Welcome to Auto-ISAC!

Monthly Virtual Community Call

June 2, 2021

AUTO-ISAC
Automotive Information Sharing and Analysis Center

AGENDA

Time (ET)	Topic
11:00	**Welcome** ➢ Why We're Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities ➢ Heard Around the Community ➢ What's Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker:** ▪ **Tim Weisenberger,** *Project Manager*, **Emerging Technologies at SAE International**
11:45	**Around the Room** ➢ Sharing Around the Virtual Room
11:55	**Closing Remarks**

Welcome - Auto-ISAC Community Call!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ *Stay informed of Auto-ISAC activities*
- ✓ *Share information on key vehicle cybersecurity topics*
- ✓ *Learn about exciting initiatives within the automotive community from our featured speakers*

Participants: Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – *the whole of the automotive industry*

Classification Level: **TLP:GREEN -** May be shared within the Auto-ISAC Community and "off the record"

How to Connect: For further info, questions or to add other POCs to the invite, please contact us! (sharmilakhadka@automotiveisac.com)

Engaging in the Auto-ISAC Community

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC membership
- ❖ If you aren't eligible for membership, connect with us as a Partner
- ❖ Get engaged – *"Cybersecurity is everyone's responsibility!"*

AUTO-ISAC
Automotive Information Sharing and Analysis Center

❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

22 *OEM Members*

21 *Navigator Partners*

❖ Share – *"If you see something, say something!"*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

41 *Supplier & Commercial Vehicle Members*

15 *Innovator Partners*

Membership represents **99%** *of cars and trucks on the road in North America*

Coordination with **26** *critical infrastructure ISACs through the National Council of ISACs (NCI)*

2021 Board of Directors

Executive Committee (ExCom)

Kevin Tierney
Chair of the Board of the Directors
GM

Josh Davis
Vice Chair of the Board of the Directors
Toyota

Jenny Gilger
Secretary of the Board of the Directors
Honda

Tim Geiger
Treasurer of the Board of the Directors
Ford

Todd Lawless
Chair of the Advisory Board
Continental

2021 Advisory Board (AB) Leadership

Todd Lawless
Chair of the Advisory Board
Continental

Michael Feiri
Vice Chair of the Advisory Board
ZF

Chris Lupini
Chair of the SAG
Aptiv

Larry Hilkene
Chair of the CAG
Cummins

Member Roster

As of June 1, 2021

Highlighted = Change

Aisin	Hyundai	Oshkosh Corp
Allison Transmission	Infineon	PACCAR
Aptiv	Intel	Panasonic
Argo AI, LLC	John Deere Electronic	Polaris
AT&T	Kia	Qualcomm
Blackberry Limited	Knorr Bremse	Renesas Electronics
BMW Group	Lear	Subaru
BorgWarner, Inc.	LGE	Sumitomo Electric
Bosch (Escrypt-Affiliate)	Luminar	Tokai Rika
Continental	Magna	Toyota
Cummins	MARELLI	TuSimple
Denso	Mazda	Valeo
FCA	Mercedes-Benz	Veoneer
Faurecia	Meritor	Volkswagen
Ford	Mitsubishi Motors	Volvo Cars
Garrett	Mitsubishi Electric	Volvo Group
General Motors	Mobis	Waymo
Geotab	Motional	Yamaha Motors
Google	Navistar	ZF
Harman	Nexteer Automotive Corp	
Hitachi	Nissan	
Honda	NXP	*63 Members*

Business Administration

➢ Auto-ISAC Activities ***Members Only***

- ❑ **June 16, 2021** – ***Members Teaching Members Presentation*** – **TLP:AMBER** – 10:00 – 11:30 a.m. EDT.
  Presentation Speaker: *Josh Davis- Toyota, Vice President for Toyota Motor North America, CISO - Auto-ISAC Board Vice-Chair,* ***Title*****:** "*Balancing IT, OT and Product Cybersecurity"*

  - ***CISO Executive Working Group*** established - Meeting ***Third Thursday of Every Month.***

➢ Community Activities:

- ➢ **July 7th, 2021:** ***Community Call Speaker***: Ben Willis, *Principal Security Engineer*, **HackerOne, Presentation Title: "**Hacker-Powered Data: The Most Common Security Weaknesses and How to Avoid Them"

- ➢ ***Auto-ISAC Mid-year Community Call Survey***, will be sent after June Community Call. Please provide your thoughts and recommendations for improvement of this monthly engagement.

➢ **October 13-14, 2021:** ***Auto-ISAC Annual Cybersecurity Summit,*** 8:00 am – 5:00 pm

Auto-ISAC Mid-year Community Call Survey

Sample Questions

1. In the last six months, how many Auto-ISAC Community Call sessions have you attended?
2. Which sessions have you attended?
3. Did you find value in the presentations you attended?
4. Would you recommend Auto-ISAC Community Call sessions to others? 10 being the highest score
5. Do you find monthly Cybersecurity and Infrastructure Security Agency (DHS, CISA) updates helpful during each Community Call sessions?
6. Do you like the current format such as Auto-ISAC business update, trending update , CISA update, speaker presentation length, Q&A time etc.?
7. Please provide feedback on future topics or speakers you would like to see.

Estimate time to complete the survey- 2 Minutes
Your feedback is important to us.

Senior Cyber Intelligence Analyst

Matthew Cook

We would like to welcome a new addition to our Auto-ISAC Staff Team, Matthew Cook. Matt holds a MS from Utica College in cyber security (concentration in intelligence) and a BA from Empire State College.

Prior to joining our organization, he came from the defense contractor environment. He was a lead analyst in cyber threat intelligence, and cyber security. He worked on cyber response, intelligence products and information security assessments. In addition to his primary responsibilities, he served as a liaison with external stakeholders, vendors and even led a NIST program.

Matt brings a great deal of cyber security experience, an analytical mindset and an eagerness to work with you all at the Auto-ISAC.

Auto-ISAC Intelligence

Know what we track daily by subscribing to the DRIVEN
Send feedback, contributions or questions to analyst@automotiveisac.com

Know our strategic perception of and outlook for the cyber threat environment by reading the 2020 Threat Assessment in the Auto-ISAC 2020 Annual Report
Email us to request the Report, provide feedback, or ask questions

Intelligence Notes

- In the wake of the ransomware attack on Colonial Pipeline, ransomware groups did not rule out attacking the automotive industry (Sources: KrebsonSecurity, Recorded Future, ThreatPost)
  - There is **no** intelligence indicating increased attacks on automotive companies are imminent, but companies should anticipate and prepare for that possibility
- We continue to see reporting (captured in the DRIVEN) about vulnerabilities in mobile devices and the proliferation of malicious links, websites, and attachments in emails and text messages (Sources: Sophos, Arstechnica, The Hacker News, Darkreading, ThreatPost)
  - This is a concern given that users could sync compromised devices with their vehicles and/or leverage in-vehicle Wi-Fi to access the internet
  - Ideally, all companies should have internal mechanisms to locate vulnerabilities and identify novel attack chains **before** threat actors

CISA RESOURCE HIGHLIGHTS

TLP: WHITE – CISA Current Activity (CA) – Updates to Alert on Pulse Connect Secure

- **Alert AA21-110A: Exploitation of Pulse Connect Secure Vulnerabilities updated with new information on threat actor TTPs IOCs, and updated mitigations.**
- **CA includes CISA and vendor resources to address Pulse Connect Secure vulnerabilities**
- **See:**
  - **https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/05/27/updates-alert-pulse-connect-secure**
  - **https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-110a**
  - **https://cyber[.]dhs[.]gov/ed/21-03/**

TLP: WHITE – CISA CA - Joint CISA-FBI Cybersecurity Advisory on DarkSide Ransomware

- First released on May 11th, updated on May 19th
- Includes technical details, mitigation recommendations and resources to address ransomware
- Updated to include downloadable STIX file of IOCs
- https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/05/19/update-cisa-fbi-joint-cybersecurity-advisory-darkside-ransomware
- https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-131a
- https://us-cert[.]cisa[.]gov/sites/default/files/publications/AA21-131A.stix.xml

TLP: WHITE – CISA CA - Joint CISA-FBI Cybersecurity Advisory on Sophisticated Spearphishing Campaign

- **Released on May 28, updated on May 29, highlighting spearphishing campaign targeting government, intergovernnmental and non-governmental organizations**
- **Sophisticated cyber actor compromised an end-user account of a legitimate email marketing software company to spoof a US-based government organization**
- **Details provided in AA21-148A and MAR-10339794-1.v1**
- **https://us-cert[.]cisa[.]gov/ncas/alerts/aa21-148a**
- **https://us-cert[.]cisa[.]gov/sites/default/files/publications/AA21-131A.stix.xml**

TLP:WHITE – CISA CA – CISA Publishes Eviction Guidance for Networks Affected by SolarWinds and AD/M365 Compromise

- **Published as Analysis Report AR21-134A "Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise"**
- **AR21-134A provides detailed steps for affected organizations to evict the adversary from compromised on-premises and cloud environments**
- **https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/05/14/cisa-publishes-eviction-guidance-networks-affected-solarwinds-and**
- **https://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar21-134a**

TLP: WHITE – Additional Resources From CISA

- CISA Homepage - https://www[.]cisa[.]gov/
- CISA News Room - https://www[.]cisa[.]gov/cisa/newsroom
- CISA Blog - https://www[.]cisa.gov/blog-list
- CISA Publications Library - https://www[.]cisa[.]gov/publications-library
- CISA Cyber Resource Hub - https://www[.]cisa[.]gov/cyber-resource-hub
- CISA Vulnerability Management (formerly known as the National Cyber Assessment and Technical Services (NCATS) program) - https://www[.]us-cert[.]gov/resources/ncats/
- CISA Cybersecurity Directives - https://cyber[.]dhs[.]gov/directives/
- CISA COVID-19 Response – https://www[.]cisa[.]gov/coronavirus

For more information:
cisa.gov

Questions?
CISAServiceDesk@cisa.dhs.gov
1-888-282-0870


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

Why Do We Feature Speakers?

- These calls are an opportunity for information exchange & learning
- Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

- Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- Goal is to showcase a rich & balanced variety of topics and viewpoints
- *Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC*

30+
Featured Speakers to date

How Can I Be Featured?

- If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

7 ***Best Practice Guides available on website***

2000+
Community Participants

Slides available on our website – www.automotiveisac.com

Featured Speaker

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Tim Weisenberger - SAE International

Project Manager, Emerging Technologies

Tim Weisenberger is Project Manager, Emerging Technologies at SAE International. He leads SAE efforts in automotive cybersecurity and is integral to managing the SAE emerging technology portfolio. His efforts include standards development and managing pre-competitive research projects notably the development of an EV Charging Industry PKI Platform.

Tim is a transportation thought leader and innovator with over 30 years of professional experience in public, private, and non-profit sectors. He holds an MPA from Harvard Kennedy School, an MBA from University of Illinois at Chicago, and a BS in Electrical Engineering from Illinois Institute of Technology.

SAE INTERNATIONAL

GLOBAL GROUND VEHICLE STANDARDS

Developing an EV Charging Public Key Infrastructure

an SAE Cooperative Research Project

Tim Weisenberger
Technical Program Manager
Emerging Technologies
SAE INTERNATIONAL

The Research Opportunity and How it Emerged…

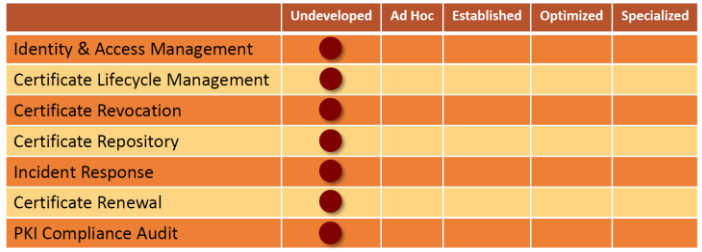
EV Charging systems have crucial and growing interface points between the Automotive industry, EV drivers, and the Electric Grid/Energy industry

- It is critical that these interfaces be ***secure and trusted***
- ISO 15118 is believed by some to provide a complete message authentication and security approach for EV Charging systems and transactions

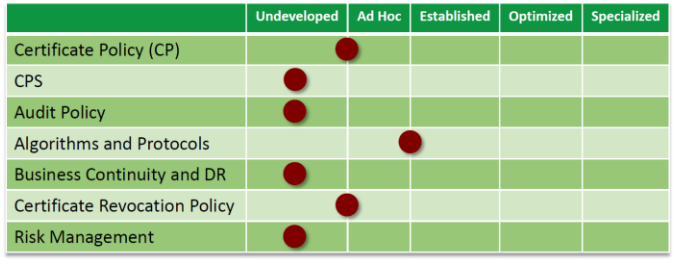
In June 2018 ChargePoint, DigiCert, and eonTi performed a "360 Assessment" (gap analysis) of ISO 15118 PKI and cybersecurity

Findings- Significant Gaps in 15118 Requirements and Processes

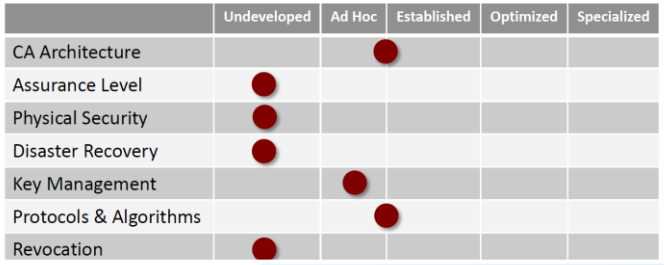
Operations Score: 1.0 out of 5



Governance Score: 1.4 out of 5



Technical Score: 1.6 out of 5



SAE Gathers Industry to Secure the EV Charging Connection

SAE Cooperative Research Program

Solutions by Industry for Industry

- SAE Cooperative Research Program (CRP) projects are joint ventures of industry companies that meet project criteria to preform targeted, pre-competitive research to solve an industry problem.
- SAE CRP projects develop industry deliverables that can then be fed into SAE standards to develop a needed J standard.

Core Team Members are recruited from SAE standards experts and throughout industry

- OEMs/Developers
- Service Providers
- Public/Government Sector
- Research/Academia

SAE is administrative Project Manager

Project team provides technical oversight

Technical work is done by a paid Contractor

Differences Between Open Standards and Pre-competitive Research

Open Standards Groups

Groups comprised of SMEs volunteers

who represent *themselves*

All technical development is done collaboratively by volunteers led by a volunteer "document sponsor"

Anyone can join an SAE committee or task force

Multi-step ballot process

Cooperative Research Projects

Groups comprised of *companies who opt-in* and must meet criteria.

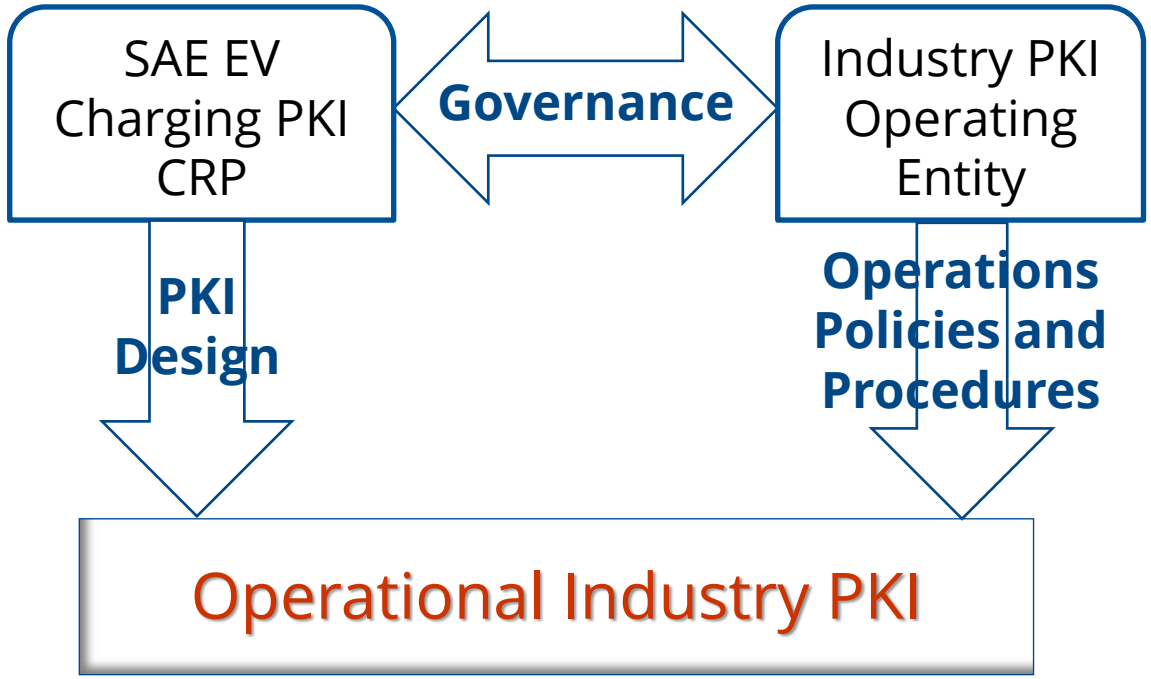
Experts scope and guide technical work, closely manage technical development.

Technical development is done by contractor(s).

Agile development emphasizing collaboration, feedback from stakeholders and allies, frequent publication of incremental results.

Project Mission and Goals

- The EV Charging PKI CRP will *design and test an inclusive, worldwide EV charging industry PKI platform* that is secure, trusted, scalable, interoperable, and extensible.
- A PKI platform is *not just a specification, it is a business that must be run*. Therefore, our PKI Platform will be transitioned to an operational entity to provide industry a *solution for all that is secure and trusted*.
- Project Deliverables
  - EV Charging PKI Platform
  - Handover Plan for fielding an operational industry PKI



We *will* strengthen the global EV charging ecosystem security.

SAE Gathers Industry to Secure the EV Charging Connection

SAE EV Charging PKI project

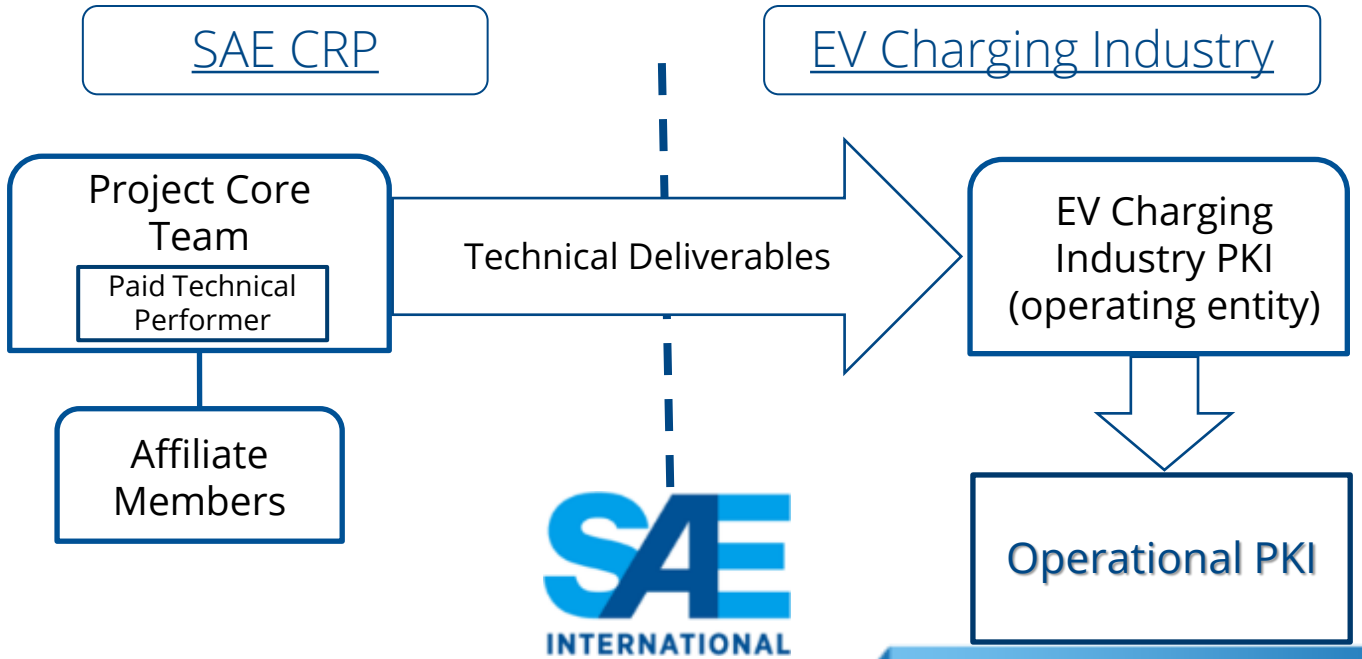
- The project is an ***industry-led, pre-competitive research*** project to strengthen electric vehicle charging system security.
- The project will ***design and test an inclusive, worldwide EV charging industry PKI platform*** that is secure, trusted, scalable, interoperable, and extensible.

Core Team Members must be:

- EV OEMs/Developers
- EVSE Providers
- Charging Network Operators

Affiliate Project Members drawn from:

- Industry Companies and Associations
- Research/Academia
- Public/Government Sector



Project Technical Approach

Estimated Schedule and Budget

- 18-24 month project, 1.0-1.5M budget

Technical Deliverables

1. World Class EV Charging PKI Platform
2. Handover Plan to field an Industry PKI

Technical Approach

- All technical work is done by paid Technical Contractors
- Core Team is project technical lead
- SAE is administrative Project Manager

Current Project Team

- ChargePoint
- eMobility Power
- Ford
- General Motors
- MBRDNA (Daimler)
- Shell
- Stellantis (formerly FCA)

SOW Elements

Phase 1: EV CHARGING PKI PLATFORM DESIGN

- State-of-the-Industry PKI Review and Gap Analysis
- Threat modeling and risk analysis
- PKI Platform Requirements
- *Operationalizing PKI Report*
- Industry Outreach and Comment
- Final Draft PKI Platform Design

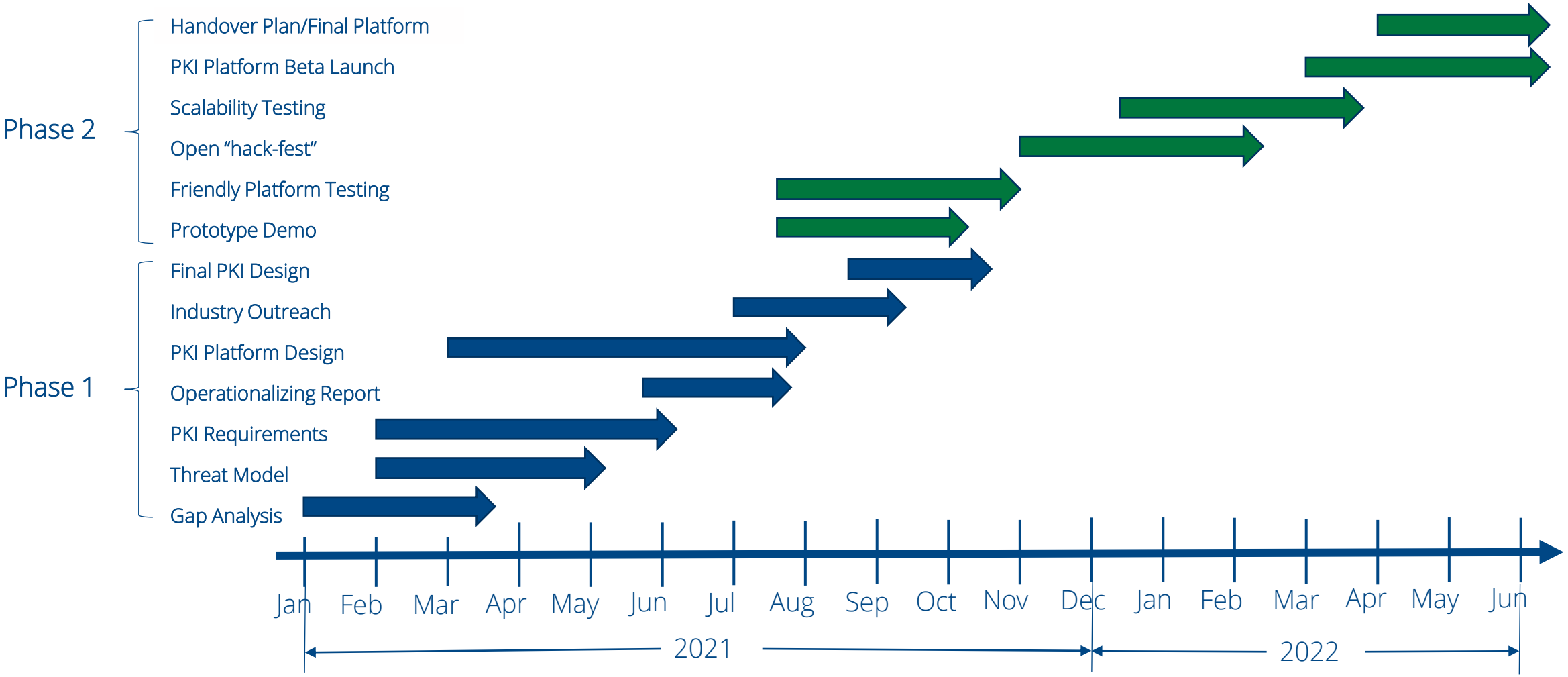
OTHER CRP TASKS

- Marketing, Public Relations, and Outreach
  - Performed by SAE

Phase 2: PKI PLATFORM TESTING

- Functionality Testing
- Friendly Platform Testing (project members and invited parties)
- Open Hack-Fest (DEFCON/Blackhat)
- Proof of Scalability (Alpha Launch)
- PKI Platform Beta Launch
- Final Industry PKI Platform Launch
- *Handover plan*
  - Fielding the PKI Platform
  - Industry coalition/collaborative

Technical Development Schedule

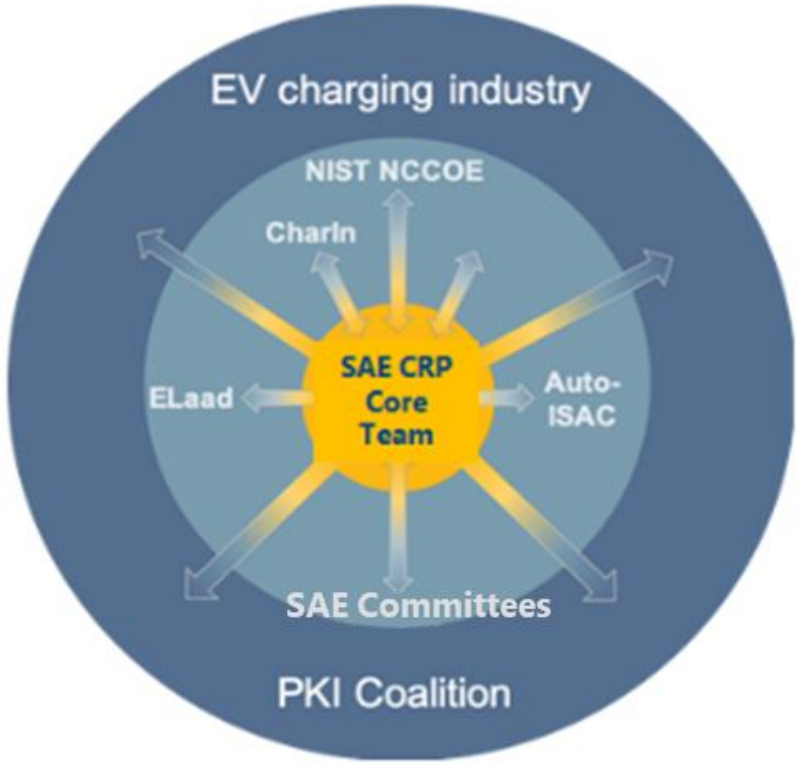


Industry Value Proposition

Industry Gap	Feature	Value Add
No global industry-wide EV Charging PKI solution	Industry-led Business Consortium to implement and operate PKI Solution. • Comprehensive Governance Policy and organizational structure agreed upon by members	• Improved PKI compliance by participants • Reduced variability between hardware manufacturers • Heightened level of security • Consistent global PKI implementation and operations
Customized solutions limit compatibility	Normative policies and procedures allow automated operation & life-cycle management	• More efficient certificate generation / Out-of-band operations eliminated • Robust, cradle-to-grave certificate life-cycle mgmt • Response robustness in disaster scenario
	Flexible PKI design allows ability to create trust anchors directly between ecosystem participants	• More choice in the marketplace • Faster implementation
	PKI Platform is based on established security industry best practices and is therefore: • Scalable and extensible • Strengthened to enhance security	• Improved customer experience • Lower manufacturing and implementation cost • Easier to introduce new services, market innovation
Charging protocol-specific solution; ***no competition***	PKI decoupled from EV-EVSE charging communication standards • Platform is protocol & charging system-independent	• Device independent • Future-proof cybersecurity framework • Inclusive of all worldwide ecosystem parties

Industry Outreach

SAE will perform robust outreach to industry stakeholders to ensure acceptance of project technical approach.



Entity	Role	Detail
DOE and National Labs	Government Liaison	Engage federal gov't experts, coordinate with existing R&D portfolio, and liaison with Electric grid sector (PUCs, IOOs, etc.)
NIST/ NCCOE	Government Liaison	Engage federal gov't experts, host testing events
DHS S&T	Government Liaison	Engage federal gov't experts, broaden sphere of outreach, coordinate with existing R&D portfolio
Auto-ISAC	Cybersecurity Liaison	Engagement to gain broad industry feedback and acceptance
ELaad	International Liaison	NL Smart Charging experts, can promote EU industry involvement and acceptance.
Chademo, CharIn, etc.	International Liaison	Trade associations can promote global industry involvement and acceptance
Others	International Liaisons	SDOs and others, e.g. JAMA, JSAE, JARI, IEC, ISO, CATARC, CEC, …

Come Join Us!

Tim Weisenberger
Technical Program Manager, Emerging Technologies

e: tim.weisenberger@sae.org
m: 248.840.2106

Open Discussion

Any questions about the Auto-ISAC or future topics for discussion?

How to Get Involved: Membership

If you are an OEM, supplier or commercial vehicle, Carrier or Fleet, please join the Auto-ISAC!

- Real-time Intelligence Sharing
- Intelligence Summaries
- Regular intelligence meetings
- Crisis Notifications
- Member Contact Directory
- Development of Best Practice Guides
- Exchanges and Workshops
- Tabletop exercises
- Webinars and Presentations
- Annual Auto-ISAC Summit Event

To learn more about Auto-ISAC Membership or Partnership, please contact Auto-ISAC! fayefrancy@automotiveisac.com

Auto-ISAC Partnership Programs

Strategic Partner | **Community Partners**

Solutions Providers

For-profit companies that sell connected vehicle cybersecurity products & services.

Examples: Hacker ONE, IOActive, Karamba, Grimm

Associations

Industry associations and others who want to support and invest in the Auto-ISAC activities.

Examples: Auto Alliance, ATA, ACEA, JAMA

Affiliations

Government, academia, research, non-profit orgs with complementary missions to Auto-ISAC.

Examples: NCI, DHS, NHTSA, Colorado State

Community

Companies interested in engaging the automotive ecosystem and supporting & educating the community.

Examples: Sponsors for key events, technical experts, etc.

INNOVATOR
Paid Partnership

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed
- Must be educational provide awareness

NAVIGATOR
Support Partnership

- Provides guidance and support
- Annual definition of activity commitments and expected outcomes
- Provides guidance on key topics / activities
- Supports Auto-ISAC

COLLABORATOR
Coordination Partnership

- "See something, say something"
- May not require a formal agreement
- Information exchanges-coordination activities
- Information Sharing / research & development

BENEFACTOR
Sponsorship Partnership

- Participate in monthly community calls
- Sponsor Summit
- Network with Auto Community
- Webinar / Events

Current Partnerships

Many organizations engaging

INNOVATOR
Strategic Partnership (15)

Security Scorecard
ArmorText
Celerium
Cybellum
Ernst and Young
FEV
GRIMM
HackerOne
Karamba Security
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Trillium Secure
Upstream

NAVIGATOR
Support Partnership

AAA
ACEA
ACM
American Trucking Associations (ATA)
ASC
ATIS
Auto Alliance
EMA
Global Automakers
IARA
IIC
JAMA
MEMA
NADA
NAFA
NMFTA
RVIA
SAE
TIA
Transport Canada

COLLABORATOR
Coordination Partnership

AUTOSAR
Billington Cybersecurity
Cal-CSIC
Computest
Cyber Truck Challenge
DHS CSVI
DHS HQ
DOT-PIF
FASTR
FBI
GAO
ISAO
Macomb Business/MADCAT
Merit (training, np)
MITRE
National White Collar Crime Center
NCFTA
NDIA
NHTSA
NIST
Northern California Regional Intelligence Center (NCRIC)
NTIA - DoCommerce
OASIS
ODNI
Ohio Turnpike & Infrastructure Commission
SANS
The University of Warwick
TSA
University of Tulsa
USSC
VOLPE
W3C/MIT
Walsch College

BENEFACTOR
Sponsorship Partnership

2020 Summit Sponsors-
Claroty
Upstream
Escrypt
Blackberry
Cybellum
Blockharbor
C2A
Synopsis
Intsignts
ValiMail

2019 Summit Sponsors-
Argus
Arxan
Blackberry
Booz Allen Hamilton
Bugcrowd
Celerium
Cyber Future Foundation
Deloitte
GM
HackerOne
Harman
IOActive
Karamba Security
Keysight
Micron
NXP
PACCAR
Recorded Future
Red Balloon Security
Saferide
Symantec
Toyota
Transmit Security
Upstream
Valimail

Auto-ISAC Benefits

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency

Building Resiliency Across the Auto Industry

THANK YOU!


thank you
danke
謝謝
ngiyabonga
شكراً جزيلاً
рахмат
teşekkür ederim
Баярлалаа
спасибо
gracias
dank je
tapadh leat
obrigado
dziękuję
bedankt
go raibh maith agat
sukriya
kop khun krap
merci
terima kasih
arigatô
dakujem
mochchakkeram
hvala
mauruuru
sagolun
grazie
takk
tạ ơn
ευχαριστώ
감사합니다
ধন্যবাদ
xièxie
merci
mersi
barka
welalin
tack
spas
faafetai lava
vinaka
спасибі
blagodaram
misaotra
matondo
paldies
grazzi
mahalo
хвала
asante
manana
obrigada
tenki
murakoze
chokrane
mamnun
дякую
djiere dieuf
tau
akun
dankon
aciu
kiitos
dankie
nanni
nandri
dhanyavad
bayarlalaa
gracie
köszönöm
enkosi
chnorakaloutioun
gratias ago
gracies
sulpáy
dēkuji
sobodi
mesi
didi madloba
kam sah hamnida
rahmat
najis tuke
ありがとう
tanemirt
rahmet
diolch
dhanyavadagalu
shukriya
merce
мерси
trugarez

Our contact info

Faye Francy
Executive Director

20 F Street NW, Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

Sharmila Khadka
Information Technology

20 F Street NW, Suite 700
Washington, DC 20001
sharmilakhadka@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com
@auto-ISAC