SECURE TECHNOLOGY ALLIANCE

MAY 2019

SECURE TECH TALK

A quarterly newsletter for members and friends of the Alliance

Executive Director Message

As mobile identity and mobile payments continue to advance, the Secure Technology Alliance will be at the center of the industry collaboration and education needed to guide those developments. The organization will also be driving awareness of the various use cases where mobile technology is fundamentally and rapidly changing the market. I encourage you to join this effort and help make the Secure Technology Alliance the organization at the center of change. Read more about advances in mobile technology in my letter this quarter.

Click to Read Letter ...

In This Issue:

On the Web:

Feature Article:

Industry Recommendations for Implementing PIV Credentials with Physical Access Control Systems

The National Institute of Standards and Technology (NIST) released a revision of NIST SP 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS) in June 2018. The Secure Technology Alliance and the Access Control Council developed a new resource, Industry Recommendations for Implementing PIV Credentials with Physical Access Control Systems: A Quick Guide to Implementing Essential NIST SP 800-116 R1 Requirements, to identify the essentials for a successful deployment of a physical access control system (PACS) that complies with FIPS 201. This article is an extract from the guide, focusing on industry recommended best practices for deploying PIV-enabled PACS.

Click to Read More …

Upcoming Event:

Securing Federal Identity 2019 – Limited Spots Open

We have a handful of spots available for Securing Federal Identity 2019, providing comprehensive coverage of efforts toward strong authentication technology, scheduled for June 4-5 at the Hilton Crystal City in Arlington, VA. New this year is an optional half-day add-on mobile identity workshop at the conclusion of the second day; the Mobile Identity Workshop will explore mobile drivers' licenses and the federal government's use of various mobile identity technologies solutions. Please note that this June 5th afternoon workshop is a separate event requiring separate registration; you can find all you need by visiting www.securingfederalidentity.com. If you would like to attend, register today to ensure your spot!

Click to Read More …

Spotlight on Government and Mobile Identity

Dear Members and Friends of the Alliance,

The Secure Technology Alliance will soon be shining a spotlight on the federal government and its use of interoperable, strongly authenticated digital identity credentials to secure access to critical resources and physical workplaces. The 16th annual Securing Federal Identity Conference will be held June 4-5 at the Hilton Crystal City hotel in Arlington, VA.

This year's agenda was designed with the changing digital identity landscape in mind. Increasing security threats, coupled with the need to enable secure multifactor authentication across multiple domains – and increased mobility – are stressing the limits of the current standards and identity policies. We're seeing new identity risks, innovations and challenges arising within the federal space, and we're bringing these topics to the forefront at this year's conference.

Attendees can look forward to insights from government and industry on the latest new policy documents and NIST publication revisions affecting federal identity credentialing and access security efforts that are underway and planned. New topics will look at the use of mobile identity applications, the impact on managing risk when data breaches expose privileged identity credentials, and government initiatives that are leveraging authentication technologies commonly used in commercial environments for federal use.

The issue of mobile identity and the prospect of storing digital credentials, such as state-issued mobile driver's licenses and derived PIV identity credentials for use on mobile devices, will be in the spotlight in a major way at this conference. Mobile identity is at a critical nexus where new standards are fueling pilots and initial implementations involving multiple states to use mobile versions of physical driver's licenses and federal government agencies applying new NIST 800-63-3 guidelines for federating use of credentials for authentication using existing platforms such as SAML, OpenID Connect, and FIDO.

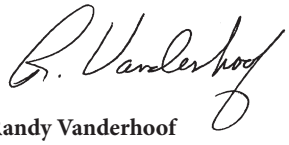
To explore these mobile identity topics more completely, the Alliance has organized an add-on Mobile Identity Workshop on the afternoon of the second day of the conference on June 5, to enable a deep discussion on mobile driver's licenses, mobile derived credentials, and mobile identity standards and best practices.

As mobile identity and mobile payments continue to advance, the Secure Technology Alliance will be at the center of the industry collaboration and education about advancing mobile application security and will be driving awareness of the various use cases where mobile technology is fundamentally and rapidly changing the market.

I encourage you to join this effort and help make the Secure Technology Alliance the organization at the center of change.

We hope to see you at the conference.

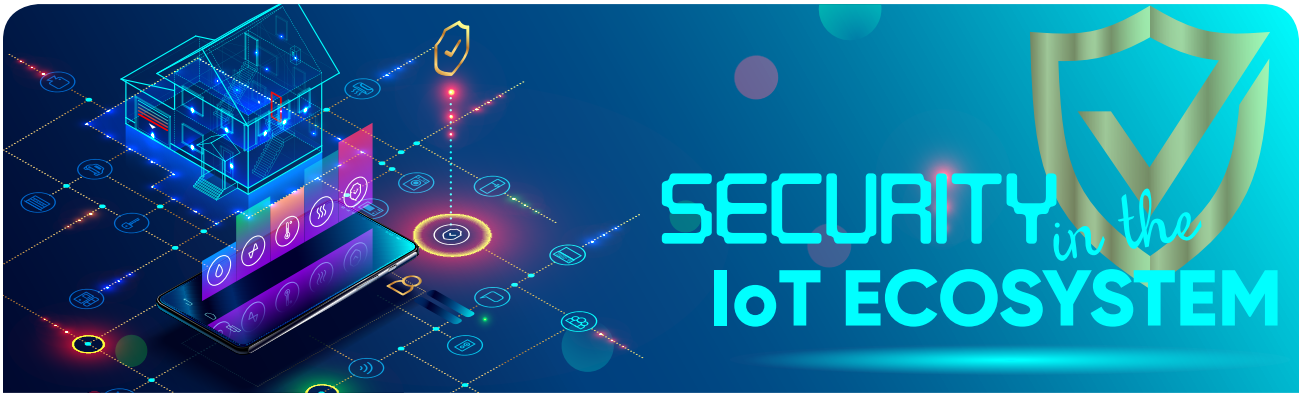
Sincerely,



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

Securing Federal Identity 2019 – Last Chance Registration

We have a handful of spots available for Securing Federal Identity 2019, scheduled for June 4-5 at the Hilton Crystal City in Arlington, VA. If you've not yet registered, take a minute to do so now. This highly focused, high-energy event will feature federal government identity, security policy issues and technology developments for today's federal agencies and federal market security leaders. Come participate, and learn what's new in the government efforts toward strong authentication technology using PIV credentials and mobile devices in government identity programs. This day and a half event will also feature our popular exhibit area. Join us in the best arena to learn, communicate and network with fellow government security industry colleagues.



Secure Technology Alliance Webinar: Security in the IoT Ecosystem

The IoT Security Council held a successful webinar series on key security topics for the IoT ecosystem.

The first webinar, The Role of PKI in IoT, described the role of PKI in securing the IoT ecosystem, with Josh Jabs, Entrust Datacard, presenting.

The second webinar in the series, Trusting Data at the Edge, presented by Sri Ramachandran, G+D Mobile Security, described the security requirements for trusting data collected and/or stored at the edge and discussed approaches for ensuring data integrity, privacy and authenticated access control and for managing data at the edge.

The webinar recording is available at: https://www.securetechalliance.org/security-in-the-iot-ecosystem-webinar-series/.

Individuals who participate in both webinar sessions (or listen to the webinar recordings) and complete and pass short online assessment quizzes will receive a certificate of participation from the Secure Technology Alliance. The deadline for completing the assessment quizzes is May 31st.

Updates from the Alliance Industry Councils

Secure Technology Alliance councils launched new projects, completed educational webinars and resources, and added new guidance for Federal government PIV identity credential implementation.

Access Control Council

- The Access Control Council completed a new resource, Industry Recommendations for Implementing PIV Credentials with Physical Access Control Systems: A Quick Guide to Implementing Essential NIST SP 800-116 R1 Requirements. The Council developed this guide to focus on the content of NIST SP 800-116 R1 Guidelines for the Use of PIV Credentials in Facility Access that provides the essential information required to successfully implement PIV cards with physical access control systems, without including discussion of how the card is made or how it works "under the hood." Council members contributing to the guide included ID Technology Partners; Integrated Security Technologies; Lenel; SigNet Technologies; U.S. Department of Homeland Security; XTec, Inc.
- The Council reviewed and developed comments on the Transportation Worker Identification Credential (TWIC®) NEXGEN specification
- The Council will be holding an in-person meeting on June 4th at the Securing Federal ID conference

Identity Council

- The Identity Council elected its 2019/2020 Steering Committee. Members elected to the Steering Committee were: David Coley, Intercede; Jatin Deshpande, G+D Mobile Security; David Kelts, IDEMIA; Tom Lockwood, NextgenID; Jeff Nigriny, CertiPath; Neville Pattinson, Gemalto; Steve Rogers, IQ Devices; Sridher Swaminathan, First Data; Rob Zivney, ID Technology Partners
- The Council is working on a new project to review the draft ISO 18013-5 mobile driver's license (mDL) specification and discuss use cases for the mDL
- The Council will be holding an in-person meeting on June 4th at the Securing Federal ID conference

Internet of Things Security Council

- The Internet of Things (IoT) Security Council held a successful webinar series with sessions on the role of public key infrastructure (PKI) in IoT and trusting data at the edge. Webinar recordings are posted on the Secure Technology Alliance web site

Payments Council

- The Payments Council published a new white paper, Biometric Payment Cards, to provide a primer on biometric payment cards for issuers, issuer processors, payment networks and merchants
- The Council is launching four new projects as a result of discussion at its well-attended in-person meeting at the 2019 Payments Summit. New projects are: biometric payment cards webinar; dynamic security code cards white paper; wearables white paper update; and open payments framework for electric vehicle charging

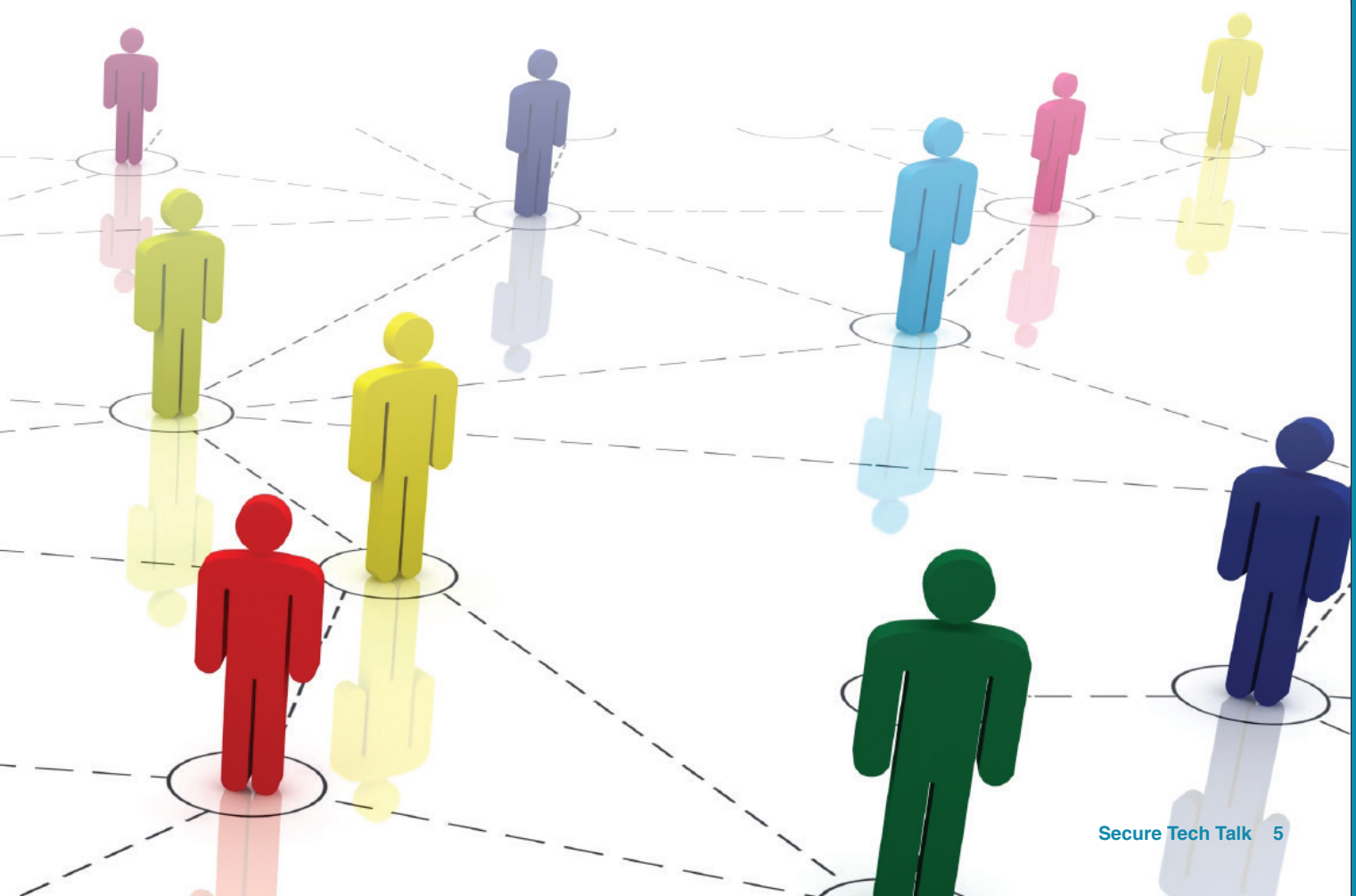
Transportation Council

- The Transportation Council is discussing its 2019 activities based on discussions at its in-person meeting at the 2019 Payments Summit. The Council will be expanding activities on multimodal payments for Mobility as a Service (MaaS) initiatives

Other Council Information

- Secure Technology Alliance members are now able to request guest participation in U.S. Payments Forum projects. The list of active Forum projects is available on the Alliance member web site. If you would like to participate in one of the Forum projects, please contact Cathy Medich. 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.



Industry Recommendations for Implementing PIV Credentials with Physical Access Control Systems

The National Institute of Standards and Technology (NIST) released a revision of NIST SP 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS) in June 2018. The revised document is called NIST SP 800-116 Revision 1: Guidelines for the Use of PIV Credentials in Facility Access. NIST SP 800-116 R1 covers the risk-based strategy to select appropriate PIV authentication mechanisms as expressed within Federal Information Processing Standard (FIPS) 201 and other related documents.

The Access Control Council developed a new resource, Industry Recommendations for Implementing PIV Credentials with Physical Access Control Systems: A Quick Guide to Implementing Essential NIST SP 800-116 R1 Requirements, to identify the essentials for a successful deployment of a physical access control system (PACS) that complies with FIPS 201. This article is an extract from the guide, focusing industry recommended best practices for deploying PIV-enabled PACS.

When deploying, agencies should:

- Follow the threat/risk assessment determination of the classification that applies to the entry point to each area (Controlled, Limited, Exclusion)
- Select PACS equipment that's included in the GSA Approved Products List and services from service providers with the Certified System Engineer ICAM PACS (CSEIP) certification
- Plan for how to accept high assurance credentials issued by other agencies

Rollout Considerations

Agencies moving towards FICAM-compliant PACS should consider the impact to the federal facility population when modernizing PACS assets. Installation of FICAM-compliant PACS solutions requires agencies to establish PKI authentication capabilities that are used when registering a PIV card to the PACS and when presenting PIV cards to card readers during physical access requests. Agencies implementing strong authentication for access control require cardholders to present their PIV or PIV-Interoperable (PIV-I) card to a card reader capable of performing a proper PKI challenge, based on the required factors of authentication.

A FIPS-201-compliant PACS implementation requires that all card readers support strong authentication and that all issued credentials contain the appropriate PKI certificates. Use of a "hybrid or mixed-mode" card reader is contradictory to FIPS 201 compliance by allowing the use of card products that do not support proper PKI authentication.

PIV Identifiers

The primary identifiers on a PIV card are the Federal Agency Smart Credential Number (FASC-N), Card Universal Unique Identifier (Card UUID), and the

> USE OF A "HYBRID OR MIXED-MODE" CARD READER IS CONTRADICTORY TO FIPS 201 COMPLIANCE BY ALLOWING THE USE OF CARD PRODUCTS THAT DO NOT SUPPORT PROPER PKI AUTHENTICATION.

Cardholder Universal Unique Identifier (Cardholder UUID). These identifiers are found in the PIV card CHUID data element and are typically stored in the PACS database when PIV cards are registered. Each PACS included in the GSA FIPS 201 Evaluation Program APL is capable of selecting and processing the correct identifier based on the card that is presented to the PACS reader.

PACS Registration

Registration of a PIV card can occur by two means:

1. Local single-card enrollment through the PACS solution enrollment
2. Bulk enrollment of cards through the use of the PACS product application programming interface (API) capability based on agency/enterprise authoritative identity management repositories and/or systems

The first mechanism can be used in any environment, allowing the PACS enrollment capability to harvest and validate card data as new cards are registered. The second mechanism, integration of the API, can be leveraged in an environment where an agency has an identity management solution. This API integration provides more instantaneous provisioning (or de-provisioning) as the card/cardholder identity data can be "pushed" to the PACS system or the identity data can be "pulled" from identity management services by the PACS through integrated automated processes.

Temporary Badges

Agencies considering the use of temporary cards for physical access need to define the use cases for temporary card issuance and usage. Currently there is no Federal guidance on this issue. Each agency must consider its own needs and policies for temporary badges. Agencies have considered, and some employ, high-assurance credentials such as PIV-I, Commercial Identity Verification (CIV), or Transportation Worker Identification Credential (TWIC) for temporary credentials where a PIV credential would prove expensive or impractical to issue to a range of cardholders.

The following groups can have a need for temporary badge/credential usage:

1. **Employees/contractors** who need to access the agency's facility, but who do not meet the PIV issuance requirements, such as only being employed for six months or less (per OMB M-05-24)
2. **Visitors** from other government agencies who are subject to local security policies to determine if a visitor who has a PIV credential issued by a different agency may use his/her PIV card for unescorted access to the visited site if properly registered and assigned authorization privileges. Students and the general public are usually provided an escort while visiting. Some agencies' security policies require issuing a temporary visitor badge that may be registered in a local PACS and used as temporary access credential. Each agency and location may have their own policies for visitors

When an employee's or contractor's PIV card is lost or stolen, it is considered compromised. Cardholders experiencing a loss or theft of the PIV card should contact the agency security department immediately, and the agency should perform a revocation of the PIV card, which includes revocation of the PKI certificates. In addition, the account associated with the PIV card should be disabled in the local PACS. Agencies that employ strong authentication and certificate validation practices can minimize risk, since the revocation of the PIV card's PIV Authentication and Card Authentication certificates will prevent the successful validation of a stolen PIV card during physical access attempts at a PACS.

The CHUID-Only "Authentication" Issue

The previous version of SP 800-116 included the CHUID authentication mechanism as an option for transitioning from Unrestricted to Controlled areas. The CHUID, however, is not included in SP 800-116 R1 as it has been deprecated, since the CHUID provides "little or no" confidence in the identity of the cardholder. New PACS implementations must support other approved authentication mechanisms (e.g., PKI-CAK), and older systems must be updated to comply with current requirements.

Agencies were directed in 2011 to PIV-enable their existing IT and PACS systems, or upgrade to new PIV-enabled implementations. (See OMB M-11-11.) Many agencies complied, but many of their PACS installations were based solely on CHUID-only authentication. These existing systems are at risk due to the ease with which the CHUID can be read by handheld devices and played back to the PACS. Handheld devices such as Android smartphones have demonstrated that they can easily be programmed to read the CHUID from PIV cards, store the CHUID, and play it back to PACS PIV card readers through the smartphone's Near Field Communication (NFC) contactless interface. This vulnerability negates the intent of HSPD-12 (e.g., resistance to cloning, forgery, alteration and terrorist exploitation).

The PKI authentication supported by the PIV card is superior to CHUID authentication. The use of CHUID-only authentica-

tion simply provides an identifier, and thus, cannot be considered an authentication mechanism. As a result, FIPS 201-2 has deprecated the CHUID-only mechanism.

Summary

The new Access Control Council guide enables the reader to more quickly grasp the required concepts in SP 800-116 R1 and apply the correct authentication mechanisms to their facility and access control use cases. An analogy is: NIST SP 800-116 R1 is a "dictionary;" the guide uses this dictionary to craft a story suitable for the unique needs of a PIV-enabled PACS solution implementor.

To simplify the process, implementors should define three progressive levels of security based on risk assessments:

- Begin with one-factor authentication for Controlled areas
- Progress to two-factor authentication for Limited areas, and
- Use three-factor authentication for Exclusion areas

After authentication mechanisms are determined, it is easier to scope the PACS configuration, procurement and implementation. This also assists in the process of defining acceptance tests performed to an agency's satisfaction.

About this Article

This article is an extract from the Secure Technology Alliance Access Control Council resource, Industry Recommendations for Implementing PIV Credentials with Physical Access Control Systems: A Quick Guide to Implementing Essential NIST SP 800-116 R1 Requirements. In addition to deployment considerations, the guide also includes detailed discussions of characteristics of PIV implementation, PIV authentication mechanisms in PACS applications and PACS use cases. Council members contributing to the guide included: ID Technology Partners; Integrated Security Technologies; Lenel; SigNet Technologies; U.S. Department of Homeland Security; XTec, Inc.

U.S. Payments Forum Resources

- The U.S. Payments Forum held the Contactless Open Payments for Transit webinar to review the benefits and challenges of contactless open payments in transit and to review the Forum-developed approach for transit acceptance of contactless cards and devices
- The U.S. Payments Forum held the EMV 3-D Secure Data Elements webinar that provided an overview of EMV 3DS and presented detail about the new EMV 3DS data elements
- The Forum launched the GetContactless.com web site to answer the most important questions merchants have about contactless payments, including: what are contactless payments? Why offer contactless payments? Are contactless payments as secure as contact chip card payments?
- The Forum's successful Mobile and Digital Wallet webinar series covered the market landscape, security technologies and strategic considerations for merchants and issuers
- The Forum white paper, PIN Bypass in the U.S. Market, was updated to add discussion of PIN Entry Bypass and No CVM limits on contactless transactions
- The Forum white paper, Understanding Fraud Liability for EMV Contact and Contactless Transactions in the U.S., was updated to provide up-to-date information on fraud liability shifts and add expanded content on counterfeit and lost-or-stolen fraud liability for contactless transactions

Alliance in the News

- "High-tech check-ins are fast and efficient — but who can access your information?" NBC News. Executive Director Vanderhoof comments on the importance of prioritizing security over getting new technology to market.
- "Contactless Card Transactions Could Overtake Taps from NFC Phones 'Quickly' in the U.S.: Industry Veteran" NFC Times. Executive Director Vanderhoof shares predictions for contactless card transactions and NFC-enabled wallet transactions in the coming years.
- "Secure Technology Alliance publishes white paper to explain biometric payment cards" Biometric Update. This story highlights an Alliance resource for card issuers, issuer processors, payment networks and merchants to explain the business case, impact, and considerations for deploying biometric payment cards.

Welcome New Member

- IDentity Check

Congratulations New Certificants

CSCIP

- Mark Vita, Department of State

CSCIP/P

- Oluseyi Ainenehi, UL
- Adam Ashbee, American Express
- Phillip Davidson, CPI Card Group
- Kyle Nahrgang, First Data
- Keith North, CPI Card Group
- Rebecca Speck, Discover
- Jerrin Thomas, UL
- Alex Zamaskov, Sole Proprietorship

CSEIP

- Glen Ballew, Security Install Solutions*
- Dustin Mastay, Security Install Solutions*
- Cameron Paul, Security Install Solutions*
- Ryan Todd, Security Install Solutions*

- Jared Wischkowski, Security Install Solutions*
- Dean Alcorn, Netsync Network Solutions
- Alexander Henry, Minuteman Security Technologies
- Thomas Kirchman, Signet Technologies
- Richard Mofor, Condortech Services
- Katherine Parker, Defender Security and Communication Company
- Joseph Peltier, Johnson Controls
- Russell Swartz, Security 101

CSEIP Recertified

- Brent Arnold, XTec, Inc.
- Jacob Cangelosi, Secure Mission Solutions
- Richard Case, Systems Engineering
- Susan Doherty, Security Install Solutions
- Jeffrey Drill, Communications Resource
- Edgar Freeze, Security Install Solutions
- Ken George, Caprock Consulting Group
- Brian Havekost, Signet
- Derrick Parker, Defender
- Blake Smith, Gallagher Group
- Collin Smith, Communications Resource
- Jefferson Tross, Versar
- Paul Wojdynski, Controlled Key Systems

**Denotes corporate exam. For more information, contact Randy Vanderhoof*

Upcoming Industry Events

Embedded Technologies Expo & Conference (ETC)

June 25-27, 2019
McEnery Convention Center
San Jose, CA
https://www.embeddedtechconf.com/

At this inaugural event, attendees will experience over 100 hours of education and training covering embedded systems, IoT, connectivity, edge computing, AI, machine learning, and more. **Secure Technology Alliance members – to receive $100 off Conference Passes and a Free Expo Hall Pass, use this promotional code when registering: STA100.**

Mobile Payments Conference

August 26- 28, 2019
Chicago, IL
https://www.mobilepaymentconference.com/

Global Security Exchange (GSX)

September 8-12, 2019
McCormick Place
Chicago, IL
www.gsx.org

Formerly the ASIS International Annual Seminar and Exhibits, Global Security Exchange (GSX) builds on a 65- year legacy of event excellence, uniting the full spectrum of security—cyber and operational security professionals from across the private and public sectors, allied organizations and partners, and the industry's leading solution providers—for the most comprehensive security event in the world. **Secure Technology Alliance members – to receive 20% off Conference fees, use this promotional code when registering: ASIS20DISC** (excludes workshop).

Money 20/20

October 27-30, 2019
The Venetian, Las Vegas
https://us.money2020.com/register

Money20/20 USA is the most anticipated Payments, FinTech and Financial Services event. It's the premier platform where the entire ecosystem unites to create and revolutionize the disruptive ways in which consumers and businesses manage, spend, invest, protect, share and borrow money.

Secure Technology Alliance members – save $250 at registration by entering this code: STA250

For complete details, visit https://www.securetechalliance.org/news-events/

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).