Meeting Between Staff of the Federal Reserve Board and Representatives of Mastercard
June 10, 2019

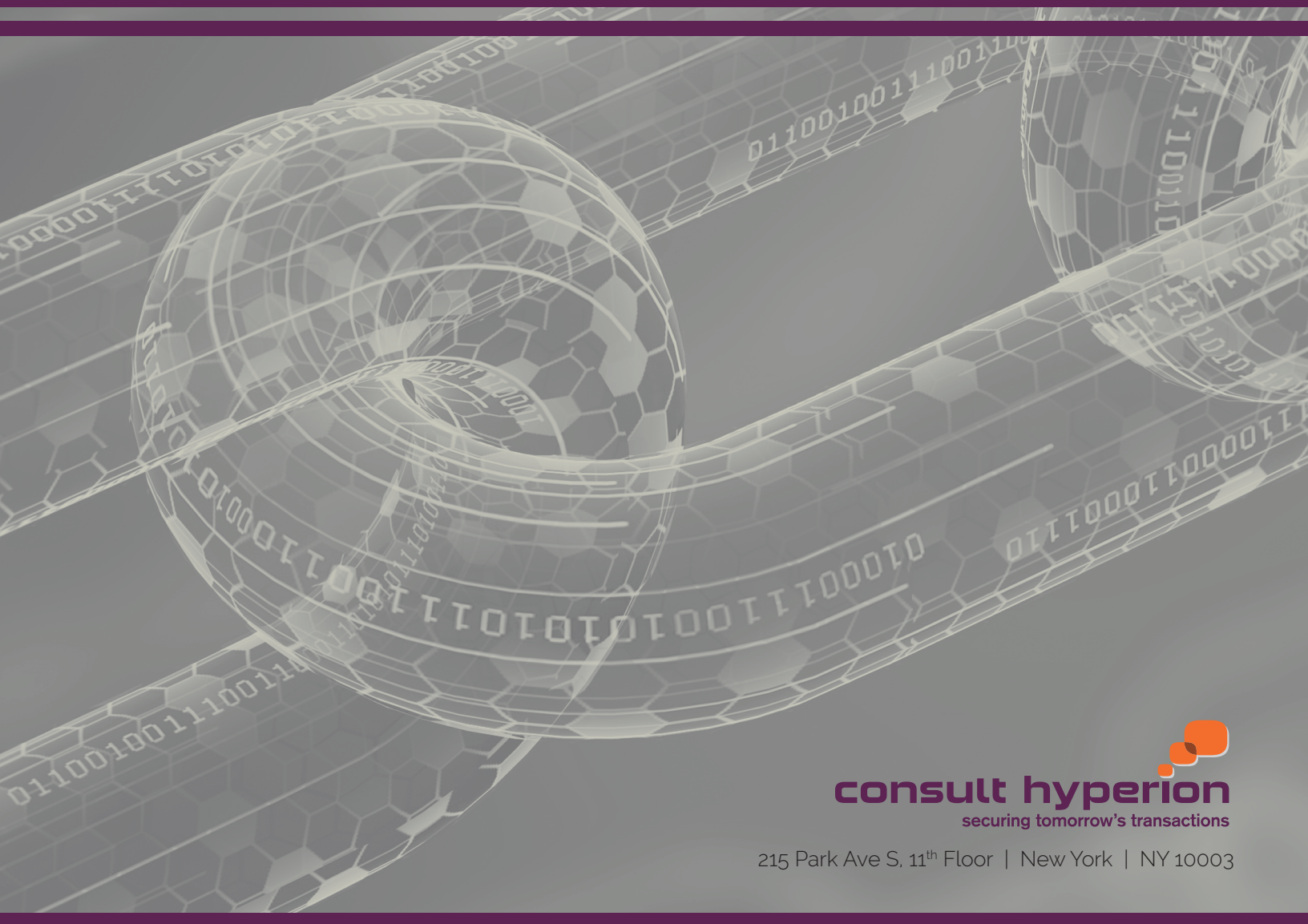
Participants: Julian Alcazar, Clinton Chen, Nicholas Ehlert, Susan Foley, Jason Kim, Mark Manuszak, Stephanie Martin, Emily Massaro, David Mills, Hayden Parsley, Ian Spear, and Krzysztof Wozniak (Federal Reserve Board)

Randi Adelstein, Chirodeep Aikat, Rob Keenan, Jessica Turner, and Tina Woo (Mastercard); Joel Feinberg (Sidley Austin)

Summary: Representatives of Mastercard met with Federal Reserve Board staff to discuss topics related to the routing of debit card transactions in the United States. As a continuation from a 2018 meeting, representatives of Mastercard provided more detail about the prioritization that merchants can make between the common and global debit application identifiers (AID), as well as Mastercard's role in tokenization. Representatives also discussed Mastercard's implementation of EMVCo's Secure Remote Commerce specifications.

Attachment

The Application Identifier or Aid for Debit



consult hyperion
securing tomorrow's transactions

215 Park Ave S, 11th Floor | New York | NY 10003

Table of Contents

Application Identifier or AID for Debit

I. Executive Summary

Consult Hyperion has been asked to consider the technical ramifications of the US Debit Networks[1] using their own application identifier (AID). Today the US Debit Networks license the use of the various International Card Schemes' (ICSs) Common AIDs and related applications to support their own EMV requirements.

When determining the ability of the US Debit Networks to create or acquire solutions, one must consider the various use cases that the US Debit Networks are seeking to support. These use cases, as considered in this report, are the ability to interface to the point-of-sale (POS) via the contact and contactless terminal interface.

Currently, the US Debit Networks rely on technology provided by the ICSs, but based on the factors discussed herein and similar use cases outside of the US, they could develop their own technology to operate independently. Indeed, many non-US debit networks have either developed their own unique specifications or embrace other available solutions so that they do not need to license from an ICS a Common AID.

These other solutions include, but are not limited to, ACXSYS's (Interac) Flash, Gemalto's Pure and the European Card Payment Association's (ECPA) CPACE. These commercial products have provided value-added features, such as the use of a mobile device and contactless interface, and led to the creation of proprietary revenue or risk-reducing techniques for the debit networks that have adopted them. Examples of such risk-reducing techniques would include improved data that enables the network to mitigate potential fraud risk, protect from fraud tactics such as transaction replay, and improved anti-counterfeiting capabilities.

Through the use of these available solutions, many domestic networks outside of the US have successfully implemented EMV, without the need to depend on the AID or related card, mobile and terminal applications of the various ICSs.

1 Examples of the largest US Debit Networks include: AFFN, ATH, CO-OP Financial Services, Jeanie, NETS, NYCE, Presto!, PULSE, SHAZAM, Culiance and STAR.

As discussed in the analysis below, Consult Hyperion concludes that that there are no technical barriers restricting any US Debit Network from developing or otherwise obtaining access to its own competitive EMV-based application and AID, whether individually or through collaborations, such as the Debit Network Alliance. There would be costs and changes required of the US Debit Networks, but making an investment could benefit them. However, these organizations are well funded and technically astute.

II. The EMV specifications

This section provides a summary primer on the EMV specifications. An understanding of these specifications is essential to assessing whether a US Debit Network can develop or otherwise obtain access to its own EMV-based application and AID.

All EMV cards use an integrated circuit, designed with the ability to securely store asymmetric private keys (RSA) and symmetric secrets (TDES or AES) and execute EMV-card-scheme-defined logic, within a trusted and secure execution environment. With the magnetic stripe on cards, we were accustomed to swiping our cards through a card reader. This reader processed the information on the stripe and accessed the proper data and accounts. EMV has the same goal, but with a different approach. With EMV, we insert a card into a reader. The reader locks the card in place and accesses payment information. The card creates a unique cryptographic signature for this transaction with input from the reader. This cryptographic signature, known as a cryptogram, must be validated by the issuer during transaction processing. This process makes perpetrating fraud much more difficult.

To ensure the interoperability of EMV cards, EMVCo established a common set of requirements and embraced the use of the ISO 7816 specification as the base for the creation of a set of specifications branded the "EMV Integrated Circuit Card Specification of Payment Systems" (EMV Specifications). The EMV Specifications are a set of cryptographic and terminal-centric documents that define the transaction flow, a set of commands, processes and data elements that are used by each EMV card network's unique chip card-specification. The EMV Specifications do not define how the chip card application should be implemented. It is the responsibility of each EMV card network to define the details of the transaction flow, how the card will act and specify what is to be included in the card's response to the terminal.

Given that the EMV specifications are designed as a toolkit, it is reasonably straightforward for a card scheme to specify and customize a contact implementation of EMV to be used at a POS terminal to meet unique local requirements in a jurisdiction.

Before the introduction of near-field communication (NFC) as a method of payment, and based on European market demand, EMVCo defined two additional contact specifications:

- The Common Core Definitions (CCD), a minimum set of data elements required to perform a contact chip transaction.
- The Common Payment Application (CPA), which defines a common chip application that implements CCD.

These specifications are designed to create a single application that issuers can use to support any contact-based EMV card network. Certain markets embrace this approach and have implemented accordingly.

A. Meeting the core requirements

The EMV Specifications address the following core requirements:

1. To reduce payment card fraud and, in particular, counterfeit and lost and stolen fraud.
2. To shift offline authorization from the merchant terminal floor limits to chip based parameters, defined and controlled by the issuer.
3. To support multiple means of payment within the same card. The concept allows the inclusion of multiple EMV applications and application data files associated with multiple sources of funds, payment brands and/or financial institutions.
4. To provide an opportunity for issuers and payment brands to expand their service offerings, given the power and flexibility of a computer in chip cards and devices.

Multi-Application Chip Cards and Application Selection

It is important to appreciate both what an AID is and what it represents. Each AID represents the analog of a corresponding network brand historically displayed by the merchant at the POS and printed by the issuer on the card. The AID is a pointer to the directory (or application) within the card where the account specific credentials and data reside.

When the ISO 7816 specification was originally developed, the value of supporting multiple applications, within a single chip, was clearly understood and the ISO standards clearly outlined how this could be achieved. Further, as the multi-application card operating systems were developed, the need to isolate each application from interference from another became a key requirement of these operating systems.

The only technical challenges associated with issuing a multi-application card are:

- Selecting a chip with enough memory to support each of the applications and associated data that could be enabled within that chip.
- If common data, parameters or keys are to be shared among the various applications within the chip, then the applications themselves must be expressly designed to support these mutually agreed requirements.
- Issuers must be aware of which applications and AIDs are active in the card at the POS, when any processes are performed that receive data from, or seek to update, card-specific keys or data.

The EMV specifications define how the "SELECT" command is used by the terminal to support how the merchant and cardholder jointly determine which AID (and therefore which payment network, financial institution and account) is selected to attempt to pay for the goods and services. The principal concept EMV defines in book 1, section 11 is the creation by the terminal of the candidate list.[2] Once constructed, this list identifies those AIDs which are supported by both the terminal and the card.

Assuming the card has been inserted into the terminal's "contact interface" and the candidate list has been created, the merchant then proceeds to either:

1. Select the highest priority application, from the candidate list; or
2. Offer the consumer the ability to choose from this same list.

These methods are clearly defined in EMVCo book 1, section 12.

At the end of this process, the terminal is able to read data from the card and is capable of communicating with the application in the card over a logical channel, based on the selected AID. The card utilizes the software, data and secrets associated with that AID and the terminal using the unique software and configuration details associated with that AID. Based on the unique EMV card specifications and terminal specifications for the EMV transaction flow, the transaction proceeds according to the rules, procedures and specifications as defined in the applicable EMV card network's operating regulations.

2 EMV Integrated Circuit Card Specifications for Payment Systems Book 1 Application Independent ICC to Terminal Interface Requirements

B. Domestic Contact Implementations

Contact EMV refers to the EMV contact chip specifications defining how financial transactions are conducted using contact chip cards. These cards support cryptographic functions to prevent counterfeiting of cards and additional functions that make them more secure than traditional magnetic-stripe cards. Any organization can have access to these specifications.

C. Contactless and Dual Interface

Unlike in the case of contact transactions, each payment scheme has developed its own unique and proprietary approach to how to support contactless payment transactions. Each ICS utilizes the basic principles of the EMV Specifications and ISO 14443 and 18092 standards, yet its individual efforts have resulted in the development of unique kernels. An EMV kernel is a set of functions that provides the processing logic and data that are required to perform an EMV contact or contactless transaction. The kernel is part of the merchant terminal payment application. Each kernel is based on the proprietary approach each ICS embraced in its implementation of contactless payment transactions.

A kernel controls the interaction between the terminal and the card. In a contact transaction, there is only one kernel, the so-called tool kit. The tool kit is as specified by EMVCo and the terminal manufacturers and adds the necessary customizations defined within each payment scheme's terminal specifications. In a contactless transaction, EMVCo specifies how the card is selected and matched to its kernel, which is specific to each payment scheme.

This lack of a single contactless kernel means the domestic payment networks have to obtain the right from an ICS to buy or develop a consumer device application able to operate within a kernel or develop (or license) their own kernel.

Some examples of how some country and domestic schemes addressed their requirements are:

- Interac in Canada created "Flash"
- Bankaxept in Norway, a new scheme in UAE and ELO in Brazil selected "Flash"
- NPCI in India developed Rupay
- Other domestic schemes like, EFTPOS in Australia, MEPS in Malaysia, TROY in Turkey, EC in Switzerland turned to entities like Discover, Gemalto and Oberthur and licensed a full suite of solutions
- Most recently, the ECPA came together to develop CPACE to address contactless payments. The approach they took was to utilize the original CPA contact specification and use it as a base to design their own contactless kernel and associated chip card specifications.

1. NFC "contactless" based Mobile Payment

With the release of the ISO 18092 NFC standards, mobile handset manufacturers (OEMs) and mobile network operators (MNOs) introduced NFC contactless capabilities with a goal of enabling contactless mobile payments. The software developed to run inside these mobile devices is based on the EMV card networks' contactless mobile payment specifications based on their contactless card specifications.

These transactions use digital card credentials (known as tokens) the standard for which is the EMV Payment Tokenization Specification. Payment credentials are provisioned by the OEM either:

- Within the secure element built into the iPhone or other OEM mobile devices; or
- Using Android's Host Card Emulation and refreshing short-term credentials derived from the payment credentials held securely within the token service provider's (TSP) Host Security Modules (HSMs).

These credentials are created at the time of card issuance and can be managed in a deliberate and scheduled manner. In the case of a mobile device, the cardholder determines which cards he or she would like to load into the mobile wallet. More importantly, the cardholder has the ability to select which card to use for the transaction, or which card is the default for most transactions.

2. Contactless Application Selection

When a cardholder presents his or her card or device to the terminal contactless interface, the terminal selects the Proximity Payment System Environment (PPSE), which contains a list of the payment applications available on the card or device. Use of the PPSE enables payments technology providers to ensure their products adhere to EMVCo's Contactless Mobile Payment Product Type Approval requirements.

The terminal creates a candidate list of mutually acceptable AIDs using the PPSE. It then simply selects the first AID in the list, without involving the cardholder, as described in book B, section 3.[3]

III. EMV Debit in the United States

In most of the world, debit cards evolved through the creation of a common national debit network. In the United States, they evolved from multiple regional ATM and debit networks. At one stage there were 35. Today, as a result of consolidation, 16 remain. The introduction of EMV in the United States brings with it added complexity, given the way debit had been implemented in the United States and the Durbin Amendment and its requirement that at least two unaffiliated payment networks be enabled on each debit card in the US.

In September 2012, the EMV Migration Forum (now known as the US Payment Forum) was formed with the objective of bringing a representative body of stakeholders together to discuss and address the migration of the US payments market to EMV. This body was made up of merchants, issuers, processors vendors, interested parties, the ICSs and US Debit Networks. Early on, the EMV Migration Forum recognized the implementation of EMV for US debit would be complicated.

The EMV Specifications assume that the issuer has ultimate control over the personalization and order of presentation of applications configured on its cards. This is achieved, at personalization of the card, by setting the value of the Application Priority Indicator (API) associated with each AID. When the merchant creates the candidate list, the API defines the order the terminal presents the payment networks to the cardholder at application selection.

3 EMV® Contactless Specifications for Payment Systems Book B Entry Point Specification.

Regulation II grants the merchant choice as to how it may route the transaction. Therefore, this requires the merchant to have the ability to recognize which applications are associated with a debit card and enable the merchant to deselect from the candidate list the AIDs associated with payment networks that are not enabled on the debit card.

To increase EMV adoption, the EMV Migration Forum, the ICSs and the US Debit Networks agreed to the concept of the Common AID for "US Debit". The ICSs agreed to a set of terms and conditions with the US Debit Networks. As a result, each of the ICSs licensed its card applications, created its own application-specific Common AID for debit and offered use of its terminal implementations. These licensing arrangements define the scope of the capabilities, within the ICS applications, the US Debit Networks can employ.

Recognizing the need to assure merchant choice, the EMV Migration Forum published a proposal describing how a merchant could modify the standard EMV application selection process, the U.S. Debit EMV Technical Proposal. This document described how a merchant could suppress an ICS's International AID and select the card's Common AID.

Once published, chip card vendors, terminal manufacturers, merchants, acquirers and the ISOs, VARs & ISVs learned how to implement the software necessary to support merchant identification of a debit card and selection of the Common AID.

Today, merchants either route according to the cardholder's selection or implement logic similar to that described in the U.S. Debit EMV Technical Proposal and thereby select only the Common AID and then route transactions as the merchants so choose.

IV. The Future of the Common AID concept

In other markets, upon the advent of contactless and mobile, domestic EMV card networks successfully defined and implemented their own unique EMV specifications or licensed those of another EMV card network.

Now that the US implementation of EMV has moved from a major national initiative to business as usual, financial institutions and the US Debit Networks are seeking to take advantage of the "secure element" within a card or the power of a smart mobile device. To this end, some of the US Debit Networks want to be capable of handling transactions independent of the ICSs.

A. Developing US Debit Network Specific Implementations of EMV

Each of the US Debit Networks has, either individually or through its participation in an industry consortium called the Debit Network Alliance (DNA), the resources and ability to acquire the skills to create its own competitive EMV implementation. Alternatively, as other debit networks have done outside of the US, a US Debit Network, on its own or through, DNA could license one of the many available EMV-based specifications for contactless transactions. As examples, it could:

- License a solution from one of the ICSs, such as MasterCard's M/Chip.
- Renew pursuit of a D-Pas licensing arrangement with Discover.
- License the Interac Flash solution.
- Look to the work of ECPA and develop a meaningful working relationship.
- License the Pure technology Gemalto offers.
- Talk to any number of vendors that have developed the components necessary to create a competitive EMV implementation elsewhere in the world, as discussed below in this paper.

As part of the work, the US Debit Networks will need to help the issuers address:

- The impact and implications on each issuer's cards and key management systems.
- What must change relative to the personalization of the multiple AIDs and applications associated with an account, be it in the card and/or within a mobile device.
- How to authenticate the card and account from the cryptographic signature generated by the application on the card. This may require identifying which application was used from the authorisation data passed to the issuer in the authorisation request as different applications may generate cryptographic signatures differently.
- Education of the cardholder relative to the new application selection process that each will experience at the POS.

B. Issuer US Debit Network Selection

If a US Debit Network develops its own application and AID, this approach will require the issuer, when it changes US Debit Networks, to redefine the applications and AIDs in its chip cards. If the issuer is terminating the relationship with a US Debit Network, it will have to personalize and re-issue these newly configured chip cards to all of its cardholders.[4] This is the same process that an issuer must undertake currently if it changes the ICS on the front of the card. In the case of the mobile device, a mechanism will have to be developed to inform the OEM of the need to replace one AID with another and request a new token.

This could be avoided if the US Debit Networks develop a common application and AID, such as through DNA.

V. Deployment is Possible

The US Debit Networks have a level of both financial wherewithal and technical expertise to execute on a technical roadmap, independent of the ICSs. The US Debit Networks could, as was originally intended, work together within the DNA and register their own Common AID and define their own set of EMV specifications for use among themselves. Or, each could register its own AID. This would be a business decision.

4 This can be mitigated if the issuers personalize multiple AIDs in their cards prior to issuance, and activation/de-activation can be done during any contact EMV transaction if the relevant networks use M/Chip as their card application and use its "Dynamic Activation" feature.

We should also recognize that there is a robust ecosystem of technology vendors, service providers and consultants that can support the US Debit Networks in each step of the development and implementation process.

- Defining a new application selection process and sharing it with the merchant community.
- Working with terminal and chip card suppliers to develop the requisite card and terminal software.
- Working with the various suppliers, vendors, acquirers and test labs to define and create the requisite certification processes for:
    - Chip card applications
    - Terminal kernels
    - Card personalization processes
    - Card and key management changes
    - End to End testing
- Implementing a TSP to support payment tokenization
- Working with the various OEMs to
    - Develop the requisite software
    - Configure the mobile wallets to support their AIDs
    - Provision the cardholders selected debit accounts and issue multiple Token Requests, one per AID
- Defining a mobile device specific methodology to support multiple AIDs, each with an individual format preserving token, associated with a singular account or "card"
- Working with the VARs, ISOs and other members of the acquiring community to upgrade the Point of Sale infrastructure to include the necessary AIDs, kernels, terminal parameters, encryption keys the associated software.

- Informing the issuers to configure their cards according to the various US Debit Network EMV card network specifications.
- Expanding the BIN table to include the various Token BINs each of the TSPs support and define the related routing, provisioning and detokenization procedures

VI. Commercial Considerations

Beyond the technical capabilities, however, below are some of the commercial issues that the US Debit Networks would have to take into consideration in deciding whether to develop and implement their own EMV implementation.

1. Merchant Choice

As defined in Regulation II, the merchant has the ability to determine which payment network through which it would like to route the payment transaction.

EMV describes a process for application selection, yet it does not limit the ability for a party or a group of parties to define, as the EMV Migration Forum did, an alternate mechanism for application selection. Book B of the EMVCo Specification clearly defines a process to support application selection. Like that which was described by the EMV Migration Forum, it is possible to define a methodology to allow the merchant to decide which of the multiple AIDs to select and therefore which route to choose.

2. Mobile Payment and Mobile Wallets

The market is embracing the idea of loading EMV based payment credentials into the various Mobile Payment wallets that issuers, OEMs and others are promoting. EMVCo has defined a coherent architecture for the provisioning and support of EMV payment credentials within a mobile wallet. Each EMV card network can use these as a base to define its mechanism and techniques associated with the provisioning of and transaction support for mobile wallet-initiated payment transactions.

3. Issuer re-issuance

Depending on how the US Debit Networks elect to implement their AIDs, issuers will have to consider the impact on how they negotiate and manage

their relationships with the various US Debit Networks. Today, they can easily shift allegiances without giving a thought to the implications on the reissuance of the card or the EMV payment credentials in a mobile wallet. The US Common AID made these non-issues.

If each US Debit Network is to establish its own AID and either collectively or individually defines the card application, then each time issuers change their US Debit Network affiliations, they will have to reissue their cards and arrange to replace the EMV payment credentials in the mobile wallet. This is something that issuers already do when they change their ICS on cards. There are no technical challenges in supporting such a situation, it is simply a question of cost.

4. Contactless, Mobile and Biometrics Value-Added Services

One issue requiring consideration is the market value of being able to exploit technical capabilities to drive increases in revenue. The adoption of contactless as a method of presenting EMV payment credentials to the merchant terminal offered payment networks the ability to further drive the migration away from cash and towards revenue generating opportunities for issuers and cost-enhancing methods for the merchant community.

Inevitably, as more transactions are shifting from card to mobile, and more cardholders seek to use biometrics to authenticate transactions, , the US Debit Networks would be faced with a decision to either not offer these services because they are not part of the license of the Common AID from the ICSs or to invest in the development of their own proprietary technology.

5. Economic Considerations

Clearly there is a cost to change. The ICSs chose to bear this cost early in the U.S. transition to chip cards, and now the US Debit Networks would need to bear this cost too.

VII. Conclusion

It is possible for any EMV card network to create its own EMV implementation. Any US Debit Network, either individually or through an alliance with DNA, can deliberate or determine if it is best to design its own or license the appropriate components from others.

As a result, and as was the original vision of the EMV Specifications, the US Debit Networks would be in a position to competitively develop enhanced services as part of their wider appeal to the merchant, issuer and/or consumer base.

In summary there are no technical limitations, save time and cost, why the Debit Network Alliance or each US Debit Network cannot:

- License or develop their own EMV card, mobile device and terminal kernel specifications;
- Arrange the development and deployment of the necessary software to support merchants accepting their payment products;
- Arrange the development and deployment of the necessary software to support chip cards supporting their payment products;
- Arrange the development and deployment of the necessary software to support mobile devices supporting their payment products; and
- Develop their own TSP to support tokenization and support potential card, mobile or card-on-file token requests from merchants, issuers or OEMs.

Based on the experience of those debit networks outside of the US that currently license the use of an EMV application and associated AID, the US Debit Networks should be able to enhance and differentiate their products as the ICSs have done.

It goes without saying, change is inevitable. The ability to differentiate is essential in a competitive environment. Consumers and merchants are accustomed to change. Investments to take advantages of revenue or security enriching enhancements are business as usual.

There are no technical limitations that prevent the US Debit Networks from achieving these goals. Also, achieving these goals would position US Debit Networks to innovate in ways that would make their services more competitive.

Thank You

consult hyperion
securing tomorrow's transactions

Becoming a Token Service Provider

01.07.2019

Levvel
101 North Tryon
Suite 1500
Charlotte, NC 28202

Preface

The purpose of this publication is to explore the basics of network Tokenization and how the evolution of Tokenization has led to the opportunity for third parties to play a greater role in card security through the use of digital tokens. It begins with a brief outline of the development of a token service followed by a deeper dive into the technical framework of the various Tokenization models. Finally, it concludes with a walk through of how a third party could create a token service through detailed use cases.

Development and Implementation of a Token Service

The current state of Tokenization provides ample opportunity for a new Token Service Provider (TSP) to be formed and launched into the ecosystem. Launching a new TSP has specific requirements, support models, and considerations that will need to be reviewed and integrated into the launch strategy for any organization considering becoming a TSP. The following overview provides a view into these areas.

Considerations

Motivating the Ecosystem

While there can be a monetary business case for Tokenization, many parts of Tokenization focus less on monetary gain and more on security, operations, or Cardholder experience benefits Tokenization services could provide. Keeping this in mind, any new TSP will need to ensure the value it offers to the ecosystem is a sufficient motivator for other players to participate in utilizing the new TSP services. For example, many cards have already been Tokenized using existing TSPs, and Token Requestors would need additional motivation to Tokenize these cards again using a new TSP. Any new TSP will need to spend time on developing its value proposition to each player within the Tokenization environment, and begin conversations with each of these parties to ensure end-to-end support. This is a consideration that is common to parties that are not the first movers in any industry.

One approach to ease this path of entry would be for a new TSP to focus on use cases not currently solved with Tokenization by the current TSPs.

Reducing Friction

The current implementation of Tokenization closely aligns with the processes and flows that are present in non-Tokenized transactions for routing, authorization, clearing, and settlement. This design was intentional to allow the added benefits of Tokenization to be realized, while limiting the impact to players that exist in the non-Tokenized transaction flow. While there may be opportunities to innovate using Tokenization as a platform, the impact on Merchants, Acquirers, Issuers, and Token Requestors must be analyzed in comparison with the overall business case for any innovative implementation.

The Cardholder experience is of particular importance as a consideration for any implementation. Often technical challenges can be overcome, but present a reduction in the overall Cardholder experience. While Tokenization offers many benefits to each player in the environment, ultimately Cardholder adoption will determine the adoption of Tokenization across the industry. If the experience using tokens for payment does not offer a value proposition to the Cardholder, he or she will not have a motivation to participate.

Ecommerce has a particular opportunity to create an experience that significantly reduces friction for the Cardholder while simultaneously providing a more secure and trusted transaction for Merchants and Issuers. For any new TSP, these use cases that reduce friction for the Cardholder and the Merchant should be in strategy and design discussions.

Resources

Becoming a TSP means more than offering Tokenization services, it means that the organization will be adding Tokenization as a product to its suite of offerings for those it serves. Because Tokenization is positioned as a product but also is a service, the resources and investment into Tokenization will require more than technical ability and infrastructure. It will require the build out of both business and technical teams to drive, manage, and promote this new offering.

Product owners will be needed who ideally have experience with Tokenization, specifically in building or launching token strategies at financial institutions, networks, digital wallets, or others. These resources will need to assist in building the strategy for launching the TSP offering, as well as participate in the implementation process. The product owner will also be instrumental in building a strategic roadmap for insertion of the new TSP into current and new areas of Tokenization, as well as enhancements to the existing product. This is a key resource that will be imperative to the success of the TSP.

Solution architects will be required that have experience with Token Vaults, Tokenization infrastructure, and an understanding of payments flows. These resources will be critical when developing the design strategy for launching the TSP. They will be able to analyze internal systems, gauge existing strengths and weaknesses, and suggest a design architecture that will position the TSP for launching an efficient and productive Tokenization service. After launch, the solution architects will be able to analyze any new innovative Tokenization features added to the product, as well as design for entrance into new Tokenization areas within the market.

Both the business and technical resources will need to work in close communication during the design of the strategy for launch, maintaining the Tokenization product, and in evaluating roadmap opportunities. Additional business and technical resources will need to be included, such as business analysts, program managers, and developers, to create a team of resources supporting the product.

Requirements

The EMVCo Tokenization framework clearly outlines the requirements for an entity to register as a Token Service Provider; however, the framework does not provide a certification service to facilitate a

structured TSP launch. Instead, EMVCo states that a TSP should, "work with Card Issuers and potentially Payment Networks to ascertain additional program and participation requirements." The lack of a formal EMVCo approval process and structure means third parties need to work individually with Traditional Card Network or Issuer to determine what technical and business requirements must be met to serve as a Token Service Provider. Most Traditional Card Networks make these requirements available to interested parties.

Issuer Support

Given that a TSP is Tokenizing cards on behalf of one or more Issuers, it is not possible for an entity to assume this role without integration with the Issuer(s). Often these agreements manifest as a combination of business terms and technical specifications agreed to by both parties. In some cases, the TSP could also provide services on behalf of the Issuer such as token risk management, de-Tokenization, and Token Cryptogram validation.

The business terms of the agreement often include the Issuer portfolio to be supported with Tokenization, any service level agreements (SLAs) provided by the TSP, and any TSP provided interfaces and tools that will be utilized by the Issuer. The Issuer will identify a BIN range or ranges to be supported, and the TSP will be responsible for Tokenizing those cards that fall within the BIN range(s) identified. The TSP will communicate the SLAs, and offer escalation chains for the Issuer to utilize if there are any problems with performance or servicing. The Issuer will also choose what interfaces or tools that will be used including: ID&V management, token status notifications, card eligibility checks, and one-time passcode creation and validation.

The technical specifications detail specific messaging and connection details between the TSP and the Issuer. The BIN assignments will be loaded into BIN tables within the TSP to validate the PAN from any incoming token request as within the Issuer specified BIN range(s). Also access and messaging specifics will have to be identified and agreed upon by the TSP and the Issuer for any TSP provided tools as well as the interface with which the TSP and Issuer will communicate. The Issuer may choose to use only application program interface (API) web service messaging, International Organization for Standardization (ISO) messaging, or a mixture of both. The connection details between the Issuer and TSP will also need to be agreed upon. This could be a multiprotocol label switching (MPLS) connection, virtual private network (VPN), or another type of secure connection that can be used to transmit the necessary data and messaging securely and efficiently.

Traditional Card Network Approval

For the card Tokenization of a Traditional Card Network issued PAN, the TSP will need to obtain approval from the Traditional Card Network that owns the BIN of the PAN being Tokenized. The TSP also may request a Token BIN Range to utilize to create its tokens, which will be supported by the Traditional Card Network, and align with EMVCo Tokenization Framework. The Token BIN would be managed by the TSP, and utilized each time a Provisioning request is received.

Digital Wallet Support

The original use case for EMVCo Tokenization started with the creation of digital wallets such as Apple Pay and Android Pay, and these entities still play a critical role in the viability of any TSP services. The digital wallet serves as both the initiator of the Tokenization process and the presentment mechanism to the Merchant in many cases. As such, a TSP will be required to have both a technical integration and business agreement with the digital wallets who will present the token as a form of payment.

The business agreements usually consist of the BIN range or ranges to be supported, the interfaces to be used, and any specific authentication options that will be supported (call center, banking application, and/or one-time passcode). A new TSP would need to adhere to the interface and communication options that the most common Token Requestors support. Most Token Requestors utilize a combination of APIs and ISO messages to initiate Provisioning, lifecycle management, and notifications. The ID&V authentication options are normally chosen by the Issuer; however, they also must be supported and displayed by the Token Requestor.

The technical specifications can take two forms: adhering to what the Token Requestor offers as messaging design, or forming a standard design for the TSP and allowing the Token Requestor to connect using the TSP specified messaging design. Most common token requesters in the market have specifications that are used across their current TSPs, and will likely want to remain as close to that design as possible. Any new TSP, especially in spaces that have not previously had Tokenization services provided, such as ecommerce, a TSP standard design would be more feasible. Furthermore, if the TSP is introducing an additional token for a single PAN, the wallet provider may require user experience changes to accommodate multiple tokens.

Design

The design for a new TSP is similar to the technical design based on the EMVCo Tokenization Framework, but incorporates some important nuances. In addition, the prospective TSP's internal systems and infrastructure will need to be assessed to determine the best architecture strategy to implement an efficient and manageable TSP solution.

Internal Systems and Processes

As the designs for Provisioning and transactions are being considered, an in-depth analysis of internal systems and processes will need to be completed in order to obtain the following:

- Gaps in hardware or software to support the TSP functionality
- Gaps in resources to support the TSP service as a product
- Current state architecture for design and internal integration of the Token Vault and Tokenization based communications
- Current connection types and bandwidths supported to support the integration of one or more Token Requestors, new or additional Issuer connections, and network-based notifications

- Current reporting capabilities, and structure for external access to reports, whether ad hoc or scheduled

In order to design support for TSP functionality, gaps must be realized and filled to create the holistic support framework Tokenization requires. The Token Vault services will need to be developed and integrated where necessary internally, which includes internal messaging, manipulation of data, and delivery of notifications. These foundational services will support operations teams as they perform daily support functions, assist in maintenance and upgrades to the Tokenization service, and are notified of any potential issues through SLA monitoring services placed on the system. Whether it is Token Requestors, a major Traditional Card Network (i.e., Mastercard or Visa), or an Issuer, SLAs will need to be accounted for in order to provide equal service standards as are present from current TSPs. Finally, Issuers and Token Requestors will request and fully utilize reporting capabilities based on their use of the TSP services. These reports will provide them insights on the performance of their portfolios, fraud controls, and any marketing effort.

Provisioning

For the Provisioning flow, a new TSP could follow the same pattern as a Traditional Card Network TSP. When a customer goes to add or use a card in a new digital wallet or Merchant site for the first time, the wallet/Merchant (or Token Requestor) would capture the card number and pass it to the new TSP based on a routing table that it maintains, or it could be routed to a new TSP through an Acquirer based on a similar routing capability. A common way this routing would be configured would be a specific BIN range. The TSP would take the number and either route it to the appropriate Issuer for additional verification and approval, or handle those steps on the Issuer's behalf. Once approved, the TSP would create a token and push it back to the Token Requestor.

If the TSP is Tokenizing a PAN that another party will also Tokenize, such as in the case of an Alternate Debit Network, the Token Requestor would need to make multiple calls to each supported TSP for a given PAN, or a call to a major Traditional Card Network TSP in addition to an Acquirer that would route the request to any other TSPs.

Transactions

The design for transactions is a bit more complicated due to a variety of technically feasible approaches. Much of this variation depends on if the new TSP is replicating its token database with other parties in the transaction flow. As an example, if an Alternate Debit Network were to generate its own tokens for a Visa/Mastercard issued BIN, the Acquirer would need to know where to route this token when it processes a transaction. This design would require that the Acquirer store token variations for each network it intends to support for a given PAN.

Technical Overview

EMVCo Network Tokens

Provisioning

For EMVCo network tokens, the token is created and stored with Issuer/Processor involvement, and the Issuer/Processor is responsible for determining what card BIN and products are eligible to be Tokenized by a given Token Requestor. This involvement creates more steps in the Provisioning flow, but also provides the benefits of Issuer updates for lifecycle management events.

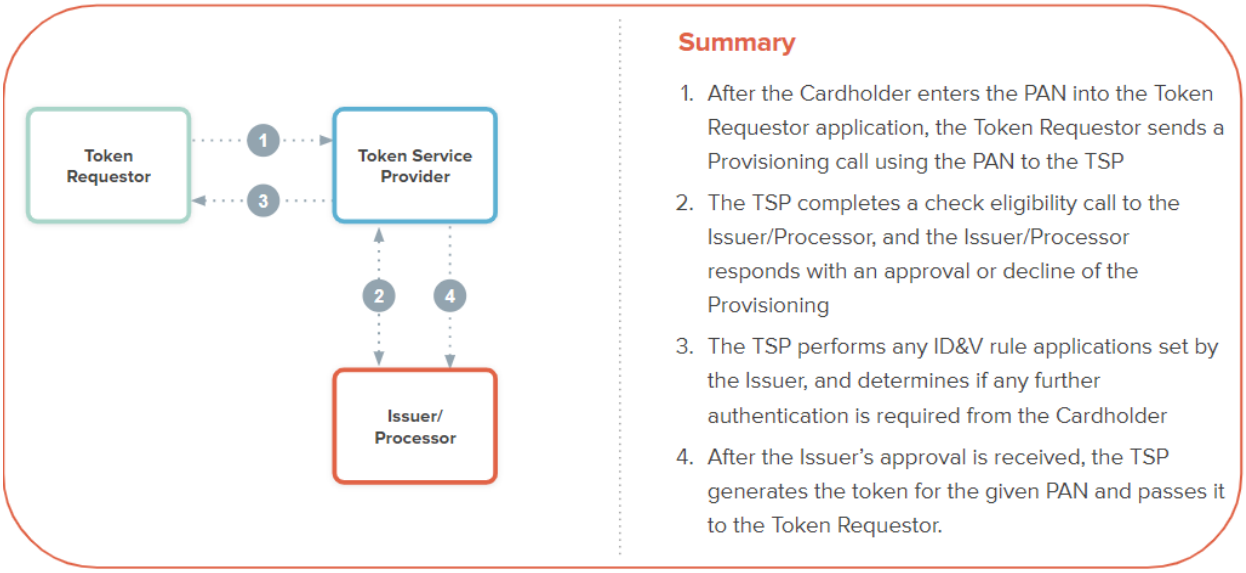


Figure 1: EMVCo Network Token Device Bound Provisioning Flow - No Further Authentication

In this case the Token Requestor will send the PAN to the TSP and request a token through Provisioning. The TSP communicates with the Issuer/Processor to ensure the card BIN and product are eligible to be Tokenized, and the Issuer/Processor responds with the result of an approval or denial of the Provisioning. If approved, the TSP would create the token and store the token to PAN mapping using the Token Vault. The TSP then sends the token and related payment information to the Token Requestor. The Cardholder is then able to use the token for payments.

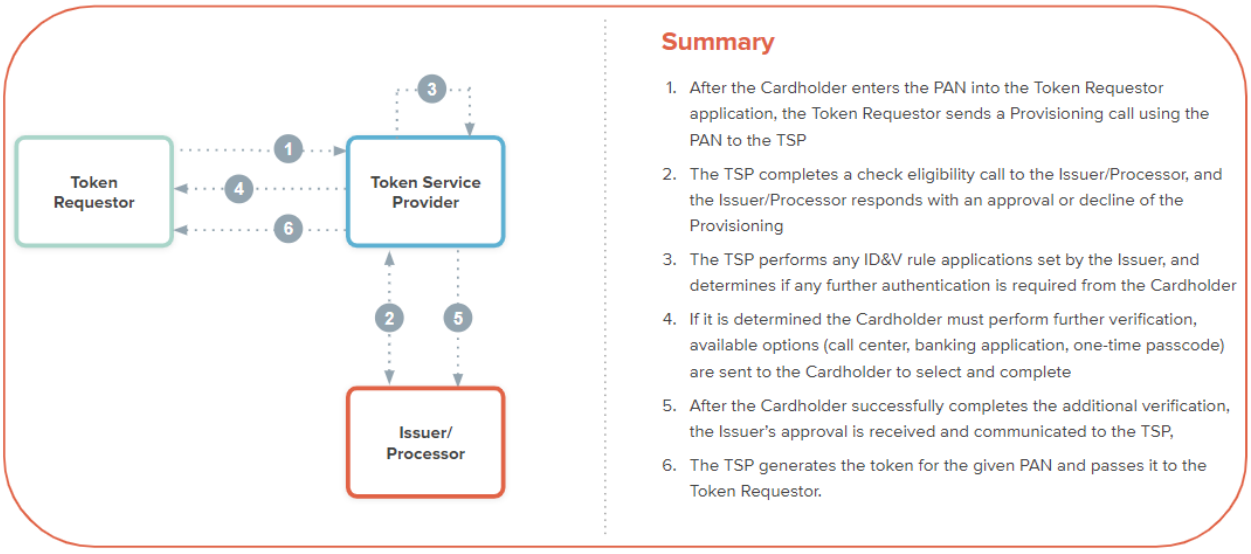


Figure 2: EMVCo Network Token Device Bound Provisioning Flow - Further Authentication

If the Issuer ID&V rules dictate that the Cardholder will need to provide further authentication, as shown in *Figure 2*, then the flow is suspended until the verification is performed and communicated by the Issuer/Processor. The TSP communicates with the Token Requestor the need for further verification, and offers the available options for the Cardholder to complete this step. The Token Requestor will display the available options to the Cardholder (call center, banking application, or one-time passcode), and the Cardholder selects the option he or she wishes to use. Once the Cardholder completes the verification, the Issuer/Processor will notify the TSP, and the process continues by the TSP passing the token and related payment data to the Token Requestor for use.

Transactions

EMVCo network tokens also provide a more complex transaction flow; however, the complexity is balanced with additional security. The token can be used end-to-end during the transaction lifecycle, leaving little to no room for a breach to occur within the flow. This allows for more control over the transaction by the Issuer, and more security and confidence in the transaction from the Merchant.

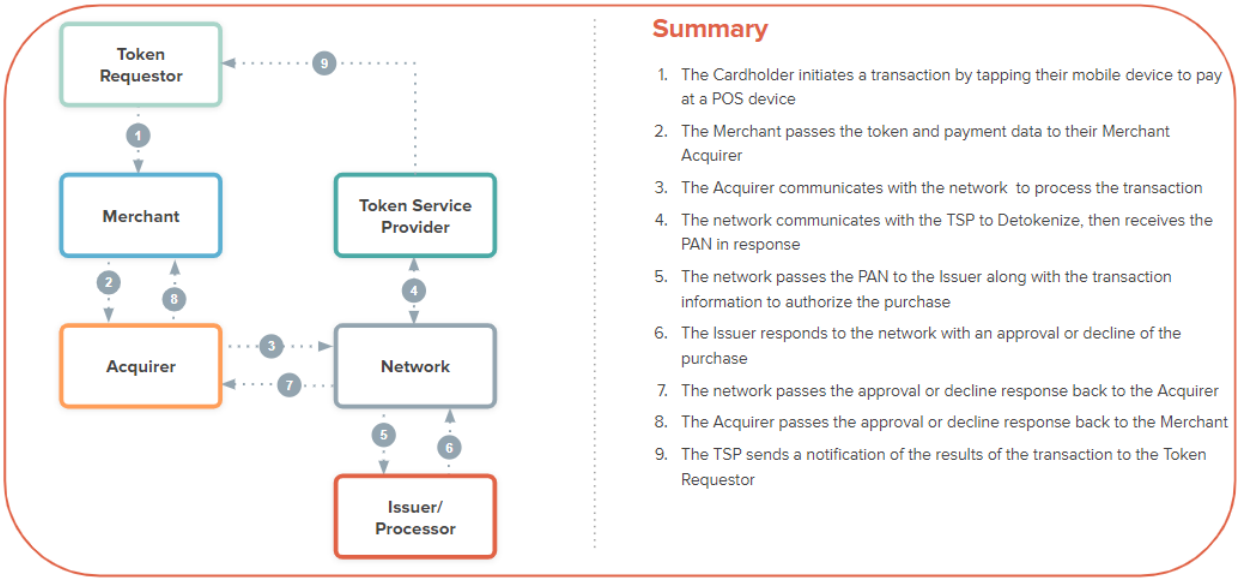


Figure 3: EMVCo Network Device Bound Token Transaction Flow

The transaction flow begins as the Cardholder uses the Token Requestor application on his or her device to tap and pay at the POS. The token is passed by the Merchant to the Acquirer, along with any relevant payment data. The Acquirer then passes the information to the relevant network for processing. It is at this step that the token is Detokenized by the TSP as a result of the network requesting the Detokenization. The major Traditional Card Networks also have TSP offerings, and act as the network processing the transaction, as well as the TSP to Detokenize. Once Detokenized, the network is able to pass the PAN to the Issuer in order to obtain the authorization result of approval or decline for the purchase. After the Issuer responds to the authorization request from the network, the approval or decline result is passed using the token to the Acquirer and on to the Merchant to display on the POS device. The TSP also provides the result of the transaction in the form of a notification to the Token Requestor. The Token Requestor can then use its application to provide the Cardholder with a notification on the device of the transaction details.

Ecommerce and Mobile Tokenization

Provisioning

In cases where the Provisioning occurs in an ecommerce or mobile application environment, the Provisioning process remains much the same. In current ecommerce models, step up authentication using customer service, a one-time passcode, or the mobile banking application is not used; however, step up authentication is possible with support of the TSP, Issuer, and ecommerce participant. Once the card is Provisioned, the token is delivered to a wallet (e.g. Samsung Pay, Apple Pay, or Google Pay) or the ecommerce participant (e.g. Merchant, payment gateway, etc.).

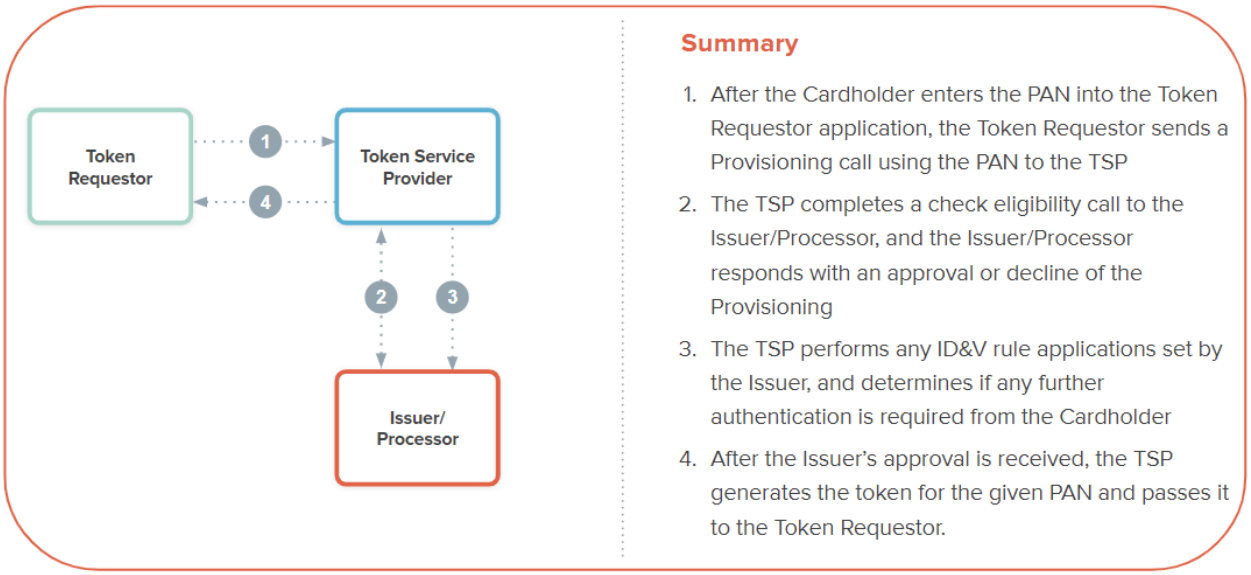


Figure 4: Ecommerce/Mcommerce Provisioning

The Provisioning process for ecommerce and mcommerce mirrors the device bound token Provisioning. The difference is namely in the Token Requestor position. The Token Requestor in this case can be a third-party wallet provider, Merchant, or other payment gateway that is approved to request tokens.

Transactions

Transactions using tokens for ecommerce and mobile applications create some interesting nuances. One component of the transaction flow for ecommerce and mobile application transaction can often complicate the process - the Token Cryptogram. Because the token information is not always stored on a physical device, a method must be used in order to properly validate the transaction is valid and has been performed by the Cardholder. The Token Cryptogram is a cryptographic value provided by the TSP that only the TSP can validate. This allows the Issuer, Merchant, and TSP to have confidence in the validity of the transaction. The Token Cryptogram can either be delivered as a part of the Provisioning flow, to be used during the first transaction, or as a part of the transaction flow itself. The Token Cryptogram is passed through the authorization flow, and is validated by the TSP. Once the Token Cryptogram has been validated, the transaction flow continues to the Issuer and back to the Merchant delivering the result. If the Token Cryptogram is not able to be validated by the TSP, the transaction will be declined.

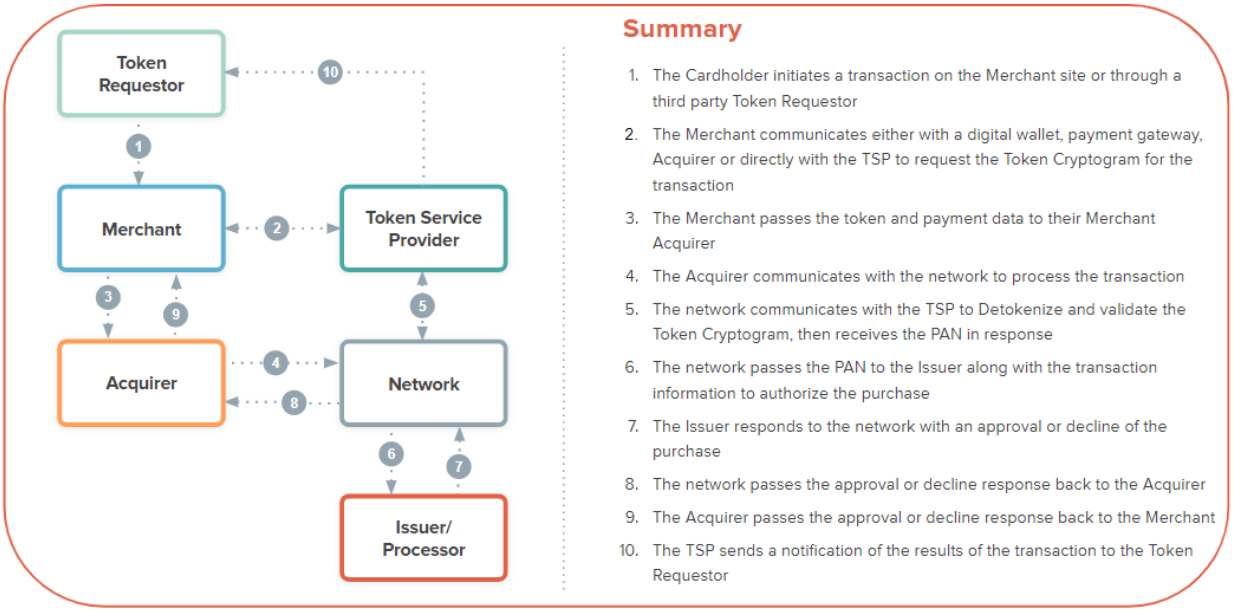


Figure 5: Ecommerce and Mobile Application Transaction Flow with Token Cryptogram

The Token Cryptogram allows ecommerce and some mobile application payments to be validated and promotes trust for the transaction overall. Currently, ecommerce Merchants do not have a field in the authorization flow to send the Token Cryptogram information; however, over time, adoption should increase as the value proposition for Merchants increases.

Supporting Card on File Tokens

The Provisioning process for card on file tokens using the EMVCo token framework operates the same way as the ecommerce tokens. One of the nuances for the transaction is that the Token Cryptogram may or may not be required, depending on the type of transaction being performed. The differences are namely the following:

- Recurring/subscription type card on file transactions using a token only use the Token Cryptogram for the initial transaction, and only use the token for all subsequent recurring transactions
- Split shipment type card on file transactions use the same Token Cryptogram for each transaction of the overall purchase. For example, if the total purchase is for $100, and will be billed in 4 increments of $25 as the items are shipped, the same Token Cryptogram would be used for all four transactions.

An additional variation of card on file Tokenization leverages recently announced partnerships between the major Traditional Card Networks and several large Acquirers. For many large Merchants with card on file portfolios, the Merchant is leveraging Acquirer generated tokens to avoid having to store customer PAN data. These Merchants depend on tools like the Acquirer JavaScript and hosted page card capture tools to ensure they do not receive card data at all.

Due to this new partnership, Merchants can continue to leverage these Acquirer tokens while the Acquirers partner with Token Service Providers to obtain and store EMVCo tokens. In this model, the Acquirer could continue to offer tokens to Merchants as it does today; however, upon receiving a card credential, the Acquirer could make a new call to a TSP or TSPs to request a token or tokens for the card. This would allow the Merchant to receive the same benefits of the current EMVCo token (token remapping on reissue or expiration, etc), but would not require them to take on any additional sensitive data.

Case Studies

Use Case 1: Domestic Payment Scheme as a TSP - Canada

Structure

Direct Debit schemes exist in many countries and often have local requirements for which transactions they are allowed/required to process. In the case of Canada, these schemes only work within the country and debit cards are often issued with both the local network, Interac, and a Traditional Card Network such as Visa or Mastercard. When the co-badge card is used for a debit charge in Canada, it is processed by Interac, and when the card is used out of country, the Traditional Card Network is used. The roll out of digital wallets created an interesting challenge for Interac. The local network wanted to maintain the use of its cards both inside and outside of Canada, but it did not want to have the Traditional Card Network generate tokens for its cards.

The first step for Interac was to become its own TSP so that it could control the creation of its own tokens. Interac could have leveraged a Traditional Card Network token and signed business agreements to allow for its use both in Canada and throughout the world; however, that was not its decision. Due to this design, all co-badge cards issued in Canada are actually Provisioned twice to digital wallets, and both Interac and the Traditional Card Network issue separate tokens. We will walk through the design in more detail below.

We have previously spoken about how a TSP must be aligned with the Issuers and provide a clear reason for use. For that reason, it is important to note that Interac is owned by the major banks in Canada and accepted as the way to process all local Debit transactions.

Design

In order for a digital wallet to support the inclusion of a co-badge debit card, it essentially performs Provisioning twice. Whenever a customer goes to add a card to Apple Pay or another wallet, the digital wallet looks at its BIN tables and recognizes that the card is a co-badge card. The wallet first initiates the standard series of EMVCo ID&V calls to the local network, Interac. These calls include secondary steps for user verification per normal EMVCo requirements. Once complete, an Interac token is created and Provisioned to the device for use.

Once this experience completes, the user is then able to also add the card to the digital wallet for international use. When the user starts this process, the digital wallet triggers a second set of ID&V calls to the Traditional Card Network and a second token is issued. The end result for the user is two separate cards in the digital wallet and the user must select which card to use at each purchase.

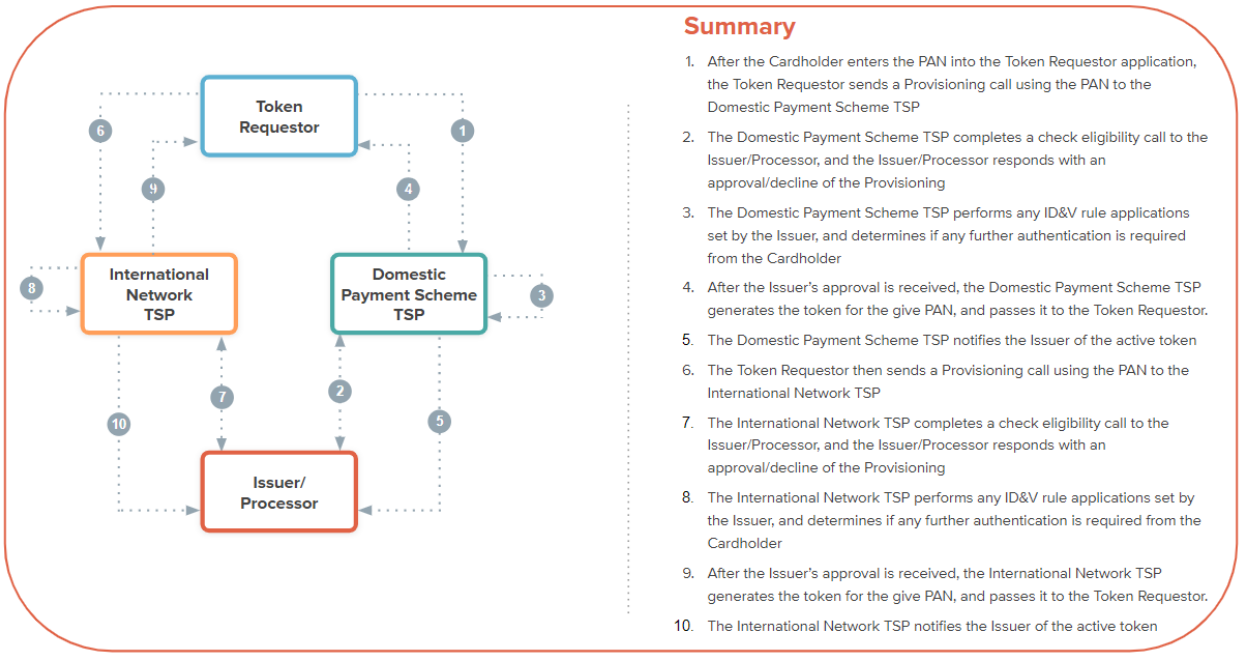


Figure 6: Domestic Payment Scheme Provisioning Flow

Due to the creation of two separate tokens, much of the complexity in implementing this model is managed by the digital wallet. From a TSP perspective, both the Traditional Card Network TSP and the local network TSP simply get a token request and process it normally as per the EMVCo specifications. This makes this model a fairly common one for handling multiple TSP environments; however, it is almost always used when the secondary TSP is local network and either required due to regulation or influenced by the bank relationships. Additionally, this required that the end user has an awareness of when to use which token and there is brand awareness of both networks available.

Implementation Considerations

This model has been proven to work for domestic debit schemes when leveraged by a digital wallet; however, it does face challenges if being considered for ecommerce or mobile. In the case of the Interac example used above, Interac does not currently support the use of its tokens in ecommerce. This is due to Canadian regulation that requires the Issuer to specify which network it uses for a specific transaction type, and most Issuers have chosen to use a Traditional Card Network for online transactions.

If a party were to follow this model, it would need to account for this gap and create an ecommerce flow that would enable to Merchant to route the transaction to the party's TSP for Tokenization and

processing. This could be done through integration with Merchants directly, through Merchant Acquirers, or through the digital wallets.

Use Case 2: Token Service Provider Managed by an Alternate Debit Network

Structure

Alternate Debit Networks in the United States are in a unique position in the ecosystem. They have many of the same connections as the Traditional Card Networks, and service many of the Issuers' debit portfolios. Some Alternate Debit Networks even support signature debit transactions, which allow them to fully service debit cards ecommerce and mcommerce Tokenized transactions.

An Alternate Debit Network could set up a TSP to support the debit card transactions as Tokenized transactions for its Issuers. Additionally, depending on the strategy of the Alternate Debit Network as a TSP, it could also be able to provide Tokenization services supporting its partner Issuer's credit card portfolio. This would provide it with a position in the overall Tokenization movement, strategic placement for new Tokenization use cases and innovation, and further enhance its services to its Issuer partners.

Design

The design of an Alternate Debit Network as a TSP would need to align with the current EMVCo structure, and allow both Provisioning and transactions to flow through existing channels, as they do today. Many of the connections needed already exist within the current framework of the network; however, internal investments must be made to support a Token Vault which will create, maintain, and manage the tokens for its portfolios. In order to allow for seamless integration of the tokens into the current infrastructure, an Alternate Debit Network could request a Token BIN Range from an existing major Traditional Card Network in order to use that range as its own tokens within its vault. This way the tokens will be recognizable by the Acquirer, and able to be routed to the alternate debit Token Vault for Detokenization and Token Cryptogram validation.

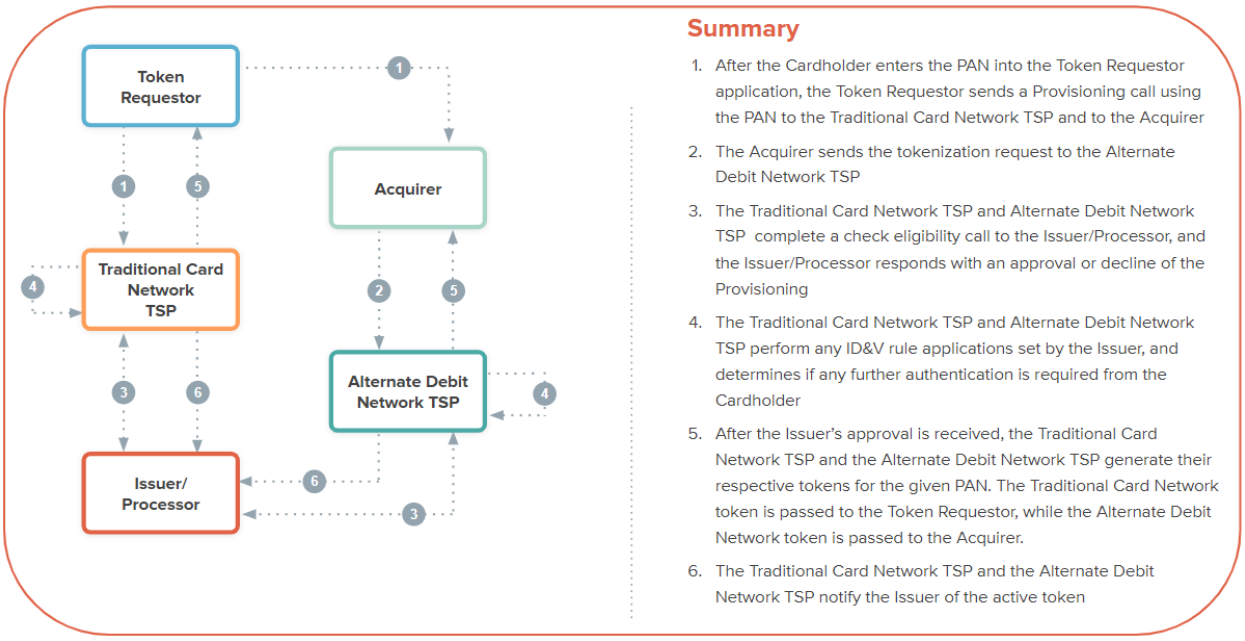


Figure 7: Alternate Debit Network TSP Ecommerce and Mcommerce Provisioning Flow

In the Provisioning process, the token is created and maintained by the Alternate Debit Network, and stored using its Token Vault. The Provisioning flow is similar to that of the EMVCo device bound tokens; however, the Acquirer is leveraged to route the request to the Alternate Debit Network. Additionally, the major Traditional Card Network would still create and deliver token credentials to the Token Requestor simultaneously. The major Traditional Card Network will use its specific Token BIN for the specified PAN portfolio, and the Alternate Debit Network would use a Token BIN unique to its Token Vault. This will allow the correct token to be used based on the routing choice of the Merchant.

In the Provisioning example where a third-party Token Requestor (e.g. Google, Apple, Samsung, etc.) is used, the payment account reference (PAR) could be used to tie the major Traditional Card Network TSP token and the Alternate Debit Network TSP token to the underlying PAN. This would allow the Acquirer to add the PAR value to the routing tables, and replace the major Traditional Card Network TSP token with the Alternate Debit Network TSP token if the routing options chosen by the Merchant warranted use of the Alternate Debit Network TSP token.

In the case of the transaction, the Acquirer would play a significant role in proper routing, as it does today for debit transactions. In order to allow for proper routing of the tokenized transaction, Acquirer-provided Merchant tokens can be used and translated by the Acquirer to the correct TSP Token BIN.

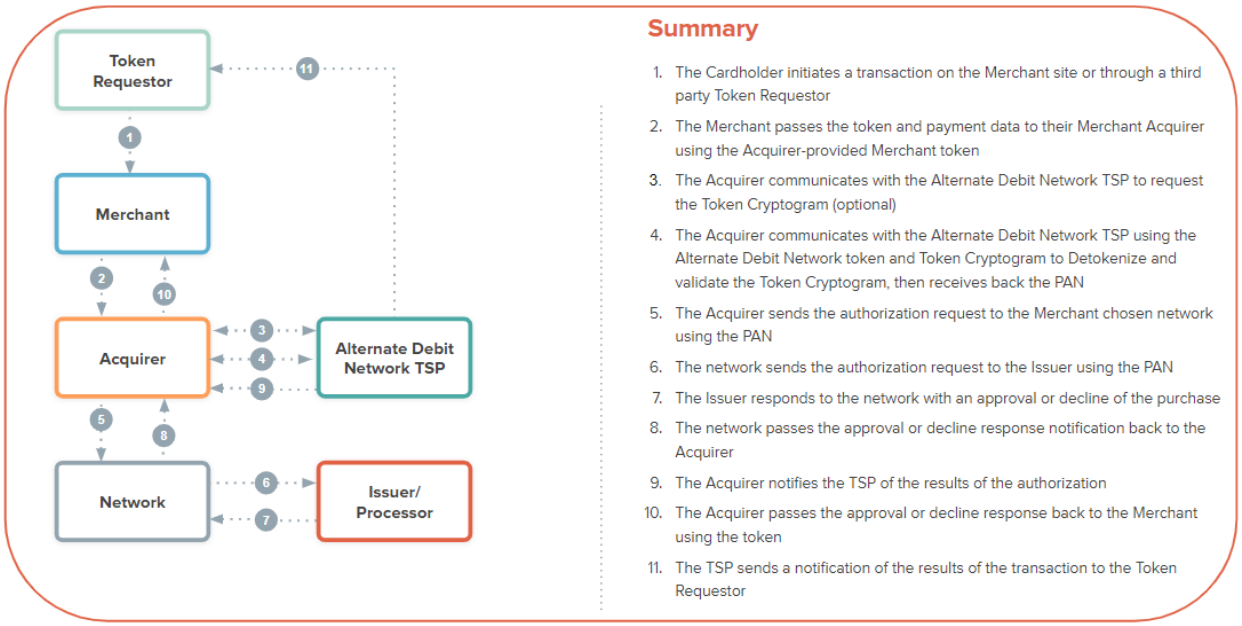


Figure 8: Alternate Debit Network TSP Ecommerce and Mcommerce Transaction Flow

The Alternate Debit Network would be placed in line with the Acquirer in the flow. The transaction would flow through the Merchant to the Acquirer, who would utilize the Alternate Debit Network TSP to request a Token Cryptogram for the transaction (the Token Cryptogram request is optional depending on the details of the transaction). The Acquirer would then submit the token for the alternate debit TSP to Detokenize and validate the Token Cryptogram. After successful Detokenization and Token Cryptogram validation by the TSP, the Acquirer would pass the transaction through to the Merchant's chosen network (this network could be the same network providing the TSP or a different network) which communicates with the Issuer for authorization. This would be followed with the network communicating the result of the authorization decision, using the PAN, back to the Acquirer, which would facilitate it being passed back through the flow, ultimately reaching the Merchant. The TSP would then send a notification of the completed transaction to both the Token Requestor and Issuer/Processor.

For the transaction to operate correctly, the Acquirer must receive the token it has provided the Merchant along with the Merchant's routing choice. The Acquirer will then be able to utilize the correct token (either the major network or Alternate Debit Network token) to pass to the appropriate TSP to Detokenize and complete the transaction. In cases where the major Traditional Card Network token is used, the major Traditional Card Network would operate as the TSP to Detokenize and complete the transaction.

Implementation Considerations

In this model:

- The Acquirer will need to add logic to properly route the Tokenized transaction based on the Merchant's choice

- The Acquirer will need to house and utilize both the Alternate Debit Network token as well as the major Traditional Card Network token, and utilize the correct token based on the routing option chosen by the Merchant

Acquirers will need a value proposition to participate in this new implementation, as well as assistance in implementing the design. Acquirers will have to be intricately involved in the strategic planning when launching the new TSP.

Cost

The primary cost drivers for the development of any new TSP include the following:

- The staffing of business development, product management, IT, and support personnel to design, build, and operate the service
- The build-out or purchase of a token creation and management platform
- Ongoing infrastructure cost to host and update the product over time

While the cost for these items can vary widely based on the availability of existing resources, the existence of similar technology that can be leveraged, or specific vendor deals, any new TSP can expect to see costs range between $18M and $30M with an average implementation period of 18 months from initial requirements through testing.

The biggest factor in the timeline for new launches is often influenced by the partners selected. In many cases, aligning testing windows with Issuers, Merchants, Acquirers and other parties can lead to timeline delays and increased cost as all parties are required to simultaneously test and certify a TSP for launch. It is also important to keep in mind the number of Issuers, networks, or Merchants that are attempting to be included at launch as each network has its own requirements for integration and complexities in doing so.

Conclusion

As demonstrated, an entity that has a desire to become a TSP could invest the time, capital, and resource to insert themselves into the Tokenization ecosystem. For any organization with aspirations to offer TSP services, the following must be considered:

- Strategy - what are the motivations for launching a TSP? Who will be the primary client focus (Issuers, Token Requestors, etc.)? What problems will be solved through Tokenization?
- Design - Based on the defined strategy, what design provides efficient integration with internal systems, while offering the Tokenization product to the intended clients? What design provides the opportunity for future enhancements and innovations to the Tokenization model?

- Business Case - What will be gained by becoming a TSP? After considering the potential monetary benefits, what other benefits would becoming a TSP offer the organization? Are direct competitors making any movements towards becoming a TSP?

When the strategy and design have been identified, the business case should be fully evaluated. Current TSPs have and are poised to create more points of entry into the Tokenization ecosystem, and there are options utilizing existing players in the ecosystem, such as Acquirers described in the Alternate Debit Network use case that allow a third-party TSP to be created and operate as a stand-alone provider of token services. The technical environment of Tokenization supports the creation of third-party Token Requestors, and should be explored by existing participants in the ecosystem, as well as prospective new players that have interest in Tokenization services.

Appendix

Glossary

Term	Definition
Acquirers	The financial institutions that hold accounts of Merchants and process transactions including capturing, clearing, and performing exception processing.
Alternate Debit Networks	The national and regional debit card networks in the United States other than the Mastercard and Visa Signature Debit Networks (e.g. STAR, Pulse, NYCE, and Interlink).
BIN or Bank Identification Number	BINs are assigned by Traditional Card Networks to Issuers and, consistent with ISO 7812 requirements, allow for the identification of the Traditional Card Network based on the range.
Cardholder	Individual that has been issued a financial account Provisioned to a Card by an Issuer.
Detokenization	The process of redeeming a token for its associated PAN value based on the token-to-PAN mapping stored in the Token Vault.
ID&V or Identification and Verification	A valid method through which an entity may successfully validate the Cardholder and the Cardholder's account in order to establish a confidence level for token-to-PAN / Cardholder binding. Examples of ID&V methods are: - Account verification message - Risk score based on assessment of the PAN - Use of one-time password by the Card Issuer or its Agent to verify the Cardholder
Issuers	The financial institutions that issue the payment account to which a debit card is linked.
Mastercard and Visa Signature Debit Networks	The debit networks for Visa and Mastercard.
Merchants	The entities accepting payment for a good or service which can also act as a Token Requestor to process transactions using tokens they request.
PAN or Primary Account Number	A variable length, 13 to 19-digit, ISO 7812-compliant account number that is generated within account ranges associated with a BIN by an Issuer.
Processors	The organizations that serve the Issuer by performing card processing functions, receive additional token related fields from the networks, call the TSP for Detokenization, and perform authentication (identity and

	verification, ID&V), in each case, on behalf of the Issuer, if requested.
Provisioning	The act of delivering the token and related values, potentially including one or more secret keys for Token Cryptogram generation, to the location in which the token is stored.
Token BIN	A specific BIN or range within a BIN that has been designated only for the purpose of issuing tokens and is flagged accordingly in BIN tables.
Token BIN Range	A unique identifier that consists of the leading 6 to 12 digits of the Token BIN. The Token BIN Range may be designed to carry the same attributes as the associated Issuer card range and will be included in the BIN routing table distributed to the participating Acquirers and Merchants to support routing decisions.
Token Requestor	An entity that is seeking to implement Tokenization according to EMVCo and initiate requests that PANs be Tokenized by submitting Token Requests to the Token Service Provider. Each Token Requestor will be registered and identified uniquely by the Token Service Provider within the Tokenization system.
Token Requestors	The entities that request to receive a token instead of using and storing the real account data for payments. These entities can be identified as a digital wallet (Google Pay, Samsung Pay, etc.) or a Merchant, as well as an Acquirer or payment gateway on behalf of a Merchant.
Token Service Providers	The entities that store and maintain the Token Vault, implement security controls (application identifier and Token Cryptogram), Provision tokens when they are requested, handle lifecycle management if any account data attached to the token is updated, and manage Token Requestor registry services for any entities that desire to become Token Requestors.
Token Cryptogram	A Token Cryptogram generated using the token and additional transaction data to create a transaction-unique value. The calculation and format may vary by use case.
Token Vault	A repository, implemented by a Tokenization system that maintains the established token-to-PAN mapping. The Token Vault may also maintain other attributes of the Token Requestor that are determined at the time of registration and that may be used by the Token Service Provider to apply domain restrictions or other controls during transaction processing.
Tokenization	A process by which the Primary Account Number (PAN) is replaced with a surrogate value called a token.
Traditional Card Network	The international card networks, such as Visa, Mastercard, American Express, and Discover.