SECURE TECHNOLOGY ALLIANCE

NOVEMBER 2019

SECURE TECH TALK

A quarterly newsletter for members and friends of the Alliance

Executive Director Message

Recently, the Secure Technology Alliance announced its yearly top individual contributors in each of the industry councils and the council Honor Roll – the individuals who were leading contributors and participants in council projects and activities. This recognition is an opportunity for the Alliance to highlight the dedicated individuals and organizations who contribute their time and talents to the rest of the secure technology industry through the year. Read more about the individuals and member organizations who led the Alliance to success in 2019.

Click to Read Letter ...

In This Issue:

On the Web:

Feature Article:
EMV Payment Tokenization

Tokenization substitutes placeholder characters or a surrogate, called a payment token, for the primary account number (PAN) in a financial transaction. As used in this article, tokenization means replacing a PAN with a non-sensitive value that represents a card number for the purpose of payment processing. The tokenization service is offered by a token service provider (TSP), which is typically a payment network, an acquirer, a third-party service provider, or an issuer.

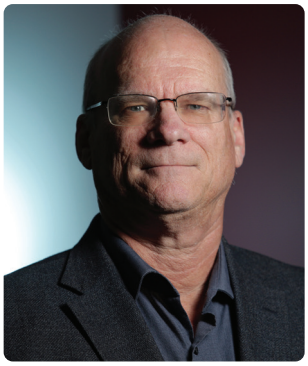
Click to Read More …

Upcoming Event:

13th Annual Payments Summit
Feb. 24-27, 2020
Salt Lake Marriott Downtown at City Creek, Utah
www.stapayments.com

Join us at The Payments Summit in February, the premier industry event covering all things payments, including FinTech, payment technology, mobile payments, NFC, contactless, transit payments, mobility as a service and more. Registration is now open for the event. The additional audience from the co-located U.S. Payments Forum All-Members meeting results in the most comprehensive gathering of card and payments professionals ever.

Secure Technology Alliance Recognizes Members for Outstanding Contributions in 2019



Recently, the Secure Technology Alliance announced its yearly top individual contributors in each of the industry councils and the council Honor Roll – the individuals who were leading contributors and participants in council projects and activities. This recognition is an opportunity for the Alliance to highlight the dedicated individuals and organizations who contribute their time and talents to the rest of the secure technology industry through the year.

The 2019 Honor Roll was compiled based on council leadership, project leadership, project participation and meeting participation from July 2018 through June 2019. Last year, we had a total of 436 individual members who were involved in one or more councils. They came from 76 different organizations, which represents 76.8% of our membership companies.

This year's Honor Roll consists of 77 top contributors from six different industry councils – Access Control, Identity, Internet of Things Security, Mobile, Payments, and Transportation. Special recognition awards went to the council chairs and top ranked contributors in each council and certificates were awarded to the other 2019 Honor Roll members.

The top contributors for each industry council are:

Access Control Council. Chair Adam Shane, LEIDOS; Chair Clay Estes, HID Global; and top contributors Mark Dale, XTec, Inc.; Lars Suneborn, ID Technology Partners; and William Windsor, Department of Homeland Security

Identity Council. Chair Tom Lockwood, NextgenID, Inc.; and top contributors David Coley, Intercede; John Fessler, Exponent, Inc.; and David Kelts, GET Group North America

Internet of Things Security Council. Chair Sri Ramachandran, G+D Mobile Security; and top contributors Sandy Carielli, Entrust Datacard; Josh Jabs, Entrust Datacard; Andrew Jamieson, Underwriters Laboratories (UL); and John Neal, NXP Semiconductors

Mobile Council. Co-chairs Sadiq Mohammed, Mastercard; and Sridher Swaminathan, First Data, now Fiserv; and top contributors David Dekozan, Cubic Transportation Systems, Inc.; Jako Fritz, UL; and David Worthington, Rambus

Payments Council. Chair Oliver Manahan, Infineon Technologies; and top contributors Jose Correa, NXP Semiconductors; Gerry Glindro, IDEMIA; and Nick Pisarev, G+D Mobile Security

Transportation Council. Chair Jerry Kane, Southeastern Pennsylvania Transportation Authority (SEPTA); and top contributors Mike Dinning, U.S. Department of Transportation/ Volpe Center; Jennifer Dogin, Mastercard; Amy Linden, Metropolitan Transportation Authority; Tina Morch-Pierre, Dallas Area Rapid Transit; Nick Pisarev, G+D Mobile Security; and David Weir, Metropolitan Transportation Commission

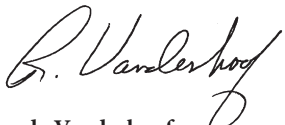
The contributions from these member-driven councils included publishing education and outreach material for different markets, hosting webinars and workshops, developing industry positions on key government and private initiatives, and establishing relationships with related industry groups. The results of the councils' work are viewed as authoritative educational material for both the U.S. and international secure technology markets and help drive secure technology implementations in the U.S.

The Secure Technology Alliance also announced the organizations receiving the 2019 Secure Technology Alliance Center of Excellence (COE) designation. This program recognizes an elite mix of member organizations who, each year, reach the highest level of active participation in the Alliance by having made outstanding contributions in the form of organization-wide leadership of time, talent and resources across a wide mix of Alliance activities.

The 13 member companies that were awarded the Center of Excellence recognition for 2019 are: American Express; CPI Card Group; Cubic Transportation Systems, Inc.; Department of Homeland Security; Discover Financial Services; First Data, now Fiserv; G+D Mobile Security; Gemalto, a Thales Company; IDEMIA; Infineon Technologies; Mastercard; UL and Visa.

Congratulations to all of the 2019 award winners and thank you for contributions you have made to the Alliance and the entire security market over the past year.

Sincerely,



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

Updates from the Alliance Industry Councils

Secure Technology Alliance councils continue to be active in providing education and commentary on new and emerging secure technologies.

Access Control Council

- The Access Control Council is developing a new white paper on temporary identity credentials for Federal agencies

Identity Council

- The Identity Council has focused its efforts on the mobile driver's license (mDL) initiative. The Council's mDL project team has an active outreach program to engage participants from multiple industry sectors. The goal is to raise awareness, support development, accelerate adoption and educate the market on the technology and applications for state-issued mDLs. This initiative includes discussion of key adoption issues such as interoperability, utility, ease of use, and privacy
- The Council is now developing an mDL overview white paper which discusses mDL technology and uses and key implementation considerations

Payments Council

- The Payments Council has three active projects: dynamic security code cards white paper; wearables white paper update; and open payments framework for electric vehicle charging
- The electric vehicle charging open payments framework project is discussing a number of approaches to streamline payment, including: contract payment using the new ISO 15118 standard; direct payment leveraging the ISO 15118 standard; and external payment with a payment terminal integrated into the charging station

Transportation Council

- The Transportation Council is developing a vision white paper focused on payments integration for Mobility as a Service (MaaS) initiatives and planning 2020 activities in support of MaaS

Other Council Information

- Secure Technology Alliance members are now able to request guest participation in U.S. Payments Forum projects. The list of active Forum projects is available on the Alliance member web site. If you would like to participate in one of the Forum projects, please contact Cathy Medich. A list of active Secure Technology Alliance Council projects is also available to promote cross-council participation

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.

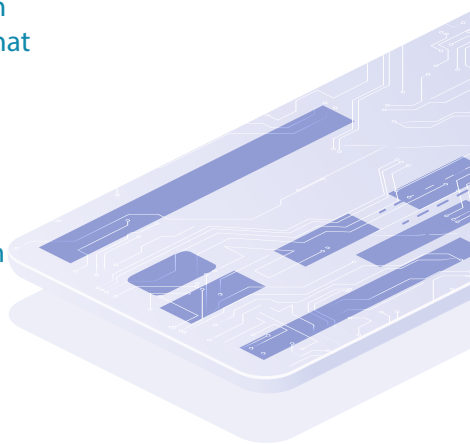
EMV PAYMENT TOKENIZATION

Tokenization substitutes placeholder characters or a surrogate, called a payment token, for the primary account number (PAN) in a financial transaction. As used in this article, tokenization means replacing a PAN with a non-sensitive value that represents a card number for the purpose of payment processing. The tokenization service is offered by a token service provider (TSP), which is typically a payment network, an acquirer, a third-party service provider, or an issuer.

Tokenization protects payment data using a combination of techniques, such as secure storage of sensitive data or and/cryptographic controls, ensuring that an unauthorized party cannot mathematically reverse the token value to the original PAN. Token domain controls protect the token against unauthorized use.

Tokenization may use various format options for tokens, ranging from token values that are distinguishably different from the PAN to others that maintain some of the original digits of the PAN and look similar.

This article discusses tokenization and provides an overview of the EMV payment tokenization process and use cases.



Types of Tokens

Two types of tokens are generally in use today: acquiring domain tokens (aka merchant or acquirer tokens) and payment tokens.

Acquiring domain tokens were developed over a decade ago, as a solution to protect data at rest and as a way to comply with PCI DSS requirements. Many merchants use a tokenization service offered by their acquirer, and they are often intended to work with merchant processes such as return, loyalty, and analytics.

Some larger merchants create and manage their own tokens for a variety of reasons, including needing a PCI-compliant solution before acquirers had introduced such solutions, preserving independence from acquirers to allow for multiple acquirer relationships, and accommodating proprietary or closed-loop payment networks such as private label and gift cards.

An e- or m-commerce card-on-file (COF) token is a specific type of acquiring domain token that is used in online or mobile channels. COF acquiring domain tokens are typically unique to a particular channel and merchant.

EMV payment tokens are open-loop tokens provisioned by a token service provider (TSP) and, like other tokens, are used to replace the actual payment credential (e.g., PAN) with another numeric value. Payment tokens may vary depending on implementation, but typically there is a unique token for each device, which bears no resemblance to the PAN (e.g., the final four digits do not match). They are used both for proximity contactless EMV transactions and, in some cases, for in-app transactions (e.g., Apple Pay). The same token value is used across all merchants.

Because tokens are typically unique to a device and channel, a single PAN can be represented by many tokens. For example, suppose Joe and Betty Smith share a credit card. That card can be represented by the following different tokens:

1. Joe's Apple Pay token in his iPhone
2. Joe's Apple Pay token on his Apple watch
3. Betty's Google Pay token on her Android device
4. Joe's e-commerce COF token with Merchant B
5. Betty's token with a pay button

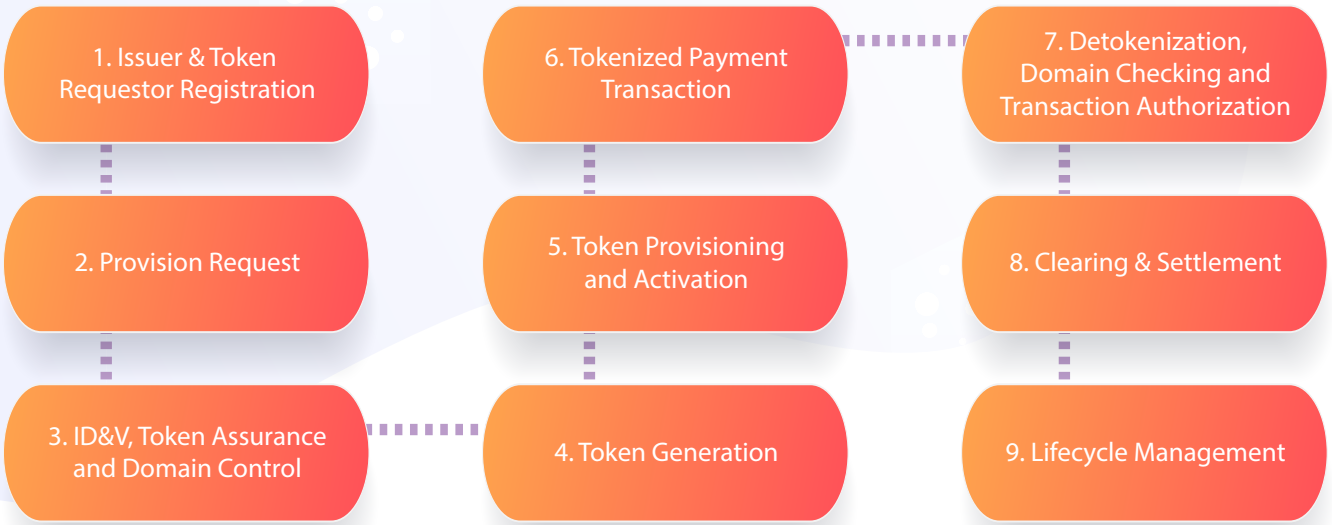
Payment Tokenization Process

The payment tokenization process involves three primary participants: the token requestor, the TSP, and the payment card issuer. Each role performs different functions, as listed in Figure 1.

FIGURE 1. Participants in the Tokenization Process and their Associated Functions

Token Requestor	Token Service Provider	Issuer
Integrates to token service provider in order to request tokens	Facilitates identification and verification between Token Requestor and Issuer	Integrates to token service provider in order to approve tokens
Provides interface for consumers and cardholders	Pre-screens and passes token request to issuer	Evaluates and approves tokens based on cardholder identification and verification
Requests tokens for PANs based on cardholder entry of account data	Establishes mapping and domain controls for approved tokens	Manages lifecycle of token and authorizes transactions
	Acts as token delivery mechanism to Token requestor	

FIGURE 2. Overview of the Tokenization Process



The tokenization process includes nine major activities (Figure 2):

1. The issuer and token requester register with a token program.
2. The token requestor sends a provisioning request.
3. The issuer validates the card credentials and cardholder through an identity and verification (ID&V) process and sets the assurance level and any domain controls for the token.
4. The token is generated.
5. The token is provisioned and activated.
6. The cardholder uses the token in a payment transaction.
7. The token from the authorization message is detokenized and validated and the transaction is authorized.
8. The token is used to clear and settle the transaction.
9. The token is managed through its lifecycle.

Tokenization Use Case Scenarios

Payment tokenization can be implemented in a variety of environments and use cases:

- In-store EMV contactless payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)
- In-app payments with device-centric digital wallets
- Card-on-file (COF) and recurring payments
- Pay button payments
- Payments made with wearables
- Payments made with Internet of Things (IoT) devices

In-Store EMV Contactless Payments with Device-Centric Digital Wallets. Apple, Google, and Samsung were among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases. These device-centric digital wallets play the role of a token requestor; they may capture the cardholder's PAN and request that it be replaced with a payment token from a TSP. Tokenization of payment credentials in digital wallets enables issuers to establish a secure presence on a wallet.

In-App Payments with Device-Centric Digital Wallets. In-app payments with device-centric digital wallets use a token that is already present in a digital wallet for checkout using a merchant's mobile app. In many cases, the digital wallet provider works with the merchant to enable the capability to pass the token during the transaction. In-app payments alleviate the need to enter payment card details, and other relevant information, manually into the merchant app while protecting the PAN.

Merchant Card-On-File and Recurring Payments. E-commerce merchants may store the customer payment credentials for use in recurring payments, installment payments, or on-demand purchases. Storing PAN information can create risk for merchants. Tokenization can mitigate these risks by replacing the PAN with a payment token, similar to the token used in a digital wallet. In this case, the merchant is the token requestor. Traditional e-commerce transactions are more secure when the TSP domain controls en-

sure that tokens are unique to each merchant and that transactions are secured with token cryptograms.

Pay Button Payments. Pay buttons are used by e-commerce sites in cases where the e-commerce merchant does not want to keep a card on file but still wants to take advantage of the security offered by tokenization. The button can tokenize the credentials, similar to the process that occurs when the customer uses a digital wallet. Pay buttons can enable tokens to be stored for multiple issuers and multiple payment network brands, and can also provide billing and shipping addresses to complete the checkout process. As in the in-app payment use case, consumers need not enter payment card information into the merchant app, and the PAN is protected where a token is provided.

Payments Using Wearables. Wearables are personal devices, such as fitness trackers, smart watches, clothing, or apparel, that are typically connected to the Internet through a separate WiFi- or Internet-enabled device. Wearables may or may not have a user interface and rely on a companion app that is resident on another mobile device (for example, a mobile phone with the app associated with a fitness tracker). This connectivity allows the wearable to be linked to a token requestor. Tokenization is facilitated through the app and then enabled for NFC transactions only. At present, tokenization provisioning and processing are typically the same as for device-centric digital wallets.

Payments Using the IoT. The IoT is a category of connected devices that expands beyond wearables to devices such as refrigerators or cars. Unlike wearables, IoT devices have direct network connectivity and may include a user interface. The connectivity and user interface facilitate both tokenization and e-commerce transactions. For example, a refrigerator may have a touch screen that can be used to order groceries. The payment credentials can be entered into the screen and tokenized for payments. Currently, IoT devices typically support e-commerce transactions. At present, tokenization provisioning and processing are typically the same as for merchant card-on-file transactions.

Conclusions and Additional Information

EMV payment tokenization was introduced as a tool to protect payment card data and reduce the opportunity for using card data for fraudulent purposes. Tokenization provides an important layer of payment security. Tokenization impacts all payment stakeholders, has implementation considerations across the ecosystem, and affects the retailer payment and customer service processes. The U.S. Payments Forum white paper, EMV Payment Tokenization Primer and Lessons Learned, from which this article was extracted, provides additional details on EMV payment token services, provisioning and transaction processing flows, and impact on merchant processes.

U.S. Payments Forum Resources

- The Forum Testing and Certification Working Committee published a new white paper, Options for Reducing Level 3 EMV Certification Time for Retailer Systems using Electronic Payment Servers. The white paper discusses solutions to help reduce the implementation time and effort required for the automatic fuel dispenser (AFD) community to meet the October 2020 fraud liability shift deadline. It documents the "Redundancy Reduction Approach (RRA)" – an approach that may reduce the number of formal Level 3 (L3) certifications required, reduce time lags when a solution is being certified, and reduce wait time between submission, review and response
- The Forum hosted a well-attended webinar, Contactless POS Experience Best Practices, on October 8th. The webinar discussed best practices for consumer communications at the POS, consumer transaction prompting and flow, and cashier training. Speakers included: Berke Baydu, Mastercard; TJ Considine, Visa; Randy Vanderhoof, U.S. Payments Forum. The webinar recording is available on the Forum web site
- The Forum Mobile and Contactless Payments Working Committee published a new white paper, How Emerging Data Elements Can Support Mobile Wallet Use Cases. The white paper provides an educational resource on the emerging data elements – Wallet ID (WID), Token Requester ID (TRID) and Payment Account Reference (PAR) – and outlines their use in face-to-face transactions

The full list of active U.S. Payments Forum projects is available on the Alliance members-only site.

Alliance in the News

- "How digital driver's licenses may replace the password" PaymentsSource. This article features comments from Director Vanderhoof on digital identity, mobile driver's licenses and the future of the identity ecosystem.
- "Secure Technology Alliance launches Mobile Driver's License Initiative" SecureIDNews. This feature on the Secure Technology Alliance highlights the recently-announced Mobile Driver's License Initiative.
- "Older, custom transit technology puts the brakes on payments innovation" PaymentsSource. Director Vanderhoof shares insight on security compliance challenges for open-loop transit.

Congratulations New Certificants

CSCIP/G

- Chris Chapman, Johnson Controls*
- Jennifer Hicks, Johnson Controls*
- Erik Larsen, Johnson Controls*
- Stafford Mahfouz, Johnson Controls*

CSEIP

- Joe Barbone, RedTop Group
- Jennifer Hicks, Johnson Controls
- Scott Hunter, Johnson Controls
- Kyle Murphy, Johnson Controls
- Duane Poliey, RedTop Group
- Gregory Sehrt, Xpect Solutions
- Ricard Smith, Parsons Corporation
- Joseph Stinnett, Johnson Controls

CSEIP Recertified

- Colin Doniger, Department of Homeland Security/Officer of the Chief Security Officer
- Richard Dietz, Secure Mission Solutions
- Nasir Durrani, Secure Mission Solutions
- Paul Hagen, Secure Mission Solutions
- James Hansen, Hansen Technical Services
- Donald Hamilton, Department of Homeland Security
- Martin Hoffman, Johnson Controls
- Nicolas Johnson, M.C. Dean
- Douglas Kim, Business Integra
- Brian Mann, SETEC
- David Miller, Business Integra
- Dan Novak, Convergint Technologies
- Nicola Pisani, M.C. Dean
- Shawn Ruddo, Integrated Security Technologies
- Job Rushdan, Diamond Security
- Adam Somers, M.C. Dean
- Kathryn Spangler, M.C. Dean
- Nigel Stewart, M.C. Dean
- Michael Taylor, M.C. Dean
- William Windsor, Department of the Treasury
- Brian Young, Integrated Security Solutions
- Edward Yu, M.C. Dean

**Denotes corporate exam. For more information, contact Randy Vanderhoof*

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).