for the PnC.
+ TLS uses the first set of certificates, and *can* provide hints about the root CA that can be used for securing the communication, but nothing about the root CA used for PnC.

Conclusion

- EVs with multiple contract certificates for PnC need help to choose a contract that will be supported by an EVSE.
- EVSE can provide hints to the EV by two methods – SDP and VAS.
- The ISO 15118-2 User Group has discussed this proposal in great depth, and agrees that the 2 solutions solve the problem.
- SDP method can work with any number of MO Identifiers, but VAS is limited to 255.
- My recommendation is for everyone to implement the SDP method.

Discussion

Questions welcome.

Thank You

For further information on this topic,
please contact Peter Thompson:
peter.thompson@chargepoint.com

References

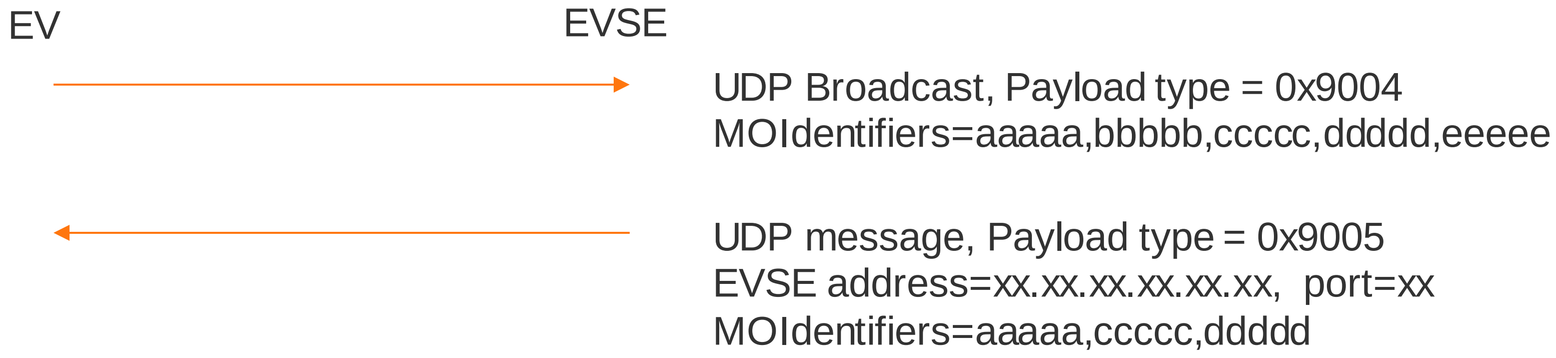
- ISO 15118-2
- ISO 15118-20
- RFC 5246 – TLS 1.2
- RFC 5280 – X.509 PKI Certificate
- RFC 6066 – TLS 1.2 extensions

Message Exchange

Examples for SDP and VAS

SDP message exchange flows

- Message exchange for SDP:



EV

EVSE

UDP Broadcast, Payload type = 0x9004
MOIdentifiers=aaaaa,bbbbb,ccccc,ddddd,eeeee

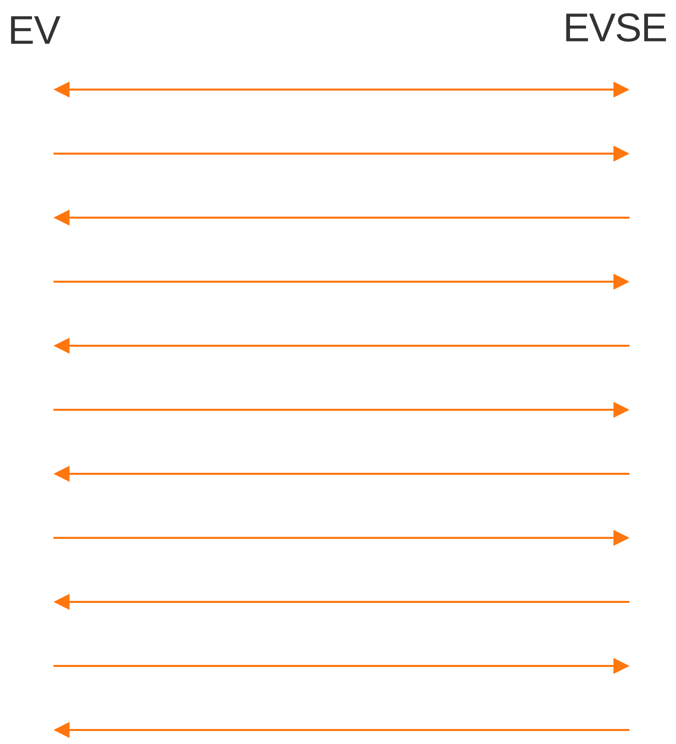
UDP message, Payload type = 0x9005
EVSE address=xx.xx.xx.xx.xx.xx, port=xx
MOIdentifiers=aaaaa,ccccc,ddddd

The first message is a UDP broadcast that has a payload type 0x9004, and a comma-separated list of MO Identifiers that the EV supports.
The SDP Server will see this broadcast, and if it supports this payload type, will send back a UDP message with payload type 0x9005. The message will contain the IP address and port for the exchange of 15118 messages, and a subset of the list of the supported MOIdentifiers (which both EV and EVSE support).

In the case of no match, the list of MO Identifiers would be empty.

This section provides VAS message exchange flows

- Message exchange for VAS:

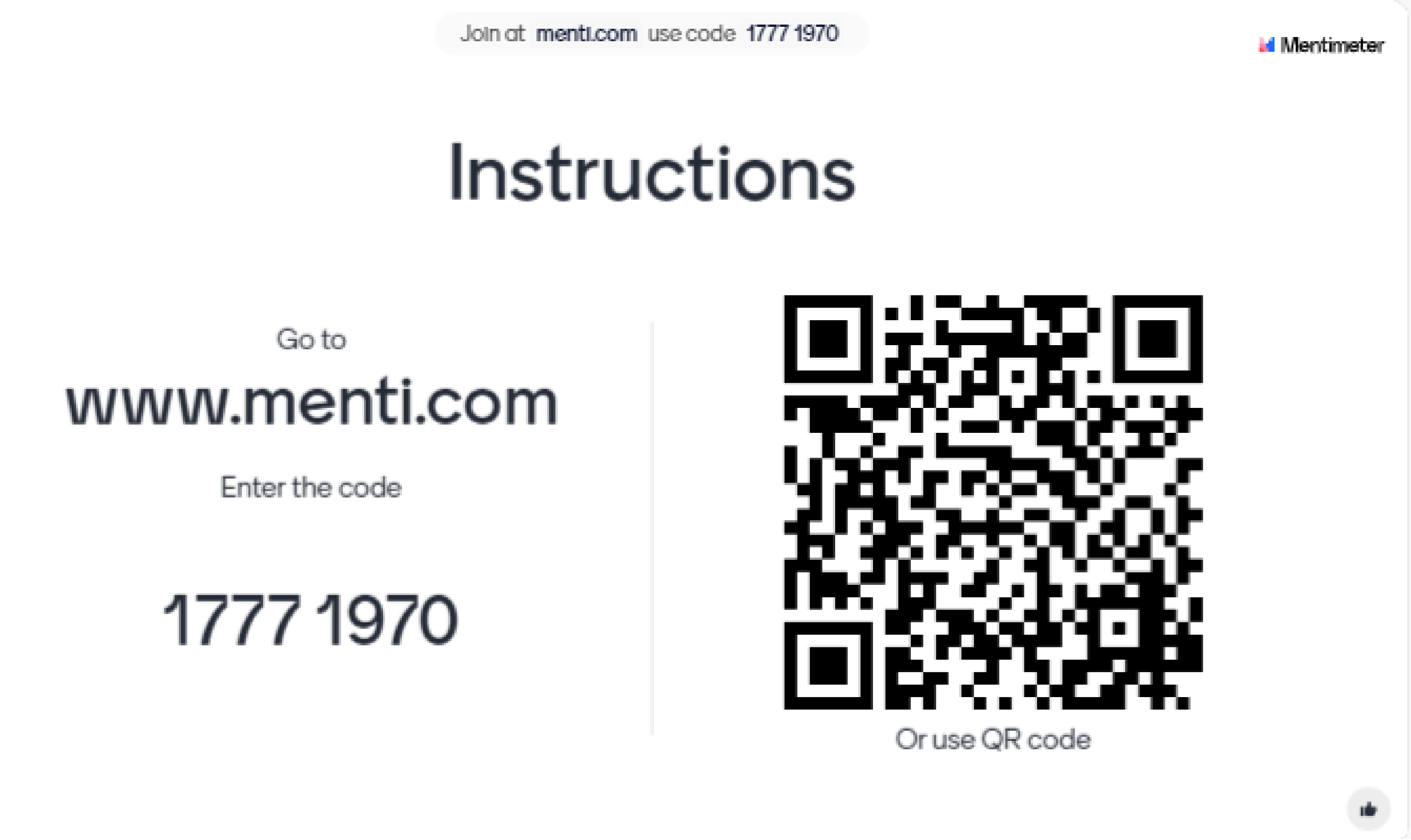


TLS Handshake (unchanged)
SupportedAppProtocolReq (unchanged)
SupportedAppProtocolRes (unchanged)
SessionSetupReq (unchanged)
SessionSetupRes (unchanged)
ServiceDiscoveryReq (unchanged)
ServiceDiscoveryRes (New service ID=64 – SupportedMO listed in ServiceList)
ServiceDetailReq (service ID=64)
ServiceDetailRes (List of supported MOIdentifiers in ServiceParameterList)
ServiceDetailReq (service ID=1 – AC_DC_Charging)
ServiceDetailRes (unchanged)

The EVSE will provide a new service as part of the ServiceDiscoveryRes – but only if that VAS is supported. The ServiceDetailRes will contain the list of MOIdentifiers that are supported on the EVSE.

Determining a Path for North America

Framework for Determining PKI Governance and Rules in North America



Join at menti.com use code 1777 1970

Mentimeter

Instructions

Go to

www.menti.com

Enter the code

1777 1970

Or use QR code

Polling from the Audience #1

As an OEM, how soon can you implement the User Group proposed solution?

<6 months

6 - 18 months

18 + months

Polling from the Audience #2

As an CPO/EVSE provider, how soon can you implement the User Group proposed solution?

<6 months

6-18 months

18+ months

Determining a Path for North America

Near term objectives: Review near term objectives and outcomes from the VOLTS PKI Workshop

B) Discussion: (immediate/medium term) solutions for PnC enablement in NA

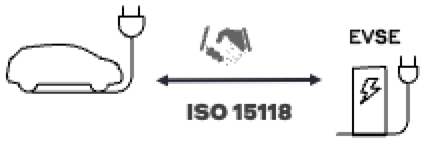
Handling TLS with Mutli-V2G Root PKIs - Hubject

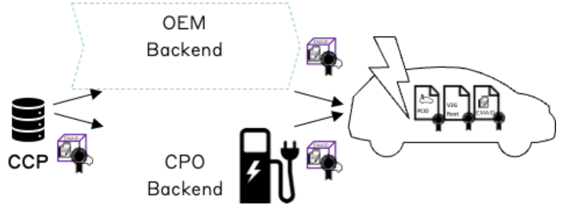
TLS with Multi-PKI

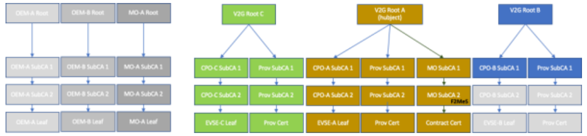
HUBJECT INC. USA / JUNE 14, 2023

Critical Topics for Interoperability with multiple PKIs for Plug&Charge

1. Multiple V2G PKIs
    1. TLS Handshake between EV and EVSE
    2. Contract Installation in EV
2. Interoperability between multiple PKIs
3. Interoperability between Plug&Charge Ecosystems & Services
4. Multi-contract handling for Plug&Charge







HUBJECT SOLUTION

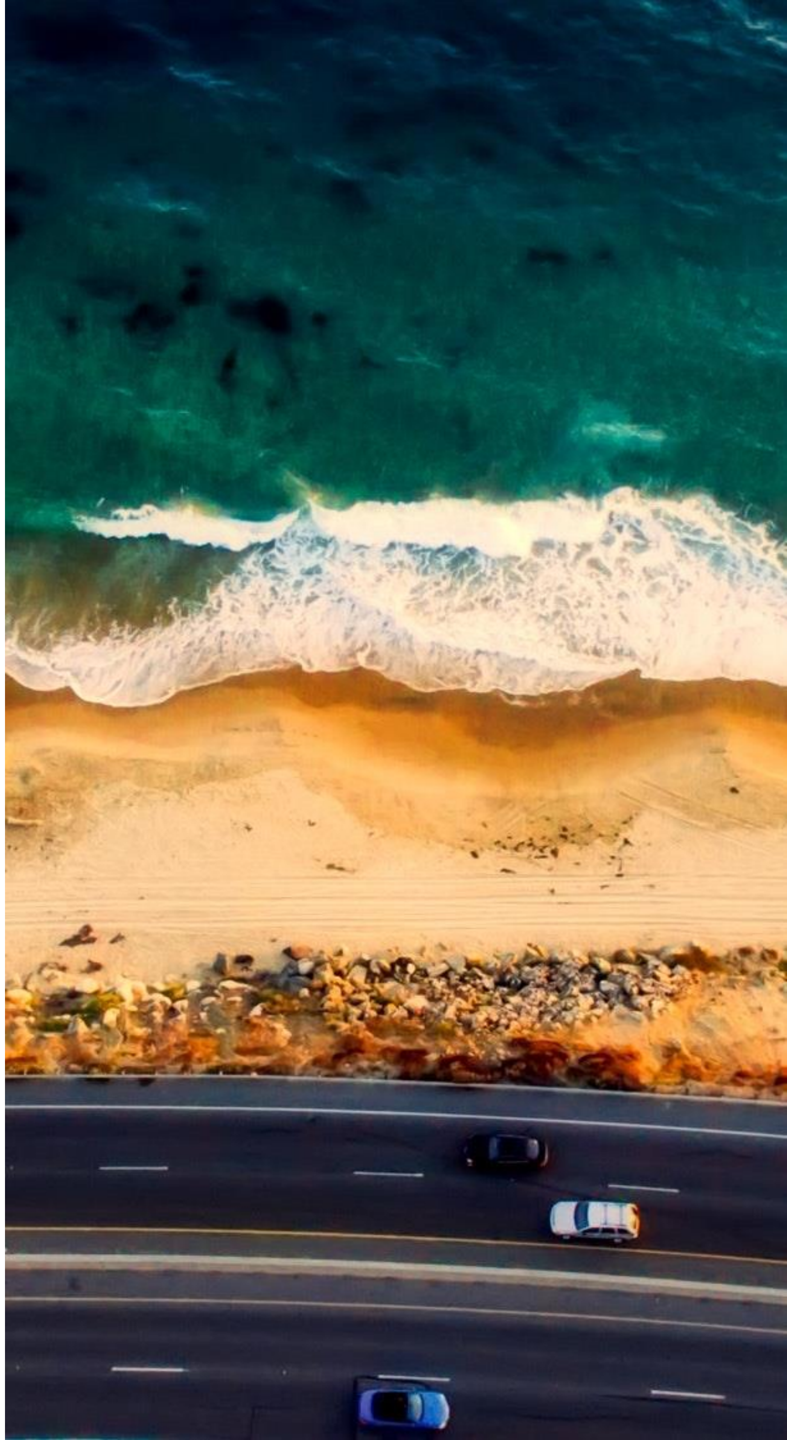
How will TLS work with multiple V2G PKIs in -2?

Recognize available V2G Roots

- Multiple V2G Roots in market (cross-recognition)
- Auto OEMs should trust available V2G PKIs & install all available V2G Roots
- EVSE installs EVSE leaf certificate from one of the available PKIs

Benefits

- Requires multiple V2G Root certificates to be installed in EV -> 800 bytes per Root cert – Common Behavior in the IT industry
- No impact to CPO → CPO chooses EVSE leaf certificate from one of the available V2G PKIs to install in EVSE



Thanks for attending!

AMIT BHONSLE

Head of Product, North America

+1 847 331 6184

amit.bhonsle@hubject.com

STEFFEN RHINOW

Director of Plug&Charge

+49 172 9563362

steffen.rhinow@hubject.com

B) Handling TLS with Mutli-V2G Root PKIs - Exception in Handling Use Case #1

If the EV sends a contract certificate that is either expired, revoked or unknown and now required to send a different certificate. How should this transition be handled?

Does this require the TLS session to abort and restart?

What are the solutions?

B) Handling TLS with Mutli-V2G Root PKIs - Exception in Handling #1

Does the interruption in the TLS handshake introduce the possibility of cyber threat?

Polling from the Audience #3

Are there issues with establishing TLS that have not been solved?

Describe the issue

Polling from the Audience #4

C) What are some other immediate solutions that can to be deployed within the next 12mos

Should the industry explore solutions outside of ISO-15118?

Determining a Path for North America

Framework for Determining PKI Governance and Rules in North America

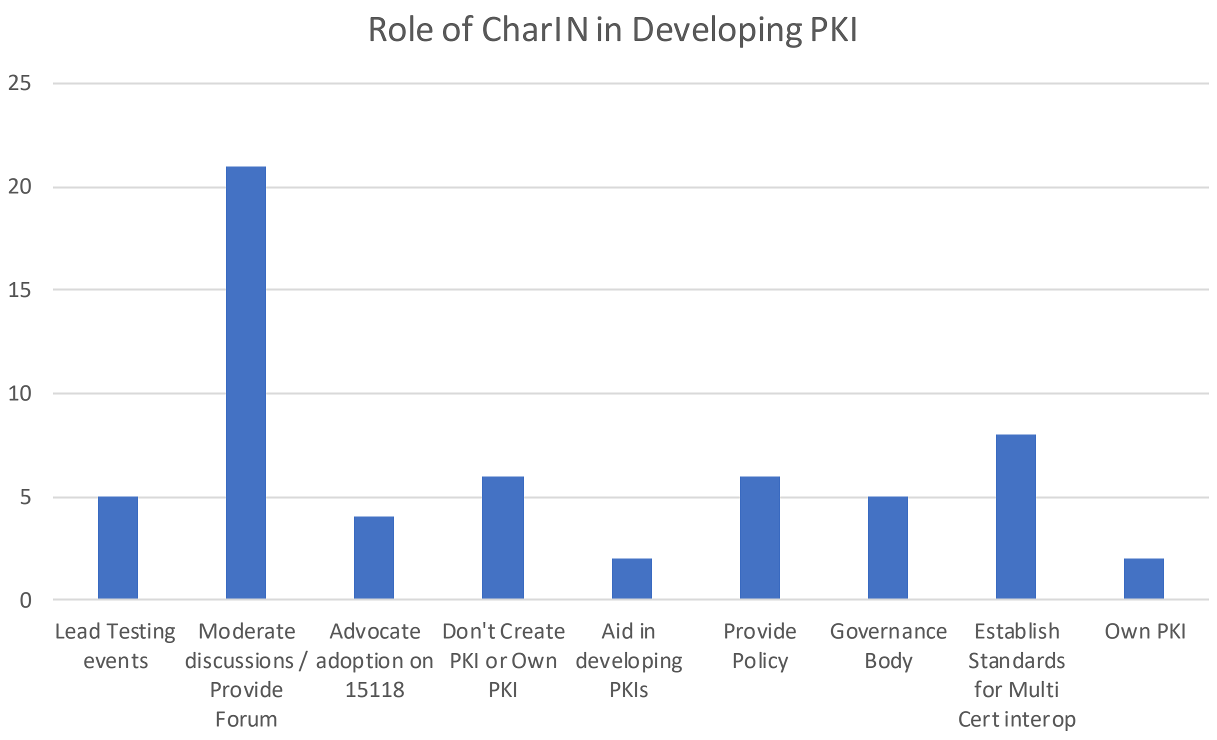
A) CharIN’s process for commonly developing PKI governance and Market guidelines in NA.

B) Agree upon appropriate forum going forward for determining governance and market guidelines

CharIN’s Proposal and Roadmap

A case for CharIN NA

Feedback from Last Workshop

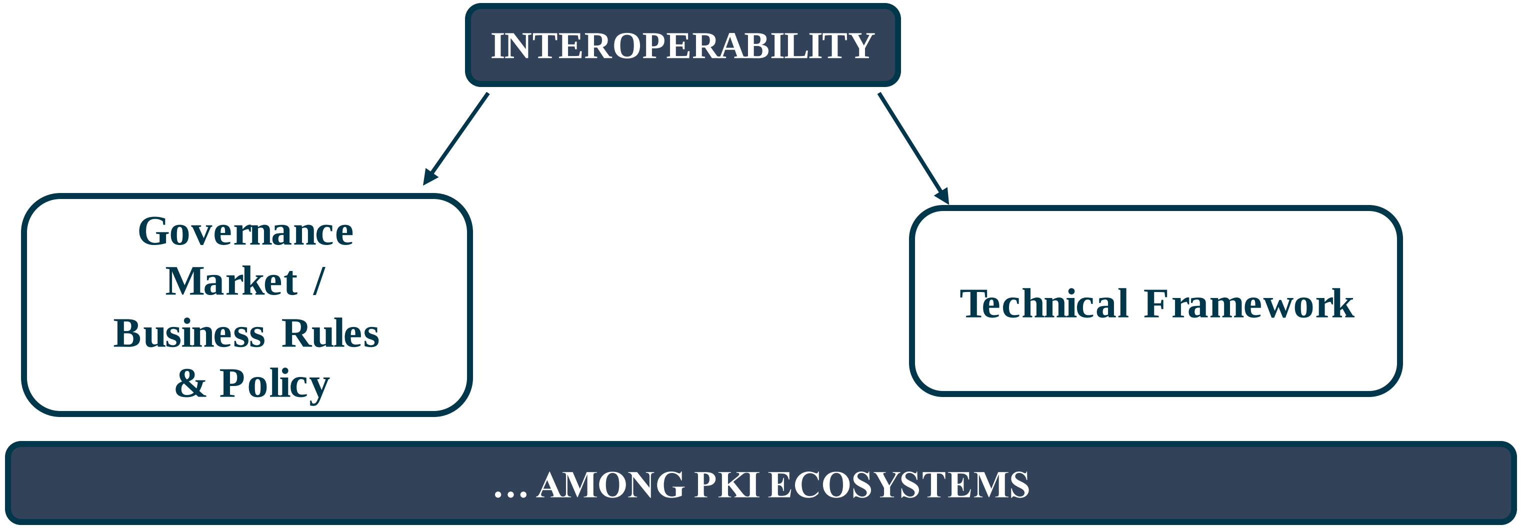


- Workshop participants were to provide comments on the role CharIN should play in developing PKI
- 59 comments were received and tabulated as shown in graphical form.
- A majority of participants wanted CharIN to Moderate Discussion, convene a forum and help establish standards for Multi Certificate interoperability.
- There was little support for CharIN establishing its own PKI

Why is CharIN uniquely suited to resolve the PKI conundrum?

- Committee to providing EV drivers with a seamless & interoperable charging experience
- CharIN, an inclusive, industrywide coalition represents over 300 leading e-mobility stakeholders
- Supports global standards and defines the requirements based on inputs from its members
- Convener of Focus Groups bringing industry participants together to develop the best solution for the customer

CharIN's Proposal and Roadmap



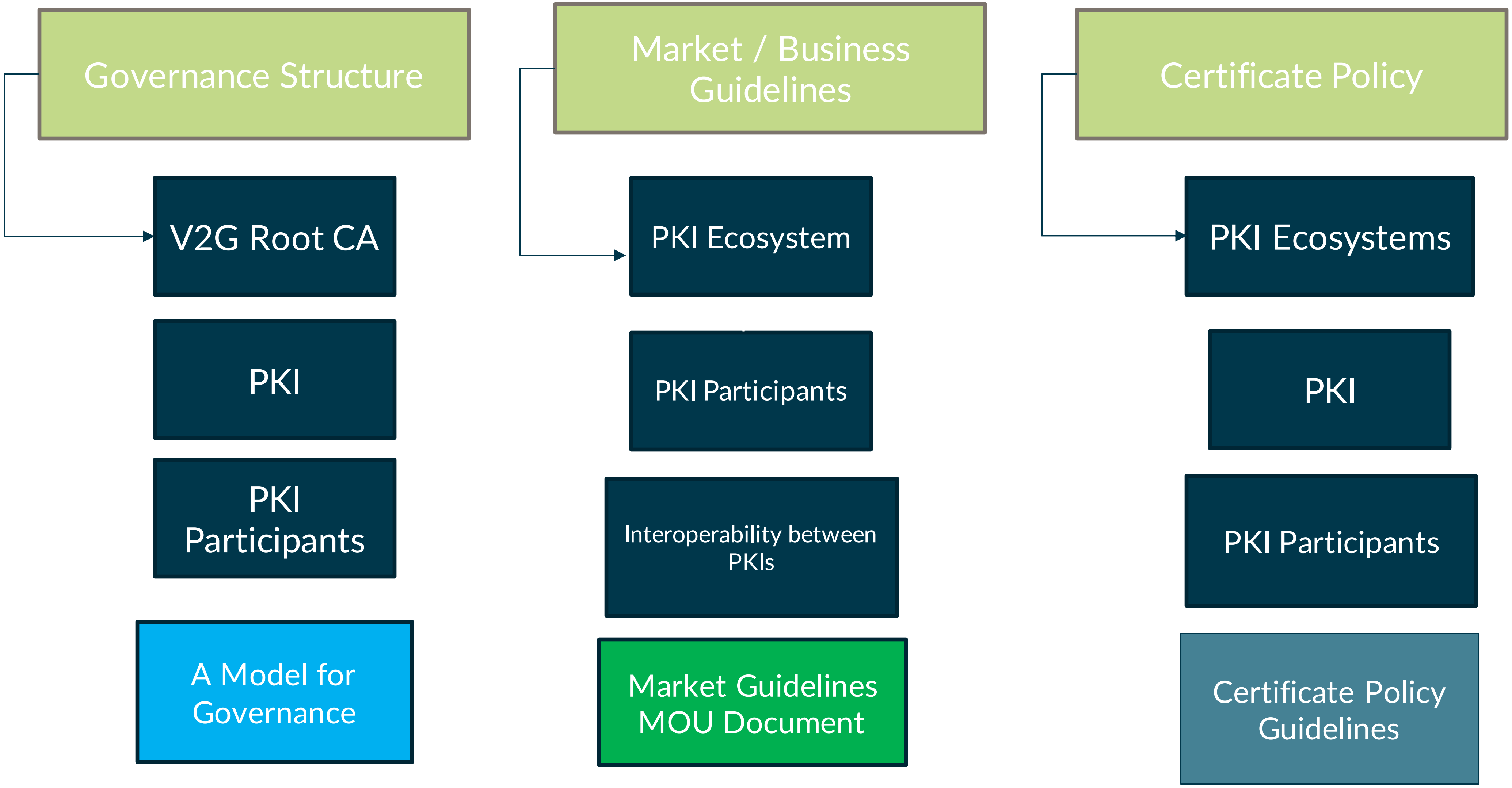
Convene a series of Focus Group discussions with industry stakeholders to develop:

1. A comprehensive operational document to serve as a blueprint for B2B engagements.

2. Agreement on Technical solutions for multi-PKI Ecosystems handling leading to standardization

Long Term Solutions for PKI Interoperability & Governance

Determining a Path for North America



Governance Structure

V2G Root CA

PKI

PKI Participants

A Model for Governance

Market / Business Guidelines

PKI Ecosystem

PKI Participants

Interoperability between PKIs

Market Guidelines MOU Document

Certificate Policy

PKI Ecosystems

PKI

PKI Participants

Certificate Policy Guidelines

Determining a Path for North America

Framework for Determining PKI Governance and Rules in North America

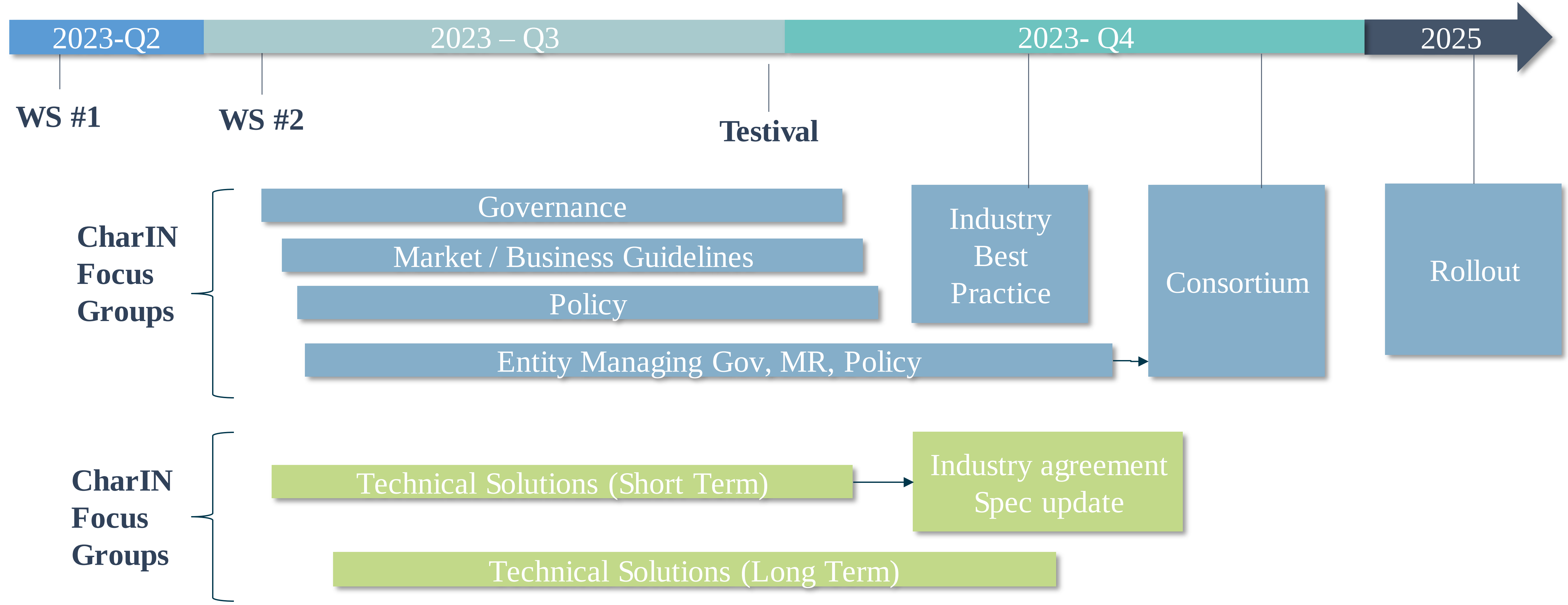
CHARIN

PKI Interoperability: Technical Aspect

Cross Recognition	Cross Certification	Certificate Trust List	Other
Cert Pool needed. - 2/-20 confirmed	Cross Cert Pool & CRL for revoking -2/-20 confirmed	CTL Manager Value Added Service in 15118	Technical Solutions – 2 /-20
V2G Root CAs --> EV, EVSE	Cross Certs in EVSE 1 in EV during Cert Install and TLS init	V2G Root CAs from CTL --> EV, EVSE	V2G Root CA handling
Interop via EV installing CC & TLS setup --> EVSE validating CC	InterOP via EVSE/PnC Ecosystem --> Bi-Lateral Trust	InterOP via Trust List Manager, establishes Trust for PKI	Technical Requirements

Establish Technical Framework for updates need to support NA Market

Timing plan


2023-Q2
2023 – Q3
2023- Q4
2025
WS #1
WS #2
Testival
CharIN Focus Groups
Governance
Market / Business Guidelines
Policy
Entity Managing Gov, MR, Policy
Industry Best Practice
Consortium
Rollout
CharIN Focus Groups
Technical Solutions (Short Term)
Industry agreement Spec update
Technical Solutions (Long Term)

CharIN's Proposal and Roadmap

Discussions / Comments ?

Enter comments in Menti - #5

Determining a Path for North America

Framework for Determining PKI Governance and Rules in North America

A) CharIN’s roadmap for process for developing PKI governance and Market rules in NA.

B) Agree upon appropriate forum going forward for determining PnC/ecosystem governance and market rules

Polling from the Audience #6 & #7

Do you agree with CHarIN- NA leading the development of NA PKI Governance, Market Guidelines and Policy?

Yes – Explain your Rationale

No – Explain your rationale

Abstain - Comment

Polling from the Audience # 8

If not CharIN, what organization or entity should lead the PKI effort?

Polling from the Audience #9

Which Focus Group/s would you be willing to join and support actively?

Determining a Path for North America

Long term Solutions

Discussion: Longer term solutions for PKI interoperability and governance:

This discussion will be transferred to the above forum when that forum is established.

Determining a Path for North America

Long term Solutions

Discussion: Developing a framework for PKI (V2G Root) Governance in NA

Longer term solutions for PKI interoperability and governance
Developing a framework for PKI (V2G Root) Governance in NA

Why is PKI Governance Needed

- To maintain freedom of choice and open market for all participants including the consumer.
- Independent governance of the market rules would benefit the acceptance of these rules and will help with dispute resolution
- Independent governance is needed regardless of the number of PKIs in the market, the owners/operators of the PKI or interoperability mechanisms.

Role of properly established Governance

- Guarantee interoperability for consumers
- Monitor PKIs and the fair, reasonable and non-discriminatory access to a PKI
- Monitor the terms, fees charged, and Quality of Service Level (response times, availability)
- Monitor the Independent Quality Auditors Act as an intermediary in case of conflict
- Organize the acceptance of new V2G Root Cas Set and / or Monitor the Quality rules V2G Root CAs and Sub CAs should adhere to
- Monitor the Cross Certification process and the fair, reasonable and non-discriminatory access to Cross Certification
- Monitor the Certificate Trust List Manager and the fair, reasonable and non-discriminatory access to a Certificate Trust List

Polling from the Audience #10

What potential/additional roles of Governance are you expecting?

Conclusion
& Next Steps

Jacob Mathews
Technical Advisor, CharIN

Thank you for your kind attention!

Any questions?

Contact

Phone (202) 886-3842
E-Mail northamerica@charin.global

www.charin.global

@CharIN e.V.