Smart Card Alliance

Smart Card Talk

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

February 2015

In This Issue:

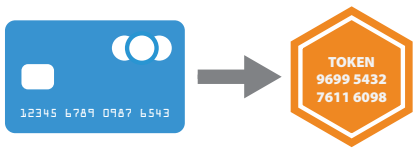
On the Web:

EMV Chip Migration: A Top Priority

At last week's Smart Card Alliance 2015 Payments Summit in Salt Lake City, two distinct themes played out frequently among the 100+ speakers selected to participate in front of a group of more than 600 attendees. I expand on those themes and more in my letter in this quarter's Smart Card Talk newsletter. We also have an update on Alliance Councils, a Member Profile on TSYS, new CSCIP and CSEIP recipients, and much more. Thank you for your interest and support of the Smart Card Alliance.

Sincerely,
Randy Vanderhoof
Executive Director, Smart Card Alliance

Click to Read Letter ...



Feature Article:
Tokenization 101

A hot topic in the payments industry is "tokenization" – replacing the payment card's primary account number with an alternate number that is used in the transaction process. This month's article provides a primer on tokenization, describing the different types of tokenization used in the payments industry and outlining how "EMV tokens" are being used to secure payment data.

Click to Read More …

Member Profile:
TSYS

For the first issue of 2015, Smart Card Talk spoke with Sarah Hartman of TSYS, who serves as Senior Director of Consumer Payment Solutions for the global payments processor. Her responsibilities include product and strategy activities associated with the consumer credit and debit card issuing business.

Click to Read More …

Smart Card Alliance Events

14th Annual Smart Card Alliance Government Conference
June 9-10, 2015
Walter E. Washington Convention Center, Washington, DC

Smart Card Alliance Member Meeting
October 4-6, 2015
Arizona Grand Resort, Phoenix

Smart Card Alliance NFC Solutions Summit
October 7-8, 2015
Arizona Grand Resort, Phoenix

EMV Chip Migration: A Top Priority

Dear Members and Friends of the Alliance,

As more than 600 payments industry people gathered at the Smart Card Alliance's 2015 Payments Summit in Salt Lake City last week, there were two distinct themes that played out frequently among the 100+ speakers selected to participate. The opening keynote topics epitomized the important role in each of these major themes: the progress made and expectations ahead for EMV chip migration for the U.S., and the rise of tokenization as another major innovation to watch on the near horizon.

The topic of the closely watched transition of the U.S. market to EMV chip, which is less than 150 days from the October fraud liability shift date, opened the conference. Kimberley Lawrence from Visa provided promising numbers on the volumes of chip-enabled credit cards and debit cards expected to be in consumer's hands and the number of merchant terminals expected to be installed by October. She presented the Payments Security Taskforce's consensus forecast that 575 million chip cards will be issued by the end of 2015, representing about 71 percent of credit cards and 41 percent of debit cards. Discover's Ellie Smith told attendees that in the year since the last conference, her conversations with issuers have now shifted to "how and when" they will get chip implemented. Smaller banks and credit card issuers are getting into the action as well, according to Dr. Art Harper from PSCU. His organization is advocating mass reissuance with chip cards to their 700 credit union members.

Patty Walters from Vantiv weighed in on the merchant's readiness for EMV acceptance from the merchant acquirer perspective. She was far less optimistic about the number of merchants being fully tested with EMV accepting terminals in operation by the October liability shift. She expressed more confidence that the highest rick merchants, such as mass retailers, grocery, and convenience stores, will be ready for EMV credit transactions, pointing out that it was only in the last year that merchants had adequate specifications for developing and certifying EMV debit point of sale (POS) applications. Small to medium sized merchants may struggle to be ready, even though they have less custom software integration testing to complete.

Karen Czack with American Express said that all American Express card portfolios are available as chip cards today, and made a strong endorsement for keeping contactless EMV and NFC payments in the mix. She shared statistics on how consumers in the United Kingdom and Australia have rapidly adopted contactless payments at merchants who support and promote contactless transactions. London's busy transportation system is an example. Subways, buses, and the rail system are accepting contactless American Express cards, and consumers who use contactless payments just a few times get hooked on tapping to pay. She offered the observation that this could be a model for how payments behavior may evolve in the U.S. once the EMV infrastructure in in place and cardholders have adjusted to a world without magnetic stripes.

The collective message that came from these presentations was that while EMV migration has moved incredible lengths in the third year of a planned four year migration, it's been at an uneven pace for the infrastructure players, with issuers far ahead of most merchants. Further, the issuance of contact-only chip credit cards is well ahead of contactless chip cards and debit cards.

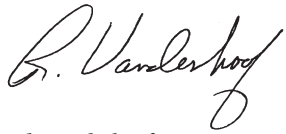
The rise of tokenization as a transformational technology for the future of mobile and Internet payment transactions emerged as another dominant theme. James Anderson from MasterCard kept the audience engaged by explaining how the roots of modern tokenization first appeared 25 years ago when check cards replaced paper checks and the 16 digit debit card PAN (primary account number) was a permanent token connected to your bank account. Anderson also cited how consumers use payment cards differently from the past, not only to shop across multiple merchants, but also store them in merchant accounts like Amazon for faster checkout, and link them to recurring charges like utility bills. PAN usage in today's world cuts across multiple channels (cards, mobile phones, cloud), so protecting it increases the cost, complexity, and security risks of these new channels.

Tokenization addresses a limitation in the payments infrastructure. Rather than storing and protecting the single PAN on multiple devices (e.g., mobile phone, card), a token is stored. The token may be single use, restricted to a single merchant or restricted to a single channel. With this model, if the token is lost or compromised on one of the devices, you don't have to replace the card with the original PAN.

Lee Manfred from First Annapolis discussed tokenization in the context of Apple Pay by observing that Apple Pay has created a great user experience with tokenization, but it is limited today to owners of iPhone devices. David Lott from the Federal Reserve Bank of Atlanta, spoke of the progress that the Fed's Mobile Payments Industry Workgroup has made in developing a tokenization landscape paper. He also shared how various stakeholders view the potentially fragmented nature of the standards around tokenization.

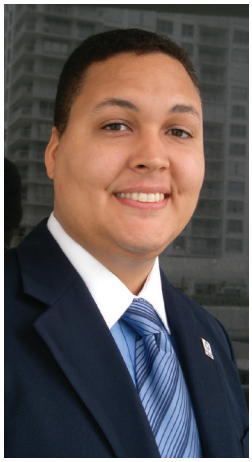
Now that the intense week in Salt Lake City for this year's Payments Summit is behind us, we are already looking towards the 2016 Payments Summit with much anticipation. After many years in Salt Lake City, we have outgrown the location and will be moving to Orlando for the event, scheduled for April 4-7, 2016. We are also co-locating the Summit with the ICMA Expo, bringing the payments industry and card manufacturing industry together under one roof. This combined event will surely attract an even broader audience of industry leaders. For some, this means trading in snow skis for jet skis, but there will be plenty of new attractions to satisfy everyone's needs. We thank you for your continued support of the Smart Card Alliance.

Sincerely,



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

Nothing Is Stronger Than an Idea Whose Time Has Come



Dear SCALA Members and Friends,

Victor Hugo, a French poet of the 19th century once said "*Nothing is stronger than an idea whose time has come*." While these words can easily be put into the context of any great transformation in our history, I believe we are now living through another significant time in history where unique ideas are needed to transform humankind. These ideas have to be bold and carefully communicated, and require alliances to help push forward the changes.

Change often generates adversity or uncertainty, especially in those who benefit from the status quo. When new ideas are analyzed and begin to question our preconceived notions of reality, these ideas are considered radical.

In the area of technology, all new ideas are radically changing our concept of reality in ways we had never thought of. Technology is changing the way we live, communicate, and interact with each other. Interestingly, once the ideas receive our buy-in, challenges and adversity disappear.

In my experience, after seeing how both disruptive and beneficial smart card technology has been in the identity space in the United States, Latin America, and the Caribbean, it is clear that we have to understand the problem it is solving in order to generate innovative, transformative ideas to improve our technology to better serve humankind.

First, let's acknowledge that the U.S. Federal government's Common Access Card (CAC) and Personal Identity Verification (PIV) card have been a great success in terms of identification, security, access control, cost/benefit, and interoperability. Their approach has become a standard that most of the world's countries are trying to understand and replicate, but lack the infrastructure, funding, and advanced identity systems to incorporate.

While this initiative has served well for implementing secure identification of U.S. federal employees, it provides limited experience for countries issuing national identity documents. In those regions, most countries have mandated national identity card requirements for citizens/residents, with very few issuing smart cards. And the countries that have implemented smart card solutions in the region have issues surrounding their implementation.

In part, this is because the industry is great at selling the capabilities of smart card technology, but lack details on how to implement the technology. Also, government representatives don't have a clear understanding of what is being implemented and seldom use the full capacity of the solution they have just bought.

Due to a lack of interoperability standards for nationally issued identity documents, international funding organizations and governments have based their identity project specifications on ICAO 9303 Basic Access Control. This specification is required for passport and travel documents, which I agree provides a great base, but it's limited in scope and capability. Passports are not mandated documents for all citizens of a country; it does not take into consideration other functions required in identity documents; and it can't be applied to other related identity documents such as driver's licenses.

So to address this scenario, the SCALA Board of Directors has come up with a radical proposal, one which we believe whose time has come. The chapter will be developing an interoperability specification for national identity documents in the Latin America and Caribbean region. If this initiative gathers significant industry support and government participation, it quite possibly may change the way all us look at identification in the region.

The key benefits of our proposed specification are:

- A document that can be mutually recognized/validated among countries in the region
- Specifications for identity cards that provide with uniformity in: formats, information, and security mechanisms
- A reduction in government cost and an increase in the volume of identity documents
- An immediate recognition of citizenship
- An increment in transnational cooperation

I know that our proposal and associated changes won't happen overnight. We also know that our proposal may face adversity in some government circles and in industry, but we invite all of you to join our efforts to transform our industry for the benefit of all.

Lastly, SCALA invites you to join the discussion on this and other topics from March 3rd – 5th, 2015, in our **Open Identification and Payments Summit**.

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

Sarah Hartman

For the first issue of 2015, Smart Card Talk spoke with Sarah Hartman of TSYS, who serves as Senior Director of Consumer Payment Solutions for the global payments processor. Her responsibilities include product and strategy activities associated with the consumer credit and debit card issuing business. Sarah has over 25 years of payments industry experience, as well as extensive product management, marketing and sales experience. An elected member of the Steering Committee of the EMV Migration Forum, she also participates in other industry organizations including ACT Canada. Sarah has a B.S. degree in Accounting from Miami University and an M.B.A. from the University of Dayton.

1. What is your main business profile and offerings?

At TSYS® (NYSE: TSS), we believe payments should revolve around people, not the other way around. We call this belief "People-Centered Payments™." By putting people at the center of every decision we make, TSYS supports financial institutions, businesses and governments in more than 80 countries. Through NetSpend®, A TSYS Company, we empower consumers with the convenience, security, and freedom to be self-banked. TSYS offers issuer services and merchant payment acceptance for credit, debit, prepaid, healthcare and business solutions.

2. What role does smart card technology play in supporting TSYS's business?

This is a very exciting time to be involved in the payments industry. Smart card and mobile payment usage is growing rapidly. TSYS supports both issuers and merchants with their payment needs, which means that smart card technology plays an enormous role. We believe it's critical we understand the needs of our clients and also stay current on what's happening in the industry, which is one of the reasons we belong to the Smart Card Alliance. TSYS has been issuing chip cards for well over 10 years, initially supporting the European region, moving on to Canada, and now focusing our efforts in the U.S.

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

This list will continue to evolve as the market does. A few areas of current focus are the roll-out of EMV to the U.S. market and overall global opportunities with advanced card capabilities, mobile technologies and tokenization. The roll-out of EMV to the U.S. market has given us the opportunity to expand our Client Advisors' Consulting Service and to offer a "Chip on Demand" card offering to our issuing clients. We're excited about the flexibility our new milling and embedding services provide to our clients and the fact that they don't need to worry about things such as chip expiration dates and inventory management if they utilize this new service. We are also excited about the expanded opportunities which chip cards bring to the overall market, with the availability of multi-application chip cards which can combine multiple payment options and/or payment and non-payment activities.

> **We believe it's critical we understand the needs of our clients and also stay current on what's happening in the industry, which is one of the reasons we belong to the Smart Card Alliance.**

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

While there are not necessarily technological obstacles, client and end consumer demand and education are needed to capitalize on new opportunities. And, it's important to have a business case which has benefits for all of the parties involved. Even with that, one of the other challenges with new opportunities is how best to prioritize new activities with "business as usual" activities which are already underway. TSYS is focused on meeting our clients' current business needs, while also ensuring we have the bandwidth available for innovation and other new activities.

Specific to the U.S. migration to chip and our acquiring business, we are seeing similar trends to what is being reported throughout the industry. While larger merchants/retailers are proactively installing new terminals and completing the necessary set-up to accept chip cards, other merchants are reluctant to move forward and believe themselves at low risk. We have found that continual education on the upcoming liability shift and the potential impacts is critical.

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

Our commercial card clients were some of the first to adopt chip cards in the U.S. They wanted to ensure those traveling internationally had payment cards which would work in other countries. We believe there are several factors driving the adoption of smart card technology in government and commercial markets. Those include: 1) global interoperability (ensuring the cards work consistently); 2) identity management (providing a more secure way to verify and authenticate an individual's identity); 3) physical security (enabling access to physical buildings); 4) government or privately run mass transit; and 5) data management (e.g., payment usage patterns, buying behaviors, health records). The government's support for smart cards was further reinforced in October 2014 when President Obama signed an executive order stating that credit and debit cards issued by the government would include "chip and PIN" capabilities beginning in January. And, there continue to be a number of state and federal proposed laws surrounding data security and/or cyber security and crimes.

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

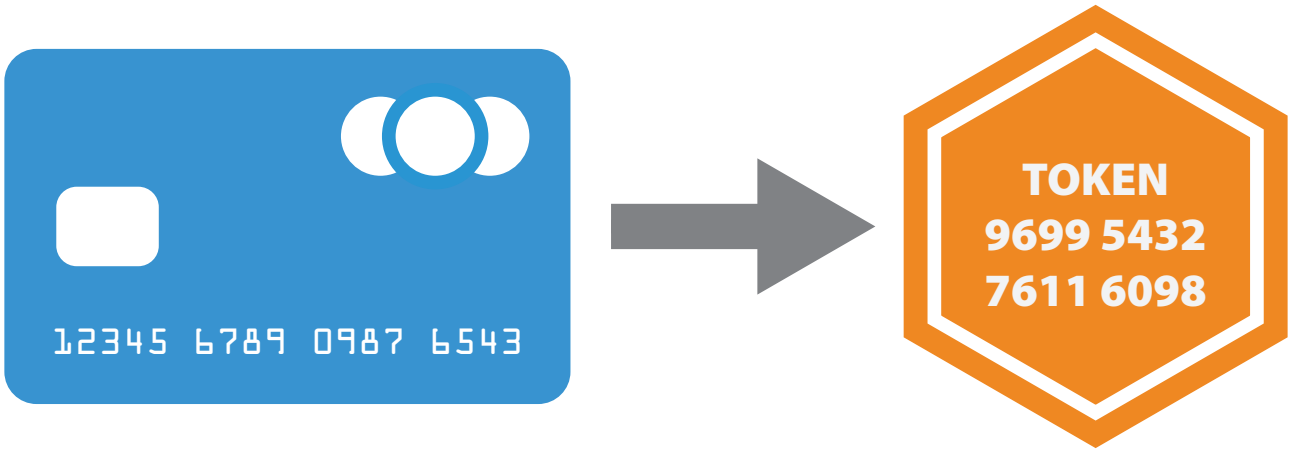
As mentioned previously, we are a strong supporter of the Smart Card Alliance and its various industry councils. We've been a principal member of both the Smart Card Alliance and the U.S. EMV Migration Forum for many years. We have a number of people from TSYS actively involved with the organization, and have had a large number of our team members become CSCIP certified. The information we receive from the Alliance on trends and regulatory changes, combined with the educational components and the opportunity to interact with the wide range of companies and individuals who participate, helps us to better meet our clients' current needs and to plan for the future.

7. What are some of the challenges you see confronting the smart card technology industry?

Beyond initial chip card launches, there are many different ideas and applications for using smart card technology to further business activities. Prioritizing the next best application/opportunity, ensuring the business case exists to gain the traction needed for widespread use, and confirming the cardholder adoption are some of the challenges which need to be addressed. We also see a continued need for consumer and merchant education. If new cards are issued with little or no information provided to the consumer on what's changing, and/or merchants' employees are not familiar with the changes, confusion and slow-down during the check-out process can result.

Member point of contact

Sarah Hartman
Senior Director, Payment Solutions, TSYS
SHartman@tsys.com
706.649.4360



Tokenization 101

Tokenization is a process that replaces a high-value credential (e.g., a payment card primary account number (PAN), a Social Security number) with a surrogate value that is used in transactions in place of that credential. Tokenization can map the credential to a new value that is in a different format or that is similar to the format of the original high-value credential (e.g., a payment card PAN in the payments industry). In payments, the objective of tokenization is to remove account data from the payment environment and replace it with something that is useless outside of the environment in which the token was created. While tokenization is not a new concept, recent data breaches have increased awareness of the need to protect payment account credentials. Tokenization is one approach that can be used to safeguard payment credentials from being stolen and used for fraudulent transactions.

There are different kinds of tokens and different ways to create them. A token can be merchant specific. It can be single use or multi-use. It can be stored and managed in the cloud, in a token vault, or at a merchant location. A token is created using a process defined by the token solution provider. Once a token has been created, it may be tied to a card on file, individual transaction, payment card, or device.

Two types of tokens are being used and/or defined in the payments industry [1]: tokens that will function in place of the actual PAN to perform a payment transaction [2]; tokens that replace the PAN and are stored by merchants and/or acquirers in place of actual PANs and used for other uses (e.g., for loyalty programs). [3] The tokenization creation and management process, use of tokens in a payment transaction, and business relationships differ based on the type of credential.

Various proprietary tokenization solutions are commercially available and already used by merchants and acquirers to protect cardholder data in both card-present and card-not-present (CNP) environments. New tokenization standards are also being introduced. Industry bodies such as the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X9, EMVCo, PCI Security Standards Council (PCI SSC), and The Clearing House have started to develop tokenization specifications for bank card payment industry use.

ANSI ASC X9 [4]

The X9 F6 work group is working on a security tokenization standard that addresses tokens used after initial payment authorization, such as when an acquirer provides tokenization services to merchants. The merchant securely sends payment authorization requests to the acquirer, which replaces the payment card number with a token. This token is returned to the merchant and stored in place of the payment card number. The acquirer keeps a record of the PAN-token pairing for situations where the PAN is required such as for settlement or disputed charges. This token has no use other than to replace the payment card number in the merchant data repositories. If the underlying payment card number is needed, an authorized request containing the token must be sent to the tokenization service (i.e., the acquirer).

X9 F6 is working on the requirements for secure design and implementation of this security tokenization process, including:

- A list of acceptable algorithms to implement the random mapping of USVs to tokens and the required strength of those algorithms
- Requirements for the protection of the tokenization service
- Requirements for tokenization service access control

X9F6 is currently working on a security tokenization standard named X9.119 Part 2 which is scheduled for release the first part of 2015.

EMVCo

In March 2014, EMVCo published version 1.0 of its tokenization specification [5]for payment industry participants. [6]This specification defines a framework to be used by payment brands, payment issuers, acquirers, merchants, and mobile and digital commerce solution providers to enhance transaction security at various points in the payment process. Various entities are creating token services based on the EMVCo specification.

EMVCo tokenization was designed to use current ISO/IEC 8583 message formats that support interoperability with the existing payments infrastructure; the specification adds additional values which may be mapped to existing fields. EMVCo's tokenization approach is intended to guard against fraud in current CNP channels, such as online account-on-file transactions. Tokens based on the EMVCo specification (referred to "EMV tokens") can also be used in the card-present channel with EMV chip cards, where a token replaces the PAN that would otherwise be encoded on the chip, while the magnetic stripe and embossing/printing on the card would contain the PAN. Lastly, EMV tokens can be accepted in emerging mobile channels whether they are using QR codes, Near Field Communication (NFC), Bluetooth low energy (BLE) or a range of other future possibilities.

The intent of the EMVCo tokenization model is to limit risk levels in case of a data breach, and within specific defined domains (e.g., by a specific online merchant or a particular device in a specific acceptance channel). Additionally EMV tokens have an associated token assurance level which is determined by the identification and verification process performed at the time of token issuance. EMV tokens are designed to be interoperable between payment networks. Tokenized payment data is far less attractive to attackers and may eventually reduce data protection requirements for merchants and acquirers.

The EMVCo tokenization model introduces a new entity, called a token service provider (TSP). The TSP creates tokens and manages them throughout their life cycle. Token life-cycle management can be implemented using a method such as ISO/IEC 8583 message exchange, batch files, or Web services that are established for secure token-based interactions. The TSP is responsible for managing a registry of entities that can request tokens, a token provisioning system, token security, token vaults (to secure tokens and PAN mappings), APIs, and detokenization. The APIs allow participants to interact with the TSP.

In the EMVCo tokenization model, the token, referred to as a payment token, shares the same overt characteristics of a PAN (including the Luhn check mechanism, bank identification number (BIN) range, and expiration date) to support the current transaction flow and minimize friction in the existing payment processing environment. However, tokens are required to be guaranteed to never collide with PANs. In practice this means that tokens must be issued from separately designated BINs (or ranges within a BIN).

Once a token requestor has enrolled with a TSP and identified the domain in which its tokens may be used, the token issuance process starts with a request to a TSP, using a token service API, to tokenize a specific PAN. The token requester can be a merchant, a digital or mobile wallet service provider, a card-on-file system, an issuer, or any other payment enabler. The token is generated within a range of token BINs that are associated with a specific issuer to avoid conflicts with a PAN, and is assigned to a domain within which it can operate.(For example, a token issued for an NFC payment domain will not work in an e-commerce or magnetic stripe environment.)

A two-digit token assurance level, similar to a payment instrument risk score, is also assigned to indicate what identification and verification (ID&V) process was done to validate the cardholder's identity and ownership of the original payment credential; a value of 00 would indicate no ID&V and 99 would indicate the highest level of assurance. The token assurance level can be used by specific programs or for transaction classification and can be influenced by the security requirements for token storage location. ID&V methods can be used for different purposes such as card-on-file account number replacement with a token, or medium or higher assurance level transactions. ID&V methods generally fall into the following categories:

- No ID&V performed
- Account verification
- Risk score derived from the TSP
- Risk score derived from token user data combined with payment network data
- Card issuer authentication of cardholder

Detokenization is the reverse of tokenization and is necessary for transaction processing, settlement and chargebacks. When requested by an authorized and authenticated entity, the detokenization process returns the PAN associated with a token, the associated expiration date, and status. Depending on where the TSP is located in the transaction flow, it may perform the token domain restriction controls directly or provide the transaction processor with the details needed for it to, in turn, perform that task.

The BIN plays an important role in routing transactions to the right endpoint. The BIN token range used in transactions will have

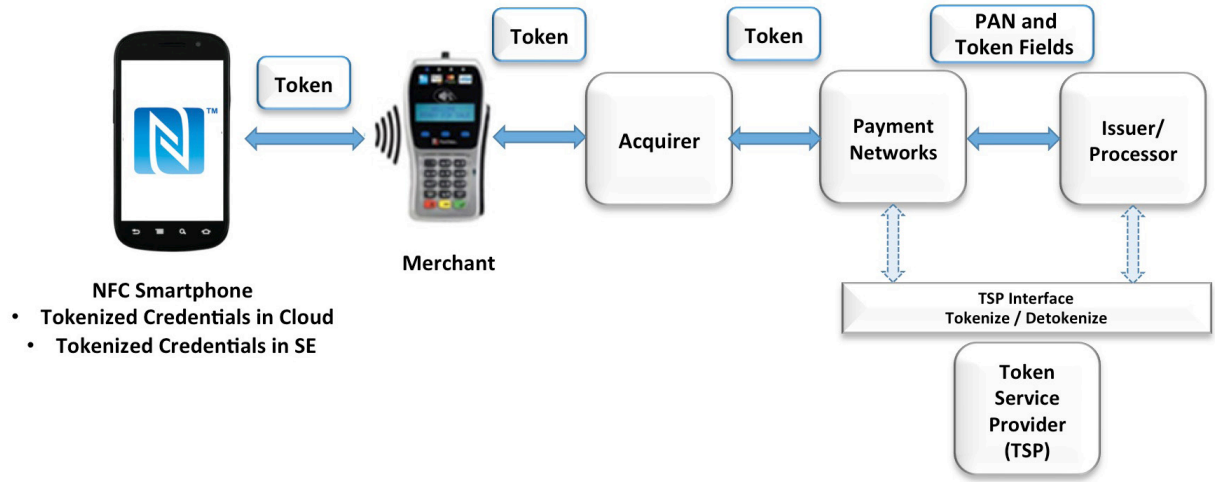


Figure 1. Use of Tokenization in an NFC Transaction

similar characteristics to the BIN range for the cards and will be part of the BIN routing table distributed to participating entities to support routing of tokenized transactions.

Payment tokens have life cycles similar to PAN life cycles. While payment tokens experience their own life cycle events (such as expiration, fraud, loss, transfer of devices, reissuance, theft, changes due to customer profile updates), they may also be affected by changes to the PAN life cycle. The TSP is responsible for communicating changes to the token (or to the PAN associated with the token) to token users in the payments transaction process.

Tokenized payment transaction processing passes the token instead of the PAN, so it becomes the responsibility of the TSP and the payment processing platforms to restrict a particular token to specific payment channels or domains. This restriction will affect the current data fields and require the definition of both mandatory and optional new fields that have been defined for tokenized transactions. Some of the fields required to control domain restriction are already in place, such as POS Entry Mode, and merchant detail fields. New field use may depend on the specific payment use case, in which merchants, acquirers, and processing platforms may be affected by such use cases.

Figure 1 illustrates the use of EMVCo tokenization in an NFC mobile payment transaction. Tokenization is expected to be used in NFC mobile payment implementations using either secure elements (SE)or host card emulation (HCE).[7] For example, as announced in September 2014, Apple Pay is using tokenization along with a secure element. [8]

PCI Tokenization Initiative [9]

The PCI SSC is currently developing security requirements for tokenization products (e.g., tokenization applications or appliances) that replace a PAN with a token. The tokenization processes described by PCI include functionality to exchange a token back to the original PAN ("detokenization") as well as "irreversible" tokens for which there is no mechanism supported to reproduce the PAN. The goal of this effort is to remove the need to store PANs, thereby reducing the risk of unauthorized disclosure, and is focused on tokens used in the acquiring environment.

It is anticipated that use of secure tokenization products will help to minimize the locations, systems and networks where cardholder data is stored, processed or transmitted. A secure tokenization implementation may help minimize the retention of payment card data in an entity's environment and hence simplify their PCI DSS compliance efforts. These tokenization security requirements are part of the Council's ongoing work to provide standards and guidance on technologies that can improve cardholder data security along the payment transaction chain.

The PCI effort will provide tokenization product vendors and developers with detailed technical requirements for how to generate and store tokens securely. A mechanism to evaluate tokenization products against the requirements is under consideration.

PCI security requirements are developed with the input of the PCI community of participating organization members, security assessors, testing laboratories and other key stakeholders. In addition, PCI SSC has held conceptual and technical discussions with a number of organizations that already offer tokenization products or services. PCI SSC also liaises with X9 and EMVCo on their respective tokenization efforts.

The Clearing House Tokenization Initiative [10]

As a member organization of 23 commercial banks, The Clearing House (TCH) operates under a directive to both assist in the development of tokenization standards, as well as operate a multi-issuer token vault that works across all major card networks. The Secure Token Exchange effort began in 2012, was piloted in 2013, and now has participating banks that represent 70% of U.S. retail card vol-

umes. In addition to card volumes, the Secure Token Exchange will also support the future tokenization of Automated Clearing House (ACH)/demand deposit account (DDA) payments.

The initial Secure Token Exchange standards were very similar to the EMVCo standards published in March 2014. The Clearing House is adopting the core EMVCo messages to allow for industry interoperability while retaining proprietary provisioning, exceptions and lifecycle management flows. The Clearing House has also proposed several changes to the current EMVCo specifications to include these flows and to increase the overall safety and soundness of the framework. It is the position of U.S. banks that greater standardization of tokenization specifications will allow for faster adoption and innovation.

Assurance Process for Token Issuance

In many token use cases, the sole purpose of the token is to remove sensitive card data from the payments ecosystem. In such cases, there is little need to validate that a given PAN is authorized prior to tokenizing it. The payment system will perform that function during transaction processing. However, in some instances, principally when the token replaces a PAN for use in an NFC transaction or similar situations, simply replacing the PAN with a token doesn't address the risk of a criminal using stolen payment credentials and having a valid token assigned to the stolen credential.

To address this, critical parts of the tokenization process are to identify and verify that the cardholder presenting the payment account for tokenization is the valid cardholder and to associate an assurance level to each token to indicate the confidence level in the token to PAN/cardholder binding.

As discussed earlier, the EMVCo tokenization specification refers to several possible ID&V methods that may be performed via card issuer verification of the cardholder. The ID&V methods are utilized to assign an assurance level to each token that will be used to transact. ID&V processes are critical to tokenization initiatives to prevent fraudulent use of payment card data.

Summary

Commercial acquiring tokenization solutions are currently available and in use by merchants to remove cardholder data from their business environment (e.g., for loyalty programs or card-on-file transactions).

Tokenization standards are also now being developed and published by a number of industry organizations, with commercial solutions starting to use those specifications to provide tokenization services. Some standardization efforts are focused on data-at-rest, protecting data within a merchant's environment, while other are focused on data-in-transit, protecting data throughout the transaction process.

Tokenization standardization and broader implementation are evolving. The industry is starting to see alignment among the standardization efforts around the EMVCo tokenization specification. The EMVCo tokenization framework also references its use with EMV chip cards, combining the security benefits of EMV chip with tokenization. Acquirers will also continue to offer tokenization solutions to merchants that address specific merchant needs not otherwise addressed.

References and Notes

[1] Tokenization specifications are currently being defined by the industry, with different names for the types of tokens being proposed.
[2] These types of tokens are being referred to as "payment tokens" or "EMV tokens."
[3] These types of tokens are being referred to as "security tokens" or "acquirer tokens."
[4] Content was developed with contributions from ASC X9.
[5] EMV Payment Tokenisation Specification – Technical Framework, Version 1.0, EMVCo, March 2014
[6] The EMVCo specification defines "payment tokens" or "EMV tokens" that will function in place of the actual payment account number to perform a payment transaction.
[7] Additional information on NFC mobile payment using secure elements or HCE can be found in the Smart Card Alliance white paper, "Host Card Emulation (HCE) 101."
[8] "Apple Announces Apple Pay," Apple press release, Sept. 9, 2014
[9] Content was contributed by the PCI Security Standards Council.
[10] Content was developed with contributions from The Clearing House.

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 will be hosting a full-day preconference workshop, "Enterprise Physical Access Control Systems (EPACS) Using Smart Card Technology for Government and Commercial Organization," at ISC West on April 14, 2015.
- Newly elected Council officers for 2015-2015 are: David Helbock, XTec – chair; Frazier Evans, Booz Allen Hamilton – vice chair; Steve Rogers, IQ Devices – secretary.

Health and Human Services Council

- The Health and Human Services Council is working on a patient identity brief and planning activities for 2015.
- The Council collaborated with the Workgroup for Electronic Data Interchange (WEDI) on the white paper, "Secure Patient Identification: Feasibility of a Security Role for Subscriber ID Cards," which was published in November.
- Newly elected Council officers for 2015-2015 are: Morgan Richard, XTec – chair; David Batchelor, LifeMed ID – vice chair.

Identity Council

- The Identity Council is planning activities for 2015, with statements of work for two projects currently being developed: a white paper on derived credentials and a brief on the role of smart card technology in FIDO protocol implementations.
- Newly elected Council officers for 2015-2015 are: Bryan Ichikawa, Deloitte – chair; Neville Pattinson, Gemalto – vice chair; Sal D'Agostino, secretary.

Mobile and NFC Council

- The Mobile & NFC Council held a well-attended in-person meeting at the 2015 Payments Summit and is planning activities for 2015.
- Newly elected Council officers for 2015-2015 are: Sadiq Mohammed, MasterCard – chair; Sree Swaminathan, First Data – vice chair; Tony Sabetti, Softcard – secretary.

Payments Council

- The Payments Council held a well-attended in-person meeting at the 2015 Payments Summit and is planning activities for 2015.
- The Council is currently completing on a white paper on the true cost of data breaches.
- Newly elected Council officers for 2015-2015 are: Jack Jania, Gemalto, and Oliver Manahan, MasterCard – co-chairs; Deborah Baxley, Capgemini – vice chair.

Transportation Council

- The Transportation Council held a well-attended in-person meeting at the 2015 Payments Summit and is planning new activities for 2015.
- The Council hosted a cross-industry workshop, "Multimodal Payments Convergence," on Jan. 15th in Washington, DC, in conjunction with the Transportation Research Board (TRB) annual conference. Mike Dinning, U.S. DOT/Volpe Center, Mike Nash, Xerox, and Carol Kuester, MTC, led this project. The workshop included participation of individuals from the U.S. Department of Transportation and key industry organizations, including the American Association of State Highway and Transportation Officials (AASHTO), International Bridge, Tunnel and Turnpike Association (IBTTA), ITS America, Association for Commuter Transportation, and the International Parking Institute (IPI).
- The 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.
- Newly elected Council officers for 2015-2015 are: Jerry Kane, SEPTA – chair; Katina Vaughan, DART – vice chair, transit; Mike Nash, Xerox – vice chair, tolling; Steven Grant, LTK Engineering Services – vice chair, parking.

Other Council Information

- Members from the Mobile and NFC, Payments and Transportation Councils presented in the 2015 Payments Summit pre-conference workshop, "Payments Technologies and Innovations: Payment Strategy Considerations for Issuers, Retailers and Transit Agencies," on Feb. 2nd.
- All Smart Card Alliance Industry Councils planned and hosted breakout sessions during the 2014 Member meeting in Orlando, FL. Presentations from these sessions are available on the Smart Card Alliance members-only web site (member login required).
- Councils completed elections for 2015-2016 Steering Committees and officers. The newly-elected Steering Committees and officers can be found on the Council public web pages.
- The Smart Card Alliance announced the 2014 Council Honor Roll and Top Contributors at the Member Meeting. The Honor Roll recognizes the individuals who were leading contributors and participants in the council projects and activities.
- 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 Smart Card Alliance Members

- E4 Security Consulting, LLC, Associate
- Morpho (Safran), General
- NextGen ID, Inc., General
- Quadagno & Associates, Inc., Associate
- SPARC Security Solutions, General
- TRI County Metropolitan Transportation District of Oregon, Government
- TYCO Integrated Security, General

New CSCIP Recipients

- Muhammad Naumann Ahmed, TSYS Acquiring Solutions
- Deborah Andreozzi, TSYS*
- Ben Bruno, TSYS Acquiring Solutions
- Natalie Bullard, TSYS*
- Jessica Burch, TSYS*
- Rico Cantrell, TSYS Acquiring Solutions
- Audria Crain, TSYS*
- Gus Damian, TSYS Acquiring Solutions
- Abigal Floyd, TSYS*
- Thomas Fluegel, TSYS Acquiring Solutions
- Tom Griffin, TSYS Acquiring Solutions
- Sandra Gunnels, TSYS*
- Joseph Handschu, HQS International
- Megan Hofer, TSYS*
- Jenifer Kennedy, TSYS*
- Alicia King, TSYS*
- Stacey C. McCarthy, TSYS*
- Andrew Patania, First Data
- Patrick Plazas, TSYS*
- Lance Robinson, TSYS*
- Chadrick Sine, SAIC
- Keith Stephan, TSYS*
- Sean Stern, TSYS*
- Tiffany Szabo, TSYS*
- Kelly Urban, First Data
- Mario Urquilla, Xtrategies, LLC
- Michael J. VanBibber, TSYS*

**Denotes corporate training class recipients*

New CSEIP Recipients

- Gunvir Baveja, eVigilant.com Inc.
- Kevin Beacom, HID Global
- Thirl Berry, Executive Technologies Corp.
- Ryan Breeden, Pentagon Force Protection Agency*
- Christopher Byron, CertiPath Inc.
- Aldrich Camat, Department of Homeland Security
- Kathryn Captain, M.C. Dean, Inc.
- Joe Cunetta, Brivo Systems, LLC
- Mark Dale, XTec
- Forrest Davenport, ICF International
- Susan Doherty, Security Install Solutions, Inc.
- Nasir Durant, Secure Missions Solutions, Inc.*
- David Fick, Pentagon Force Protection Agency*
- Steven Gray, Johnson Control Security Services
- Matt Greer, Orion Management
- David Harris, HID Global
- Nicholas Johnson, M.C. Dean, Inc.
- Mike Kelley, Secure Missions Solutions, Inc.*
- Dan Novak, Convergint Technologies
- Dwayne M. Pfeiffer, Northrop Grumman IT
- Brandy Sloan, Gallagher Group Limited
- Adam Somers, M.C. Dean, Inc.
- Nigel Stewart, Secure Missions Solutions, Inc.*
- Darryl Stringfellow, Chenega Management
- Michael Taylor, M.C. Dean, Inc.
- Edward Yu, Secure Missions Solutions, Inc.*

**Denotes corporate training class recipients*

New CSCP/G Recipients

- John Moore, Intercede Limited
- Nicholas C. Wryter, XTec

For more information, 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.