Charging Network Cybersecurity:
status quo and arising challenges

Craig Rodine

Director, Standards
Member, IEC TC69 (USTAG, USNC)
Voting Member, SAE Hybrid & EV Technical Committee

Outline

- Introduction, perspective
- A secure *bespoke* EV charging network (EVCN)
- Developing *standards-based* EVCN cybersecurity
- New IEC TC69 Cybersecurity WG
- Call for US-German collaboration

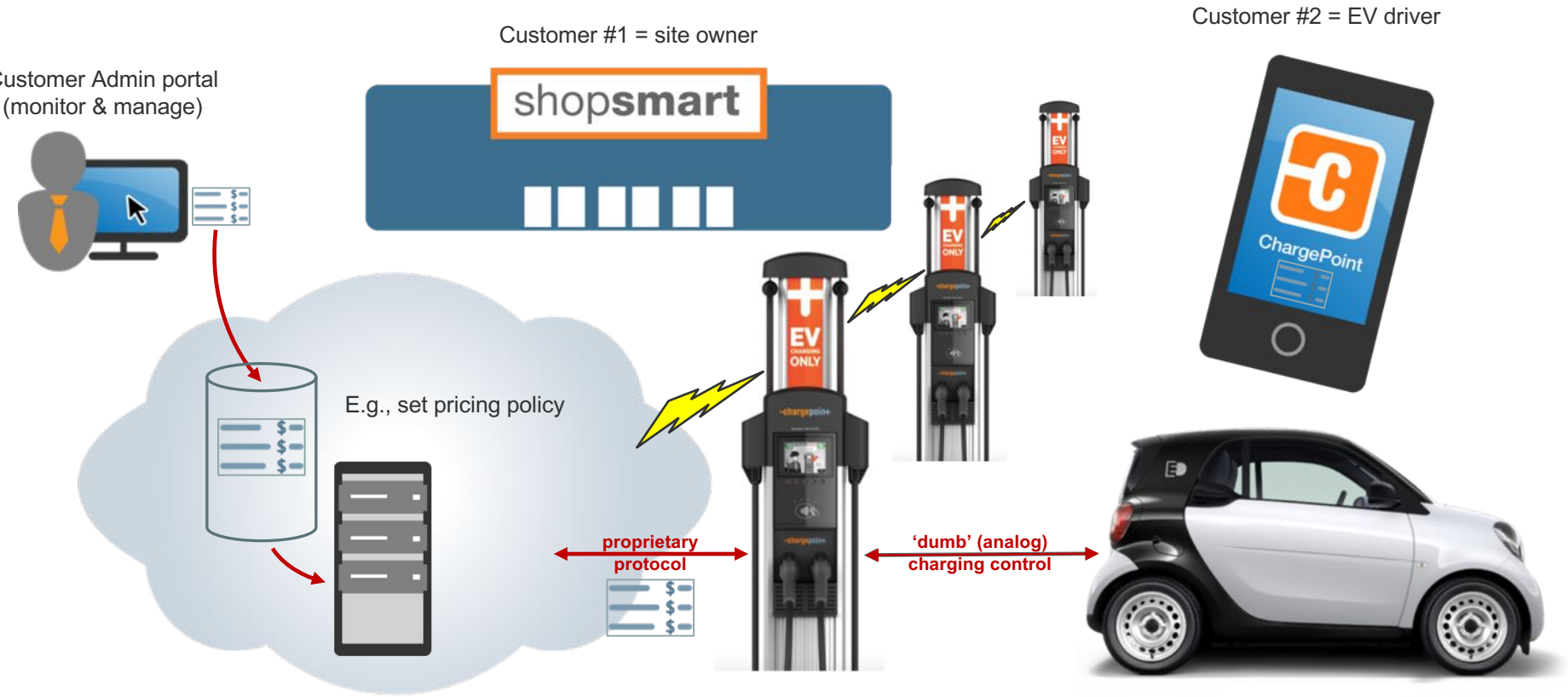
Introduction

- Bespoke: designed from the ground up
  - Built in commercial-grade cybersecurity from the start
  - Enjoyed complete control (technology selection, development schedule, customer experience, business model, etc.)
  - Benefited from learning/refinement feedback loop
- Standards-based: establish critical foundations
  - Champion cybersecurity as EV charging becomes software-intensive
    - Graft functional requirements onto quality cybersecurity rootstock
  - Should result in more safe, sound, and trustworthy EV charging
  - Should facilitate regional market growth and worldwide alignment

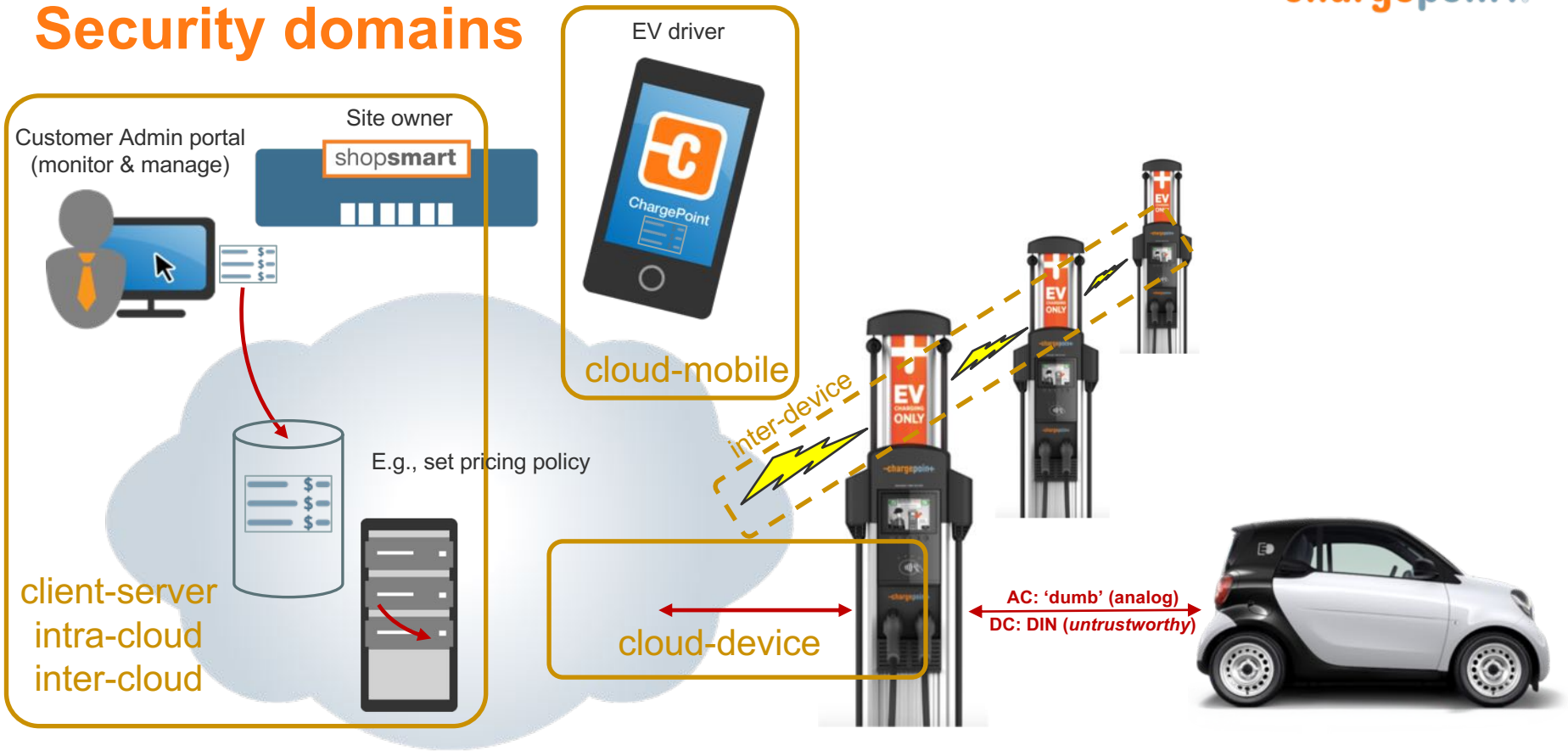
Perspective on cybersecurity

- Goal: standards to bolster system-wide IT *trust*
  - Beyond ‘mere’ device safety and performance
  - Fundamentally a *social* construct and process
- Assumed ground rules for EVCN cybersecurity standards
    - Orchestrate work among domain and security experts
    - Practice outreach, transparency and inclusiveness
    - Re-use intelligently, don’t ‘innovate’ unnecessarily
    - Judgment is critical, tradeoffs will be required
- In operation: a set of cybersecurity *practices*
  - Both technical and administrative
  - With critical process feedback loops

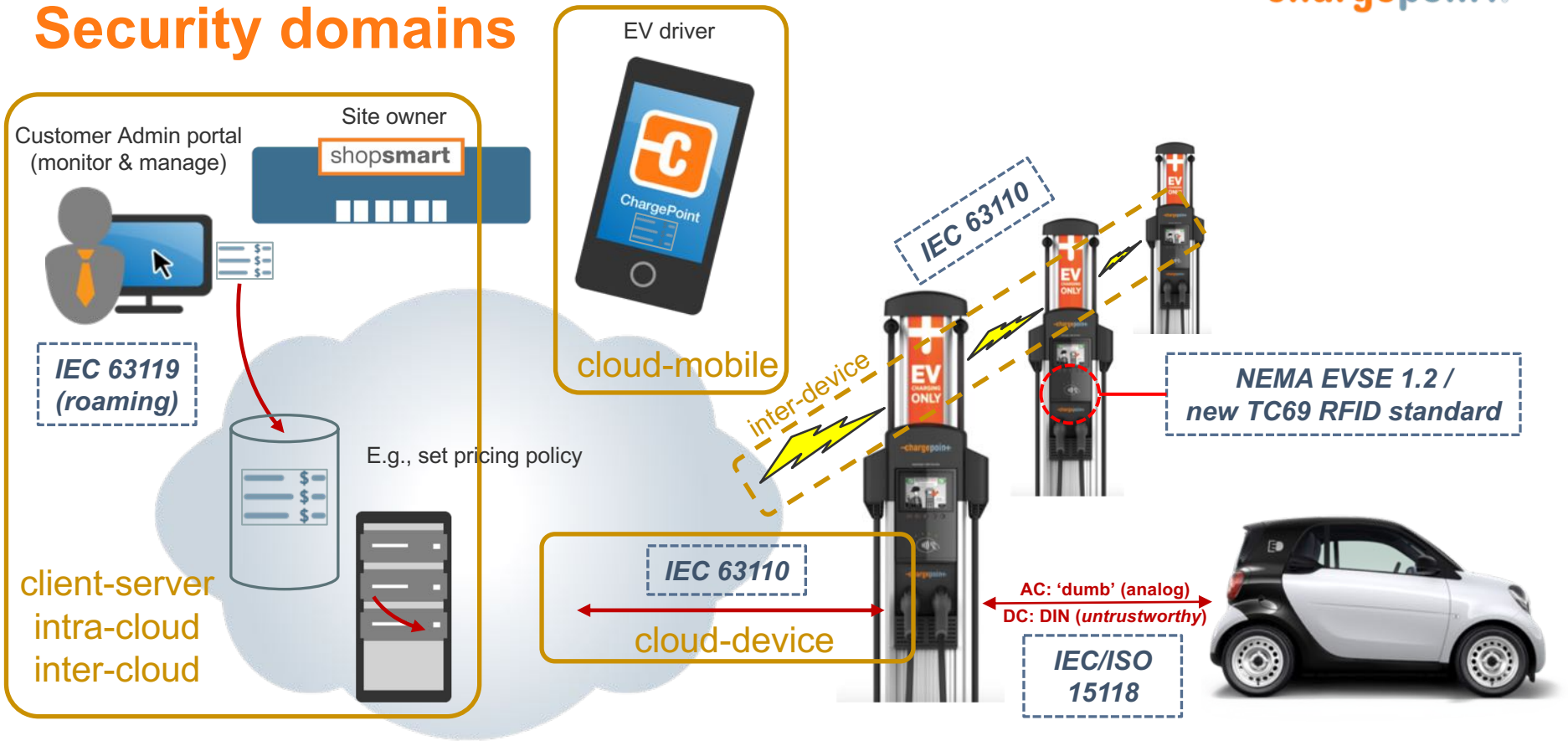
A secure network as designed and deployed



Security domains

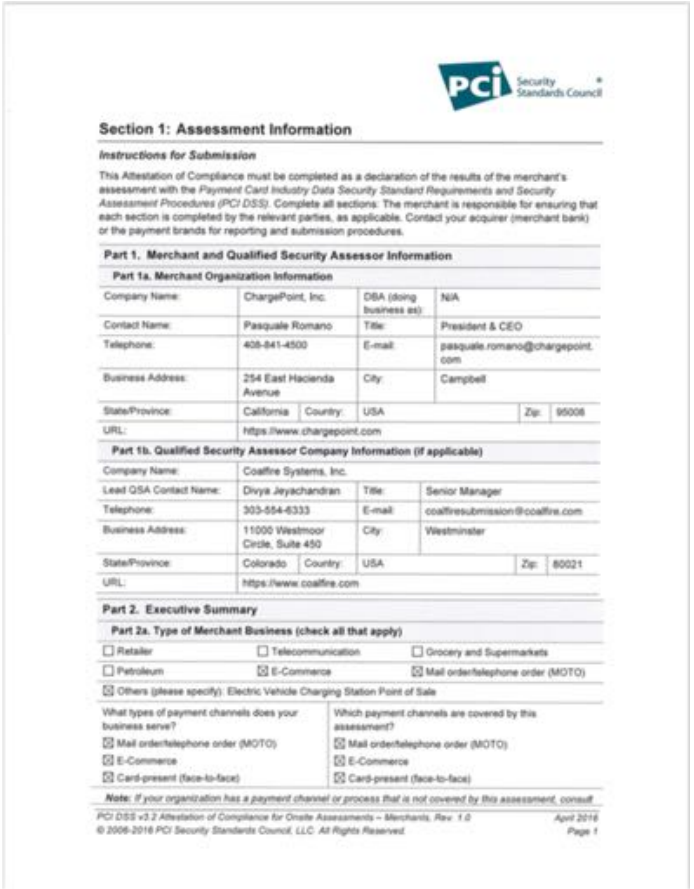


Security domains



Rigorous verification

- PCI DSS 3.2 Certification
  - Comprehensive formal requirements
    - Technical and process
    - Software, hardware, communications, physical integrity, data storage, …
  - Based in banking industry/community
    - Very large scale, demanding sector
    - Regular formal audits (minor versions)
    - Continuous testing and improvements
- Also verified by a major utility
  - Cyber-physical security requirements
  - Third-party penetration testing



PCI Security Standards Council

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the merchant's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact your acquirer (merchant bank) or the payment brands for reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:	ChargePoint, Inc.		DBA (doing business as):	N/A	
Contact Name:	Pasquale Romano		Title:	President & CEO	
Telephone:	408-841-4500		E-mail:	pasquale.romano@chargepoint.com	
Business Address:	254 East Hacienda Avenue		City:	Campbell	
State/Province:	California	Country:	USA	Zip:	95008
URL:	https://www.chargepoint.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Divya Jeyachandran		Title:	Senior Manager	
Telephone:	303-554-6333		E-mail:	coalfiresubmission@coalfire.com	
Business Address:	11000 Westmoor Circle, Suite 450		City:	Westminster	
State/Province:	Colorado	Country:	USA	Zip:	80021
URL:	https://www.coalfire.com				

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

☐ Retailer ☐ Telecommunication ☐ Grocery and Supermarkets
☐ Petroleum ☒ E-Commerce ☒ Mail order/telephone order (MOTO)
☒ Others (please specify): Electric Vehicle Charging Station Point of Sale

What types of payment channels does your business serve?	Which payment channels are covered by this assessment?
☒ Mail order/telephone order (MOTO)	☒ Mail order/telephone order (MOTO)
☒ E-Commerce	☒ E-Commerce
☒ Card-present (face-to-face)	☒ Card-present (face-to-face)

Note: *If your organization has a payment channel or process that is not covered by this assessment, consult*

PCI DSS v3.2 Attestation of Compliance for Onsite Assessments – Merchants, Rev. 1.0 *April 2016*
© 2006-2016 PCI Security Standards Council, LLC. All Rights Reserved. *Page 1*

AAA using open-standard RFID

- Includes higher-security RFID access
- Built on trusted ISO standards
  - Open standard: NEMA EVSE 1.2
  - Granular, strong challenge-response
  - Identifies each transaction (swipe)
  - “Leading edge” of end-to-end AAA
- Engineered for cost-benefit balance
  - Within a broad range of possible solutions
- Also accepts contactless credit cards
  - Banks, CCs moved to chip&pin, chip&sign
- Could also support NFC payment
  - Apple Pay, Google Wallet, Samsung Pay

NEMA EVSE-1.2 Secure RFID standard

General design goals and features

- Provide a state-of-the-art secure RFID standard for EV charging
- Agnostic as to EV charging network protocol and business model
  - Supports subscription-based (pre- or post-paid), aggregated term-based, tiered and discounted usage rate plans; pay-per-use, anonymous (e.g. gift card) or attributed (account-based) transactions, etc.
- Focuses on authentication, doesn't constrain authorization logic
- Provides fine-grain accounting of authentication transactions
- Agnostic as to peer-to-peer or clearinghouse-based roaming models

NEMA EVSE-1.2 Secure RFID standard

High-level description and experience to date

+ An EV-charging-domain-specific application protocol built on widely implemented, strongly proven RFID standards
  - ISO 14443-2/3/4 and ISO 7816-4/5/8
  - These ISO standards are used worldwide for access control
    - In corporations and high-security government agencies
    - In the passports of more than 85 countries
+ Can be implemented in smartcards, tags, and smartphones
+ Now deployed in tens of thousands of tags and charging stations (NA)
+ Has secured tens of millions of charging sessions without known breach
+ Is designed specifically to support e-mobility
  - EV charging roaming aka “network interoperability”

NEMA EVSE-1.2 Secure RFID standard

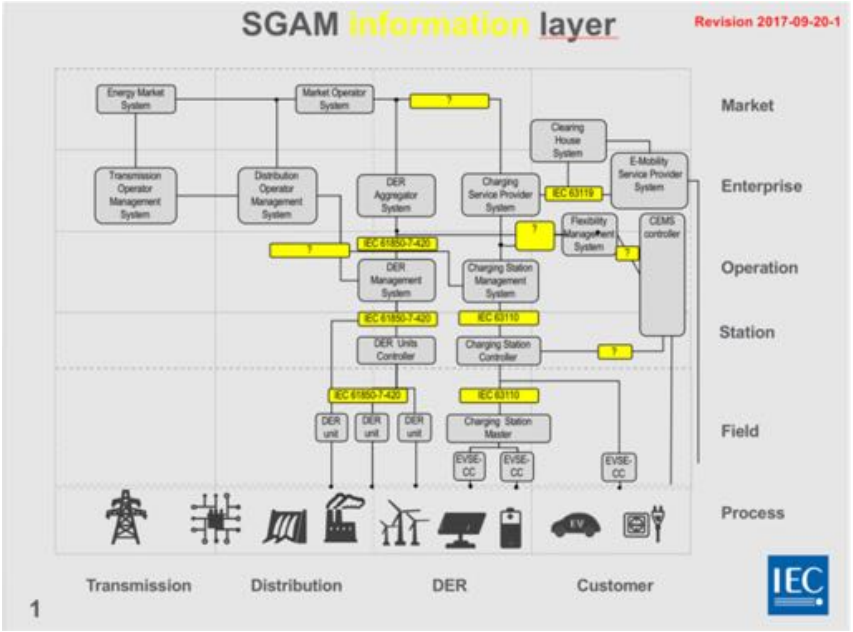
Technical design goals and features

+ Robust against credential compromise
  - ISO 14443 designed to make cloning and penetration very difficult
  - Counters brute-force, microscopy, power analysis, other types of attack
+ Robust against man-in-the-middle and replay attacks
  - Encodes time and location of each authentication attempt (card swipe)
  - Provides sufficient data to tie authentication to overall transaction
  - Credential can include transaction counter (must sustain >10K x)
+ Allows issuer a choice of cryptographic algorithms and materials
  - To meet security requirements and address cost/implementation tradeoffs
    - To be cost-effective, credentials should use commercial off-the-shelf devices
  - Symmetric and asymmetric cryptosystems are supported
+ High security without exposing secrets to visited networks
  - Strikes a balance between cooperation and competition among EMSPs
  - Isolates compromises to a single network, they don’t propagate

Continuing the work of PT62831

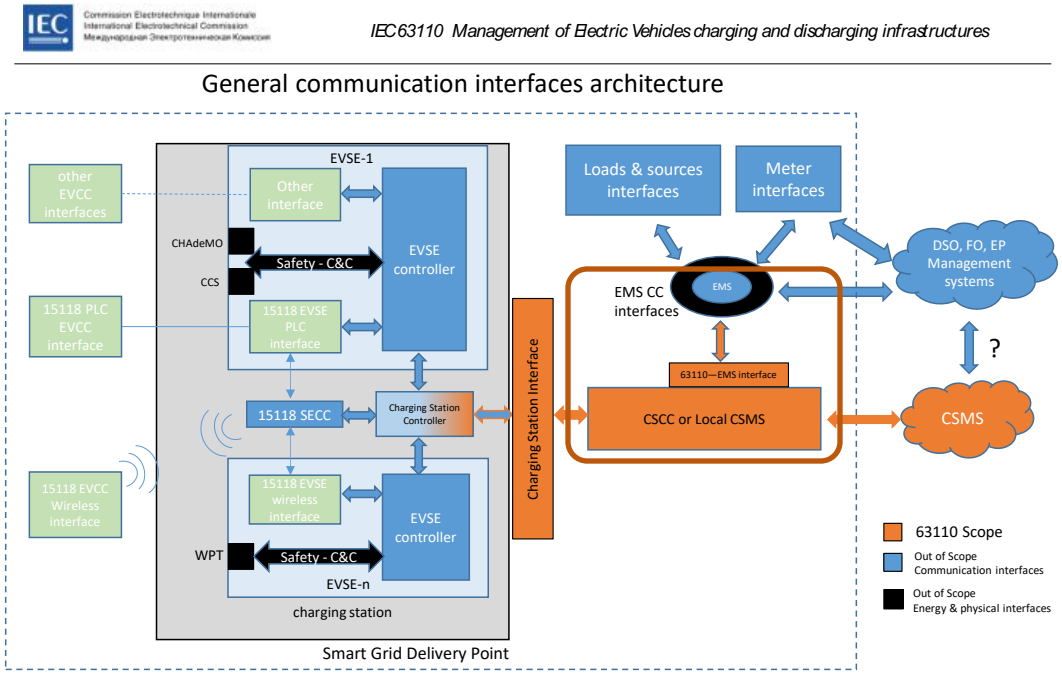
- PT62831 is the TC69 RFID standard effort
  - Started, stalled, will now time out
- Reviewed US (NEMA) RFID standard
  - Gained in-principle support of experts
  - No other candidates were proposed
- Looked at accommodating 15118 Certificates
  - Would allow EIM (RFID) for same contract as Plug-and-Charge (PnC)
  - Would need to be tested (payload size, interaction speed, etc.)
- The need for a secure RFID standard remains, has actually grown
  - Recent 15118 Ed2 realization: EIM has some strong advantages over PnC
  - US experience: first industry standard, aggressive deployment, strong proof point
  - German community: recently launched a separate national effort
- We should nourish and coordinate these developments in TC69
  - See recent TC69 structure, end of this presentation

A brief look at IEC TC69 efforts



+ Address levels above charging station
  - IEC 63110: could-station standard
    - To enable multi-vendor networks
    - Strong emphasis on energy mgmt
    - Concerned with site-level integration
      - This is new, leaning towards IoT
  - IEC 63119: cloud-cloud standard
    - To support internetwork roaming
    - Peer-peer or clearinghouse
+ Each includes a security TF or focus
  - Analysis and requirements
  - But no coordinated end-to-end analysis!
+ Proposal: form TC-level System Security WG

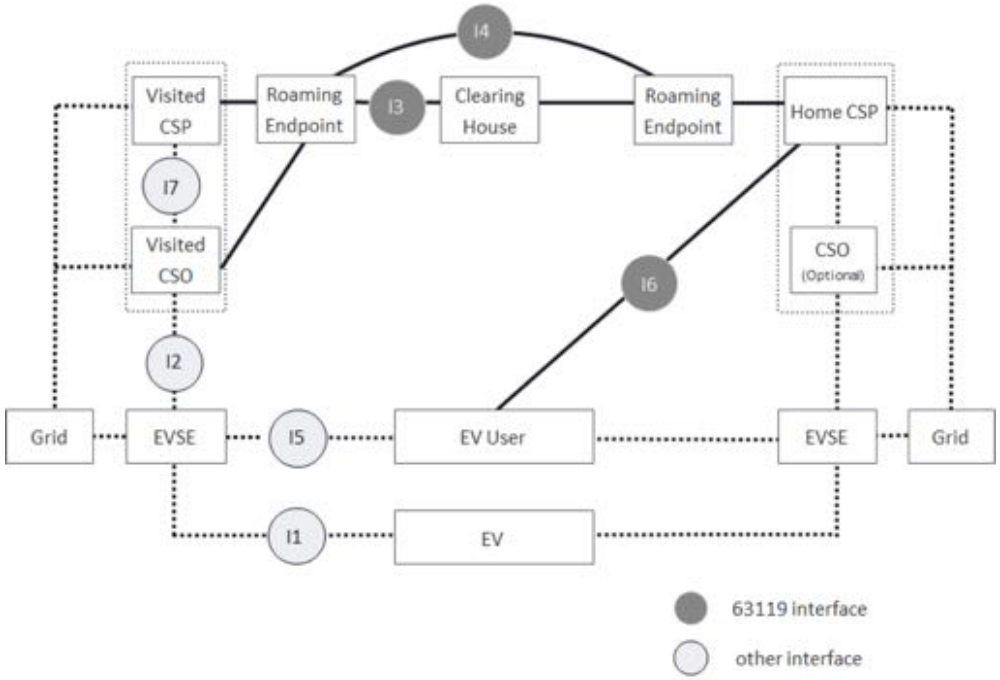
Draft IEC 63110



Principle of the diagram: Two Communication Controllers talk together through Communication Interfaces (last update 07/21/2017)

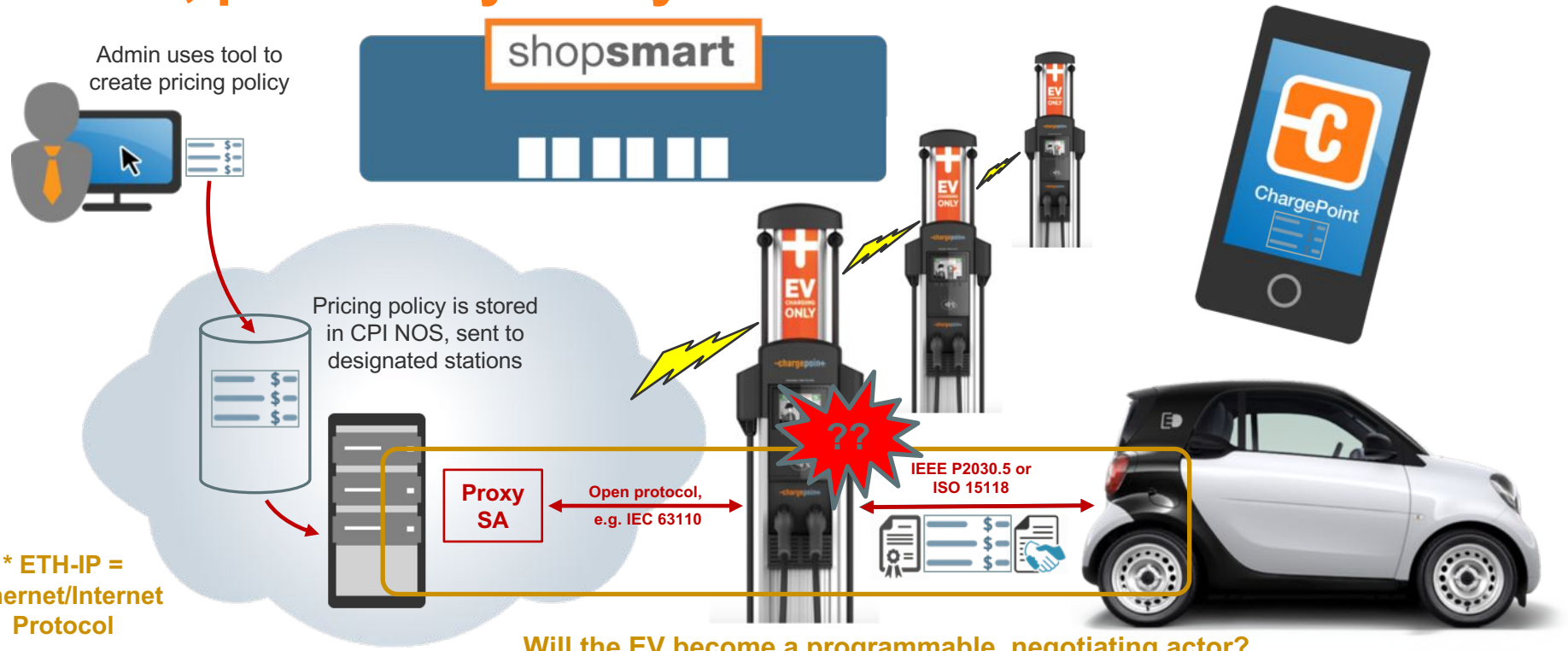
- Discrete JWG11 Security Task Force
  - Goals, participation, and process are well defined
  - Based on ISO/IEC 27005 (2011, new edition under development)
    - References ISO/IEC 27001, 27002
  - Initial step: risk analysis
- Upstream and downstream requirements being discovered
  - Federation of security domains?
  - Management of crypto materials?
  - Data at rest? in device and cloud?
- Includes a local “CSMS” entity and communications interface
  - For site-based load management
  - The first “sideways” requirements

Draft IEC 63119



- Well started with system architecture (Part 1)
  - Architecture and framework of multiple parts
  - Use cases, requirements (messages), conformance
- 63110-1 now going to CDV
- Reviewing existing roaming schemes
  - Available specs: NEMA, OCHP, OCPI, …
- Cybersecurity treatment (in Part 2)
  - NP submitted, approval expected Summer 2018
- Anticipated cybersecurity framework:
  - Extensible “plug-in” authentication (I5)
    - allowing RFID, secure QR codes, NFC, etc.
  - Cloud-cloud (I3) requirements and standards
    - Need to choose best fit among candidates
  - Mobile-cloud (I6) requirements and standards
    - Need to choose best fit among candidates

ETH-IP* (PEV-EVSE) interface introduces a new, potentially nasty attack surface.



New functionality in IEC/ISO 15118 Ed2

Note: IEEE P2030.5 enables/envisions similar complexity

+ Wireless Power Transfer
  - Including Wi-Fi communications
  - For ‘supporting services’ *and* charging control – all modes (!)
+ Expanded Energy Management functionality
  - Scheduled Mode and Dynamic Mode
  - Target-setting for optimization, support for Grid Codes
+ Bi-Directional Power Transfer
  - Including fast ‘open-loop’ charging control (e.g. for freq reg)
  - A novel energy source with its own requirements
+ Absolute pricing {$, €, ¥, £, ₩, ฿, ₽, ₱, …}
  - Required for legal metrology (public-access charging)
  - Brings pricing details ‘in-band’ per established practice (NA)

IEC/ISO 15118 security design

Source		Destination		Protocol	Port	Action
IP Address	Interface	IP Address	Interface			
all	untrusted	all	trusted	UDP	15118	allow
all	untrusted	all	trusted	TCP	V2G_DST_TCP_DATA	allow
all	trusted	all	untrusted	all		allow
all	trusted	all	trusted	all		allow
all	untrusted	all	untrusted	all		deny
all	all	all	all	all		deny

Source		Destination		Protocol	Interface		Action
IP Address	Port	IP Address	Port		Inbound	Outbound	
all	EVCC Port (dynamic range)	ff02::01	15118	UDP	untrusted	trusted	allow
all	EVCC Port (dynamic range)	SECC IP Address	SECC Port (V2G_DST_TCP_DATA)	TCP	untrusted	trusted	allow
all	EVCC Port (dynamic range)	SECC IP Address	1080	TCP	untrusted	trusted	allow
SDP Server IP Address	15118	EVCC IP Address	EVCC Port	UDP	trusted	untrusted	allow
SECC IP Address	SECC Port (V2G_DST_TCP_DATA)	EVCC IP Address	EVCC Port	TCP	trusted	untrusted	allow
SECC IP Address	1080	EVCC IP Address	EVCC Port	TCP	trusted	untrusted	allow
all	all	all	all	all	trusted	trusted	allow
all	all	all	all	all	all	all	deny

Table 4 – Firewall action for wireless communication

Missing: an independent, comprehensive, publicly available security analysis.

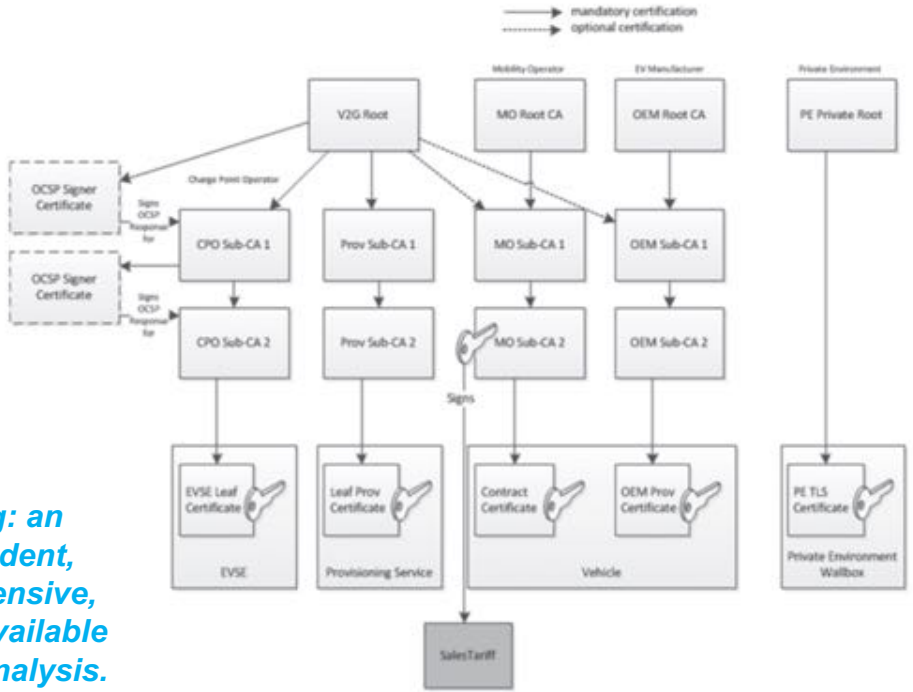
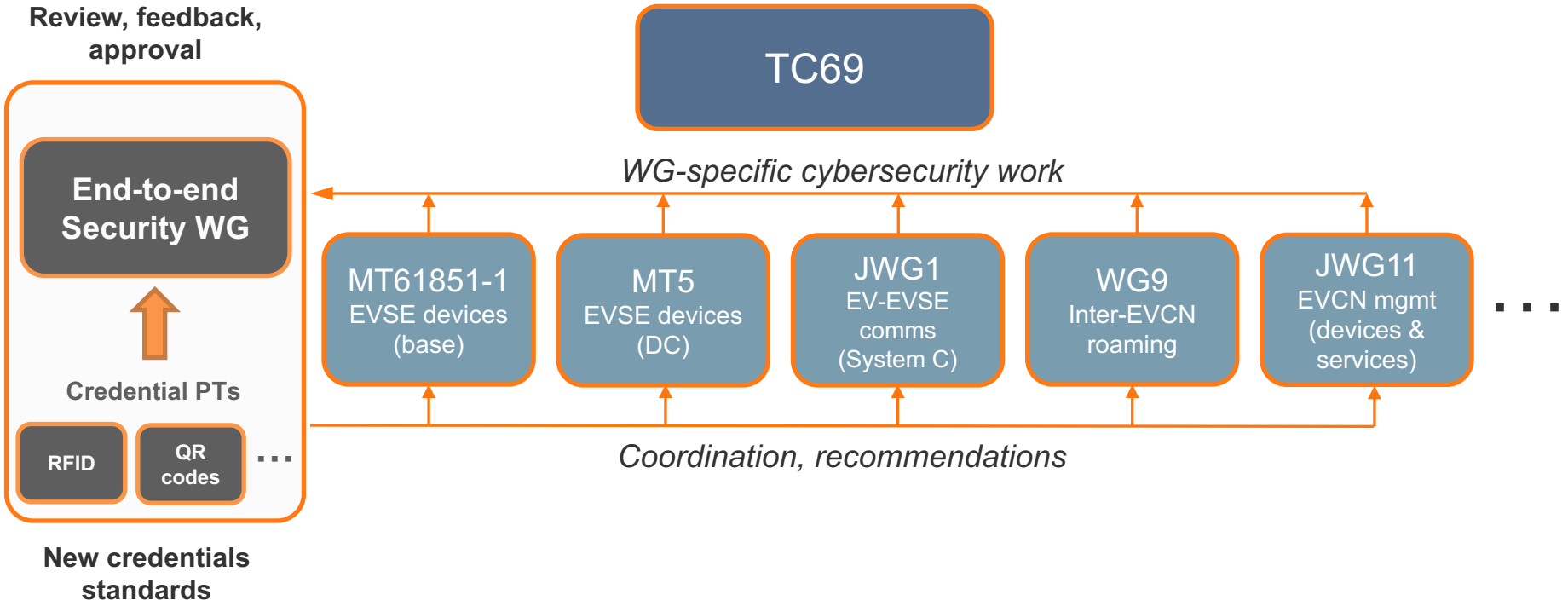


Figure E.1 — Overview certificate structure

Proposal: TC69-level Cybersecurity WG

- No existing WG covers end-to-end cybersecurity
  - To coordinate security between/across WGs
- No existing WG examines cybersecurity of PEV-charging system interface
  - TC69 standards cover CHAdeMO, GB/T, and CCS (safety, design, comms)
  - Cybersecurity is not addressed, is not in scope
- Need to assume and complete PT62831 plan and work
  - Issue a new, separate NP?
- Need to liaise with other IT security efforts and experts
  - Specifically, ISO/IEC JTC 1/SC 27
  - Also with other pertinent efforts (e.g. in US SAE)
- Need to understand and apply/re-use relevant existing standards, for example:
  - ISO/IEC 27000 series (information security risk analysis)
  - ISO/IEC 15408 series? (information security evaluation)
  - NIST SP 800-53 series (security and privacy controls)
  - ISO/IEC 29147 & 30111 (vulnerability disclosure & management)
- Need to liaise with auto industry efforts
  - See above re: new functionality in IEC/ISO 15118 Edition 2 and IEEE P2030.5
  - To protect dis/charging within PEV security architecture

TC69 Structure



IEC TC69 cybersecurity WG: status

- Decision to create a PWI for End-to-End Cybersecurity WG
  - Approved in TC69 Plenary, 6 April 2018
  - CN and US NCs will submit joint NP for the WG
  - All NCs will be able to submit NPs for credentials PTs
    - CN intends to lead on secure QR Codes
    - US intends to lead or co-lead on secure RFID
- Timeframe
  - April-May 2018: NP draft development
  - June-August 2018: NP our for NC votes
  - September 2018: launch the WG
  - Oct-Dec 2018: submit NPs for credential PTs

Summary: call for US-German cooperation on EV Charging Network cybersecurity

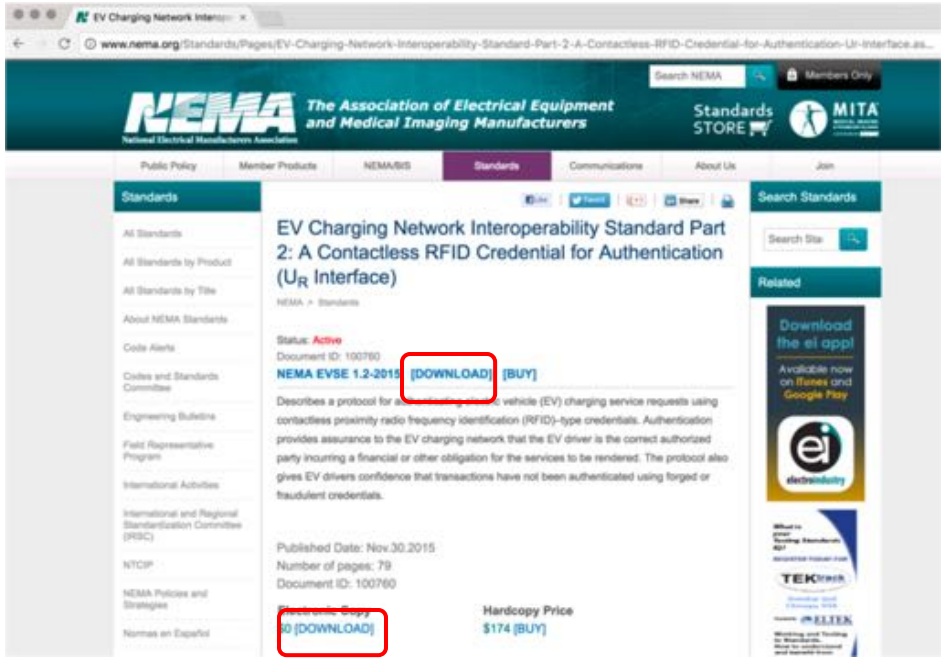
- Support creation of IEC TC69-level cybersecurity WG
  - USTAG available for consultation with German Mirror Committee and NC
    - E.g. share NP drafts and incorporate DE feedback prior to publication
    - This should lead to both NCs voting to approve the NP (Jun-Aug 2018)
    - Sustained DE and US leadership and participation in the WG
- Close coordination of/on Secure EVCN RFID standards
  - Provide USTAG with visibility into DKE/AK 353.0.8 work
  - Consider (co-)leading an RFID Credential PT within TC69
- Joint work on IEC/ISO 15118 cybersecurity review
  - Establish terms and references for risk analysis and mitigation
  - Perhaps liaise with SAE Trust Anchors and Authentication TF

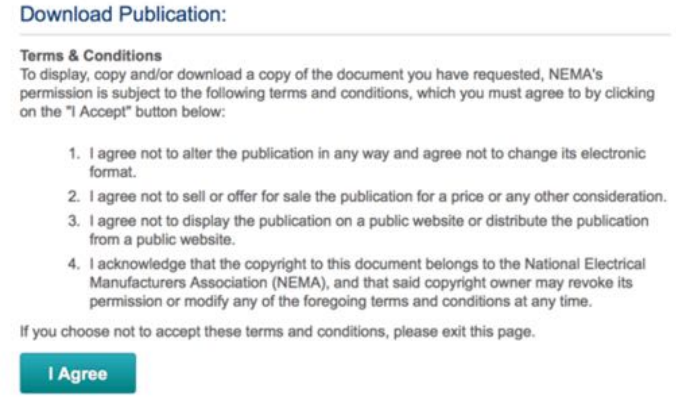
Thank You

For further information on this topic,
please contact Craig Rodine:
craig.rodine@chargepoint.com
+1.408.872-7515

How to obtain the NEMA RFID standard

http://www.nema.org/Standards/Pages/EV-Charging-Network-Interoperability-Standard-Part-2-A-Contactless-RFID-Credential-for-Authentication-Ur-Interface.aspx





System reference model

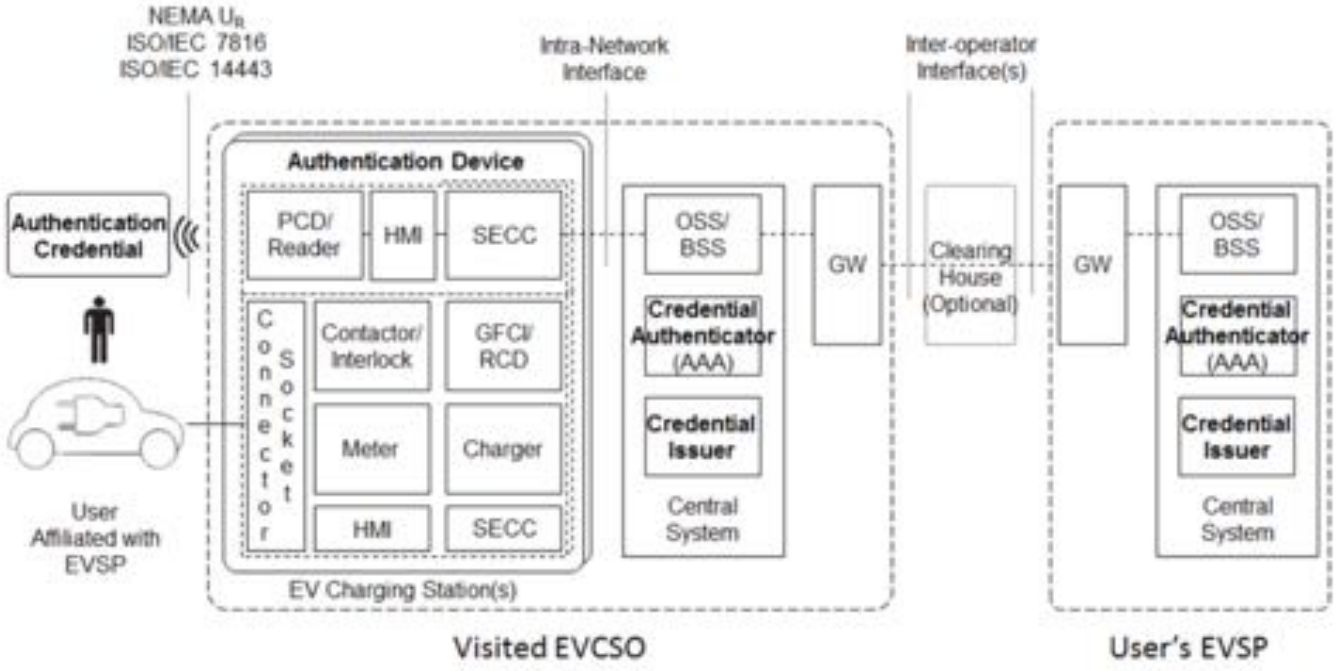


Figure 4-3
System Reference Model (with Integrated Authentication Device)

Domain-appropriate challenge-response

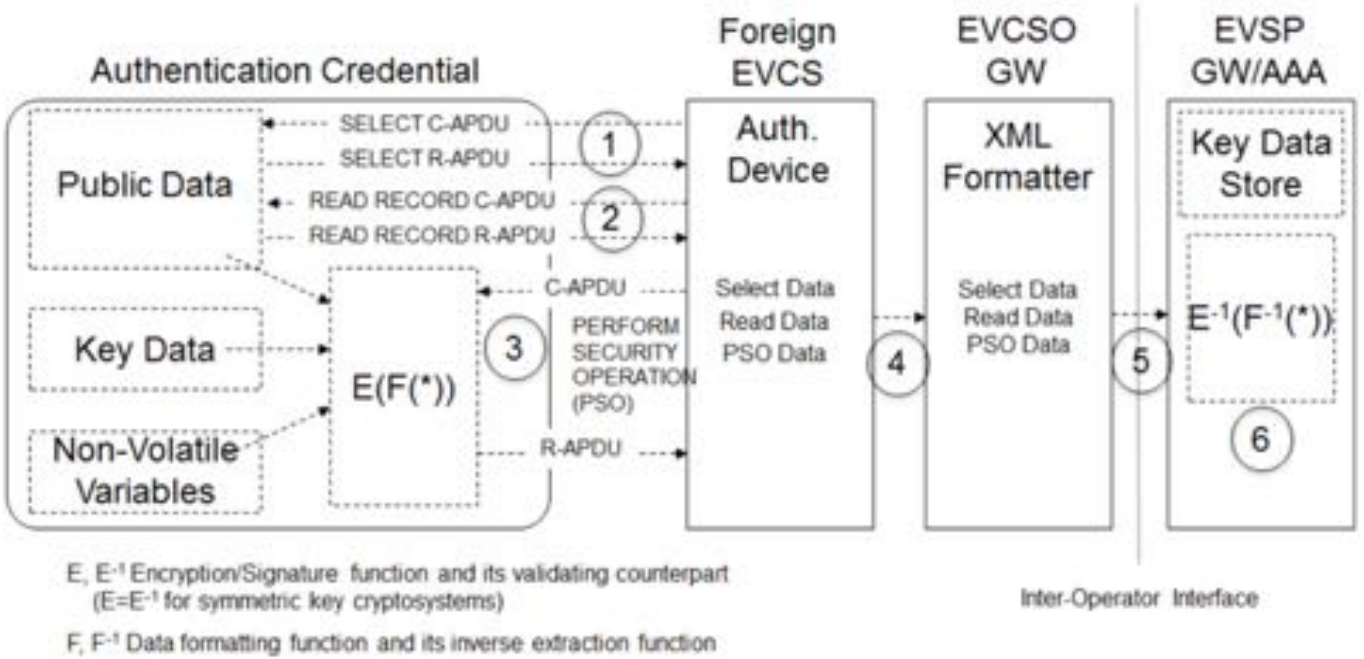


Figure 5-1
Challenge-Response Authentication Process

More details

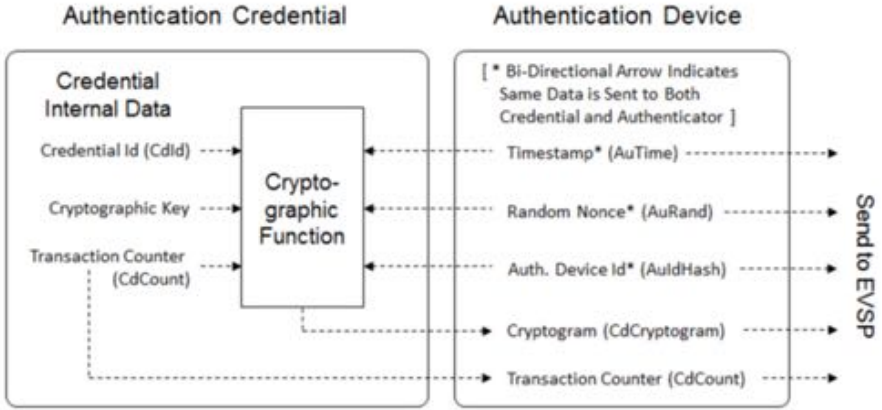


Figure 5-2
Cryptogram Generation Process

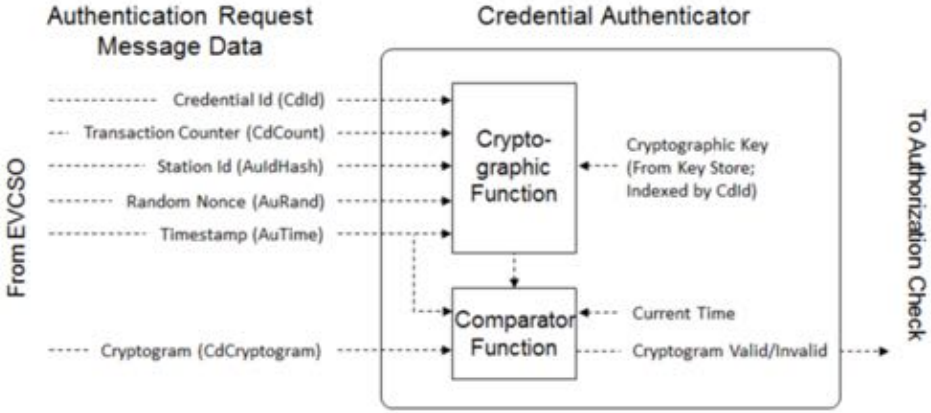


Figure 5-3
Cryptogram Validation Process

Non-secure EV charging networks

- Report in December, 2017 showed flaws in implementation
  - From a neutral research institute, presentation at 34C3
  - RFID UID (= account ID) in the clear, no challenge – easily stolen
  - Cloud-station communication not encrypted, easily intercepted
  - De facto standard control protocol published, available to all
    - Includes ‘reboot station’ and ‘download new firmware’ functions
  - Along with accessible and unprotected USB port …
  - Demo showed a charging station quickly and thoroughly pwned
- Applies to many (most) public charging networks in Europe
- Screaming out for remedies (article in Der Spiegel)
  - This is driving IEC TC69 work on end-to-end security

Is all publicity good publicity?

Sicherheitslücke

Wenn Betrüger an der Elektro-Tankstelle Strom zapfen

Eine Seriennummer genügt - und schon können Betrüger an Ladesäulen für Elektroautos auf fremde Kosten Strom zapfen. Davor warnt ein IT-Experte. Eine Betreiberfirma bestätigte die Sicherheitslücke.