SECURE TECHNOLOGY ALLIANCE

MAY 2018

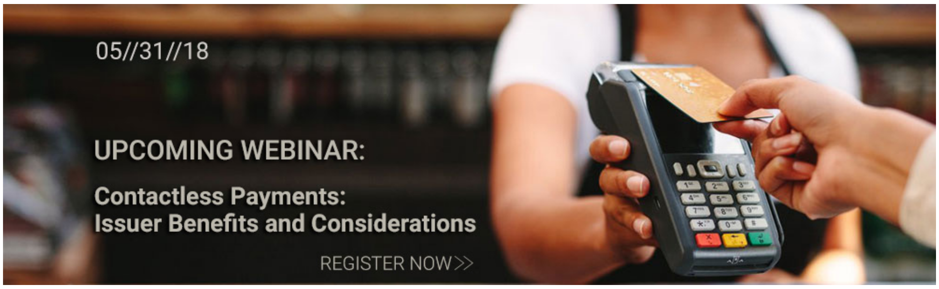
SECURE TECH TALK

A quarterly newsletter for members and friends of the Alliance

Executive Director Message

Next month's Securing Federal Identity 2018 Conference in Washington, DC is primed to focus on three main themes. I hope you join us in the discussion on the governing policies and specifications for establishing an individual's identity, the creation and management of the identity credential, and the use of those credentials for physical and logical access across the federal government enterprise. Learn more about the event **in my letter.**

Click to Read Letter ...



Feature Article:
EMVCo Payment Account Reference

The Secure Technology Alliance Payments Council produced a white paper entitled "EMVCo Payment Account Reference (PAR) 101: A Primer." This quarter's feature article is an extract of that white paper and provides a primer on the EMVCo PAR and documents expected use cases for the PAR.

Click to Read More ...

DIGITAL INNOVATION ALLIANCE
SECURE TECHNOLOGY ALLIANCE
LATIN AMERICAN CHAPTER

Latin American Viewpoint:
Developing A Digital Revolution

The Digital Innovation Alliance's goal is for every member to fully understand and partake in the expansion of the transformation of our society from electronic to digital, through professional, technological, business, social, and leadership development and participation in our training programs, council activities, and organized events. Learn more about this privilege and responsibility **in my letter this quarter.**

Click to Read Letter ...

In This Issue:

② Executive Director Letter >>
③ Latin America Letter >>
④ Feature Article >>
⑧ Council Reports >>

On the Web:

Alliance in the News >>

Members in the News >>

Upcoming Event:

Have You Registered? Securing Federal Identity 2018

There's still time to register for the two-day Government Conference scheduled for June 5-6 in Washington, DC. Securing Federal Identity 2018 will bring together the most influential thought leaders to address developments, innovations and updates in federal identity credentialing and access security. This Secure Technology Alliance event draws executives across government agencies and security and technology industries. The networking opportunities at the event are second to none in the identity, credentialing and authentication industry, and we encourage you to take full advantage of these valuable experiences. We look forward to seeing you at the Hamilton Crowne Plaza Hotel - Almas Temple next month.

Identity and Security Focus On Washington

Dear Members and Friends of the Alliance,

Lately, I have been spending a great deal of time reading and talking to others about identity and the business of managing digital identities in the lead-up to the Securing Federal Identity 2018 Conference, being held June 5-6 in downtown Washington, DC at the Almas Temple at the Hamilton Crown Plaza Hotel.

The central theme of the event, Identity management in computer security, is defined by Wikipedia as the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons." Depending on the nature of the resources in a given situation, that right to access is driven by some established rules that are put in place by the individual, organization, or government entity that has control over the physical or virtual space where the transaction is occurring.

The Secure Technology Alliance has deep roots in the identity and access security market, especially in the federal government, going back nearly 20 years, when the first Common Access Card (CAC) ID's were proposed by the Department of Defense. As the agenda comes into focus for this year's conference, much of the discussion remains centered on the governing policies and specifications for establishing an individual's identity, the creation and management of the identity credential, and the use of those credentials for physical and logical access across the federal government enterprise.

Because there is still much more to understand and new things to talk about, we decided to expand the program this year to two days. Day one will focus on the policies and guidelines that align with the new technical requirements for federal agencies implementing digital identity services, as well as cover identity proofing and user authentication. These publications define technical requirements for identity proofing, registration, authenticators, management processes, authentication protocols, and the federation of identities.

On the second day we'll look at procurement and implementation best practices, as well as the challenges facing government and industry in implementing identity management. Only recently has there been some progress by GSA in addressing the federal procurement contracting process and by NIST in completing the long-delayed update to the "Recommendations For Use of PIV Credentials in Physical Access Control Systems (PACS)" document (SP800-116). There will educational sessions on the use of derived PIV credentials on mobile devices and a cross government/industry panel discussion on use cases and lessons learned in planning, procuring, and deploying PIV-enabled PACS in federal agencies.

With an expected audience of 300-350 attendees (40% being government employees) and about 25 companies exhibiting their identity management and access control products and services, we are sure Secure Technology Alliance members and our federal government partners will benefit from the conference sessions, exhibits, and networking breaks planned for this milestone event.

I look forward to being there myself and making new contacts and renewing old acquaintances.

Thank you for your support of the Secure Technology Alliance.

Sincerely,

R. Vanderhoof

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

Developing A Digital Revolution

Dear Members and Friends of the Alliance,

The Digital Innovation Alliance's goal is for every member to fully understand and partake in the expansion of the transformation of our society from electronic to digital, through professional, technological, business, social, and leadership development and participation in our training programs, council activities, and organized events.

We have a great privilege and responsibility to reach out to the different sectors influenced by digital transformation. We are ready to prepare our members for this great task. Our educational programs equip members with the tools they need to be more effective communicators of the social, economic, and technological benefits of the digital transformation. Our members' technical background and market knowledge make them well-equipped to navigate the different sectors being influenced by this transformation – which also make them more flexible in adapting to the needs of clients around them. We hope members will build on their regional/global perspectives through the training, discussions, and outreach opportunities woven throughout our organization's initiatives.

Our wish is that members will be exposed to, and challenged by, the digital transformation through study and application of technologies within sectors. Member councils, industry outreach, and cutting-edge discussions are an important part of membership, and greater participation in our activities will assist member representatives with the challenges they may face, as well as with sharing industry best practices.

Learning about the impacts and opportunities of digital transformation is an active process and is the result of many different experiences. We understand that this vision of going from electronic to digital is not linear, but rather is multifaceted and dynamic. A higher order of thinking and forward-looking vision are critical for our industry to survive and flourish in the digital age.

I encourage you to take advantage of several resources that will assist you in understanding different technologies.

Professional and Technological Development

Tools available for members in this area include:

- Fundamentals and educational training
- Certified Smart Card Industry Professional – CSCIP certification
- White papers, industry reports, market studies and position papers

Business and Social Development

Members are encouraged to develop business, partnership, and collaboration opportunities within the Digital Innovation Alliance. This is what allows our members to provide non-partisan industry reports, case studies, and best practice resources. Tools available for members include:

- Networking activities
- Member and Council meetings
- Conference and industry events

Leadership Development

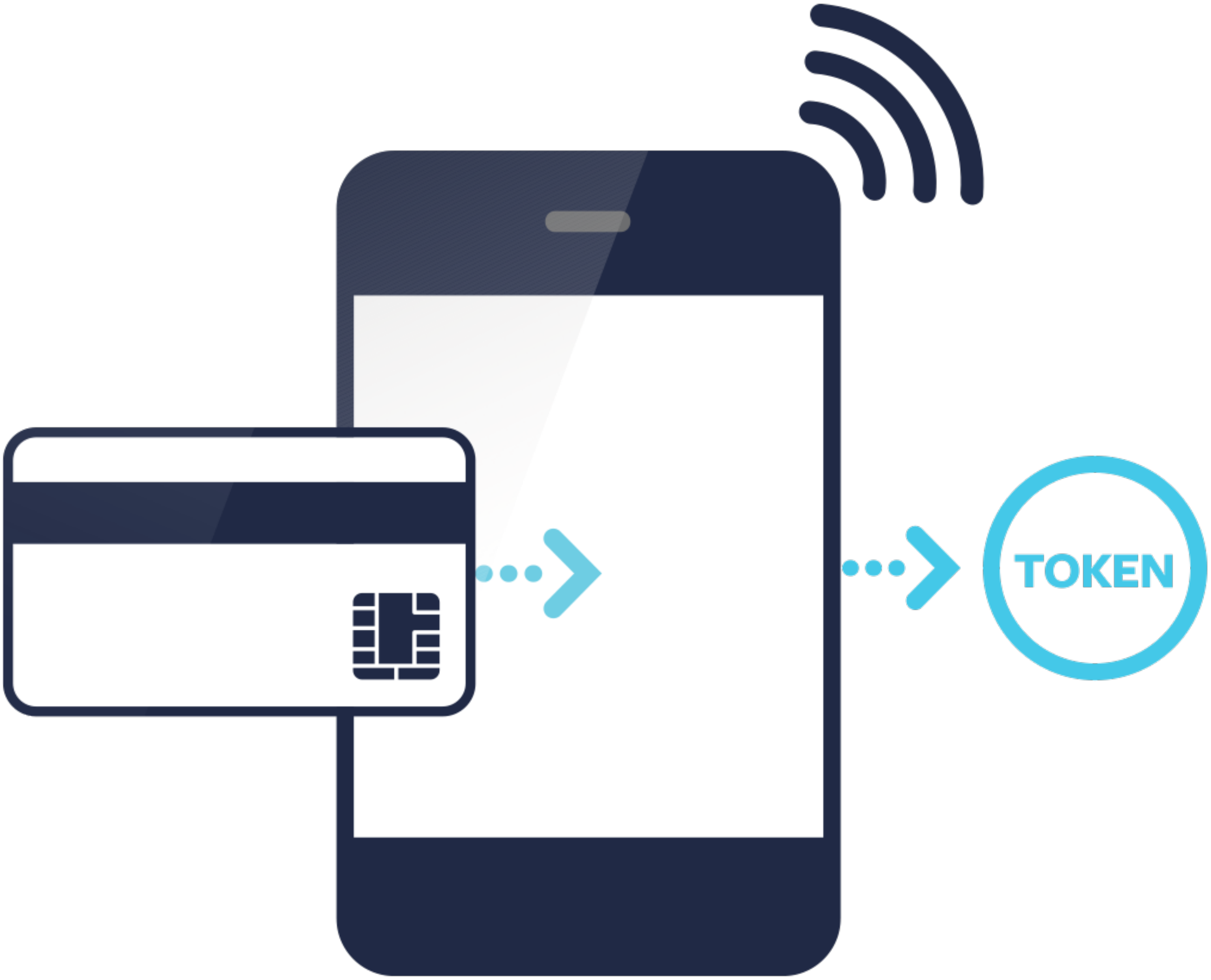
It is a long-held Digital Innovation Alliance belief that the greatest leaders are those who combine thought leadership with real-world expertise. As an organization we strive to provide members with a platform to showcase their solutions, transformative ideas, and products. These include:

- Speaking opportunities at industry-related events
- Development of impactful industry reports
- Exchanges with other thought leaders
- Cutting-edge discussions and industry outreach

We invite you to join our efforts and support the **Digital Innovation Alliance**.

Sincerely,

Edgar Betts
Associate Director
Digital innovation Alliance
ebetts@thedigitalalliance.org



EMVCo Payment Account Reference

The tokenization process in payment transactions replaces primary account number (PAN) data with a surrogate value. Use of the surrogate value, or *token*, provides increased protection against fraud and account data compromise by removing the PAN from potentially vulnerable parts of the payments environment. It is important to note that there are several types of tokenization models [1, 2, 3] such as acquirer tokenization, security tokenization, issuer tokenization and EMV® payment tokenization. [4]

EMV payment tokenization is the type of token that's used in mobile wallet transactions such as Android Pay, Apple Pay and Samsung Pay. While payment tokenization has improved the security of the payments ecosystem, it creates challenges for products and services that rely on the PAN to identify a customer's account (such as loyalty and rewards accounts), and for operational services related to a payment transaction (including customer care). For example, before payment tokenization, the PAN could be used to identify a customer's loyalty account. To address these challenges, EMVCo has introduced a new data element, called the Payment Account Reference (PAR). [5]

PAR Definition

The PAR is a non-financial reference assigned to each unique PAN and used to link a payment account represented by that PAN to affiliated payment tokens. PAR has a one-to-one relationship with the PAN and a one-to-many relationship with the payment tokens. Figure 1 shows how multiple payment tokens relate to a PAR and the PAN.

The PAR is a fixed-length, 29-character uppercase alphanumeric data element. The first four characters are a BIN Controller Identifier assigned by EMVCo to registered BIN controllers. The remaining 25 characters have unique values. The PAR value is designed to be unique across the global payments ecosystem. A BIN controller may generate the PAR itself or designate a third party, such as a payment network or other entity in the payment ecosystem, to generate it.

PAR data cannot be used to initiate financial transactions; no authorization, capture, clearing, or settlement message can be ini-

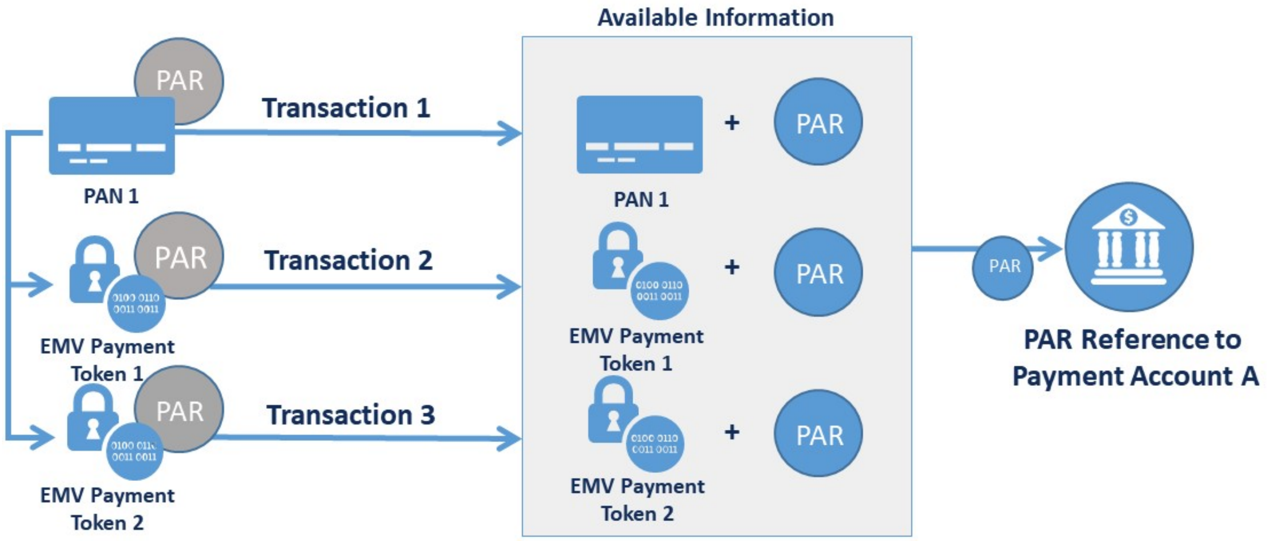


FIGURE 1. RELATIONSHIP BETWEEN MULTIPLE PAYMENT TOKENS, A PAR, AND THE PAN

tiated using a PAR. The guidelines for PAR use also indicate that a PAR value must be generated in such a way that it cannot be reverse-engineered to obtain a PAN or payment token. The PAR data structure is designed to ensure that PAR data cannot be confused with a PAN or payment token. When a replacement PAN is issued for an account, the BIN controller defines whether the PAR changes or remains the same.

Based on the EMVCo definition of PAR, the guidelines for PAR generation, and the intended functions for PAR, PAR data is not considered Payment Card Industry (PCI) account data and is not subject to the requirements for protecting PCI account data specified in the PCI Data Security Standard (PCI DSS). However, PCI DSS applies wherever PCI account data is stored, processed, or transmitted. Therefore, a system is subject to PCI DSS requirements if it stores, processes, or transmits PAR data and also stores, processes, or transmits account data (such as a PAN) or is connected to systems that store, process, or transmit account data.

Since payment tokenization replaces the PAN with a payment token, a PAN may not be available as part of the payment transaction data. In addition, there can be multiple payment tokens associated with a single PAN.

Without the PAN in the transaction, PAR provides the ability to identify and link the various payment tokens that map to the same PAN (without having knowledge of the PAN). The PAR data element is uniquely linked to a PAN; depending on how the issuer has set up their environment, a payment account may have multiple PANs, and therefore, each unique PAN will have its own PAR. An example use case is when PAR is generated, linked to a PAN, and then associated with all corresponding payment tokens when the PAN is tokenized. Other use cases are possible.

It is important to consider how PAR is implemented with payment accounts that have a primary account owner and authorized users that are all issued cards. If the additional cards have the same PAN, they will have the same PAR; if the additional cards have different PANs, they will each have a unique PAR.

PAR Use Cases

The absence of PAN data affects nonpayment use cases that rely on the PAN. Examples of use cases that would benefit from the use of PAR are loyalty programs, customer relationship management and transit open payments.

Loyalty Programs. Merchant-based loyalty programs traditionally rely on a dedicated loyalty card. The loyalty card is presented during a purchase to obtain points or rewards that can be applied to future purchases. Alternatively, certain merchants can recognize a customer based solely on the payment card used and not have a specific loyalty card. In some cases, loyalty accounts can be proactively linked to a specific payment card, or a merchant may choose to build a customer profile and provide rewards based solely on the payment card account. A PAR can be used to reestablish an effective payment-card-linked loyalty program and preserve simplified recognition of customers. The merchant can use the PAR to recognize a particular customer's PAN across multiple commerce domains and payment tokens.

Customer Relationship Management. Many merchants invest heavily in CRM programs. These programs include services such merchandise returns, customer service and support, and delivery of offers and promotions. Like loyalty programs, good CRM programs are not channel specific; they identify customers regardless of whether the customer is making a web, in-store, or mobile purchase. Multichannel CRM programs often rely on the card number used for the purchase to identify the customer. Card numbers help merchants quickly identify customers (or previous purchases made by a specific customer), providing improved service and ultimately

strengthening customer loyalty. The ability for customers to use multiple payment devices (such as smartwatches, NFC-enabled phones, and wearables) in place of a single payment card, combined with the introduction of payment tokenization, has created challenges for merchant CRM programs that rely on the PAN. The merchant can use a PAR to link a specific PAN and its affiliated payment tokens across multiple commerce domains.

Transit Open Payments. In a transit open payments system, riders can use an open-loop contactless product (e.g., a contactless bank card or a payment account credential used with an NFC-enabled mobile device) to access the transit system. In a transit system that accepts bank-issued contactless products as fare media at points of entry, the fare system must be able to identify each individual card or payment device (e.g., mobile phone, wearable). A transit system can use the PAR to link multiple cards or other devices with payment tokens that are linked to the same PAN, enhancing the rider experience and potentially enabling new transit products.

The use cases described are only examples. The BIN controller may define additional guidance on PAR uses in addition to those defined by EMVCo. Parties interested in implementing the PAR should check with the BIN controller for guidelines on allowable uses.

Conclusions

Payment tokenization was introduced to enhance the security of processing payments across card-present and card-not-present channels by reducing PAN exposure. While payment tokenization has improved the security of the payments ecosystem, it has created challenges for products and services that rely on the PAN. The PAR was defined by EMVCo to ensure

that payment processing and value-added services which currently rely on PAN can continue to be delivered seamlessly and reliably in a tokenized payment environment.

In order to realize the full potential of the PAR, however, it must be part of all payment interactions; all impacted stakeholders will need to support PAR data across all channels and across PAN and payment token usage. EMVCo specifications limit the use of the PAR to returns, chargebacks, fraud risk analysis, regulatory needs (such as anti-money laundering), and non-payment related purposes, as defined by the BIN controller. It is therefore important for service providers to avoid using the PAR beyond the scope defined by EMVCo and the BIN controller and be cognizant of local or regional regulations.

It is expected that many next generation payment devices will leverage payment tokenization. The PAR was designed to play an important role in providing the ability to link multiple payment tokens with a PAN. The Secure Technology Alliance recommends that all payments industry stakeholders become familiar with the PAR and assess how it can solve current challenges and support future requirements.

References

[1] Secure Technology Alliance, "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," white paper, October 2014

[2] EMVCo and Secure Technology Alliance, "EMV Payment Tokenization: What's New," webinar, November 16, 2017

[3] PCI Security Standards Council, "PCI DSS Tokenization Guidelines"

[4] EMVCo, "EMV® Payment Tokenisation Specification – Technical Framework," September 8, 2017

[5] "Payment Account Reference (PAR) (Spec Change)" EMV® Specification Bulletin No. 167, First Edition January 2016

About this Article

This article is an extract from the Secure Technology Alliance Payments Council white paper, "EMVCo Payment Account Reference (PAR) 101: A Primer." The white paper provides a primer on the EMVCo PAR, documents expected use cases for the PAR and describes the impact of PAR implementation on key payments ecosystem stakeholders. Secure Technology Alliance and U.S. Payments Forum participants involved in the development of this white paper included: American Express; Capital One; CPI Card Group; First Data; JPMorgan Chase; Mastercard; Metropolitan Transportation Authority (MTA); Rambus; Transportation District of Oregon (TriMet); TSYS; Visa.

Updates from the Alliance Industry Councils

Access Control Council

- The Access Control Council and Secure Technology Alliance Educational Institute completed the successful webinar series on PIV-enabled PACS implementation for government physical security specialists. The six webinars provide a comprehensive workshop covering all aspects of planning, procuring and implementing new PIV-enabled PACS. Recordings of all six webinars are available on the Secure Technology Alliance web site. Speakers in the series included: Mark Dale, XTec, Inc.; Tony Damalas, SigNet Technologies, Inc.; Daryl Hendricks, GSA; Michael Kelley, Parsons; Stafford Mahfouz, TYCO; Kevin Mitchell, GSA; Jason Rosen, U.S. Capitol Police; Mark Steffler, HID Global; Lars Suneborn, Secure Technology Alliance; Randy Vanderhoof, Secure Technology Alliance; William Windsor, U.S. Department of Homeland Security (DHS).
- The Access Control Council, in collaboration with the Identity Council, developed and submitted comments on the draft OMB M-18-XX "Strengthening Cybersecurity of Federal Agencies through Improved Identity, Credential and Access Management." Members contributing to the comments included: DHS; GSA; HID Global; ID Technology Partners; Identiv; Intercede; Lenel; NextgenID; Parsons; SecureKey; SigNet Technologies; Tyco/Software House; XTec, Inc.
- The Council has two active projects, implementing the electronic version of the GSA PACS playbook and completing the TWIC card/reader troubleshooting guide.
- The Council will be holding an in-person meeting at the Securing Federal Identity 2018 conference, June 5-6, in Washington, DC.

Health and Human Services Council

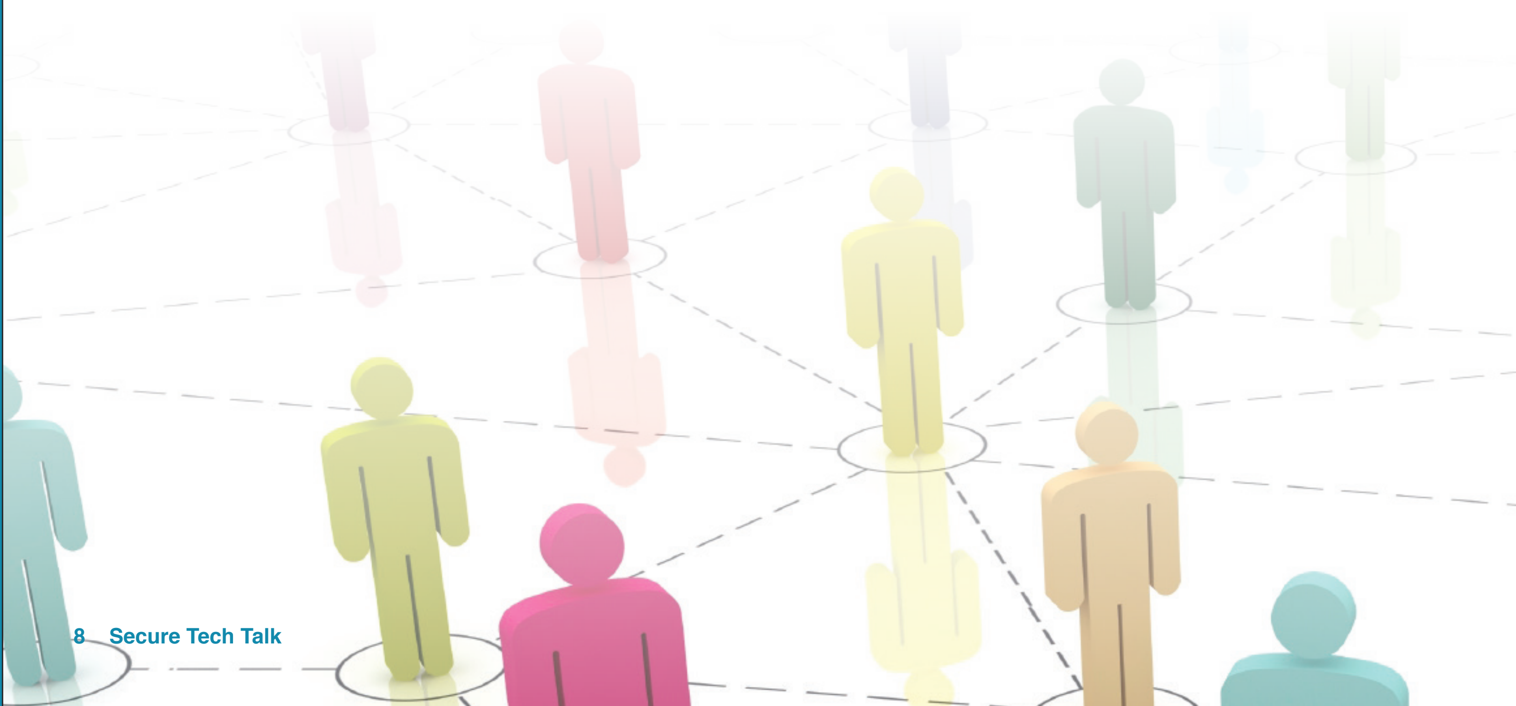
- The Health and Human Services Council has completed a survey on to get member input on healthcare-related activities and interest in Alliance Council project topics. The survey results will be used to develop the plan for the next Council activities.

Identity Council

- The Identity Council held the successful webinar, Identity on a Mobile Device. The webinar provided information for businesses looking to understand and accept mobile identity credentials and featured the mobile driver's license and derived PIV credential use cases. Webinar speakers included: David Coley, Intercede; David Kelts, IDEMIA; Tom Lockwood, NextgenID, Inc.; Geoff Slagle, AAMVA; Suraj Sudhakaran, Gemalto; and Randy Vanderhoof, Secure Technology Alliance.
- The Council collaborated with the Access Control Council to develop comments on the draft OMB M-18-XX "Strengthening Cybersecurity of Federal Agencies through Improved Identity, Credential and Access Management."
- The Council continues work on a white paper on the mobile identity landscape. The white paper will assess the market landscape, document use cases and identify best practices and requirements for industry.

Internet of Things Security Council

- The Internet of Things (IoT) Security Council completed and submitted comments on the NIST draft "IoT Security and Privacy Risk Considerations" document. Members contributing to the comments included: Entrust Datacard; Exponent; G+D Mobile Security; NextgenID; NXP Semiconductors; UL.



Mobile Council

- The Mobile Council published the new white paper, Trusted Execution Environment (TEE) 101: A Primer. The white paper describes the TEE as a candidate for a mobile security solution that supports a wide range of use cases, such as payment apps, content protection, corporate applications, and loyalty. Members and guests contributing to the white paper included: Discover Financial Services; First Data; GlobalPlatform; JPMorgan Chase; Mastercard; MIPS; Thales e-Security; Trustonic.

Payments Council

- The Payments Council published the new white paper, EMVCo Payment Account Reference (PAR) 101: A Primer. The white paper provides an educational resource on the EMVCo PAR, documents expected use cases for the PAR and describes the impact of PAR implementation on key payments ecosystem stakeholders. Members and guests contributing to the white paper included: American Express; Capital One; CPI Card Group; First Data; JPMorgan Chase; Mastercard; Metropolitan Transportation Authority (MTA); Rambus; Transportation District of Oregon (TriMet); TSYS; Visa.
- The Council is developing a contactless payments education webinar series for issuers and merchants. The first webinar focusing on issuer considerations is scheduled on May 31, at 2pm ET/11am PT, and the second webinar is being scheduled in June.
- The Council is starting to work on a new white paper on biometric payment cards. The white paper will provide a high-level description of biometric payment cards to educate issuers on functionality and benefits.

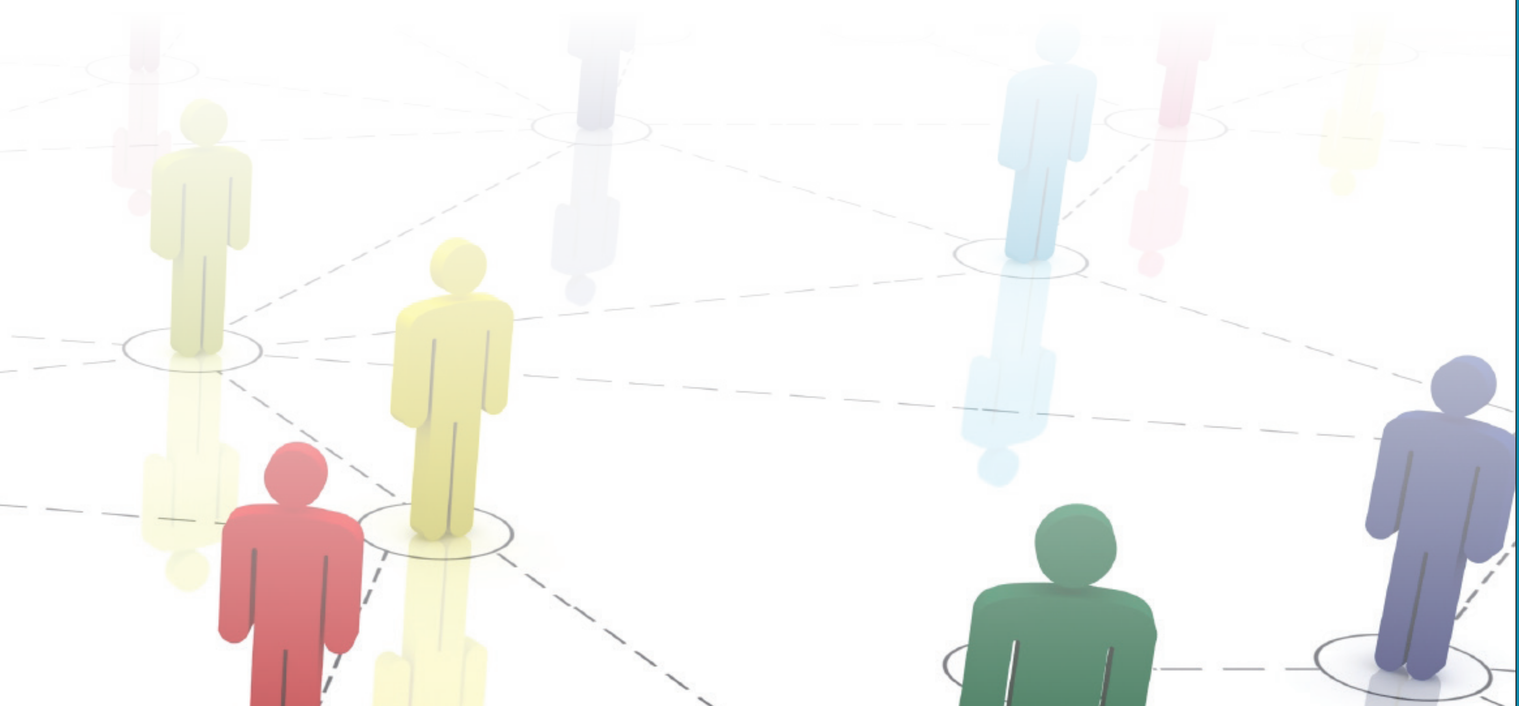
Transportation Council

- The Transportation Council currently has two active projects: a webinar on mobile ticketing and Near Field Communications (NFC); part two of the payments convergence white paper, focusing on potential barriers to implementation of multimodal payment strategies and suggesting ways of addressing these challenges.

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.



from the alliance office

New U.S. Payments Forum Resources

The U.S. Payments Forum (a Secure Technology Alliance affiliated organization) published several new industry resources on EMV and mobile payments.

The U.S. Payments Forum published the new resource, Merchant and Issuer Error Data Collection Forms. The forms were developed to assist issuers, issuer processors, merchants, acquirers and acquiring processors with gathering information in a consistent way with sufficient details to help determine the source of errors.

The Mobile and Contactless Payments Working Committee also published a new resource, Mobile and Contactless Payments Requirements and Interactions. The resource describes how mobile and contactless payments requirements are collected from mobile/contactless payments ecosystem stakeholders. The intent is to garner cross-industry understanding of mobile and contactless payments requirements and best practices and encourage standardization to meet common requirements.

New Certification Recipients

CSCIP/Government

- Brian Havekost, SigNet Technologies

CSCIP/Payments

- Sidhartha Chakrabarty, American Express
- Scott Corbridge, Community Transit
- Subhashini Golamari, ICPS Mauritius
- Robert Jensen, Community Transit
- Karin Searcy, TSYS
- Santhi Sista, Amazon
- Alan Whittemore, American Express

CSEIP

- Kenneth Becker, Integrated Access System*
- Paul Cabrera, S.E.G.
- Fred Conover, Structure Works
- Kristofer Fannon, PowerComm
- Jeremy Freeze-Skret, Prometheus Security Group Global
- Sean Harrison, LS3
- Kevin Houle, Identive*
- Henry Leahy, LS3
- Omar Lopez, LS3
- Tony Padilla, ALLCOM GS
- Brian Platenburg, GSA*
- Daniel Stafford, GSA*
- Kara Yosten, GSA*

**Denotes corporate group exam. To make arrangements for a group of employees to take a corporate exam, or for information on "On the Road" training, please contact Lars Suneborn at lsuneborn@securetechalliance.org*

Secure Technology Alliance In The News

- "Contactless II." Digital Transactions. Executive Director Randy Vanderhoof updates Digital Transactions on the status of contactless payments in the U.S., and shares his perspectives on the key considerations for adoption.
- "EMV payments in 2018: The state of the update." Retail Dive. This update on EMV in the U.S. features updates from the Secure Technology Alliance Payments Summit, and Executive Director Vanderhoof comments on the status of the migration.
- "Puttin' on Payments." Digital Transactions. In this article, Randy Vanderhoof explains why payments may "make or break" the adoption of wearables.

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).