Smart Card Alliance

Smart Card Talk

A quarterly newsletter for members and friends of the Smart Card Alliance

November 2014

Looking to the U.S. for Partnerships in Payments

Many Smart Card Alliance members make the annual journey to Paris to mingle with our European and Asian industry colleagues at the international Cartes Secure Connexions conference every November. For the first time in twelve years I was not one of them. There was another option to choose here in the United States, a relatively new event called Money 2020, which I attended. I write more about the success of Money 2020 in my letter in this quarter's Smart Card Talk newsletter, the last of 2014. (The Annual Review will be published next month.) We also have an update on Alliance Councils, a member profile on Giesecke & Devrient, new CSCIP recipients, and more. Thank you for your interest in the Smart Card Alliance.

Sincerely,
Randy Vanderhoof
Executive Director, Smart Card Alliance

Click to Read Letter ...

Feature Article:
Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization

Payments industry stakeholders are looking at many security technologies to protect their businesses and customers from fraud. This month's article describes EMV, encryption and tokenization and outlines how a layered security strategy using all three technologies is the right approach for securing payment card transactions.

Click to Read More …

Giesecke & Devrient

Member Profile:
Giesecke & Devrient

For the final quarter of 2014, Smart Card Talk spoke with Brian Russell of Giesecke & Devrient (G&D), a privately held, international corporation headquartered in Munich, Germany. The company was founded in 1852, and has over 50 subsidiaries in 32 countries. G&D is the leader in North America for RFID contactless, EMV and transit card manufacturing.

Click to Read More …

In This Issue:

② Executive Director Letter >>
③ Latin America Letter >>
④ Member Profile >>
⑥ Feature Article >>
⑪ Council Reports >>

On the Web:

Alliance in the News >>
Members in the News >>

Smart Card Alliance Events

Smart Card Alliance Member Meeting
December 7-9, 2014
Rosen Shingle Creek, Orlando, FL

Smart Card Alliance 8th Annual Conference 2015 Payments Summit
February 3-5, 2015
Grand America Hotel, Salt Lake City, Utah

All Upcoming Smart Card Alliance Conference Events

Looking to the U.S. for Partnerships in Payments

Dear Members and Friends of the Alliance,

Normally the month of November marks the time when many of our Smart Card Alliance members make the annual journey to Paris to mingle with our European and Asian industry colleagues at the international Cartes Secure Connexions conference. However, for the first time in twelve years I was not one of them. There was another option to choose here in the United States, a relatively new event called Money 2020, and I am very glad I chose to stay closer to home. Considering the large showing of over 7,000 mostly American attendees in Las Vegas, I was not the only person who made the same choice.

Perhaps it was the fact that payments has taken on enormous importance here in the United States, fueled by the active migration to EMV chip technology, now entering the critical final stretch to the fraud liability shift date in October 2015. Maybe it had to do with Apple's recent announcement of Apple Pay – which leverages a secure element-based NFC solution and is backed by the number one consumer brand with 40% of the U.S. market share– that has restarted a vociferous discussion about the future of NFC mobile payments. Those two major developments alone were motivation enough to stay close to home this time. More so, I believe there is a realization that the changes brought on by EMV migration, the mobile digital revolution in payments, and the urgency for change brought on by massive data breaches and regulatory scrutiny that followed have made the United States the center of the payments world, not Europe.

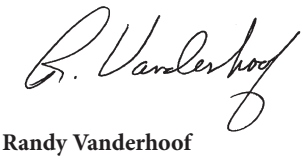
The Smart Card Alliance/EMV Migration Forum was still present at the Cartes Paris event. Cathy Medich led an excellent EMV panel including MasterCard, American Express, and Verifone that was attended by about 60 people, attendance that is typical for this event which draws many more people to the exhibition hall than to the conference sessions. However, in contrast, I spoke on a panel at Money 2020 discussing EMV, encryption, and tokenization that drew an overflow crowd in a room that seated 500 people. And I was told there were several hundred people who were turned away and watched it being broadcast on large screens in the outer hallway. This was with four other track sessions running currently with ours! That level of interest tells me that our U.S. bankers, merchants, processors, industry suppliers, consultants, and integrators see an urgent need to match payments technology and solutions to their needs, and they are looking within this country for those partnerships.

And there were hundreds, perhaps thousands, of technologies and services represented in Las Vegas. The Money 2020 show is where the payments establishment meets the payments disruptors in a cultural mashup of new ideas and new thinking that are being tested against proven business models and brands. A highlight for me was listening to keynote speakers from the most recognized companies in global digital market, such as Amazon, PayPal, Facebook, Verifone, American Express, Visa, and Discover. These speakers talked about how they are opening up their companies to new ways to transact and introducing innovative consumer experiences that are going to be faster, easier, and better than what exist today. "Digital transactions at the speed of life" was one catchphrase that captured the tone. For every Silicon Valley venture-capital-funded idea presented that professed to be the next mobile innovation or consumer shopping breakthrough, there was an established brand offering their own vision and claiming they will innovate and do it better. It was hard to differentiate the inventions from the innovations. Inventions are new ways to do things, but innovation is taking inventions and making new things work better. For every thousand inventions in the mobile and digital commerce space, there are only a few real innovations.

As a walked the crowded halls of the biggest mobile and digital payments conference the U.S. has ever seen, I was approached by dozens of people who know me from my many years with the Smart Card Alliance and now the EMV Migration Forum, or who listened to my panel. I even have a new cartoon celebrity image of myself thanks to Money 2020. The cartoon characterization of me will remind me not to take myself too seriously, yet I have never been happier to not be in Paris in November. I feel privileged to be entrusted with such an important responsibility to make sure that the payments evolution in our home market does not end at EMV or Apple Pay, but that this is just the beginning.

Don't forget to register for the 2014 Smart Card Alliance Member Meeting in Orlando in December and start making your plans for the next big payments event, the 2015 Payments Summit in Salt Lake City in February 2015.

Sincerely,



Randy Vanderhoof
Executive Director, Smart Card Alliance
rvanderhoof@smartcardalliance.org

Panama to Introduce National Identity Card

Dear Members and Friends of the Smart Card Alliance Latino America – SCALA:

The Electoral Tribunal of Panama has embarked on a journey to develop a secure multi-application smart national identity card. It is hoped that the card, which will use an integrated circuit to align government services, will become the most advanced identity card in the region. The smart card technology-based card will be a secure document to conduct transactions. The Electoral Tribunal has been working with SCALA to increase their access to impartial information, gain access to industry experts, and exchange knowledge with other governments in the Americas.

The Electoral Tribunal had asked SCALA to conduct an educational training course on smart card technology. The course, Fundamentals of Integrated Circuit Cards, was held last month for individuals involved in the development of the project, including specifications and requirements. To ensure the quality of the training, SCALA invited two CSCIP recipients and one industry professional to lead the training: Carmen Gonzalez from Visa, Nidia Ceballos from First Data, and Rolando Colchado from Giesecke & Devrient. The three were also tasked with the role of addressing any doubts and concerns related to deploying the smart card technology project.

In addition, the Electoral Tribunal of Panama assigned two of their leading staff members to accompany SCALA to the recent 13th Annual Smart Card Alliance Government Conference held in Washington, DC, last month. These representatives from the Identity and Technical Divisions accompanied me at the conference and also during the event exhibition. This relationship is an example of a good partnership, as SCALA has also coordinated several meetings for the Panama identity agency with industry experts and government agencies to exchange information and recommendations on smart card related identity projects.

I'd like to take a moment to thank the two government representatives who attended last month's Government Conference:

- **Gloriela Berroa:** Sub-Director of National Identification Card
- **Alfredo Caceres**: Chief Engineer of Information Technology

One of the key U.S. agencies which provided substantial techniccal and project information, was the National Institute of Standards and Technology – NIST. In addition to providing valuable information on key industry standards and best practices, NIST gave recommendations on convergence, interoperability platforms, and security for secure smart card credentials.

This unique opportunity will help the government of Panama to develop a much more robust infrastructure and identity credential for all of its citizens.

I would like to close this quarterly newsletter by informing our readers that the Smart Card Alliance Latin America – SCALA exhibited at Cartes Secure Connexions in Paris, France. While our participation was not as substantial as last year, we ensured that organizations and governments agencies in Latin American and Caribbean were well represented and had a place to go on the exhibition floor.

Some of the key initiatives that we were showcasing were our Open Payments Initiative for the interoperability of transportation systems and our Open Identity Initiative for government national identity cards.

We invite you to join, become active, make a difference, and help us lead markets influenced by integrated circuit cards as the single industry voice in the U.S., Latin America, and the Caribbean.

In becoming part of our organization you will gain access to:

- Impartial industry reports and market Information
- Exclusive meetings with key decision makers
- Complimentary conference passes
- Technical specifications
- Increased market credibility
- And much more!

If you would like further information, please contact us at scala@sca-la.org or visit: www.sca-la.org

Sincerely,

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

Giesecke & Devrient

Brian Russell

For the final quarter of 2014, Smart Card Talk spoke with Brian Russell of Giesecke & Devrient (G&D), a privately held, international corporation headquartered in Munich, Germany. The company was founded in 1852, and has over 50 subsidiaries in 32 countries. G&D is the leader in North America for RFID contactless, EMV and transit card manufacturing, providing data preparation and generation solutions along with card personalization services to securely enable consumer cards. Recognized as an innovative technology executive, Brian currently serves as senior vice president, Payment and Transit, for G&D's U.S. Mobile Security Division. He is based in the technology corridor of Northern Virginia and is responsible for the sales and marketing of all G&D's products to the commercial bank and transit market segments. Brian has been a member of the Board of Directors Executive Committee for the Smart Card Alliance for the past four years, serving as assistant treasurer and treasurer. He is also an active member of the Federal Reserve Bank's Mobile Payment Industry Workgroup (MPIW), has moderated and presented panels at a number of industry events, and has spoken on behalf of the Europe-based Smart Payment Association. Before joining G&D in 2009, Brian held positions with MasterCard Worldwide, Donnelley Marketing, Dun & Bradstreet and Liberty Mutual Insurance. He has a BA from Colby College and an MBA from the Wharton School of Business.

1. What are G&D's main business profile and offerings?

G&D has been developing security solutions for over 160 years, and provides a comprehensive suite of technology products and services to deliver secure digital payment solutions for our customers. As the world has advanced, we've kept pace. Today, we are a world leader in pioneering technologies that secure how people pay, communicate, and authenticate. Our solutions, products, and services range from innovative hardware and software to end-to-end solutions for EMV, SIM and device management, LTE, mobile authentication, subscription management and M2M, as well as NFC for secure elements and HCE. We are also the leading company in the world to offer banknote and security printing, security paper, and banknote processing services.

2. What role does smart card technology play in supporting G&D's business?

For G&D, it's all about securing credentials. Over the past 40 plus years, G&D has developed smart card technology, driven standards to ensure interoperability, educated our customers and built strong relationships with banks, mobile network operators, transit authorities, governments and corporations. With convergence occurring in these industries, G&D is there, securing transactions and authenticity with smart card technology. We have a unique ability to help bridge the gaps in the new ecosystem – with partnerships and technology – and to help drive adoption of new technology, such as NFC or tokenization. G&D continually develops new products and services to meet market demands and innovations to eliminate obstacles to smart card adoption. We actively participate in dozens of standards bodies and industry organizations, like the Smart Card Alliance, to further interoperability. We have regular and constant discussions with our customers, potential customers, and industry associates – like those within the Smart Card Alliance industry councils and the EMV Migration Forum – to educate, clarify, and ultimately dissolve concerns in order to continue to increase the number of cards, other devices, and solutions using smart card technology.

3. What trends do you see developing in the market that G&D hopes to leverage?

Clearly, the current focus for the U.S. payment market – and G&D – is on EMV migration. As a world leader in this area, G&D is helping our customers navigate the complexity of this space and delivering a future proof solution which supports Durbin to meet

the October 2015 deadlines. G&D is also actively participating in the emerging markets of NFC and M2M. Both of these areas are a natural extension of our expertise in smart card technology. While not new, NFC is transitioning from small pilots to commercial implementations. This market is also bringing new players into the mix who have not traditionally participated in the smart card space, which alters the landscape and encourages new partnerships. With embedded SIMs, the M2M market has introduced new complexities for subscription management, another round of new players, and new considerations as to how smart card products impact the daily lives of consumers. We're also watching the "cloud" to ensure there are appropriate measures implemented to manage the security of data and credentials. We hope to capitalize on the security mechanisms needed for the trusted execution environment.

4. What obstacles to growth do you see that must be overcome to capitalize on these opportunities?

The obstacles to growth in these areas are not new. We have been challenged by a lack of infrastructure, consumer fears, and security concerns since the inception of smart card technology. Interoperability of IT system components is another major area to overcome, particularly with legacy systems that don't communicate with each other. Over the years, consumer knowledge has greatly increased, but even some employees who work in the smart card industry are cautious about the security risks associated with using aspects of the technology. We need to provide education, not only to the consumer, but also to the issuer to ensure that they are using the inherent security mechanisms, such as encryption, to protect consumers' private information and reduce fraud.

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

Convenience for the consumer is one of the most important factors, but the technology must be secure and trusted. With smart phones now commonplace, we are in a position of capitalizing on the convenience of doing everything with one device through NFC, from paying bills and purchasing items to turning on house lights and closing garage doors to validating authenticity of people and products. The purely digital world, though, is fraught with risk, if the technology to secure the activity isn't used. In the industry, we know and understand that security and it is our duty to convey the importance to issuers of safeguarding credentials. Otherwise, fraudsters will have easy access to non-secure data and consumers will shy away from the smart card technology that enables this convenience.

The old goal of one card for all uses now looks like one phone for all uses, but is still years away. We are seeing activity toward multi-application cards, which will certainly help in the adoption of smart card technology. Movement from transit-only cards to open payment cards used in a transit environment is one of those activities.

Certainly, the transition from mag stripe cards to EMV will put a smart card, or several, in everyone's wallet (or on everyone's handset) in the next year.

6. How do you see your involvement in the Alliance and the industry councils helping G&D?

G&D's active participation in the various industry councils of the Alliance encourages networking with peers, sharing industry knowledge and trends, and furthering knowledge of and adoption of smart card technology by the end users through outreach programs. The Alliance is instrumental to our collective vertical markets, raising the bar throughout the industry and providing a non-biased information access point for our potential customers.

Member point of contact:

Brian Russell
Senior Vice President, Payment and Transit - Mobile Security
Giesecke & Devrient America, Inc.
Office: 1-703-480-2117
Mobile: 1-571-226-0371
Brian.Russell@gi-de.com

Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization

According to the Verizon 2014 Data Breach Investigations Report, restaurants, hotels, grocery stores, gas stations and other brick-and-mortar outlets suffered 285 security breaches with confirmed data losses during 2013. [1] While retailers such as Target and Neiman Marcus made the news, the report states that the vast majority of these breaches occurred against small to mid-sized companies.

Verizon's report declares that 2013 can be characterized as "a year of transition from geopolitical attacks to large-scale attacks on payment card systems." During 2013, POS intrusions accounted for 31 percent of the 148 retail breaches, with payment card skimming accounting for another six percent. POS intrusions accounted for 75 percent of the 137 accommodation sector breaches.

Three technologies work in tandem to protect those businesses processing credit and debit cards against card fraud. The three technologies are:

- EMV, which improves the security of a payment transaction by providing cryptographic card authentication that protects the merchant and issuer against the acceptance of counterfeit cards. EMV also offers cardholder verification and several means of transaction authentication that help safely authorize transactions.
- End-to-end encryption (E2EE) or point-to-point encryption (P2PE), which can immediately encrypt card data at inception – at card swipe, key entry, tap or insertion – so that no one else can read it and monetize the card data.
- Tokenization, which replaces card data with "tokens" that are unusable by outsiders and have no value outside of a specific merchant or acceptance channel.

The payments industry can provide improved payments protection by using a layered approach. Implementing EMV, encryption and tokenization; using them in combination can provide a better solution than using any single technology by itself.

To understand how EMV, encryption and tokenization work together to provide security for payment transactions, it is beneficial to understand the various use cases for customers presenting payment credentials at merchants. This article looks at several scenarios and provides guidance on how EMV, encryption and tokenization are used to provide payment transaction security.

Scenarios discussed include:

- Card-present transactions
- Card-not-present transactions
- Mobile transactions in a store with payment credentials stored in the cloud and transferred to the POS using one of multiple technologies

Payment System Security Layers: Card-Present Transactions

Card-present transactions include those where customers are in a merchant's store and are paying with a magnetic stripe card, an EMV chip card or an NFC-enabled mobile device with credentials stored on a secure element on the mobile device.

EMV was designed to combat counterfeit card fraud in a card-present environment. Key EMV security features include:

- Card authentication using dynamic authentication data (either online or offline), which proves that a card is authentic to the merchant and issuer.
- EMV chip transaction data, which cannot be used to create counterfeit magnetic stripe cards if the data is stolen.
- Potential PIN addition to an EMV transaction, providing stronger verification of the cardholder identity and addressing lost and stolen card fraud.

However, although EMV uses dynamic cryptograms, some sensitive data (such as the PAN and expiration date) that is needed to support routing and legacy system messaging, is sent in the clear during EMV transactions.

Encryption can protect transaction data at rest and in transit, whether it's a magnetic stripe transaction or an EMV chip transaction. A merchant deploying encryption without EMV will not be protected from counterfeit card transactions; EMV technology mitigates the risk of counterfeit transactions. The combination of EMV and encryption protects transactions in the card-present environment. This two-layered approach is a proactive step that merchants can take to protect their card acceptance environment from becoming a source of fraudulent transactions.

In addition, tokenization may be implemented in card-present merchant environments to secure data-at-rest for payment transactions. This will most typically be done in order to support the legitimate on-going uses of card data in an inherently secure manner. This is contrasted with encryption, where the encrypted data must typically be decrypted before it can be used. Whenever data is decrypted, it is at risk of being compromised, while tokens can be used without concern as long as the integrity of the token vault is maintained.

Use cases include the following:

- Some merchants use card information to simplify the return experience for the customers. When a consumer wishes to return an item, the merchant collects the card data, sends it to the token service to be tokenized, and then looks up the transactions in their transaction history.
- Lodging merchants may need to perform an EMV authorization upon check-in, but also perform incremental authorizations during the guest's stay. Instead of retaining the cardholder account number, the merchant may use a token specific to the merchant's use. The token vault in this case could be at a corporate host or at the acquirer/processor. Similar use cases exist for tokenization in auto rental, equipment rental and other merchant types where a deposit is taken in person, followed by a CNP balance payment.

EMV tokens can also be used in the card-present environment when they have been personalized into a mobile device or onto EMV chip cards. When the consumer is in the store and uses a device with credentials stored on a secure element and accessed through a mobile wallet (e.g., Softcard [2]) or on the EMV chip card, the transaction is a card-present transaction and is implemented as an EMV contactless or contact transaction. As with the other card-present use cases, EMV protects against counterfeit credentials and provides card authentication. The merchant may use encryption and/or tokenization to protect the transaction information while at rest or in transit. Alternatively, the issuer can personalize the chip with an EMV token in lieu of the PAN. This will protect all chip transactions from cross-channel fraud (e.g., CNP fraud) in addition to counterfeit fraud.

Payment System Security Layers: Card-Not-Present Transactions

CNP transactions are those where the customer and merchant are not interacting face-to-face. The customer may be entering payment credentials using a keyboard on a computer, tablet or mobile phone or may have previously provided the payment credentials to a merchant and the merchant uses the stored "card on file" credentials for payment (for individual or recurring payments).

Merchants and the payments industry currently take a variety of approaches to authenticate consumers during CNP transactions to help mitigate against CNP fraud. Approaches include static or ran-

How EMV, Encryption, and Tokenization Protect Transactions

	Card-Present Transactions		Card-Not-Present Transactions	
	Protects against:	**Using:**	**Protects against:**	**Using:**
EMV	Counterfeit cards	Card authentication	Not applicable. Can be used with separate reader, but not widely deployed	Not applicable
	Re-using stolen data	Dynamic data		
	Lost/stolen cards (with PIN)	Cardholder verification (PIN)		
Encryption	Stealing data in transit	P2PE or E2EE	Stealing data in transit	P2PE or E2EE
	Stealing data at rest Re-using stolen encrypted data	Various methods of encryption	Stealing data at rest Re-using stolen encrypted data	Various methods Of encryption
Tokenization	Stealing data in transit Stealing data at rest Re-using stolen data	Specific-use or limited-use token replacement for payment card data [4]	Stealing data in transit Stealing data at rest Re-using stolen data	Specific-use or limited-use token replacement for payment card data

dom passwords, dynamic information such as one-time passwords generated in software or using a smart card or mobile phone, knowledge-based approaches (such as asking secret questions) and device fingerprinting, where some information is used to identify the device by which the user is accessing an e-commerce site.

The payments industry has implemented a number of standard approaches for CNP authentication. Asking for the cardholder's zip code for address verification and entering the "card security code" printed on the card are common methods used by many, but not all, merchants. Card issuers validate that this information is correct during the transaction authorization. The payments networks have also defined the standard 3D Secure authentication protocol that is in use. The 3D Secure software protocol is used by merchants and issuers to validate cardholder identity during an e-commerce transaction. Looking at Europe's experience, the UK Cards Association reported a one-third drop in CNP fraud since 2007 due to increasing use of fraud screening tools and 3D Secure. [3]

Online e-commerce merchants typically implement multiple solutions to mitigate CNP fraud or use a commercial service to mitigate transaction risk. Since merchants today assume the costs of CNP fraud as well as typically pay higher fees for e-commerce transactions, merchants also may have their own internal fraud departments and often use tools to score the risk of online shopping behavior to determine which online purchases to accept, reject or send for review.

In the card-not-present environment, security approaches should consider:

- Some form of cardholder authentication, such as 3D Secure.
- Encryption to protect data-in-transit and data-at-rest.
- Tokenization to protect data, by creating a token for each CNP transaction that can only be used for that card and a specific merchant. This could be accomplished through either acquiring tokens or EMV tokens.

For example, e-commerce merchants can secure cardholder data by implementing the process for card-on-file tokens. The merchant, acting as a token requestor, can request tokens by submitting a token request to a token service provider. The token is provided to the card-on-file merchant. The token assigned is specific to the cardholder and merchant domain. If the token were to be compromised, it could not be used anywhere except by the registered user and at the registered card-on-file merchant.

Payment System Security Layers: Mobile Transactions with Credentials Stored in the Cloud

Mobile payment solutions that store payment credentials in the cloud but present them in a face-to-face merchant environment (e.g., those that use QR Codes, bar codes or Bluetooth) are now typically considered CNP transactions since the credentials are not authenticated during the transaction, even though the mobile device may be physically present at the POS.

The industry has launched a number of initiatives to develop network-based specifications for tokenized credentials that can be used for mobile commerce transactions (see Section 4). When these tokenized credentials are stored on the mobile device and used face-to-face for purchases at physical merchants (e.g., for host card emulation (HCE)-enabled or secure element (SE)-enabled NFC transactions), it is anticipated that these will be considered card-present transactions.

Payment System Security Best Practices

Using a layered approach – that is, utilizing all three technologies together –helps to secure the payments infrastructure and prevent payment fraud. The table and figure illustrate how each is used to protect transactions.

The layered security approach is based on the following key guiding principles.

- Continued migration away from transactions based on static authentication by implementing EMV for the card-present environment.
- Protection of data-at-rest and data-in-transit through the payment process, for both card-present and card-not-present environments.
- Adoption of encryption and tokenization technologies to protect sensitive data, including PAN and expiration date, for both card-present and card-not-present environments.
- Adoption of cardholder authentication (e.g., 3D Secure) for the card-not-present environment.

No silver bullet is available to stop fraud. However, as summarized in the table and figure, a layered security strategy that includes EMV, tokenization, and encryption is the right approach for securing payment card transactions.

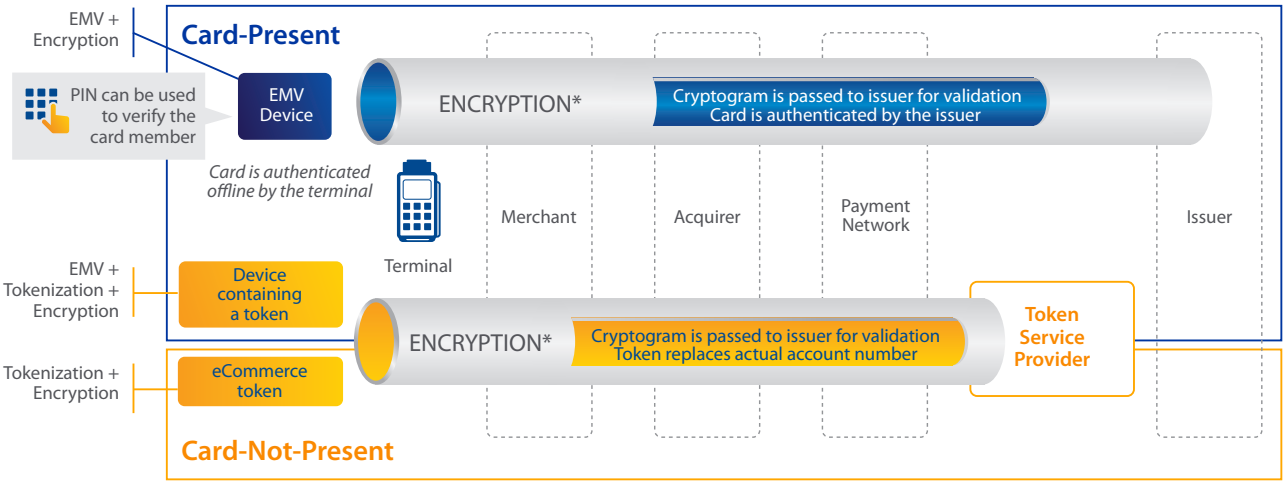
Conclusions

This article outlined the characteristics of three different technologies that are useful to securing payment transactions well into the future. Payments stakeholders seeking to reduce cost and complexity but facing limited budgets should optimize implementation based on the benefits of each technology.

EMV provides strong card authentication through the use of cryptograms to prevent counterfeit transactions. Encryption protects account numbers and other critical transaction elements that are sent through the payment system. Tokenization completes the protection of the payment card data by removing the PAN and expiration date from EMV chip, CNP and mobile transactions.

When layered, these three technologies secure the payments ecosystem. The degree of layering is determined by the need of each payments stakeholder.

Role of EMV, Encryption and Tokenization in the Payment Ecosystem



** Data at rest or in transit is protected by E2EE or P2PE*

Issuers are already moving to EMV to address counterfeit card fraud. Issuers now should consider support for tokenization to protect payment data received from EMV chip, CNP, and mobile channels.

Merchants should invest in the technologies that offer the protection they need. For example:

- A low-value-ticket card-present merchant may have very few chargebacks and may not be worried about counterfeit cards. The merchant will still have PCI and data-in-transit concerns, so their investment may focus on the encryption of data in transit and at rest.
- A high-value-ticket card-present merchant may be most concerned about counterfeit cards. The investment focus would be on EMV first and encryption of data in their network.
- A large e-commerce retailer's investment focus may be first on tokenization with cardholder authentication, and securing e-commerce transactions. Encryption of data on its way to the acquirer or processor would be another priority.
- Face-to-face merchants with complex environments that have a need to use card data for purposes in addition to authorization may wish to include an acquiring tokenization solution with encryption and EMV in order to ensure that they can securely replace sensitive card data throughout their systems as needed.

Payments stakeholders should give careful thought to their approach for layering the three technologies. The decision should be based on the needs of the particular entity, industry requirements and regulations, anticipated trends, and, of course, cost.

References and Notes

[1] Verizon 2014 Data Breach Investigations Report: http://www.verizonenterprise.com/DBIR/2014/.

[2] "A Message from CEO, Michael Abbott: Isis Wallet is Becoming Softcard," Isis press release, Sept. 3, 2014, http://news.paywithisis.com/2014/09/03/isis-wallet-becoming-softcard/.

[3] "Second Report on Card Fraud," European Central Bank, July, 2013, http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf; "Fraud the Facts 2012," Financial Fraud Action UK, http://www.theukcardsassociation.org.uk/wm_documents/Fraud_The_Facts_2012.pdf.

[4] Encryption is also used during the tokenization and de-tokenization process.

About this Article

This article is an extract from the white paper, "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," published by the Smart Card Alliance Payments Council in October 2014. The white paper describes the role of EMV, encryption and tokenization for securing the payments infrastructure and preventing payment fraud. It provides an overview of the three technologies and describes how each addresses payments security. The white paper concludes with a discussion of how payments industry implementation of the three technologies together secures the payments infrastructure and prevents payment fraud. Members involved in the development of this white paper included: Accenture, American Express, Bell ID, CH2M Hill, Chase Card Services, CPI Card Group, Datacard Group, First Data Corporation, Fiserv, Inc., Gemalto, Giesecke & Devrient, Heartland Payment Systems, Ingenico, INSIDE Secure, MasterCard, NXP Semiconductors, Oberthur Technologies, SHAZAM, Tyfone, Valid USA, Vantiv, Visa Inc., Washington Metropolitan Area Transit Authority (WMATA), Wells Fargo.

Updates from the Alliance Industry Councils

Access Control Council

- The Access Control Council is working on a project to develop a guide specification for architects, engineers, consultants, integrators, manufacturers and end users that would allow them to easily incorporate smart card-based PACS cards and readers into the A&E specification for non-government PACS.
- The Council held a well-attended in-person meeting at the 2014 Government Conference. Hildy Ferraiolo, NIST, presented the activities that NIST has underway to address PIV contactless transaction time.
- The Council is organizing breakout sessions for the 2014 Smart Card Alliance Member Meeting in Orlando. Breakout session topics include: impact of the mobile device as an authenticator for access control; PIV-I deployments and success stories.

Health and Human Services Council

- The Health and Human Services Council is developing speaking proposals to submit to 2015 industry events.
- The Council collaborated with the Identity Council on a joint in-person meeting at the 2014 Government Conference.
- The Council will be holding an in-person Council session at the 2014 Smart Card Alliance Member Meeting in Orlando.

Identity Council

- The Identity Council held a well-attended in-person meeting at the 2014 Government Conference. The meeting was used to brainstorm possible new Council projects.
- The Council is organizing breakout sessions for the 2014 Smart Card Alliance Member Meeting in Orlando. Breakout session topics include: strong authentication – what's beyond usernames and passwords; real-world contactless secure transactions; device identity – approaches, trends, use cases and security.

Mobile and NFC Council

- The Mobile & NFC Council is organizing breakout sessions for the 2014 Smart Card Alliance Member Meeting in Orlando. Breakout session topics include: biometrics and the mobile handset; mobile payments – status & approaches; implications of HCE and tokenization developments in mobile payments.

Payments Council

- The Payments Council published the new white paper, "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization." The white paper describes the role of EMV, encryption and tokenization for securing the payments infrastructure and preventing payment fraud. It provides an overview of the three technologies and describes how each addresses payments security. The white paper concludes with a discussion of how payments industry implementation of the three technologies together secures the payments infrastructure and prevents payment fraud. Members involved in the development of this white paper included: Accenture, American Express, Bell ID, CH2M Hill, Chase Card Services, CPI Card Group, Datacard Group, First Data Corporation, Fiserv, Inc., Gemalto, Giesecke & Devrient, Heartland Payment Systems, Ingenico, INSIDE Secure, MasterCard, NXP Semiconductors, Oberthur Technologies, SHAZAM, Tyfone, Valid USA, Vantiv, Visa Inc., Washington Metropolitan Area Transit Authority (WMATA), Wells Fargo.
- The Council is organizing breakout sessions for the 2014 Smart Card Alliance Member Meeting in Orlando. Breakout session topics include: EMV update; data breaches and security; tokenization.

Transportation Council

- The Transportation Council has several active projects: EMV impact on parking white paper; EMV and transit white paper; transit/payment brand project on challenges with open payments.
- The Council is organizing breakout sessions for the 2014 Smart Card Alliance Member Meeting in Orlando. Breakout session topics include: mobile ticketing in the U.S. transit industry.

Other Council Information

- All Smart Card Alliance Industry Councils completed elections for their 2015-2016 Steering Committees. The newly-elected Steering Committees are now electing their officers, with hand-off from the current Steering Committees and officers to newly-elected representatives at the 2014 Smart Card Alliance Member Meeting.
- Members-only council web pages are available at http://www.smartcardalliance.org/councils. These are password-protected pages that contain council working and background documents and contact lists. Each Council area has a separate password since Councils may have different membership policies. If you are a Smart Card Alliance member and would like access to a council site, please contact Cathy Medich.
- 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 Smart Card 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.

Welcome New Members

- Airbus Defense & Space, General
- Department of the Interior, Government
- OTI, SCALA

Congratulations

CSCIP Recipient

- Kwan Hon Luen, BT Global Services

CSCIP/G Recipients

- Thomas Casey, Intercede Limited
- Mark Dale, XTec Incorporated
- Jason Goodloe, XTec Incorporated

CSCIP/P Recipients

- David Blust, Discover Financial Services
- Cory Daugherty, First Data
- Abraham Deithloff, Discover Financial Services
- Ana Egan, Discover Financial Services
- Ben Potter, Discover Financial Services
- Akif Qazi, Discover Financial Services
- Laurie St. Ange, LTK Engineering Services

New CSEIP Recipients

- Johnny E Caldwell, Johnson Controls
- Maurice Cooper, Evergreen
- David Dersham, Evergreen
- Phillip Dersham, Evergreen
- Richard Dietz, Secure Missions Solutions, Inc.
- Paul Hagen, Secure Missions Solutions, Inc.
- Clifford M Hall, Cliff Hall Consulting
- Donald Hamilton, Department of Homeland Security
- Brian Havecost, Signet
- Jacob Haymore, Power Comm
- Brian Mann, SEEL
- Marcus Mathis, Security Install Solutions
- Douglas Oelberg, Department of Homeland Security
- William Petre, Abbey Services
- Doug Ritchey, Communications Resource Inc.
- Roger Roehr, Roehr Consulting
- John Schiefer, X-Tec
- Sean Schutte, X-Tec
- Jim Shcahnen, Brivo
- Galen Weimer, Communications Resource Inc

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

Smart Card Alliance
191 Clarksville Road
Princeton Junction, New Jersey 08550
1.800.556.6828
Fax: 1.609.799.7032
info@smartcardalliance.org
www.smartcardalliance.org

About Smart Card Talk

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

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.