SECURE TECHNOLOGY ALLIANCE

AUGUST 2017

SECURE TECH TALK

A quarterly newsletter for members and friends of the Alliance

EMV is the Medicine for What is Ailing Healthcare

It is now time for the healthcare payments transformation to begin. It has been more than 5 years since the banking and retail industry started making the transition to EMV after fraud levels reached "critical condition." Card sharing, forgery, and medical identity theft are stealing billions of dollars from our healthcare system. An EMV chip-enabled healthcare system opens the door for insurance companies to issue cards with the same EMV chip technology to strongly authenticate patients coming into medical facilities for treatment. My letter this quarter goes into more detail about the state of healthcare in the U.S., and offers some remedies. The newsletter also features updates on Alliance Councils, a profile of Leadership Council member First Data, a feature article on mobile identity authentication, and recent CSCIP and CSEIP recipients.

Click to Read Letter ...

Feature Article:
Mobile Identity Authentication: Securing Credentials

Users of online tools are familiar with the requirement for a user ID and password to access a variety of services. Although computer systems and services have evolved and become more widespread, there has been little change to the simple and reliable user ID-password requirement for user authentication, except perhaps for passwords to become more sophisticated. This quarter's article discusses the several security approaches currently used to secure credentials in mobile devices and highlights the advantages and disadvantages of each approach.

Click to Read More …

First Data®

Member Profile:
First Data

In this summer issue of the newsletter, Secure Tech Quarterly spoke with Kelly Urban, Director, Digital Commerce Solutions at First Data Corporation. Kelly helps lead the company's Integrated Token Solutions product team, specializing in the enablement of mobile payments. Since joining First Data in 1984, he has held various leadership roles in data center operations and data administration including technical client liaison, team manager, product development manager and director of product management. Kelly studied computer science at the University of Nebraska and business management, specializing in technology, at Bellevue University, also in Nebraska, where he lives.

Click to Read More …

In This Issue:

On the Web:

Upcoming Events:

IoT Payments 2017
October 10-11, 2017
Hyatt Regency Austin, Austin, TX
https://www.iot-payments.com/

Joint 2018 Payments Summit / ICMA Expo and U.S. Payments Forum Meeting
March 26-29, 2018
Omni Orlando Resort at ChampionsGate, Championsgate, FL
https://www.stapayments.com/

EMV is the Medicine for What is Ailing Healthcare

Dear Members and Friends of the Alliance,

The time has come for healthcare to embrace EMV for healthcare payments. As consumers slowly adjust to merchants using chip readers at their familiar shopping locations and pharmacies, why are patients still swiping cards for co-pays and deductibles at doctors' offices and medical clinics? A recent interview about healthcare payments shocked me. In the last few years, the percentage of medical bills that the average patient with health insurance was responsible for has increased from 5% to 40% of the bill. At the same time, the practice of family medicine has been replaced by specialists and medical centers and as a result, today's healthcare consumers might be receiving medical treatment from dozens of different doctors and patient billing systems.

As this goes on, healthcare insurance coverage for patients and reimbursements for providers has gotten infinitely more complicated. The increase is popularity of health savings accounts (HSAs) adds additional complexity for consumer payments and introduces a new payment card – the HSA debit card – into the mix. When and how that HSA card is used properly requires close attention from the consumer, because it is the consumer's money at risk. HSA cards look like regular bank cards but they don't have the same consumer protections in cases of fraud. Most HSA cards do not have EMV chips and still rely on magnetic stripes, making them easy targets for counterfeiters.

The convergence of all of these factors – higher volume of payments, increasing value of each transaction, multitude of different payments acceptance systems and office management systems, healthcare payments still processed using magnetic stripes with known security flaws are the same conditions that affected retail payments. It's also making the healthcare business ripe for massive fraud.

These are also the perfect conditions for re-examining the entire healthcare payments system. To use a medical analogy – the patient is showing all of the symptoms of a growing problem that needs to be treated before it gets worse.

This is why EMV is the medicine that healthcare needs – stat! The first step in fixing this problem is to replace the cheap, insecure mag stripe readers with new EMV chip readers. It will make paying in the doctor's office more secure for the patient and help make the office billing system more PCI compliant, while making it less of a target for hackers. If more offices had EMV chip readers, it would lead the banks to issue HSA cards with secure EMV chips on them. By the way, hackers aren't only interested in payment data from insecure mag stripe cards processed in doctor's offices; the personal healthcare information can be stolen and sold to identity theft brokers, so a total system security approach is paramount.

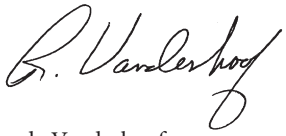
With an EMV chip-enabled healthcare system, it opens the door for insurance companies to issue cards with the same EMV chip technology to strongly authenticate patients coming into medical facilities for treatment. Card sharing, forgery, and medical identity theft are stealing billions of dollars from our healthcare system. Everyone is then penalized in the form of higher premiums and larger deductibles. Insured patients could PIN-protect their insurance cards and HSA debit cards so only the proper owner of the account can use them.

All of this security can be ported onto a smart phone or tablet as well, so patients can have one method to present their insurance identity, pay for services, and access their personal health information portal. They can review their medical records and see all of their charges as quickly and efficiently as receiving a paper receipt.

So now is the time for this healthcare payments transformation to begin. It has been more than 5 years since the banking and retail industry started making the transition to EMV after fraud levels reached "critical condition." Healthcare is already very ill and if it doesn't receive a shot of EMV medicine soon and start treating these problems I have described, healthcare payments may be on life support before we know it.

As a reminder, don't forget to mark your calendars for the IoT Payments 2017 Conference on October 10-11 at the Hyatt Regency – Austin hotel. Members can use their complimentary member pass for free admission to the event.

Sincerely,



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

Developing a Sense of Community

Dear Members and Friends of the Alliance,

We live in the most advanced time in history, where we are capable of connecting digitally with anyone, anywhere and establish a communication. Access to knowledge and content is unprecedented, yet we find ourselves more isolated, living in vacuums and physically disconnected from others.

People feel happier when they are able to share their thoughts, ideas, and be heard. If we think back through our own lives, all of our significant memories, such as celebrations, achievements, and joyful activities have been shared with people we value and respect in our community.

Companies too strive to provide communities for professionals to share ideas and knowledge that will generate growth in their professional well-being and capabilities. Sometimes friction is generated during open debates by people with different viewpoints. When this process is healthy, it sparks a respectful discussion.

I believe that diversity – of thoughts and ideas – is what allows us to learn from each other, innovate, or create positive growth.

SCALA's councils are snapshots of our community; diverse members discussing topics that sometimes reveal different viewpoints. Ultimately, we all need to find common ground. So when members talk about payments, identification, healthcare, smart cities, and biometrics, the objectives are to share experiences, knowledge and best practices, and not focus on who is a competitor or who is from a different region. We all want to learn, improve and see what more is possible.

SCALA, with the help of our members, aspires to build a community within various industries, where we can facilitate opportunities for members on convergence, interoperability, and innovative. We work with all market segments to help digital transformation, and we are proud to offer an open forum where organizations and individuals can gather to determine best practices and unite against adversity for the benefit of the industry and market sectors.

If you would like to be part of our community, participate in the discussions on the impact and opportunities that digital technologies will have in the market, we invite you to join SCALA. Please also take a look at our next event on Oct. 10-11 in Bogotá, Colombia – the eID Conference.

Sincerely,

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

First Data®

Kell Urban

In this summer issue of the newsletter, Secure Tech Quarterly spoke with Kelly Urban, Director, Digital Commerce Solutions at First Data Corporation. Kelly helps lead the company's Integrated Token Solutions product team, specializing in the enablement of mobile payments. Since joining First Data in 1984, he has held various leadership roles in data center operations and data administration including technical client liaison, team manager, product development manager and director of product management. Kelly studied computer science at the University of Nebraska and business management, specializing in technology, at Bellevue University, also in Nebraska, where he lives.

What are your main business profile and offerings?

First Data is a global leader in commerce-enabling technology and solutions, serving approximately six million business locations and 4,000 financial institutions in 118 countries around the world. The company's 24,000 owner-associates are dedicated to helping companies, from start-ups to the world's largest corporations, conduct commerce every day by securing and processing more than 2,500 transactions per second and $1.9 trillion per year.

What role does smart card technology play in supporting your business?

Smart card technology spans the entire breadth of First Data. Our Clover line offers industry-compliant POS devices supporting both contactless and contact chip cards. First Data also personalizes chip-enabled plastics for financial institutions. Additionally, we also process plastic card-based and mobile device-based chip-initiated financial transactions.

What trends do you see developing in the market that you hope to capitalize on?

My primary focus is mobile payments in the U.S., with an eye on my peers in the international markets. The number of products and services based on smart card/chip technology is growing, and I see several milestones and trends in this area.

- The introduction of a significant U.S. mobile wallet player in late 2014 was a watershed moment for Secure Element-based mobile wallets. Cloud-based payment methods, like HCE, will undoubtedly continue to grow, but the use of an SE in mobile payment products continues to support the chip-based model. Some mobile device manufacturers and wallet providers are even using a blended method of Secure Element and cloud-based credential management with a single device.

- It is good to see mobile devices enabled with NFC becoming the norm instead of the exception. The EMV liability shift in the U.S. has accelerated the distribution of NFC and contact acceptance devices. This moves both ends of the payment chain in the right direction to increase mobile payments usage.

- In general, chip technology is evolving faster than ever. Not only is the volume of available chips growing, but the capabilities of those chips are both more robust and more cost effective.

- Financial institutions are becoming increasingly nimble with regard to mobile payments. They are leveraging existing consumer contact points, like mobile banking, to enable payments. For these institutions, enabling payments from their mobile banking application is a clear next step.

- The use of tokenized payment credentials should continue to grow. Indeed, the entire payments ecosystem is moving to tokenization as a foundation instead of an add-on. Aside from all the technology and product advancements, I think the most important trend is increased consumer adoption as consumer knowledge about mobile payment functionality and security continues to grow.

What obstacles to growth do you see that must be overcome to leverage these opportunities?

A recurring challenge I see is the lack of industry cohesion, which makes the business case for mobile payments murky. For chip-based mobile payments it means tight control of critical components in the mobile payments ecosystem and pushes a big chunk of value to new/different players. The traditional value recipients are left scrambling. First Data's position as a global commerce enabler will allow us to help reduce some of those economic complexities for our customers.

On the issuing side, First Data created a method for separating the financial account number from the payment account number in 2002; a precursor to the common EMV tokenization term used today. TransArmor was introduced in 2010 to secure the merchant side of transaction data with encryption and tokenization. Industry and consumer expectations are growing around payment security. Perfect execution around security is a must. We will leverage our expertise in tokenization and encryption to ensure chip-based payments, whether they are initiated by plastic or a mobile device, are incredibly reliable and secure.

What do you see are the key factors driving smart card technology in government and commercial markets in the U.S.?

An important factor driving smart card technology is its ability to support a portable, secure, and standardized environment. Multifunction cards used for identification, authorization, and payments are on the rise and require a robust and well-developed platform. Payment products with integrated rewards/incentives also continue to grow. Whether embedded in plastic or in a mobile device, smart card technology is an ideal solution for all of these things.

Smart card technology includes arguably the best portable cryptographic engines anywhere. They are fast, tamper-resistant, and capable of creating complex cryptograms using industry standard interfaces.

How do you see your involvement in the Alliance and the industry councils helping your company?

The payments ecosystem is reliant on partnerships and cross-discipline relationships to innovate and evolve. My participation in the Alliance is a great way for First Data to stay informed about industry trends and allows me to facilitate face-to-face discussions with industry peers.

First Data is also active in several industry councils. The company prides itself in being a thought leader and uses the collaborative environment of the councils to both learn and teach.

What are some of the challenges you see confronting our industry?

Cloud-based services will undoubtedly continue to encroach on traditional chip-based services. There will likely come a time of equilibrium between the two technologies where each will hold a solid position in the market. Until that time, the industry may see the technology pendulum swing between the two, appearing to favor one over the other.

Mobile Identity Authentication: Securing Credentials

In today's increasingly connected world, users of online tools are familiar with the requirement for a user ID and password to access a variety of services. The requirement originates in the early days of computing, when systems needed a digital means to authenticate a user, and has now proliferated into every virtual relationship. Although computer systems and services have evolved and become more widespread, there has been little change to the simple and reliable user ID-password requirement for user authentication, except perhaps for passwords to become more sophisticated.

In addition, consumers are becoming more and more comfortable with online banking, investing, bill payment, and even education as systems that require strong security. Most corporate IT users are familiar with remote work access requirements and the complex encryption provided by virtual private network (VPN) systems. These systems have developed significantly more complex user authentication mechanisms as the risk of data breaches increases. Many of these mechanisms involve the need to change a password regularly, force the inclusion of special characters and numbers in a password, and use a secondary confirmation (e.g., a text message with a one-time passcode) to strengthen the authentication of the person at the other end of a remote connection.

However, the need for higher levels of security is at odds with users' desire for convenience when accessing their digital services. Asking users to develop and maintain ever increasing complex passwords, or regularly engage one-time passcodes, adds friction and potential frustration for the user.

Technology and solution providers in the mobile and digital security industries are quickly evolving techniques for digital authentication which offer a breakthrough in security while improving convenience. Mobile identity authentication approaches use a variety of technologies and architectures, with the security of storing user identity credentials a critical consideration in solution design.

When secured identity credentials are stored in a mobile phone, one key question is how to protect them. Although many experts may consider the mobile phone operating system (OS) to be more secure than a personal computer, it is still vulnerable. Best practices would require using proven, recommended security mechanisms that go beyond the security features native to a mobile phone's operating system.

This article discusses the several security approaches currently used to secure credentials in mobile devices and highlights the advantages and disadvantages of each approach.

Hardware Secure Element

One option for securely storing a mobile ID credential on a smartphone is to use a hardware secure element (SE). Credentials that are stored in an SE are protected using the same techniques that protect credentials on a physical chip card. These include both physical and software-based techniques.

The SE provides a root of trust that has specific production requirements ensuring protection of private keys. The SE also goes through a certification process that verifies the efficacy of its secure storage, access control, and cryptographic processors.

A hardware SE may be permanently soldered (embedded) in the smartphone or connected through a UICC or MicroSD. Whichever form factor is used, an SE in the smartphone is indirectly connected to the Internet. The potential for attacks is thus much higher than for attacks on a physical card, which can only be accessed if it is inserted into a contact reader or happens to be close to a contactless reader, and then only if the reader has been compromised. Therefore, it is necessary to limit access to the credential on the SE to authorized applications only.

GlobalPlatform® has standardized an SE access control mechanism. Support for this mechanism (or an equally secure alternative) should be a prerequisite for allowing any application running in the mobile operating system to access the secure mobile IDs stored on a smartphone.

Advantages

This approach has the following advantages:

- It is tamper-resistant, meaning that it recognizes and responds to both software and hardware attacks
- It can run cryptographic algorithms with hardware acceleration
- It can run multiple applications isolated through firewalls
- It can provide lifecycle management of card applications through secure channels
- Card-based applications can be migrated to the mobile SE easily
- Access from a Trusted Execution Environment (TEE) and mobile applications is well defined
- Compliance and certification programs are in place to ensure interoperability and conformance to specifications

Disadvantages

This approach has the following disadvantages:

- Memory in the SE is limited
- Lifecycle management requires trusted, secured systems
- Access to the storage space and lifecycle management requires business relationships

Trusted Execution Environment (TEE)

Another option is to store credentials in a TEE. A TEE is an execution environment that runs alongside the smartphone operating system (the rich OS). A TEE provides security services and isolates access to its hardware and software security resources from the rich OS and associated applications. In this way, a TEE can protect the mobile ID credential from threats that are potentially present in the rich OS.

A TEE implementation can leverage techniques such as encryption, tokenization, and code obfuscation to further strengthen the protections provided by the core TEE architecture.

Advantages

This approach has the following advantages:

- It uses mobile device memory secured by a dedicated cryptographic processor
- It is accepted by the Android OS and several standards groups (e.g., oneM2M, FIDO)
- Keys can be stored in the SE or other hardware-based secured system (e.g., UICC)
- There are defined specifications for a trusted user interface and secured storage.
- GlobalPlatform® has a certification program that certifies TEE security mechanisms

Disadvantages

This approach has the following disadvantages:

- The trusted application execution environment is a restricted environment, and access usually requires business relationships
- Lifecycle management requires trusted, secured systems

Host Card Emulation

The latest versions of the Android operating system support host card emulation (HCE). HCE is covered in this section because it allows secure credentials to be stored in several different ways, for example, via a cloud service, or in conventional memory on the mobile device. However, the reader should be cautioned that HCE is NOT a security mechanism. HCE implementations simply allow NFC commands to be routed to an application running in the smartphone OS rather than being routed directly to an SE. Use of HCE does not define where credentials and sensitive data are stored nor how they are processed. Nor does HCE provide or specify any security techniques, so security must be implemented on top of an HCE implementation.

It is recommended that any HCE-based mobile ID application leverage additional techniques such as encryption, tokenization, code obfuscation, or white box cryptography. Risks can also be reduced using system-level countermeasures. Back office systems should be designed to detect fraud by tracking transaction details, such as the phone's location, and looking for irregularities. HCE applications can also be implemented using an SE or TEE to enhance security. These approaches, along with similar traditional approaches, can reduce the risk of securing credentials in an HCE implementation.

Advantages

This approach has the following advantages:

- No special access control is required. The credential is stored in the mobile device's main memory.
- HCE is supported by Android OS, with similar approaches available for Windows Phone and Blackberry.
- Updates and modifications to a credential or any supporting application can be deployed rapidly and remotely.

Disadvantages

This approach has the following disadvantages:

- Security is not provided as part of HCE
- An application is installed with keys that are exposed to the rich OS
- Credentials are less secure when they are stored in a phone's main memory
- Applications need to have their own security mechanisms, which may be more vulnerable to attack

Summary and Recommendations

The best choice for secure storage of mobile identity credentials on a smartphone can depend on the specific requirements of the use case and the degree to which system-level countermeasures can be effective.

Storage in a hardware SE assures that the credentials are stored securely on a mobile handset in a consistent manner across various handset hardware and operating systems. However, several parties are typically involved in managing access to the SE. Using a TEE can reduce the complexity involved in accessing a secure storage location and managing applications. Using HCE involves assessing security and developing on-device security measures, which must be balanced against factors such as cost, time to market, and scale of interoperability.

Depending on the risk profile of a typical mobile identity credential, the recommended approach to storing mobile identity credentials on smartphones is to leverage the stronger security found in using SE and TEE implementations. HCE implementations should at a minimum use tokenization and store encryption keys in either the SE or TEE.

About this Article

This article is an extract from the Secure Technology Alliance Mobile Council white paper, Mobile Identity Authentication, published in March 2017. The white paper provides an educational resource on mobile identity authentication techniques and use cases. Mobile Council members contributing to the white paper include: Capgemini; CH2M; CPI Card Group; Discover Financial Services; Entrust Datacard; First Data; FIS; Giesecke & Devrient; GlobalPlatform; HID Global; ID Technology Partners; Intercede; IQ Devices; JPMorgan Chase; Oberthur Technologies; Paygility Advisors; SHAZAM; TSYS; Vantiv; Verifone; Wells Fargo.

Updates from the Alliance Industry Councils

Access Control Council

- The Access Control Council completed the development of a PACS deployment playbook for the GSA CIO. Member contributing to the project included: DMDC; G+D Mobile Security; GSA; ID Technology Partners; Identiv; IQ Devices; Leidos, Inc.; Lenel; Parsons; Quantum Secure; XTec, Inc.
- The Access Control Council The Council is currently developing the statement of work for a series of educational webinars on implementing PIV-enabled PACS and is updating its charter to align with the revised focus and mission of the Secure Technology Alliance

Health and Human Services Council

- The Health and Human Services Council updated its charter to align with the revised focus and mission of the Secure Technology Alliance
- The Health and Human Services Council has two active projects: the Client Advisory Board; a webinar based on the concepts in the Healthcare 2.0: A New Paradigm for a Secure and Streamlined Healthcare Industry infographic published in 2016.

Identity Council

- The Identity Council is working on a new 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 is working on a new white paper on IoT and payments. The white paper will outline best practices for implementing payments with IoT devices as guidance for developing IoT applications that will include payment

Mobile Council

- The Mobile Council is working on two white papers – mobile profiles and provisioning; Trusted Execution Environment (TEE) 101

Payments Council

- The Payments Council is working on four white papers: EMVCo Payment Account Reference (PAR) use cases; EMV contactless challenges for issuers, merchants and processors; best practices for implementing payments with wearables; and approaches to secure the card-not-present environment

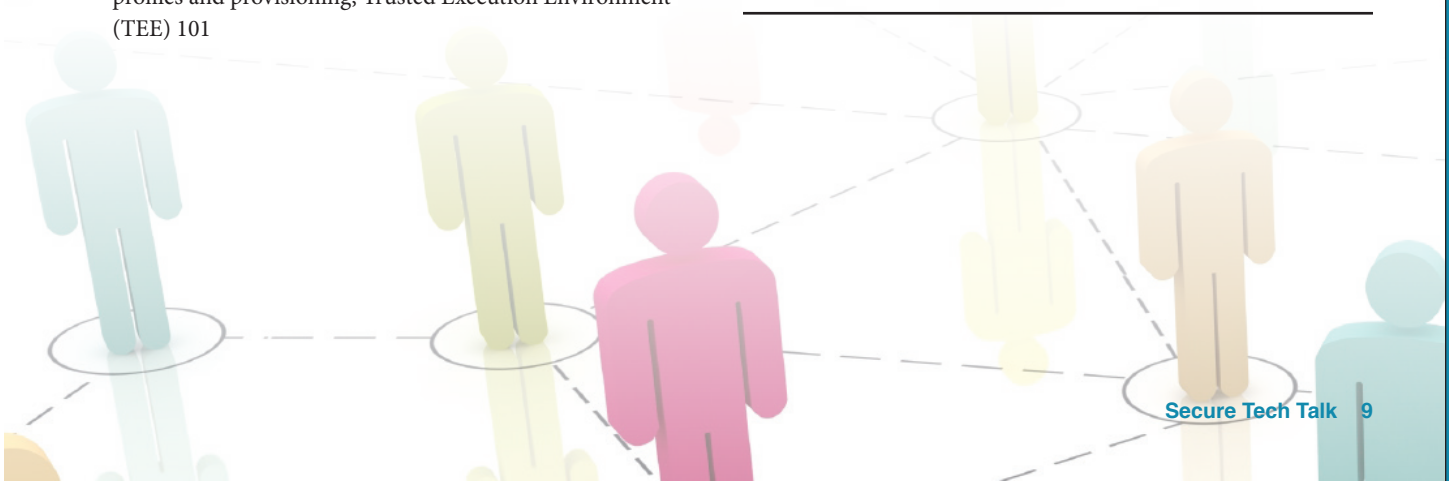
Transportation Council

- ponsored a panel on EMV and parking at the International Parking Institute (IPI) conference in May, with both IPI and Secure Technology Alliance speakers. Members contributing to the panel included Mastercard and Visa
- The Council currently has three active projects: a new 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; and an in-person workshop being planned for this fall
-

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 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.

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.



New Certification Recipients

CSCIP

- Maziya Mavvaj

CSCIP/Government

- Kevin Campbell, XTec
- Michael Casey, CertiPath
- Dan Currie, Department of National Defense
- Sok Bonn Dong, XTec
- Francisco Yuan, National Defense Canada

CSCIP/Government

- Rebecca Jackson, XTec*
- Michelle Wilson, U.S. Department of State

CSCIP/Payments

- Lokesh Rachuri, Capgemini
- John Xie, Foothill Transit
- Ahmad Husaini Ahamed Zakeri, Malaysian Electronic Payment System

CSEIP

- Jason Adams, U.S. Marshals Service
- Neil Bolin, CertiPath
- Michael Casey, CertiPath
- Eric Johnson, Volta Systems Group
- Jacon Knoll, Global Enterprise Technologies
- Robert Krecker, Booz Allen Hamilton
- Mark Meredith, U.S. Marshals Service
- David Raymond, Trofholz Technologies
- Bruce Riddle, Environmental Protection Agency
- Rob Weaver, Stanley Black & Decker
- Brandon Welling, ASI

Denotes corporate exam. For more information, contact Lars Suneborn

Secure Technology Alliance In The News

"P2PE's role with merchants shifts after EMV," PaymentsSource. Executive Director Randy Vanderhoof tells PaymentsSource that merchants should implement layered security technologies to protect payments across a variety of channels, such as in-store and online.

"Securing Federal Identity event features best of government ID and security," Secure ID News. In this article, Secure ID News highlighted the 'don't miss' sessions leading up to the 2017 Securing Federal Identity conference that was held in Washington, D.C. in June.

"14 Things Small Business Owners Need to Know," Small Biz Daily. With the 2017 IoT Payments conference coming this October, Executive Director Vanderhoof tells Small Biz Daily what to expect at the show, including updates on the most important developments, innovations and efforts driving secure, seamless IoT payments.

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).