SECURE TECHNOLOGY ALLIANCE

FEBRUARY 2018

SECURE TECH TALK

A quarterly newsletter for members and friends of the Alliance

Executive Director Message

It's been almost one year since the Secure Technology Alliance embarked on a broader mission that extends beyond smart card technology. The "new" Alliance has worked to become the digital security industry's premier association, bringing together industry providers and adopters to drive the adoption of end-to-end security solutions designed to protect privacy and digital assets in a variety of vertical markets. Read my letter this quarter to learn more about our expanded focus on other technologies and systems such as cryptography, tokenization, blockchain and trusted execution environments (TEEs).

Click to Read Letter ...

Feature Article:
Contactless Payments: Implementation Considerations for Issuers

In this rapidly evolving digital world, consumer expectations want payment to be faster, more secure, and seamless. This quarter's feature article explains how issuers can meet these changing expectations by offering contactless payments, and highlights some key recommendations for implementing contactless and Near Field Communication (NFC)-enabled form factors in North America.

Click to Read More …

DIGITAL INNOVATION ALLIANCE
SECURE TECHNOLOGY ALLIANCE LATIN AMERICAN CHAPTER

Latin America Letter:
A Digital Transition

How does someone become an influencer, or even an expert, on a specific topic? Our organization was founded on ensuring that credible industry experts have a platform to share their knowledge so that end users can trust that these representatives are explaining things in an objective, non-partisan manner. I write more about this, and the increasing emergence of others who claim to be "experts," in my letter.

Click to Read Letter …

In This Issue:

On the Web:

Upcoming Event:

PIV-Enabled PACS Webinar Series

The Secure Technology Alliance Educational Institute and Access Control Council are hosting the fourth webinar in a six-part series for systems engineers, facility managers, physical security personnel, and other government facilities' stakeholders on how to plan, procure and implement PIV-enabled physical access control systems (PACS) for government facilities.

The fourth webinar, "Developing the Procurement Strategy," is scheduled for Thursday, February 22, 2018, at 2pm ET/11am PT, and will discuss project responsibilities, standards, procurement vehicles, draft contracts, budgeting/funding, proposal evaluation and contract award. Registration is at: https://attendee.gotowebinar.com/register/4886117909279262210

Speakers include: Daryl Hendricks, General Services Administration; Kevin Mitchell, General Services Administration; Jason Rosen, U.S. Capitol Police; Lars Suneborn, Secure Technology Alliance, and Randy Vanderhoof, Secure Technology Alliance.

Recordings of past webinars and registration for upcoming webinars are available on the Secure Technology Alliance web site.

New Mission of Digital Security Takes Root in IoT-Enabled Smart Cities

Dear Members and Friends of the Alliance,

It's been almost one year since the Secure Technology Alliance embarked on a broader mission that extends beyond smart card technology. The "new" Alliance has worked to become the digital security industry's premier association, bringing together industry providers and adopters to drive the adoption of end-to-end security solutions designed to protect privacy and digital assets in a variety of vertical markets. Our goal in expanding our mission was to support industry activities and education on security technologies that protect data, enable secure authentication and facilitate commerce. Our activities now include secure chip as well as other technologies and systems such as cryptography, tokenization, blockchain and trusted execution environments (TEEs).

The digital security industry is composed of organizations involved in developing and implementing the technologies and systems needed to secure our identities, assets and transactions in the increasingly online and mobile world. The Alliance remains focused on promoting the adoption of secure digital solutions in payments, mobile, healthcare, identity and access, and transportation. Additionally, the Alliance focuses on emerging markets such as the Internet of Things (IoT) which, while in its infancy, has the power to change the way we live, work and travel, and requires similar strong security solutions.

Mature digital security industries like payments, mobile, access, and transportation have established proven implementation models that can be emulated, like EMV, Apple Pay, government-issued ePassports, and Chicago's Ventra transit card. The Alliance was active in its support of these markets to educate stakeholders and promote best practices to ensure security was built-in from the start.
New digital markets, like smart cities, autonomous vehicles, home healthcare devices, and smart home appliances, do not have the security legacy architecture to build upon. They lack the reference architectures to build secure systems based on replicable, scalable, and sustainable models that other markets have today.

This is where the Secure Technology Alliance can make a difference, but it can't lead this effort alone. I was happy to hear that NIST, the federal government standards body, has stepped in to fill this void. One example of this is the NIST Cybersecurity Framework, which was published in 2017 as a starting point for developers to better manage and reduce cybersecurity risk for critical infrastructure. A cybersecure network is essential for building secure IoT-enabled smart cities.

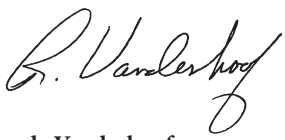
Another NIST initiative is the Smart and Secure Cities and Communities Challenge, organized with help from the Department of Homeland Security to bring together communities and industry leaders to form "action clusters" – local projects with specific areas of IoT focus like transportation, public safety, utilities, and wireless services that could become blueprints that can be replicated in other communities. By putting the proper emphasis on digital security early on, it is a promising sign that there could soon be scalable implementation models for these new markets.

There is much work ahead for Alliance member organizations before we can discuss smart cities in terms of the mature digital security we have with payments and other mobile technologies. Those of us who have been around the security industry remember when secure chips and embedded security were just starting to enter the U.S. market; today there are billions of secure cards and devices.

The Alliance will be at the center of the next big digital security revolution. We hope you stay for the journey.

Lastly, don't miss the next Secure Technology event – the 2018 Payments Summit, March 26-29 in Orlando. Visit www.stapayments.com to check out the agenda and exciting speakers we have lined up.

Sincerely,



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

Developing Industry Influencers

Dear Members and Friends of the Alliance,

As we progress more and more towards a digital society, something that has been making me uncomfortable is the history of trust and credibility. It seems that society no longer trusts traditional sources of information, and instead starts questioning the veracity of all their sources. With the introduction of new media platforms, we end up finding untested candidates presenting themselves as subject experts with little to no experience in the areas they're covering. Their literal presentation of themselves is what makes an impact, and in turn, people trust the information they deliver. What gets discarded are the traditional, reliable sources, who are overlooked, while these new "experts" take their place.

This is an issue that's impacted the subject matter from the Latin American and Caribbean chapter organization. While we gather audiences to listen about topics from our industry experts, many who have written white papers on those very topics, there are other instances where people claiming to be subject matter experts also gather paying audiences to listen to topics delivered by people with little understanding of the subject matter they claim to know.

I don't deny that with new technological capabilities and platforms, many can become well-versed on a subject. But over the past few months, I've seen a lot of "experts" who, with a little bit of knowledge, can persuade groups of people that their information is factual, which ultimately leads to misinterpretation and confusion about what is true.

Our organization was founded on ensuring that credible industry experts have a platform to share their knowledge so that end users can trust that these representatives are explaining things in an objective, non-partisan manner.

I do not mean to say that only we have the right answer. I do know it takes a joint effort, not a single voice, to continue to develop resources and generate credibility. These new platforms will allow us to better express our well-researched viewpoints, and we can ensure that we've delivered the correct information.

Our work is to make our members the new influencers, ensuring their messages are accessible and available. We want to groom these true subject matter experts into credible leaders, able to deliver their messages responsibly using the new platforms.

We welcome any of you that would like to work together to expand your visibility and access to information to join our Latin American chapter, the Digital Innovation Alliance.

Sincerely,

Edgar Betts
Director, Smart Card Alliance Latin America (SCALA)
ebetts@smartcardalliance.org
www.sca-la.org

Contactless Payments: Implementation Considerations for Issuers

We live in a rapidly evolving digital world—a world in which consumers are usually connected. This increased connectivity is altering consumer expectations. Consumers now want payment to be faster, more secure, and seamless. Issuers can meet these changing expectations by offering contactless payments. This article highlights some of the key recommendations for implementing contactless and Near Field Communication (NFC)-enabled form factors (such as cards, mobile phones, rings, and key fobs) devices in the North American market.

Issuers who are considering contactless payments face challenges unique to their role in the payments ecosystem. Issuers should consider the following:

- Contactless ROI
- Cardholder education
- Contactless POS infrastructure and acceptance
- Open loop contactless payments in transit
- Testing and certification
- Mobile contactless payment implementation

Contactless ROI

The financial viability of contactless cards has been proven by the success of dual-interface cards in Canada, the United Kingdom, and Australia, among other places. The data prove that contactless cards displace cash and drive increased transactions ("top of wallet" behavior). [1] For example, Visa has reported that European issuers in 2014-2015 saw 18 percent more transactions after issuing cards with contactless capability. [2]

Unlike other current contactless payment alternatives, such as Apple Pay, Samsung Pay, and Google Pay, contactless cards are controlled by the issuer, so the potential financial benefits to the issuer are numerous. Contactless cards do not depend on third-party apps for functionality. They offer a consistent user experience. The card requires neither a mobile device power source nor a mobile application. Additionally, contactless card technology is mature. Dual-interface cards are already in wide use for payment, while NFC-enabled mobile payments are still getting started. [1,3]

While there is a cost difference between contactless cards and EMV contact-only

cards, as dual-interface delivery volumes are increasing worldwide, costs are decreasing.

Recommendations: If required, engage with your payment network or other trusted sources to help develop the business case for moving to contactless cards or other contactless-capable devices.

Cardholder Education

Effective cardholder education and communication are essential to the success of a contactless launch. To encourage cardholders to activate and use the card or device right away, issuers need to:

- Highlight the benefits of contactless payment
- Explain how contactless payments work
- Reassure customers about potential security concerns
- Provide guidance on where contactless payment is accepted (for example, MasterCard provides a merchant locator application in most regions)
- Provide customers with consistent, frequent, multiphase marketing

Issuers should use multiple channels for conveying information, including:

- Effective staff training
- Inserts with card mailers
- National and regional media campaigns
- Marketing initiatives at selected merchants
- Joint programs with network operators or handset manufacturers for mobile payment products

In addition, issuers can create usage campaigns. Motivating contactless-enabled customers to activate and establish the tapping habit can be accomplished through usage incentives such as "tap and receive a promotion."

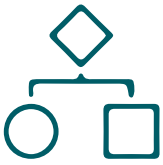
Markets that have already deployed these cards provide consumers with illustrations of the card being used at the POS. The illustration is included when the card is mailed to the customer. Television commercial campaigns sponsored in conjunction with the payment networks are also an effective tool for educating the public on the proper use of a contactless card. In addition, the card and POS terminal include standard contactless icons that indicate support for contactless transactions.

Recommendations. The figure below summarizes how to approach cardholder education.

HOW TO APPROACH CARDHOLDER EDUCATION

Make sure employees are fully trained, engaged with the rollout, and encourage customers to "tap and go"

Focus on making sure customers are aware of the contactless payment option and have a positive experience



Don't be afraid to fine-tune deployment based on lessons learned

Work with mobile ecosystem partners to address the particular implementation challenges of a new mobile device rollout

Contactless POS Infrastructure and Acceptance

Contactless acceptance is a major trend globally, with a significant percentage of POS terminals supporting contactless. The following are some key published market statistics:

- According to Juniper Research [4], 31.6% of all terminals in service in North America are contactless; North America accounts for 19.6% of the global installed base of contactless POS terminals
- Visa has reported that, as of September 2017, 40% of U.S. face-to-face Visa transactions today occur at contactless-enabled locations, illustrating that a growing percentage of merchants are enabling contactless [2]

While EMV-enabled POS terminals include EMV contactless capability, legacy magnetic stripe data (MSD) contactless terminals still represent a meaningful percentage of the contactless POS infrastructure in the United States. To provide cardholders with the best user experience, issuers should work with the payment networks and card or device personalization vendors to ensure that all EMV dual-interface cards and EMV contactless-capable form factors are backward compatible with MSD contactless terminals.

Recommendations: Merchant support for EMV contactless is expected to increase, as new EMV-capable terminals are installed and contactless device usage increases. Issuers should consider dual-interface EMV cards for the next wave of issuance, to offer their cardholders the benefits of contactless payment while enhancing their brand.

In addition, issuers should consider issuing dual-interface cards that are backward compatible with MSD contactless terminals until the issuer determines that the MSD contactless terminal base has reached an appropriate threshold.

Open Loop Contactless Payments in Transit

Transit agencies are moving, or considering moving, to open payments with next generation fare payment systems—that is, credit and debit payments made using contactless EMV devices at transit points of entry (e.g., at fare gates, on buses)— to supplement traditional closed-loop acceptance. Consumer use of contactless payments for transit can help drive incremental transactions and top-of-wallet status for cards.

Issuers contemplating transit as a factor in their contactless decisions should be aware that the specific timing for implementing transit open payments within a given region can have some uncertainty. In addition to the schedule impact of procurement and implementation timeframes, issuers should note that transit agencies interested in open payments may also consider the current state of contactless issuance and other relevant factors in their decision-making process. Other relevant considerations include the following:

- As the market for open payments in transit is still emerging, the content of the authorization/settlement messages sent from different agency back-end systems may not be consistent
- Transit merchants may require functionality that addresses transaction times and risk, such as offline data authentication (ODA) and/or deferred (or delayed) authorization [5]

The U.S. Payments Forum's Transit Contactless Open Payments Working Committee is developing additional information on transit-specific requirements as part of a resource series, which includes background information on why transit differs from a standard retail merchant environment and functional technical solutions for using contactless form factors to pay for transit.

Recommendations: Issuers should consult with the payment networks about the status of transit open payments initiatives, monitor transit agency programs and plans, and consider participating in ongoing industry dialogue such as the U.S. Payments Forum's Transit Contactless Open Payments Working Committee.

Testing and Certification

Each payment network has a unique contactless application specification that requires payment-network-specific test suites and particular certification processes similar to the EMV contact certification process. Apple Pay, Google Pay, and Samsung Pay NFC contactless payment applications that use tokens require additional testing and certification to ensure that the token and the ISO messaging are handled correctly. Most of the payment networks include mobile form factor testing as part of their profile certification processes.

Contactless also enables new form factors, such as wearables, that may require custom test suites and certification and that may be different for different payment networks. The wearable testing requirements can be addressed by the payment network, card vendor, processor, wearable vendor, or a third-party testing provider. The different form factors will follow the payment network's standard card profile validation process to confirm compliance with the respective brand requirements. [6]

Recommendations. There are existing well-defined testing and certification processes for contactless. Issuers should contact their testing partners or networks for further information on testing and certification.

Mobile Contactless Payment Considerations

CDCVM Support. Mobile payment devices perform contactless transactions in accordance with the relevant payment network specifications. The consumer device cardholder verification method (CDCVM) enables cardholder verification to be completed using the input and output options on a mobile payment device, with the CVM being verified on the device. The CDCVM can be specific to an individual card. When more than one card is digitized in the mobile payment application, there can be more than one verification method, with different values for each one.

Issuers or wallet providers can also use a wallet level CDCVM, where the CDCVM is specific to an individual wallet and all cards stored in the wallet share the same verification method. Another alternative is a device level CDCVM, which shares the CVM method among many applications on the mobile device. For example, the device unlock can be used as a CDCVM. Wallet or device level CDCVMs are referred to as "shared CVMs."

Currently, the U.S. common AID payment application is provisioned onto mobile phones when debit or prepaid cards in the U.S. are digitized into mobile wallets. Some networks may not currently support CDCVM with the U.S. common AID. Issuers should contact the payment networks for updates.

EMV Payment Tokenization. Tokens are replacing PANs in mobile phone-based payments and in other payment-enabled devices to enhance the security of the payments ecosystem. Tokens are not used by contactless or dual-interface cards at this time; however, they may be included in the future.

Recommendations. Issuers should consult with the payment networks for guidance on CDCVM and tokenization implementation. Issuers will need to work with their token service providers and trusted service managers to implement tokenization and comply with guidelines for token provisioning. [7]

Conclusions

As has been demonstrated outside of the U.S., contactless-enabled chip cards and devices can provide issuers with a competitive top-of-wallet advantage and deliver a faster checkout experience for their cardholders. The industry is simultaneously heading into the second wave of EMV chip card issuance and experiencing an expanding array of contactless-enabled devices, providing an opportune time for issuers to take advantage of contactless as the next generation of payment technology.

References

[1] "Contactless EMV Payments: Benefits for Consumers, Merchants and Issuers" white paper, Secure Technology Alliance, June 2016

[2] "Contactless in the U.S.," Visa, October 2017

[3] "An Issuer's Guide to Contactless Payments in the U.S." infographic, Secure Technology Alliance, January 2017

[4] Juniper Research: POS and mPOS Terminals 2017-2022

[5] "Technical Solution for Transit Contactless Open Payments Use Case 1: Pay As You Go/Card," U.S. Payments Forum, September 2017

[6] "Implementation Considerations for Contactless Payment-Enabled Wearables," Secure Technology Alliance, October 2017

[7] "EMV® Payment Tokenisation Specification – Technical Framework," Version 2, Appendix A, EMVCo, Sept. 8 2017

About this Article

This article is an extract from the Secure Technology Alliance Payments Council white paper, "Contactless Payments: Proposed Implementation Recommendations." This white paper was developed to discuss the challenges of issuing, accepting and processing ISO/IEC 14443/NFC contactless transactions and to help the market work through pre-EMV and post-EMV challenges to promote contactless issuance and acceptance. Secure Technology Alliance and U.S. Payments Forum participants involved in the development of this white paper included: American Express; Cardtek; CPI Card Group; Discover Financial Services; Fiserv; G+D Mobile Security; Gemalto; GlobalPlatform; IDEMIA; Infineon Technologies; Ingenico Group; Mastercard; Metropolitan Transportation Authority (MTA); MULTOS International; NXP Semiconductors; Philip Andreae & Associates; TSYS; Visa.

Updates from the Alliance Industry Councils

Access Control Council

- The Access Control Council and Secure Technology Alliance Educational Institute continue the successful webinar series on PIV-enabled PACS implementation for government physical security specialists. The second and third webinars, "Facility Characterization and Risk Assessment" and "Establishing the Project Scope," were held on November 30 and January 11, and featured Michael Kelley (Parsons), Mark Steffler (Quantum Secure), Lars Suneborn (Secure Technology Alliance), Randy Vanderhoof (Secure Technology Alliance), and William Windsor (DHS) as speakers. The fourth webinar, "Developing the Procurement Strategy," will be held on February 22.

Health and Human Services Council

- The Health and Human Services Council is developing a healthcare use case for the Identity Council mobile identity landscape white paper. The use case will describe a solution to patient misidentification and mismatching by using mobile tokens that allow all points of care to use technology more accurately to identify and assess a patient.

Identity Council

- The Identity 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. The Council is currently developing plans for a webinar to present several of the mobile identity use cases being developed for the white paper.

Internet of Things Security Council

- The Internet of Things (IoT) Security Council completed a member project priority survey and is starting two new projects. The Council is developing the statement of work for a project on IoT security risks, standards and best practices for IoT applications and is working on an industry response to a request for comments on the NIST "IoT Security and Privacy Risk Considerations" document.
- The Council has a new Steering Committee: Sandy Carielli, Entrust Datacard; John Neal, NXP Semiconductors; Sridhar Ramachandran, G+D Mobile Security; Christopher Williams, Exponent; Andrew Jamieson, UL. The Steering Committee provides overall direction for the Council, sets Council strategy, and approves project statements of work and deliverables

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.

Mobile Council

- The Mobile Council is working on one white paper – Trusted Execution Environment (TEE) 101

Payments Council

- The Payments Council published the new white paper, "Contactless Payments: Proposed Implementation Recommendations." This white paper discusses the challenges of issuing, accepting and processing ISO/IEC 14443/NFC contactless transactions and summarizes best practices to promote contactless issuance and acceptance. Secure Technology Alliance and U.S. Payments Forum participants involved in the development of this white paper included: American Express; Cardtek; CPI Card Group; Discover Financial Services; Fiserv; G+D Mobile Security; Gemalto; GlobalPlatform; IDEMIA; Infineon Technologies; Ingenico Group; Mastercard; Metropolitan Transportation Authority (MTA); MULTOS International; NXP Semiconductors; Philip Andreae & Associates; TSYS; Visa.
- The Council is working on one white paper, EMVCo Payment Account Reference (PAR) use cases, is collaborating with the U.S. Payments Forum on a white paper on approaches to secure the card-not-present environment, and is discussing project priorities for 2018.

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.
- The Council is also collaborating with the Federal Transit Administration (FTA) and the U.S. Department of Transportation/Volpe Center to hold a Smart Cities Multimodal Payments Convergence Forum later this spring.

Other Council Information

- The Mobile, Payments and Transportation Councils will be holding in-person meetings at the Payments Summit on March 27-28, at the Omni Orlando Resort at ChampionsGate. During the meetings, Council members will be discussing key industry challenges and planning projects for 2018. All Secure Technology Alliance members are welcome to attend the Council meetings.
- 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 Mike Strock. 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 Cathy Medich.

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 ATM Working Committee published a new white paper, EMV Troubleshooting Guide for ATM Owners and Operators, to provide recommendations to help ATM owners/operators prevent some common transaction problems, and offer suggestions for troubleshooting problems when they do occur.

The Testing and Certification Working Committee published an update to the white paper, EMV Testing and Certification: Current Global Payment Network Requirements for the U.S. Acquiring Community. The white paper includes up-to-date global payment network requirements and adds a new appendix on contactless EMV certification and testing processes.

The Mobile and Contactless Payments Working Committee published a new white paper, "Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions." The white paper provides guidance to merchants and financial institutions on models, technologies and usage drivers for mobile and digital wallets.

New Certification Recipients

CSCIP

- Crisanto Cafirma, American Express International
- Benedict Pang, American Express International

CSCIP/Government

- Brian Havekost, SigNet Technologies

CSCIP/Payments

- Durwoody Graddy, TSYS

CSEIP

- Rich Anderson, PSG Global
- Kenneth Butler, Williams Electric
- Phil Donatone, Williams Electric
- Jeffrey Drill, Communications Resource
- Eric Eddy, Johnson Controls
- Clinton Eppler, Cam-Dex Security
- Courtney Gant, Communications Resource
- Stephen Kellar, Defense Contract Management Agency
- Jorge Medina, Tyco Integrated Security
- Luke Pasqualucci, Communications Resource
- Cody Privette, Hunt Electric
- Kristoff Schlander, Tyco Integrated Security
- Collin Smith, Communications Resource
- Michael Smith, Surveillance One
- William Stewart, Convergint

Secure Technology Alliance In The News

"How to address PACS procurement challenges for government facilities," Security Info Watch. Executive Director Randy Vanderhoof shares insight on successfully implementing procuring and implementing compliant PACS systems in new and existing government facilities.

"The Truth about RFID Credit Card Fraud," CSO. This article provides an honest look at the likelihood of fraud using RFID technology, and Executive Director Vanderhoof encourages consumers to listen to their trusted financial institutions, the banks, and payments brands and believe them when they tell their customers that contactless payments cards are secure.

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).