SECURE TECHNOLOGY ALLIANCE

MARCH 2020

SECURE TECH TALK

A quarterly newsletter for members and friends of the Alliance

Executive Director Message

The steady flow of frightening news about the rapidly spreading coronavirus has me questioning every assumption I hold about our country's safety and security, not to mention the potential of a global recession that could hit the U.S. like a tsunami. If the truth about how this virus will impact our social, business, and political landscape turns out to not correspond with the conservative estimates, things could become much worse. Please read my letter in this issue to learn more about the possible business ramifications of this pandemic.

Click to Read Letter ...

Feature Article:
Temporary Identity Credentials for Federal PACs

This quarter's feature article is an extract from a new Secure Technology Alliance Access Control Council white paper that recommends an approach for implementing temporary identity credentials for PACS for federal agencies. The white paper outlines the requirements and presents a solution for issuing and using temporary identity credentials for federal agencies.

Click to Read More …

In This Issue:

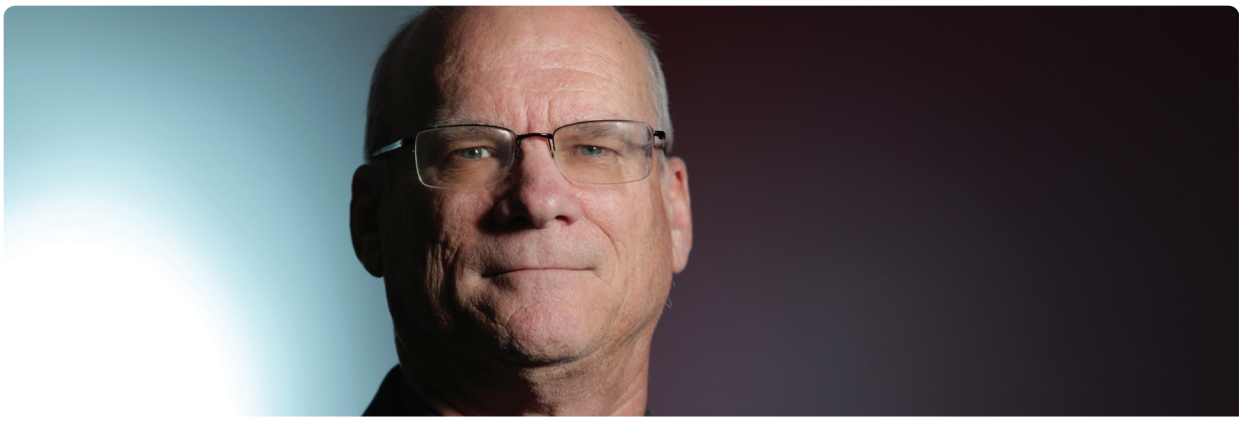
On the Web:

Upcoming Event:

Securing Federal Identity 2020

Due to the COVID-19 virus, we have postponed the Securing Federal Identity 2020 conference scheduled for June 22-23. The health and safety of our sponsors, speakers and attendees is our top priority and we will be making further announcements about this event at a later date.

The Secure Technology Alliance travels to the nation's capital to focus on one specific topic that impacts everyone – secure identity. This premier event for government-led cybersecurity policy and digital identity technology focuses on developments and innovations in federal identity credentialing, access security, and mobile credentials.



Coronavirus Has Me Questioning our Safety and Security

Dear Members and Friends of the Alliance,

The steady flow of frightening news about the rapidly spreading coronavirus has me questioning every assumption I hold about our country's safety and security, not to mention the potential of a global recession that could hit the U.S. like a tsunami. If the truth about how this virus will impact our social, business, and political landscape turns out to not correspond with the conservative estimates, things could become much worse.

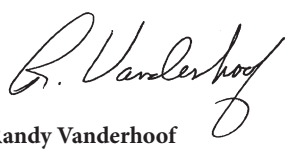
We were very fortunate to have moved our annual Payments Summit conference to February this year, just ahead of the most cautionary warning notices from the Centers for Disease Control (CDC). With the number of reported cases in the U.S. still in the few hundreds at the start of the conference, which doesn't typically serve an international base, the Payments Summit was held with no problems.

Nearly 500 payments professionals, including about 100 speakers, attended the co-located Payments Summit and U.S. Payments Forum Members Meeting in Salt Lake City February 24th -27th. The agendas of the two events demonstrated the contrasting missions of the two organizations. The Secure Technology Alliance uses the annual Payments Summit to explore and explain how payments technology is always evolving, and to discuss new technologies through a security lens. The U.S. Payments Forum, established by the Alliance in 2012 as the EMV Migration Forum to address the U.S. market's adoption of chip technology, and renamed as the U.S. Payments Forum in 2016, is more focused on addressing issues with implementing new and emerging technologies already in the market.

The Forum provides a much-needed place for stakeholders from different sides of the payments market to understand and meet the challenges facing the market today in implementing new enabling and fraud-reducing technologies beyond EMV. Some of the topics discussed at the Forum included EMV 3DS, Secure Remote Commerce, contactless EMV and mobile payments. The February Forum meeting was the first of three in-person meetings planned for Forum members in 2020.

So, what the next few months have in store for us will be largely written and decided in the next few days and weeks ahead. It was only 12 years ago that we all lived through the financial markets collapse, which disrupted the lives of millions. Many people of my generation lost their jobs, their homes, and their sense of safety and security, which they never fully recovered. Whatever bad things may be in store for us in the future, it will be better knowing that we have come through such times before and we are starting from a good place to begin with. Stay safe and be healthy.

Sincerely,



Randy Vanderhoof
Executive Director, Secure Technology Alliance
rvanderhoof@securetechalliance.org

Payments Summit

The recent 13th Annual Payments Summit, held at the end of February in Salt Lake City, brought together hundreds of industry experts looking to find new ways to overcome challenges impacting the adoption, security and usability of emerging and developing payments technologies. Once again co-located with the U.S. Payments Forum Member Meeting, the Summit lived up to its reputation as the most important payments conference of the year.

Conference themes discussed included:

- Major disruptions in fraud trends
- Securing online channels
- The consumer shopping experience
- Mobility payments in transit

A thank you and our sincere appreciation go out to attendees, speakers, panel presenters, exhibitors and sponsors! We hope to see everyone at next year's Payments Summit.

Final Weeks Remain for New Member Sign-Up and Bonus Program

A few weeks ago we let you know details about the New Member Bonus Program in case you received questions from colleagues or industry contacts for organizations interested in joining the Secure Technology Alliance. We're delighted that this program has attracted new members thanks to your outreach and efforts! Right now we're in the last phase of the membership offer, as it expires on March 31, 2020. If you have business contacts you feel may benefit from Alliance membership and industry efforts, we encourage you to share details of the program today, and encourage them to apply for membership before March 31. For any questions, please feel free to contact Randy Vanderhoof at rvanderhoof@securetechalliance.org. Remember that current members who help recruit a new organization that becomes a member of the Alliance will receive an Amazon Gift Card!

Councils Update

Secure Technology Alliance councils continue to be active in providing education and commentary on new and emerging secure technologies.

Access Control Council

- The Access Control Council submitted comments to TSA for the second-round comment period for the NEXGEN TWIC specification
- The Council is completing a new white paper on temporary identity credentials for Federal agencies and discussing new projects

Identity Council

- The Identity Council is focused on activities supporting the mobile driver's license (mDL) initiative. The Council is completing an mDL overview white paper which discusses mDL technology, uses and key implementation considerations, planning a webinar series, and discussing follow-on projects on critical mDL topics

Payments Council

- The Payments Council hosted a well-attended webinar, Electric Vehicle Charging Payments Innovations, on February 5th. The recording is available on the Alliance web site
- The Council held a well-attended in-person meeting during the **2020 Payments Summit** in Salt Lake City, UT. During the meeting, members brainstormed projects for 2020; Council members are now completing a survey to provide input on project priorities and interest
- The Council has four active projects: dynamic security code cards white paper; wearables white paper update; open payments framework for electric vehicle charging; and cryptography and the secure operating environment white paper

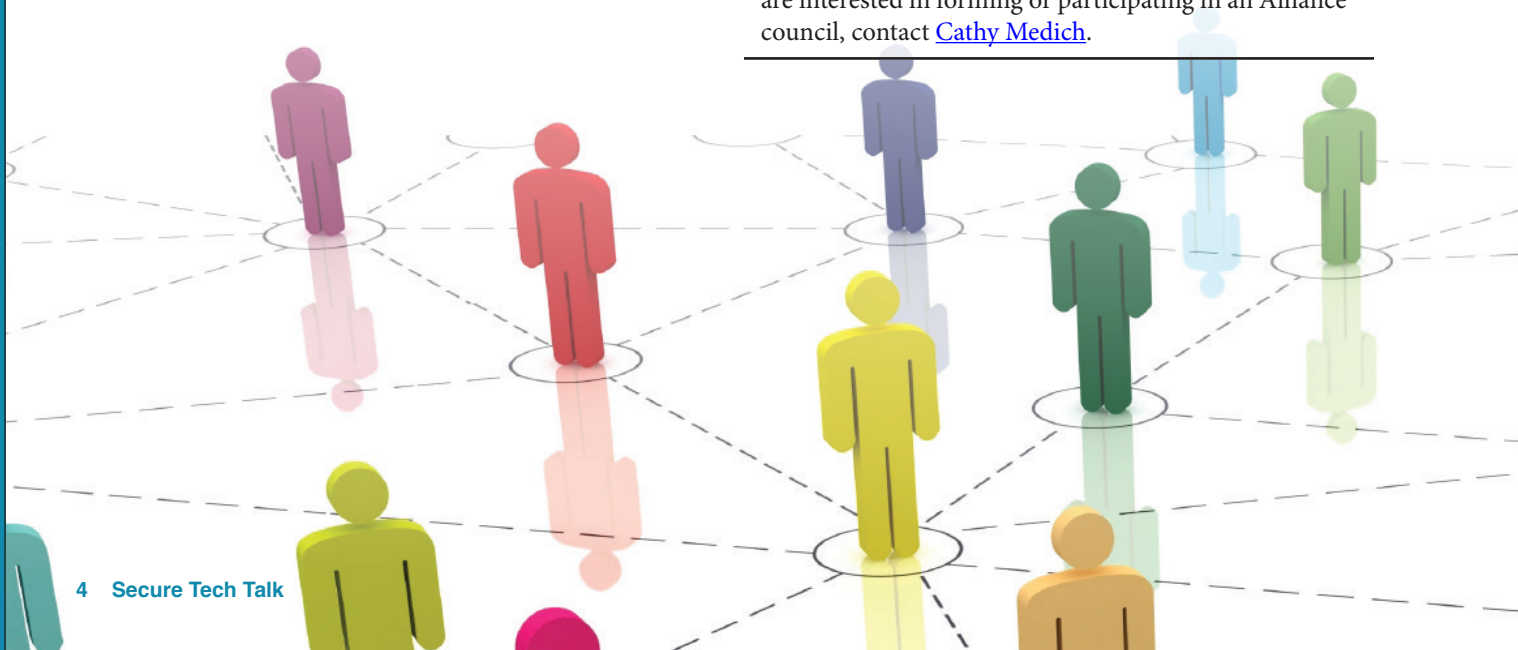
Transportation Council

- The Transportation Council held well-attended in-person meeting during the **2020 Payments Summit** in Salt Lake City, UT. During the meeting, members discussed Council strategy and approach for projects related to payments integration with Mobility as a Service (MaaS)
- The Council has opened nominations for Council officers and steering committee, with nominations closing in March. As part of its expanded focus on MaaS, the Council has added a vice chair for mobility and steering committee seats for mobility service providers. If you would like to nominate someone for the Council steering committee, please contact Cathy Medich (cmedich@securetechalliance.org)
- The Council is completing a vision white paper focused on payments integration with MaaS initiatives

Other Council Information

- A list of active Secure Technology Alliance Council projects is also available to promote cross-council participation
- If you are interested in forming or participating in an Alliance council, contact Devon Rohrer

Alliance Members: Participation in all current councils is open to any Secure Technology Alliance member who wishes to contribute to the council projects. If you are interested in forming or participating in an Alliance council, contact Cathy Medich.



Temporary Identity Credentials for Federal PACs

Homeland Security Presidential Directive 12 (HSPD-12) has been in effect since 2004 and industry and federal stakeholders have successfully met HSPD-12's control objectives with the now ubiquitous Personal Identity Verification (PIV) credential. However, new requirements have arisen over the years that caused expansion of the PIV technical model, its related policies, and its intended uses, such as:

- PIV-Interoperable (PIV-I) credentials
- PIV-Commercial/Commercial Identity Verification (CIV) credentials
- Derived PIV credentials for mobile devices

NIST publication SP 800-116 Rev. 1, "Guidelines for the Use of PIV Credentials in Facility Access," Section 6.5 [1] addresses the technical issues of temporary, interoperable credentials. While SP 800-116 Rev. 1 was first published as guidance, the Office of Management and Budget (OMB) M-19-17 "Enabling Mission Delivery through Improved Identity, Credential, and Access Management" [2] published in May 2019, made it normative.

Temporary identity credentials that interoperate with the physical access control system (PACS) are not a new concept in Federal Government policy. What has not been addressed (nor universally standardized and implemented) are *consistent government-wide policies and models* for issuing and managing short-term, temporary credentials that may be used for access to federal agency facilities, and, potentially, access to federal agency information technology resources. The United States Department of Defense (DoD) came to this same realization in 2014. One of the DoD's physical security policies, "Interim Policy Guidance for DoD Physical Access Control," Attachment 4 [3] makes electronically verifiable credentials the minimum requirement for visitors to any DoD location.

This article is an extract from a new Secure Technology Alliance Access Control Council white paper that recommends an approach for implementing temporary identity credentials for PACS for federal agencies.

Who May Need a Temporary Credential?

A temporary identity credential may be needed by different categories of visitors

- An internal visitor who has a PIV credential (e.g., a visitor

from same agency/organization but based at another location, an individual who forgot their PIV card, an individual who lost their PIV card or had it stolen)
- A visitor from a different government agency who has a PIV credential from that other agency.
- An external visitor who has a PIV-I card
- A short-term visitor without a PIV/PIV-I card or DoD Common Access Card (for whatever reason) who needs a temporary identity card
- A long-term visitor without a PIV/PIV-I card or CAC who needs a personalized (i.e., with a photo) temporary identity card

Visitors are authenticated by what they possess, their credentials. The goal of a high assurance PACS is to verify a visitor by validating a credential already in their possession thereby leveraging the identity vetting process that has already taken place.

A locally-issued CIV card can serve a solution for temporary identity credentials.

How Would a CIV Card Be Used?

A Commercial Identity Verification (CIV) card [4] is an authentication token that uses a smart card form factor technically comparable to a PIV or PIV-I card. The CIV credential was originally intended for commercial organizations that were seeking a credential for use for their employees, subcontractors, nonemployee visitors and customers. In that original context, the CIV card is equally suitable as an authentication platform that can be leveraged for agency use as a temporary credential.

The reasons why a CIV credential may be considered as the candidate for a temporary visitor credential include:

1. **Flexible Policies and Processes**. A CIV card can be a less expensive alternative to PIV or PIV-I cards since there are fewer policy and process compliance requirements for a CIV credential than there are for a PIV/PIV-I credential. That is, agencies can specify their own CIV vetting, identity proofing and issuance policies and procedures that suit their agency-specific needs to accommodate visitor access to agency facilities and resources.
2. **Proven Technology**. The CIV credential is based on the proven PIV/PIV-I credential technical model that establishes very strong authentication.

To be used in a federal agency, the CIV card would use a PIV applet that is listed on the FIPS 201 Approved Products List [5]. The PIV application on the CIV card is populated with data elements that are compliant with the data model defined for PIV and PIV-I cards (as specified in NIST SP 800-73, SP 800-76 and SP 800-78), but not all of the data elements are necessarily mandated to be populated for the CIV credential.

The CIV credential is neither tightly defined nor specified. Several CIV cards are already commercially available with some marketed under other brand names. This lack of specificity, which is a major hindrance to interoperability, is precisely because the CIV credential is not intended to be interoperable across agencies. Instead, use of the CIV credential is for local trust and local use cases. This approach is manifested in three ways:

1. The CIV credential can be issued without the burden of cross-certification to the Federal Bridge and can be anything that the issuer wants since the issuer knows what the credential will be used for, and importantly, what it will not be used for
2. The CIV credential is not certified by a trust broker to be part of a trust framework. Specifically, the CIV credential does not contain policy object identifiers (OIDs) that would cause an access control system to believe that the credential could be validated through the Federal Bridge as a PIV or PIV-I credential. Issuers of CIV credentials are concerned with a local trust use case. Simply put, a local trust use case does not require the external trust capability afforded by Federal-Bridge-backed credentials
3. A federal or commercial CIV credential issuer may create their own identity vetting policies, issuance policies and trust anchor (certificates) without the expense of cross certification to the Federal Bridge

Interoperability aside, it may benefit the federal government to recommend common CIV technical requirements for CIV temporary cards, such that PACS vendors and CIV card issuers only have to implement configurations and profiles once for CIV card issuance and CIV card authentication. Otherwise, agencies would have to pay for PACS and CIV card issuance customizations individually, rather than leverage pre-existing configurations and profiles that PACS vendors and CIV card issuers may have already implemented using a common technical model.

When a CIV card is presented to a PACS smart card reader (either ISO/IEC 7816 contact or ISO/IEC 14443 contactless), the card responds like a PIV-I card and has the following characteristics:

- The card contains a PIV applet
- The card's PIV applet has all of the required containers/structures defined by NIST SP 800-73. The CIV credential does not mandate any specific data be populated in any container. Additional containers outside of the PIV data model are optional and issuer dependent
- For a CIV card to be used in a federal PACS, the card identifier in the CHUID (and the other structures) must be encoded with the Card Universally Unique Identifier (CUUID). The FASC-N fields for Agency Code – System Code - Credential Number in the CHUID shall be all 9s (9999-9999-999999). All other FASC-N fields may be populated in accordance with the CIV credential issuer requirements and issuance practices
- The digitally signed card data objects, as well as the

cryptographic functions for all PIV-specified containers, are compliant with NIST SP 800-78. Additional containers are out of scope of this requirement
- Any biometric information stored on the card in a PIV-specified container are compliant with NIST SP 800-76

Conclusion

Temporary access cards that are vendor-agnostic and compatible with modern, GSA FIPS 201 APL access control systems may be created and issued in accordance with local agency policies and are commercially available from several manufacturers. PKI-based CIV cards are resistant to unauthorized modification, counterfeiting and cloning and may be authenticated electronically.

The CIV card can work effectively as a visitor credential where the local PACS is fully compliant with the current GSA FIPS 201 Evaluation Program specifications.

References

[1] https://csrc.nist.gov/publications/detail/sp/800-116/rev-1/final
[2] https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf
[3] https://www.cac.mil/Portals/53/Documents/DTM-09-012.pdf
[4] Additional information on the CIV credential is available in the Secure Technology Alliance white papers, "The Commercial Identity Verification (CIV) Credential Leveraging FIPS 201 and the PIV Specifications" and "A Comparison of PIV, PIV-I and CIV Credentials" at https://www.securetechalliance.org/publications-the-commercial-identity-verification-civ-credential-leveraging-fips-201-and-the-piv-specifications/.
[5] https://www.idmanagement.gov/approved-products-list-piv/

About this Article

This article is an extract from a new Secure Technology Alliance Access Control Council white paper, "Temporary Identity Credentials for Federal Physical Access Control Systems (PACS)." The white paper was developed to outline the requirements and discuss a solution for issuing and using temporary identity credentials for federal agencies. Participants involved in the development of the white paper included: CertiPath; G+D Mobile Security; GSA; HID Global; ID Technology Partners; IDEMIA; Identiv; Integrated Security Technologies; IQ Devices; Parsons; Secure Element Solutions; SigNet Technologies, Inc.; Tyco Software House; U.S. Dept. of Homeland Security; Veridt, Inc.; XTec, Inc.

Welcome New Members

- Community Transit
- Four Nines Technologies
- Sound Transit

Alliance In The News

- "Why Digital Driver's Licenses Are the Future Of ID Verification" PYMNTS. Executive Director Vanderhoof shared insight on the advantages and challenges of mobile driver's licenses as the technology starts to spread across states in the U.S.

- "Fraud Schemes Get 'Scary' as Chip Cards Push Crime Away From the Point of Sale" Digital Transactions. This article highlights information on payment-related fraud including business email compromise and synthetic identity fraud shared by two speakers at the Payments Summit conference in Salt Lake City.

- "Smart Cards Applications in IoT Security" My Tech Decisions. This piece refers to the Secure Technology Alliance recommendation for embedded hardware security to be built directly into IoT devices at the manufacturing stage.

U.S. Payments Forum Resources

- The Forum published the new resource, Contactless Operating Mode Requirements Clarification. The white paper provides an overview of each payment network's current contactless requirements for issuers, acquirers and acceptance partners electing to implement contactless technology for both magnetic stripe data (a.k.a. MSD, magstripe, magnetic stripe) and EMV mode contactless support
- The Forum has launched a new **Debit Routing Working Committee**. The Working Committee goal is to identify and describe options for successful U.S. debit routing for EMV contact and contactless, mobile, ecommerce, and emerging technology transactions, regardless of presentment method

The full list of active U.S. Payments Forum projects is available on the Alliance members-only site.

Congratulations New Certificants

CSCIP

- Alex Howard, Tx Systems
- Carlo Iaboni, Ahold

CSCIP/G

- Mike White, Idemia

CSEIP Certified

- Kristopher Hough, M.C. Dean
- Daniel Morris, M.C. Dean
- Brandon Parker, Star Asset Security

CSEIP Recertified

- Rich Anderson, PSG Global
- Gunvir Baveja, eVigilant.com
- Ryan Breeden, Pentagon Force Protection Agency
- Wayne Budd, Johnson Controls
- Forrest Davenport, ICF International
- Jeff Deweese, Johnson Controls
- Sean Eaton, Johnson Controls
- Clinton Eppler, Cam-Dex Security Corp
- Clyde Fox, Johnson Controls
- Mala Grover, Digitronics
- Cliff Hall, Cliff Hall Consultants
- Jacob Haymore, Johnson Controls
- Nathan Hott, Genesis Security System
- Bryan Ichikawa, Bryan Ichikawa Consulting
- Eric Johnson, Volta Systems Group
- Jim Kemp, COLSA Solutions
- Erik Larsen, Johnson Controls
- Michael Margolis, Integrated Security Technologies
- Matthew Martino, Business Integra
- Marcus Mathis, BL Harbert International
- Richard McGinnis, Security Install Solutions
- Brian Mooney, Genesis Security Systems
- Dan Morrisey, United Security & Communications
- Scott O'Neal, Johnson Controls
- Dwayne Pfeiffer, Northrop Grumman IT
- John Placious, Integrated Security Technologies
- Mike Plaugher, Johnson Controls
- Daniel Reilly, Business Integra
- Doug Ritchey, Communications Resource
- Roger Roehr, Integrated Security Technologies
- Brandon Sutphin, Johnson Controls
- Donald Thomas, BruckEdwards
- JC Viricochea, Johnson Controls
- Rob Weaver, Stanley Black & Decker

Upcoming Industry Event

Mobile Payments Conference 2020 (MPC20)

Aug. 24-26, 2020
Swissôtel
Chicago, IL
www.mobilepaymentsconference.com
The Mobile Payments Conference is an annual forum that brings together the leading experts in the FinTech, Mobile Payments and digital technology industries. Conference attendees will have 2.5 days of immersive learning and networking sponsored by Mobile Marketing and Technology Magazine and their generous partners.

For more information, visit our website at www.securetechalliance.org. Members can also access white papers, educational resources and other content.

SECURE TECHNOLOGY ALLIANCE
191 Clarksville Road
Princeton Junction, New Jersey 08550
1.800.556.6828
Fax: 1.609.799.7032
info@securetechalliance.org
www.securetechalliance.org

About Secure Tech Talk

Secure Tech Talk is the monthly e-newsletter published by the Secure Technology Alliance to report on industry news, information and events and to provide highlights of Alliance activities and membership.

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce and Internet of Things (IoT).