Card-on-File Tokenization Considerations, Including Debit Routing

Version 1.0

Publication Date: April 2021

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

EMV® is a registered trademark of EMVCo, LLC in the United States and other countries around the world.

Table of Contents

1. Introduction

The payments industry continues to invest in payment solutions that can minimize risk and increase data security. As the payments ecosystem migrates away from storing primary account numbers (PANs) due to the risk potential, the use of 'tokens' provides increased security.

Tokens are essentially replacement PANs used either at rest (i.e., stored) or in transit, with values that can mask and protect cardholder information. Tokens can be utilized at various points within the transaction life cycle. Payments industry stakeholders need to understand tokenization implementation considerations, including debit routing, for card-on-file environments. To assess stakeholder impact, the implementation environments and the tokenization process for each card on file with a PAN must be considered. The impact may differ depending on a particular tokenization solution.

This white paper provides a brief overview of different card-on-file tokenization solution options and stakeholder considerations for each, including debit routing. These options and considerations take into account the perspective of each payments industry stakeholder: acquirers, issuers, merchants, and payment networks.

2. Card on File (with PAN) in a Payment Vault

2.1 Overview

A common form of card-on-file storage involves the merchant storing PANs in a secure payment vault, either directly or indirectly through a third-party solution provider. This section describes the processes which could be involved with a merchant storing a card on file.

2.2 Provisioning

When a customer adds a credit or debit card to their registered profile on the merchant's system, the merchant may choose to perform some form of authentication as a prerequisite to allowing the card to be accepted in their systems for storage and use. A common method is to use an Account Status Inquiry (ASI) – a non-monetary transaction initiated by the merchant that may be used to validate whether the account provided by the customer exists and if the account is in an active state for transaction processing. The ASI may facilitate one or more card verification and cardholder authentication options, such as the following:

- Card security code – a security feature that is used with card-not-present fraud transactions.
- Address Verification Service (AVS) – a validation service optionally performed by the merchant as part of either a financial or non-financial transaction that validates the cardholder-provided address, zip code or both.
- EMV® 3-D Secure (EMV 3DS) – an EMVCo specification that may be used to authenticate a cardholder for participating issuers. Additional information on EMV 3DS is available from EMVCo.[1]

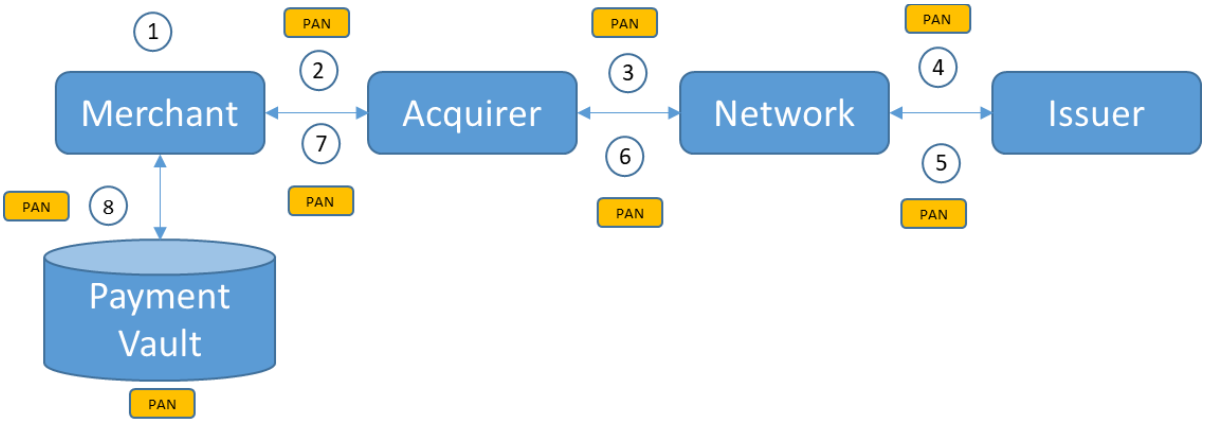

Figure 1. Process for Storing a Card on File in a Payment Vault

Figure 1 illustrates the process steps for storing a card on file in a payment vault. During the process, the following steps occur:

1. The cardholder adds their PAN to their registered profile on the merchant's web site.
2. The merchant submits an ASI transaction to their acquirer.

[1] https://www.emvco.com/emv-technologies/3d-secure/

3. The acquirer determines available networks, selects a network, and forwards the ASI transaction to the selected network.
4. The network forwards the ASI transaction to the issuer.
5. The issuer forwards the response to the ASI transaction to the network.
6. The network forwards the issuer response to the ASI transaction to the acquirer.
7. The acquirer forwards the response to the ASI transaction to the merchant.
8. The merchant receives the response to the ASI transaction and, if the merchant criteria are met, the merchant adds the card data to their payment vault.

2.3 Transaction Processing

When the merchant stores a card on file (with PAN) in accordance with the Payment Card Industry Data Security Standard (PCI DSS), all stakeholders have access to the PAN throughout the transaction.

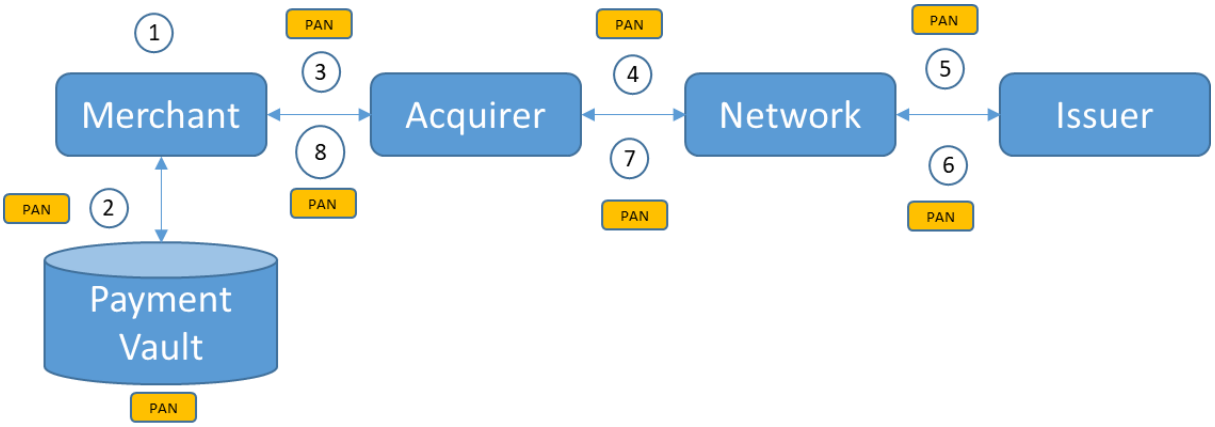

Figure 2. Card-on-File Transaction Processing

Figure 2 illustrates the card-on-file transaction processing steps. During the process, the following steps occur:

1. The cardholder checks out on the merchant site and selects their card for payment.
2. The merchant retrieves the payment credentials (e.g., PAN and expiration date) from their payment vault. **Figure 2** indicates that the merchant is the entity interacting with the payment vault. However, it should be noted that there may be other configurations where the entity interacting with the payment vault is a third-party processor (e.g., acquirer or other).
3. The merchant sends an authorization request to the acquirer using the retrieved payment credentials.
4. The acquirer determines the available networks, selects an eligible network associated with the card, and routes the authorization request to the selected network.
5. The network forwards the authorization request to the issuer.
6. The issuer generates an authorization decision and sends an authorization response to the network.
7. The network forwards the authorization response to the acquirer.
8. The acquirer forwards the authorization response to the merchant.

2.4 Impacts and Considerations by Stakeholder Group

Merchant	• Transactions processed using a PAN may be routed to any supported network. • Payment credentials must be stored in a PCI DSS-compliant manner. • Merchants can update cards on file by using account updater services or by asking the customer to re-enter a new card number for a modified PAN or to update the expiration date. • Storing payment credentials in this manner can also support customer service, loyalty, and returns purposes.
Acquirer	• Transactions processed using a PAN may be routed to any supported network. • The acquirer must handle the payment credentials in compliance with PCI DSS. The security code cannot be stored.
Network	• There is no need to detokenize.
Issuer	• If payment credentials are compromised, reissuance may be required to prevent unauthorized use through other merchants and channels.

3. Considerations for Tokenizing Cards on File

Tokenization is a method of replacing a sensitive piece of information with a less sensitive piece of information. In the payments ecosystem, different types of tokenization have been implemented, with each calling the replacement value a token. Leveraging tokenization as a method to secure cards on file is becoming more prevalent. This section discusses several areas to consider when evaluating tokenization for cards on file.

3.1 PCI Scope

Some card-on-file tokenization solutions enforce transactional security measures to reduce the risk that a token, if compromised, can be used at unrelated merchants. Examples of these security measures include limiting the use of tokens to only those merchants (or their service providers) that originally requested the token (a process known as "token domain control restrictions") and using transaction-specific cryptograms that can be validated during the authorization process to identify potentially fraudulent transactions.

As a result, tokenizing cards on file may reduce a merchant's PCI obligations (or their technology provider's obligations) related to storing highly sensitive data including payment credentials. Determining whether a particular solution is subject to reduced PCI requirements is beyond the scope of this paper. Merchants should work with qualified PCI assessors to review each solution they are considering for implementation to determine the PCI obligations for each. Consideration should be given to many factors including, but not limited to, whether a token could be used across multiple merchants in the event a token were to be compromised. PCI assessors will need to work with each supported token service provider (TSP) to evaluate their respective solutions.

3.2 Technology Considerations

Participating in a tokenized card-on-file solution requires participants to conform to specific technical requirements to obtain (i.e., provision), use and manage tokens over their lifecycles. As such, merchants (or their technology providers) may need to modify and certify their systems to support each specific tokenized solution they choose.

3.3 Transparency of Data for Processing, Customer Experience, Service and Loyalty

The transparency of data afforded by tokens varies based on the token type and implementation specifications afforded by each token solution. Consideration should be given to the formatting of the token, the means by which tokens are processed, the manner in which a tokenized card-on-file credential is displayed to customers on the merchant site, and the impact on various back office processes or loyalty programs.

Acquirer-based tokens, for example, may vary in format, and in some cases will have no resemblance to a card number. Merchants implementing this type of solution may need to adapt their systems to handle tokens that do not conform to traditional card numbering standards. The merchant or their technology providers may need to convert the token back to the PAN prior to processing the authorization request with the acquirer. In contrast, EMV payment tokens are generally formatted and processed in the same manner as PANs. Transactions using EMV payment tokens are forwarded to the acquirer as is. At the acquirer, a candidate list of supported networks is identified using BIN/IIN files,

and the network for routing can be determined by applying business restrictions and other processing logic to select a final network.

Consideration should be given to the method of presenting tokenized card-on-file credentials to customers on the merchant's web site. Customers are generally not aware of the token value, so an industry best practice is to display the card-on-file credentials in a manner familiar to the customer (e.g., a customer-selected name for the card, displaying the image of the front of card with brand logo, PAN last four digits, and expiration date).

Other back office processes, such as handling merchandise returns and managing loyalty programs, may also be affected by the use of tokenization. Merchants considering adoption of a tokenized card-on-file solution should involve their acquirers and/or technology providers early in the process and frequently throughout to ensure that the final implementation meets their expectations.

3.4 Lifecycle Management

Once tokens have been provisioned, the state of tokens and their associated PANs must be maintained. Depending on the type of change, either the issuer or the merchant creates the initiating event that results in a lifecycle management change.

3.4.1 Issuer-Initiated Lifecycle Management Events

The most common issuer-initiated lifecycle management events include PAN change, expiration date change, and account closures. Depending on the type of change, the TSP may make a corresponding change to any associated card-on-file tokens and notify the token requestor to update their information accordingly.

3.4.2 Merchant-Initiated Lifecycle Management Events

The most common merchant-initiated lifecycle management event occurs when a customer chooses to delete a stored credential from their merchant profile. Merchants may be required to notify the TSP when a previously assigned token is suspended or deleted. In cases where the token type is a merchant- or acquirer-generated token (rather than an EMV payment token based on the EMVCo framework, where a payment network is generally the TSP), lifecycle management updates generally occur as the result of optional network-based account updater and real-time account updater services. With these services, the network notifies merchants or acquirers of changes to PANs, expiration dates, and account closures. The merchant can request lifecycle changes from a batch file provided by the token generator or included in the response to an authorization request ("real-time account updates").

3.5 Debit Routing

A merchant's decision to use one or more TSP card-on-file solutions may be influenced by applicable TSP business requirements. For example, a TSP solution, related security features or support may only be available if tokenized transactions are routed to a specific network.

Acquirers and merchants may need to adjust business processes and practices to identify tokens and determine where transactions can be routed based on their business requirements.

Merchants and their respective technology providers may need to evaluate TSP features and requirements before implementing a tokenized card-on-file strategy that meets their business needs. Merchants should contact their TSP(s) to identify what, if any, such conditions may apply.

4. Token Options for Card-on-File

Merchants that hold cards on file have choices on what technologies they may use to store and secure sensitive payment data. These options range from storing payment credentials in secure payment vaults to leveraging third-party token services offering EMV payment tokens or other token types. Hybrid and alternative methods are also available to merchants but are less common. Each of these approaches has advantages and disadvantages that merchants should consider when determining the technologies to employ for their card-on-file solution.

The industry generally refers to any form of PAN obfuscation as a token; however, the types of representations for a PAN can be quite different. Stakeholders need to understand these fundamental differences to have the correct context for processing options.

Many different types of tokens can be used for card-on-file; this white paper discusses the following five types:

- Merchant tokenization
- Merchant service provider/vendor tokenization
- EMV payment token
- Combination of card-on-file (with PAN) and EMV payment token
- Combination of multiple EMV payment tokens

4.1 Merchant Tokenization

Merchant tokenization refers to tokens created by or issued to a specific merchant or group of related merchants to secure payment data. These tokens are not used in the authorization and settlement messages; rather the token is converted to the PAN for payment processing. Tokens of this type are generally merchant-specific and are not used across unrelated merchants.

4.2 Merchant Service Provider/Vendor Tokenization

Tokenization services offered by a merchant service provider or vendor (including an acquiring processor) protect data at rest from the threat of data breaches by eliminating the need for a merchant to store card account data within their card data environment. This type of tokenization is often deployed in combination with encryption of data in motion to provide a layered security solution. These tokens can be used for processing from the merchant to the service provider but will need to be converted to PANs before the transaction is sent to the payment networks. In addition to reducing the risk associated with the loss of cardholder data, service provider tokenization can also reduce the scope of merchant systems that fall under PCI DSS requirements. Using tokenization and encryption together provides an option that may reduce the time, focus and costs associated with PCI DSS compliance auditing.

Tokens created by merchant service provider tokenization services are not categorized as EMV payment tokens (i.e., tokens that can be used across the payment ecosystem). Unlike EMV payment tokens, these tokens are not issued by or on behalf of card issuers. They do not use the same format as PANs nor do they include issuer card prefixes that correspond with routable BINs found in network-routing BIN files. Merchant service provider tokenization can be used to secure stored EMV payment tokens in the same way it secures standard PANs. Whether a merchant uses service provider tokenization services has no impact on its ability to participate in EMV payment token programs.

Some service providers may also share the same token across more than one merchant.

4.3 EMV Payment Token

EMV-based tokens – called EMV payment tokens – can be provisioned as a surrogate value for PANs.[2] A payment token is useful in protecting data at rest, since the token can generally not be used outside of the context or domain for which it was intended.

An EMV payment token (for example, available through a global payment network's token service) is a surrogate value for a PAN that is a variable-length, ISO/IEC 7812-compliant number issued from a designated token BIN or token BIN range that does not conflict with an in-service PAN. Payment tokens can be used on a payment network as if they are card numbers. Merchants can use the BIN attributes of a token BIN range to discern routing options and other features available for a given payment token.

Some third parties offer services to perform the TSP role for EMV payment tokens. In this TSP role, the third party acts on behalf of a network to perform payment token processing, which may include establishing and maintaining technical connections and operability with participants, generating tokens, securing PAN and token data in a token vault, maintaining token-to-PAN mapping, managing the token provisioning and lifecycle management processes, performing domain control and cryptogram verifications, and supporting call-outs from networks where they return the true PAN in exchange for the token. Third-party providers are service providers to the TSP and perform outsourced services. They may process on behalf of a TSP, but they do not define or govern the tokenization service.

4.3.1 Overview

EMV payment tokens, obtained and stored by the merchant in place of a PAN, are used for secure card-on-file storage. The party that requests and maintains the payment token is referred to as the "token requestor." Merchants obtain a payment token either at the time a customer adds their payment card details to the customer's registered profile or some time afterwards. PANs may be deleted from merchant system storage at the time the payment token is received.

4.3.2 Provisioning

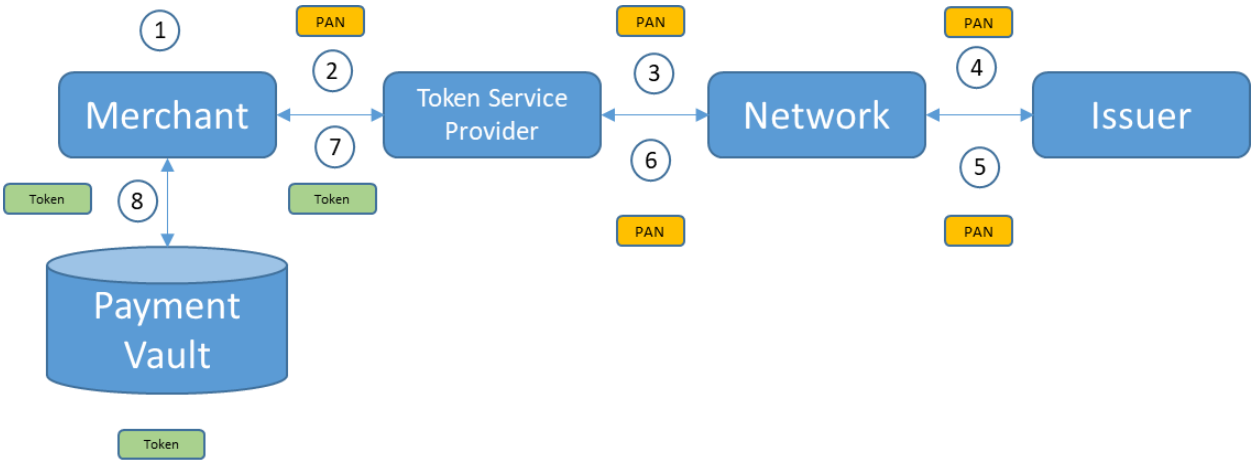

Figure 3. EMV Payment Token Provisioning Steps

[2] Additional information can be found in the U.S. Payments Forum white paper, "EMV Payment Tokenization Primer and Lessons Learned", https://www.uspaymentsforum.org/emv-payment-tokenization-primer-and-lessons-learned/

Figure 3 illustrates the EMV payment token provisioning steps. During provisioning, the following steps occur:

1. The cardholder adds their PAN to their registered profile on the merchant's web site.
2. The merchant submits a "token request" transaction to the TSP. The token request includes the PAN and expiration date and may also include AVS and card security code data.
3. The TSP validates the merchant as a token requestor and forwards the token request transaction to the network. In some cases, the TSP may send an ASI to the payment network instead of a token request.
4. The network forwards the token request transaction to the issuer for approval.
5. The issuer forwards the response to the token request transaction to the network.
6. The network forwards the token request transaction response to the TSP.
7. The TSP reviews the token request transaction response and, if TSP criteria are met, generates a payment token and expiration date, and forwards a token response to the merchant along with token data.
8. The merchant receives the response to the token request transaction and, if the merchant criteria are met, the merchant adds the token payment data to their payment vault.

4.3.3 Transaction Processing

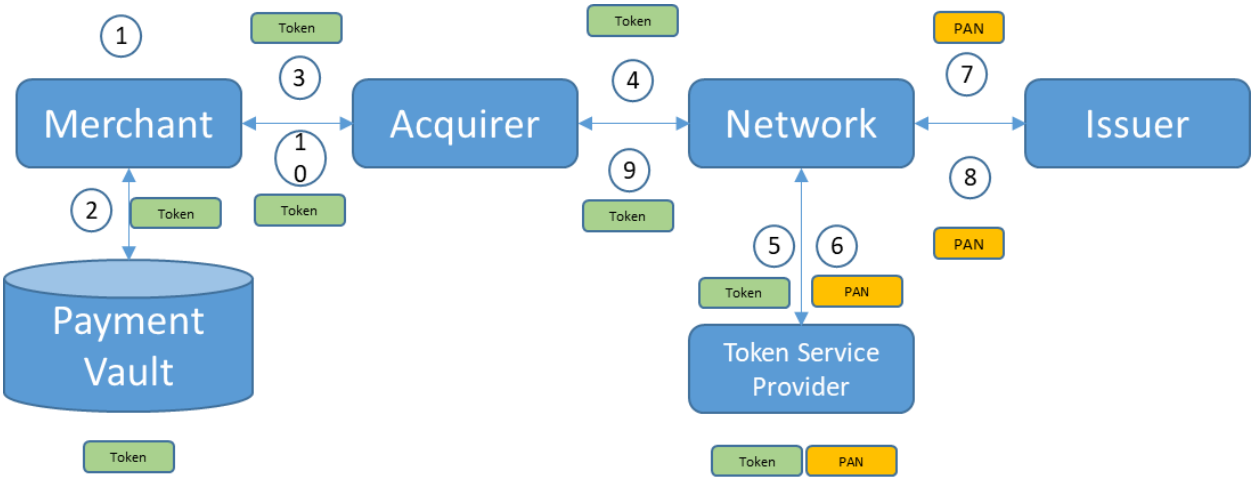

Figure 4. EMV Payment Token Transaction Processing Steps

Figure 4 illustrates the EMV payment token transaction processing steps. During transaction processing, the following steps occur:

1. The cardholder checks out on the merchant site and selects their card for payment.
2. The merchant retrieves the payment credentials (e.g., payment token, token expiration date) from their payment vault.
3. The merchant sends an authorization request to the acquirer using the retrieved payment credentials.
4. The acquirer determines the available networks, selects an eligible network following token payment network restrictions, and routes the authorization request to the selected network.
5. The network send a detokenization request to the TSP.
6. The TSP performs detokenization and responds to the network with the PAN, PAN expiration date and other detokenization results.

7. The network receives the detokenization response from TSP, reformats the authorization request to include the PAN and PAN expiration date, and forwards the transaction to the issuer for approval.
8. The issuer generates an authorization decision and sends an authorization response to the network.
9. The network replaces the PAN with the token and forwards the authorization response to the acquirer.
10. The acquirer forwards the authorization response to the merchant.

4.3.4 Lifecycle Management

With payment tokens, changes to the PAN and/or PAN expiration date are generally managed by the TSP. If a lifecycle management change results in a change to the underlying payment token, the TSP pushes updated token information to the token requestor for update in their systems. If a cardholder deletes a payment credential from the merchant system, the token requestor invalidates the token and notifies the TSP.

4.3.5 Compliance Considerations

Payment tokens may be subject to less stringent PCI compliance obligations. Payment tokens generally have token domain restrictions that ensure that tokens are only used by the token requestor to whom they have been assigned. However, some TSPs may not perform token domain control restrictions or cryptogram validation for transactions routed to domestic debit networks. Merchants and acquirers may need to determine whether the scope of PCI obligations is less stringent when domain control is not performed for tokenized transactions.

4.3.6 Impacts and Considerations by Stakeholder Group

Merchant	• When acting as the token requestor, the merchant:
	  ○ Must certify to TSP.
	  ○ Must request and maintain tokens in their payment vault.
	• When outsourcing the token requestor service to a third party, the merchant:
	  • May have to enhance systems to store token data.
	• Debit routing policies, PCI compliance and customer experience may vary from one TSP to the next.

Acquirer	• An acquirer that wishes to support tokens for their customers would seek to become a registered token requestor with each TSP they choose to integrate with.
	• When acting as the token requestor, the acquirer:
	  • Must certify to TSP.
	  • Must request and maintain tokens in their payment vault.
	• An acquirer could also offer debit routing functionality as an additional or included service with their token product. To support this functionality, the acquirer may require system changes to accommodate their preferred business logic.

Network	• The network may need to certify and maintain an interface to each TSP with which their cards participate. • The network also performs call-out interactions to the TSP on each tokenized transaction to either validate security and/or obtain the PAN. • The network may also need to make appropriate changes to accommodate token processing and communicate those to issuers and acquirers.

Issuer	• The issuer may have to certify to some networks' token-related message formats and make other system changes. • The issuer may also perform changes to their risk management processes and systems for both provisioning and transaction processing related to tokens associated with cardholder accounts.

4.4 Combination of Card-on-File (with PAN) and EMV Payment Token

4.4.1 Overview

This combination is a hybrid form of card-on-file storage where the merchant stores both an EMV payment token and the PAN.

4.4.2 Provisioning

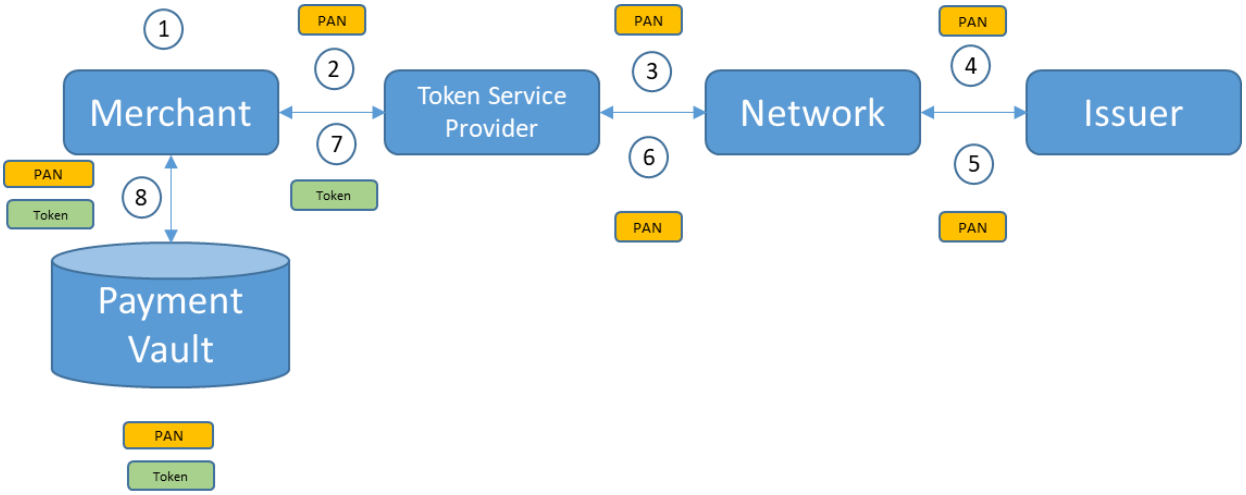

Figure 5. Provisioning Steps for Combination Card-on-File (with PAN) and EMV Payment Tokens

Figure 5 illustrates the provisioning steps for combination card-on-file (with PAN) and EMV payment tokens. During provisioning, the following steps occur:

1. The cardholder adds their card to their registered profile on the merchant's web site.
2. The merchant submits a token request transaction to the TSP. The token request includes the PAN and expiration date and may also include AVS and card security code data.
3. The TSP validates the merchant as a token requestor and forwards the token request transaction to the network. In some cases, the TSP may send the payment network an ASI instead of a token request. The network forwards the token request transaction to the issuer for approval.
4. The issuer forwards the response to the token request transaction to the network.
5. The network forwards the token request transaction response to the TSP.
6. The TSP reviews the token request transaction response and, if TSP criteria are met, generates a payment token and expiration date, and forwards a token response to the merchant along with token data.
7. The merchant receives the response to the token request transaction and, if the merchant criteria are met, the merchant adds both the token and PAN payment data to their payment vault. In addition to a unique identifier for records in the vault, storing certain descriptive meta-data outside of the vault may provide some benefit. The data stored outside of the vault may

be helpful in determining which records to retrieve – token or PAN. For example, the merchant may want to use some of the following types of information to determine which payment credential to retrieve from the vault:

a. Payment credential type (e.g., EMV payment token, PAN)
b. Card type (e.g., debit, credit, prepaid)
c. IIN/BIN range
d. Expiration date

4.4.3 Transaction Processing

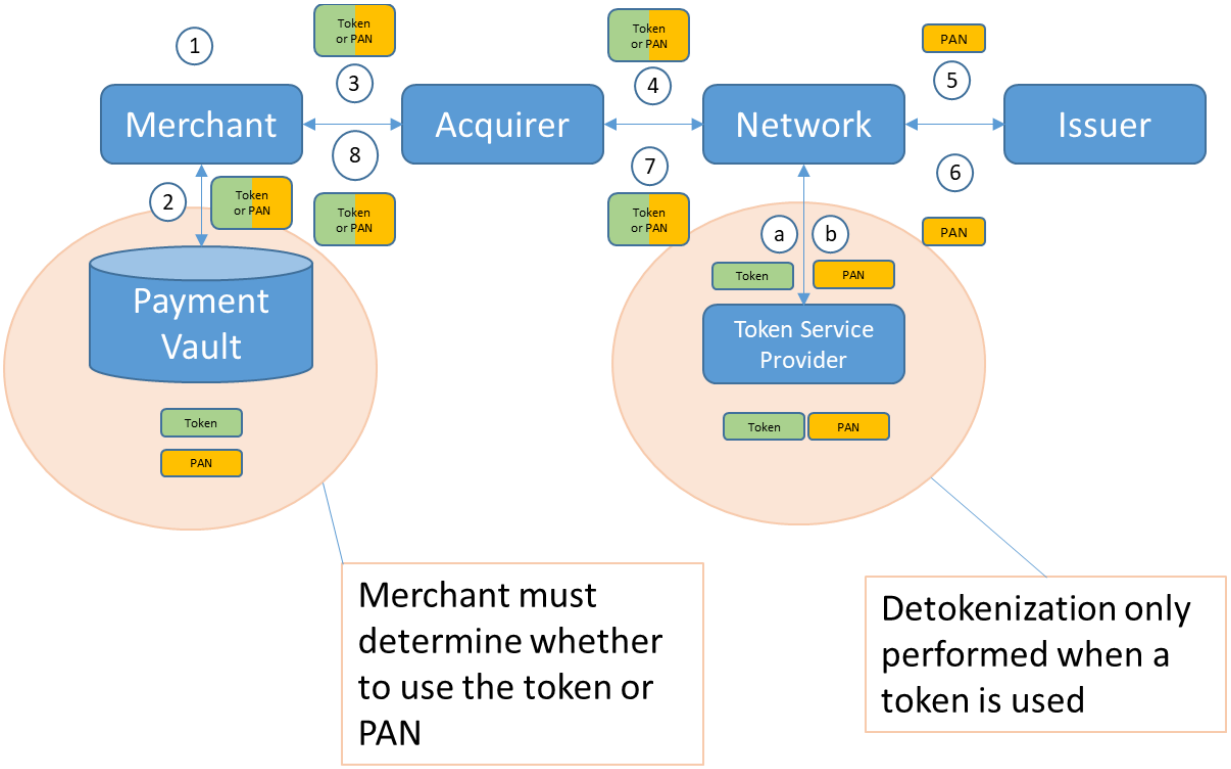

Figure 6. Transaction Processing Steps for Combination Card-on-File (with PAN) and EMV Payment Tokens

Figure 6 illustrates the transaction processing steps for combination card-on-file (with PAN) and EMV payment tokens. During transaction processing, the following steps occur:

1. The cardholder checks out on the merchant site and selects their card for payment.
2. The merchant applies business logic to determine which stored payment credential (i.e., token/expiration date, PAN/expiration date) to retrieve from the payment vault. The merchant may use data stored during provisioning to select a distinct payment credential. Alternatively, the merchant may select all records from the vault and then apply logic to select the payment credential to use for the transaction.
3. The merchant sends an authorization request to the acquirer using the retrieved payment credentials.
4. The acquirer determines the available networks, selects an eligible network following token payment network restrictions, and routes the authorization request to the selected network.
5. The network determines the payment credential type.

If the payment credential is a PAN, the network sends the authorization request to the issuer for approval.

If the payment credential is a token, the following steps are performed:

a) The network sends a detokenization request to the TSP.
b) The TSP performs detokenization and forwards the PAN, PAN expiration date, and other detokenization results to the network.

The network receives the detokenization response from the TSP, reformats the authorization request to include the PAN and PAN expiration date, and sends the authorization request to the issuer for approval.

6. The issuer generates an authorization decision and sends an authorization response to the network.
7. The network forwards the authorization response to the acquirer unless the original authorization request was received with a token, in which case the network replaces the PAN with the token and forwards the authorization response to the acquirer.
8. The acquirer forwards the authorization response to the merchant.

4.4.4 Lifecycle Management

The merchant must perform both non-tokenized and tokenized lifecycle management processes.

4.4.5 Compliance Considerations

PANs must be stored in PCI-compliant storage systems.

4.4.6 Impacts and Considerations by Stakeholder Group

Merchant	• Merchants must enhance their processing systems to choose which payment credential should be used for a given transaction.
	• Transactions processed using a PAN may be routed to any supported network.
	• PANs must be stored in a PCI-compliant manner.
	• PANs require either proactive or reactive lifecycle management.
	• Debit routing may be limited depending on the TSP that provisions the token; however, transactions processed using a PAN may be routed to any supported network.
	• When acting as the token requestor, the merchant:
	  • Must certify to the TSP.
	  • Must request and maintain tokens in their payment vault.
	• When outsourcing the token requestor service to a third party, the merchant:
	  • May have to enhance systems to store token data.
	• Debit routing policies, PCI compliance and customer experience may vary from one TSP to the next.

Acquirer	• PANs must be stored in a PCI-compliant manner.
	• PANs require either proactive or reactive lifecycle management.
	• An acquirer that wishes to support tokens for their customers would seek to become a registered token requestor with each TSP they choose to integrate with.
	• When acting as the token requestor, the acquirer:
	  • Must certify to the TSP.
	  • Must request and maintain tokens in their payment vault.
	• An acquirer could also offer debit routing functionality as an additional or included service with their token product.

	• To support this functionality, the acquirer may require system changes to accommodate their preferred business logic.
Network	• The network may need to certify and maintain an interface to each TSP with which their cards participate. • The network also performs call-out interactions to the TSP on each tokenized transaction to either validate security and or obtain the PAN. • The network may also need to make appropriate changes to accommodate token processing and communicate those to issuers and acquirers.
Issuer	• The issuer may have to certify to some networks' token-related message formats and make other system changes. • The issuer may also implement changes to their risk management processes and systems for both provisioning and transaction processing related to tokens associated with cardholder accounts.

4.5 Combination of Multiple EMV Payment Tokens

4.5.1 Overview

In this form of card-on-file storage two or more EMV payment tokens are obtained and stored by the merchant directly, or indirectly via a service provider, in place of a PAN. The party that requests and maintains the token is referred to as the token requestor. Merchants obtain payment tokens either at the time a customer adds their payment card details to their registered profile or some time afterwards. PANs are deleted from storage on the merchant system when the payment tokens are received.

4.5.2 Provisioning

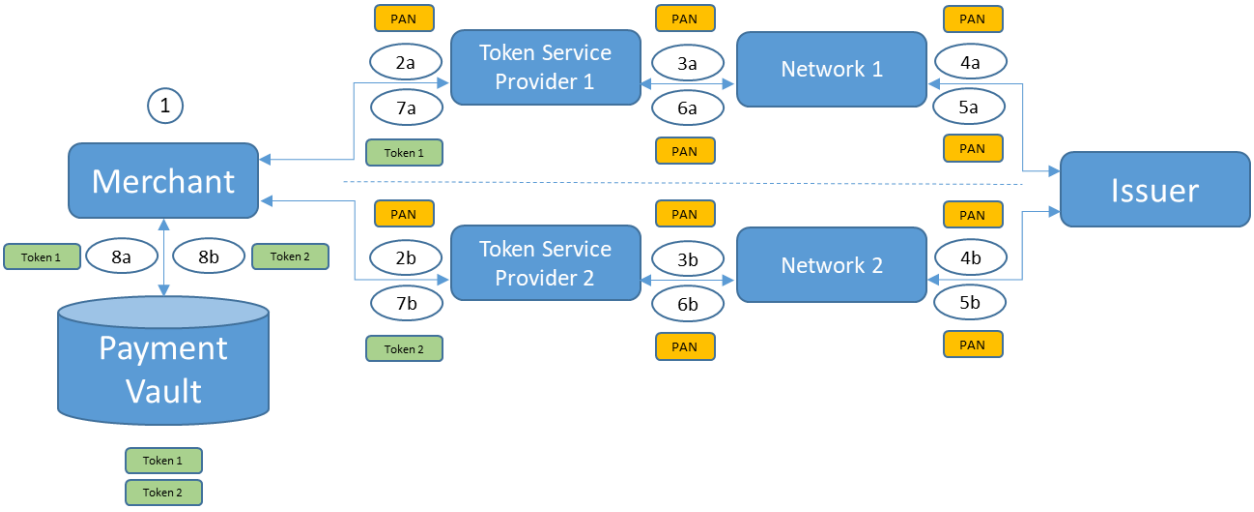

Figure 7. Provisioning a Combination of Multiple EMV Payment Tokens

Figure 7 illustrates the provisioning steps for multiple EMV payment tokens. During provisioning, the following steps occur:

1. The cardholder adds their card to their registered profile on the merchant's web site.
2. The merchant submits a token request transaction to the primary TSP (generally the payment network TSP that is shown on the front of the card). The token request includes the PAN and expiration date and may also include AVS and card security code data.

3. The TSP validates the merchant as a token requestor and forwards the token request transaction to the network. In some cases, the TSP may send an ASI to the payment network instead of a token request. The network forwards the token request transaction to the issuer for approval.
4. The issuer forwards the response to the token request transaction to the network.
5. The network forwards the token request transaction response to the TSP.
6. The TSP reviews the token request transaction response and, if TSP criteria are met, generates a payment token and expiration date, and forwards a token response to the merchant along with token data.
7. The merchant receives the response to the token request transaction and, if the merchant criteria are met, the merchant adds the token payment data to their payment vault (noted by "a" in the process flow in Figure 7). The merchant then repeats steps 2-8 (noted by "b" in the process flow in Figure 7) with the secondary TSP (generally the TSP associated with the alternate debit network on the card).

4.5.3 Transaction Processing

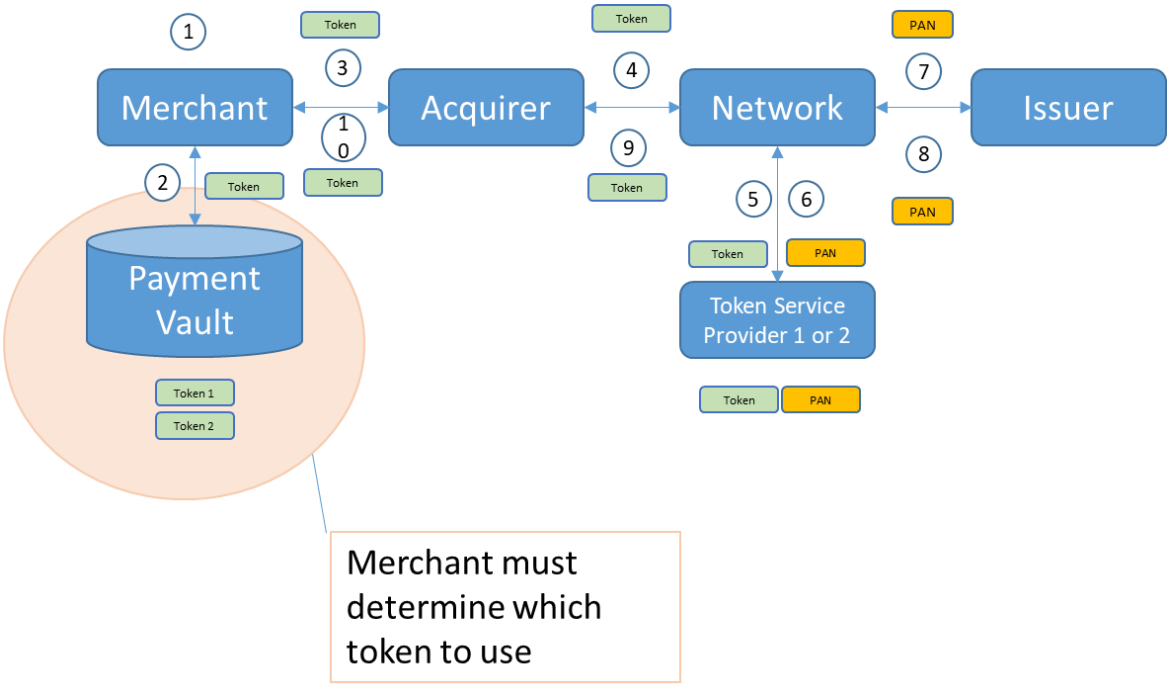

Figure 8. Transaction Processing with Multiple EMV Payment Tokens

Figure 7 illustrates transaction processing with multiple EMV payment tokens. During transaction processing, the following steps occur:

1. The cardholder checks out on the merchant site and selects their card for payment.
2. The merchant retrieves the stored payment credential data for both tokens from their payment vault.
3. The merchant selects the payment token that best suits their business requirements and sends an authorization request to the acquirer using the retrieved payment credentials.
4. The acquirer determines available networks, selects an eligible network following payment network restrictions, and routes the authorization request to the selected network.
5. The network sends a detokenization request to the appropriate TSP.

6. The TSP performs detokenization and forwards the PAN, PAN expiration date, and other detokenization results to the network.
7. The network receives the detokenization response from the TSP, reformats the authorization request to include the PAN and PAN expiration date, and sends the authorization request to the issuer for approval.
8. The issuer generates an authorization decision and sends an authorization response to the network.
9. The network forwards the authorization response to the acquirer unless the original authorization request was received with a token, in which case the network replaces the PAN with the token and forwards the authorization response to the acquirer.
10. The acquirer forwards the authorization response to the merchant.

4.5.4 Lifecycle Management

With payment tokens, changes to the PAN and/or expiration date are managed by the TSP. If a lifecycle management change results in a change to the underlying payment token, the TSP pushes updated token information to the token requestor for updating their systems. In cases where a cardholder deletes their payment credential from the merchant system, the merchant causes the token requestor to suspend the token and to notify each TSP that their respective tokens have been suspended.

4.5.5 Compliance Considerations

Payment tokens may be subject to less stringent PCI compliance obligations.

4.5.6 Impacts and Considerations by Stakeholder Group

Merchant	• Merchants must enhance their processing systems to choose which of the two or more tokens should be used for a given transaction.
	• Debit routing may be limited depending on the TSP that provisions the token.
	• When acting as the token requestor, the merchant:
	  ○ Must certify to the TSP.
	  ○ Must request and maintain tokens in their payment vault.
	• When outsourcing token requestor services to a third party, the merchant:
	  ○ May have to enhance systems to store token data.
	• Debit routing policies, PCI compliance, and customer experience may vary from one TSP to the next.

Acquirer	• When acting as the token requestor, the acquirer:
	  ○ Must certify to each TSP.
	  ○ Must request and maintain tokens in their payment vault.
	• An acquirer could also offer debit routing functionality as an additional or included service with their token product.
	• To support this functionality, the acquirer may require system changes to accommodate their preferred business logic.

Network	• The network may need to certify and maintain an interface to each TSP in which their cards participate. • The network also performs call-out interactions to the TSP on each tokenized transaction to either validate security and or obtain the PAN. • The network may also need to make appropriate changes to accommodate token processing and communicate those to issuers and acquirers.

Issuer	• The issuer may have to certify to some networks' token-related message formats and make other system changes. • The issuer may also make changes to their risk management processes and systems for both provisioning and transaction processing related to tokens associated with cardholder accounts.

5. Conclusion

Industry stakeholders have multiple options for card-on-file credentials management. Some are designed to assist with PCI compliance, others to reduce friction, others to increase security, with some solutions impacting all of these goals. It is important for industry stakeholders to distinguish and analyze differences among the options. There is no one best solution. The solution chosen by a merchant will depend on multiple factors, including that merchant's business objectives, resource constraints, and options available through the merchant's technology providers.

Of the many solutions available, some of the options discussed in this white paper provide a useful purpose in protecting data at rest and during the transaction flow. The options may or may not have an impact on transaction routing. The options included:

- Card-on-file (with PAN)
- Merchant tokenization
- Merchant service provider/vendor tokenization
- EMV payment tokenization
- Combination of card-on-file (with PAN) and EMV payment tokenization
- Combination of multiple EMV payment tokenization solutions

Other options not included in this paper may be or may become available.

Merchants, acquirers, issuers, debit networks, global payment networks and other industry stakeholders are encouraged to evaluate the solution configurations presented in this paper as they compare the relative merits of each option for security, technical implementation, and debit routing support, and as they consider whether or how best to implement EMV payment tokenization while balancing their business needs.

6. Legal Notice

This document is provided solely as a convenience for purposes of familiarizing readers with card-on-file (COF) tokenization and related considerations. While great effort has been made to ensure that the information provided in this document is accurate and current, this document does not constitute legal or technical advice, should not be relied upon for any legal or technical purpose, and all warranties of any kind, whether express or implied, relating to this document, the information herein, or the use thereof are expressly disclaimed, including but not limited to warranties as to the accuracy, completeness or adequacy of such information, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement. Any person that uses or otherwise relies on the information set forth herein does so at his or her sole risk. This document is not intended to be exhaustive; COF tokenization implementations, circumstances and considerations may differ, as may corresponding stakeholder security and business needs, requirements, capabilities, and results, any of which may impact or be impacted by specific facts and circumstances. Accordingly, stakeholders interested in implementing COF tokenization are strongly encouraged to consult with the relevant payment networks, acquirers, processors, issuers, TSPs and other stakeholders, as well as appropriate professional and legal advisors, prior to any implementation decisions.

7. Glossary

Term	Definition
Card-on-File (with PAN)	A PAN and associated data that is stored by a merchant who has been given permission by the cardholder; the data is saved for potential future transactions.
Debit Routing	Refers to the ability of a U.S.-based merchant to route a U.S.-issued debit card transaction to the merchant's choice of available networks, in accordance with the Durbin Amendment of the Dodd-Frank Act and Reg II.
EMV Payment Token	See payment token.
Lifecycle Management	Refers to the processes of maintaining current payment credentials across all involved systems, typically those at the issuer, network, TSP, acquirer, and merchant. For non-tokenized payment credentials, merchants may use account updater services, if available, to maintain stored credentials in a current state. Merchants that do not use account updater services must rely on cardholders to update stored payment credentials each time those credentials change. For tokenized payment credentials, merchants may be required to notify TSPs when a cardholder deletes a previously stored payment credential from the merchant site. All other lifecycle management functions are generally performed between the issuer and the TSP.
PAN	Primary account number assigned by an issuer to a cardholder customer for payment services.
Payment Credentials	The data used to identify and authenticate a card through a payment network, typically including values such as the PAN and expiration date.
Payment Token	A surrogate value for a PAN that is a variable-length, ISO/IEC 7812- compliant number issued from a designated token BIN or token BIN range and that does not conflict with an in-service PAN.
Payment Tokenization	The process of replacing a PAN and associated sensitive data with non-sensitive data, reducing the risk profile of the credentials if compromised.
Token	A term generally referring to a broad class of values that may be used to obfuscate payment credentials. Subclasses exist and range from proprietary, merchant payment tokens to EMV payment tokens.
Token Processing	The process by which a payment token and related data are used to enable payments across authorization, clearing, settlement and exceptions.

Term	Definition
Token Request	A request for a payment token from a token requestor to a TSP. The request includes the PAN and expiration date and may include AVS and card security code.
Token Requestor	An entity that requests a token from a TSP.
Token Service Provider	An entity managing payment token allocation to token requestors.