GENERAL GUIDANCE ON TOKENIZATION AND THE IMPACTS ON PCI DSS SCOPING

ADVANCING COMMERCE™

WHAT IS TOKENIZATION?

Tokenization is a process by which the primary account number (PAN) is replaced with a surrogate value called a token.‖ Storing tokens instead of PANs can help to reduce the amount of cardholder data in an environment. The substitution or mapping of Accounting Data (PAN, Expiration Date, etc.) to tokenized data occurs within the secure confines of a token vault. MasterCard's tokenization process and product is known as the MasterCard Digital Enablement System or MDES.

TOKEN TYPES

Within the payments industry, there are three broad types of tokens: Acquiring, Payment, and Issuer. This paper will primary focus on the difference between *Acquiring tokens* and *Payment tokens*.

1. **Acquiring tokens**– replace card data with a substitute value and are created after a cardholder presents the card.

   Use case:
   - Some acquiring tokens can be used for payment transaction initiation; however, in all cases acquiring tokens are converted back to the original PAN before being sent outside the closed environment for which they are intended.
   - Acquiring tokens may be used between the merchant and its acquirer for critical business functions without exposing the original PAN in the merchant's environment.

   Benefits of using acquiring tokens:
   - Acquiring tokens allow for the removal of sensitive account data during storage and may also protect data in transit in some cases.
   - Acquiring tokens can be used in card-not-present transactions, such as Card on File, for recurring transactions.
   - Acquiring tokens will continue to play a role in reducing the PCI footprint of stakeholders in the payments industry if properly segmented from any other clear text account data.

   Note: Acquiring tokens that can be used to initiate a payment (often referred to as High Value tokens) may still be in scope for PCI requirements and must be evaluated on a case by case basis to determine whether or not any PCI scope reduction is applicable.

2. **Payment tokens**– are used to make a payment. Unlike acquiring tokens, the cardholder presents the payment token in place of the regular PAN. Payment token presentment usually occurs through a digital wallet contained on a smartphone or smart device, or may be provisioned directly to a card on file system. Inherently, payment tokens have a higher degree of security than acquiring tokens since the original cardholder data is not exposed inside of the merchant's environment.

Use case:

- Payment tokens can be used to enable secure, digital payments for face-to-face channels, such as through mobile devices.
- Payment tokens can be used to replace sensitive data such as PAN in Card on File scenarios for card-not-present transactions.

Benefits of using payment tokens:

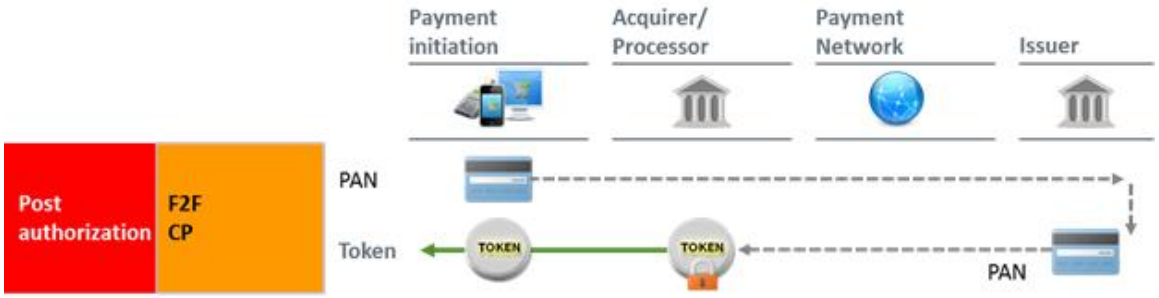
- Payment tokens allow for one-time-use dynamic cryptograms as well as domain controls to restrict or eliminate potential fraud making each transaction unique and reducing the risk of counterfeit fraud.
- Payment tokens are designed to be of such a low value to criminals, that the tokens are considered to be out of scope for PCI DSS compliance when used with dynamic cryptograms and/or domain controls.
- Payment tokens are created using EMVco specifications and provide interoperability across payment systems resident within financial entities unlike acquiring tokens which do not offer portability outside the acquirer's purview.

THE IMPACT OF TOKENIZATION ON PCI SCOPE

While acquiring and payment tokens have different use cases; they do share one commonality – they both devalue the payment card data to threat actors who commit fraud. In addition, both token types have the ability to reduce PCI DSS compliance scope. Acquiring tokens can reduce scope if proper segmentation exists between tokenized and account data; however, the greatest reduction can be achieved through the use of payment tokens whereby the token represents cardholder data that is secured in a third-party token vault. Likewise, payment card data may still be exposed via other channels or in the tokenization systems themselves. Thus, use of tokenization technology may result in differing levels of PCI scope reduction dependent upon the particular implementation. As always, any system that stores, transmits, or process PAN (or is connected to such a system) will remain in scope of PCI DSS requirements. Various acquiring token use cases exist; some illustrative examples and their representative scope reduction are included below:

Acquiring Tokens

CARD PRESENT (FACE TO FACE TRANSACTION)



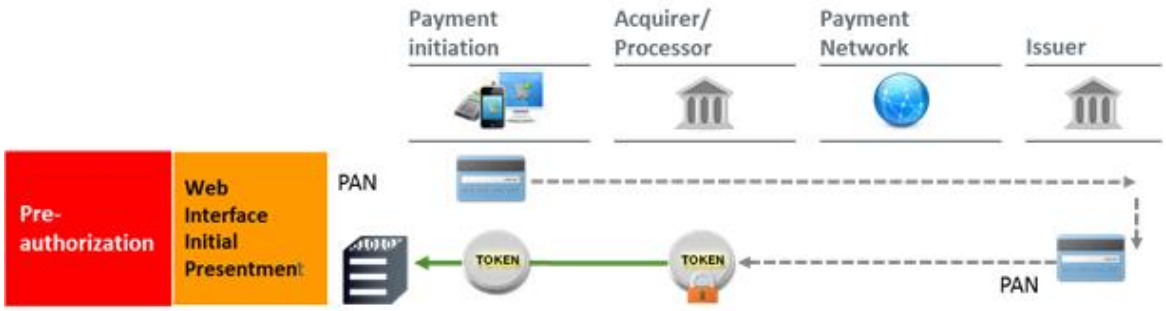
CARD PRESENT (CP) (USING THE ABOVE ILLUSTRATION)

Payment is initiated by the cardholder who would be presenting a traditional plastic card and using a payment terminal such as a magnetic stripe reader, chip reader, or NFC. Clear text cardholder data (PAN and SAD) is exposed until the data reaches the acquirer's system or token vault where the surrogate value for the PAN is created and the token is returned to the Point of Interaction (POI)/Point of Sale (POS) and/or stored on file within a database.

CP PCI SCOPE

In this scenario the entity may be eligible for PCI scope on the back-office and/or post-transaction environment. As the full PAN is present throughout the transaction authorization process, all front-end systems (i.e. merchant shop) remain in-scope for PCI DSS. However, on the back-office systems (that perform reporting, reconciliation, rewards, among other examples) PCI DSS scope may be more limited, dependent upon multiple factors; but, primarily through the use of segmentation between clear text PAN data and the token environment, as PAN has been replaced with the acquiring token.

CARD NOT PRESENT (CNP) INITIAL PRESENTMENT



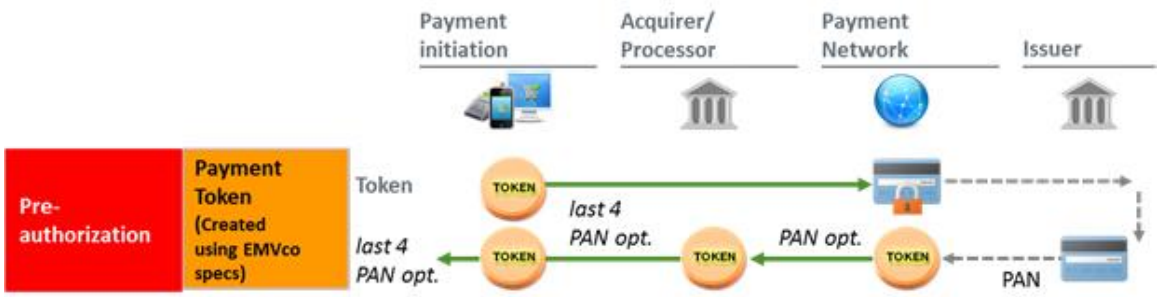
CARD NOT PRESENT (CNP) (USING THE ABOVE ILLUSTRATION)

The cardholder provides their account data remotely, such as through an e-commerce website. The merchant provides the account data to their acquirer where an acquiring token is generated and returned to the merchant. The merchant then stores the acquirer token and securely disposes of the cardholder's account data.

CNP PCI SCOPE

If the merchant is using an acquiring token stored in a database for card-on-file recurring transactions; then the potential for scope relief exists; however, this depends on appropriate segmentation being implemented between systems with account data and the tokenized data. It is important to note, if clear text PAN is accepted for transaction payments then those channels and associated systems that process, store, or transmit data must remain in the PCI DSS scope.

Payment Tokens



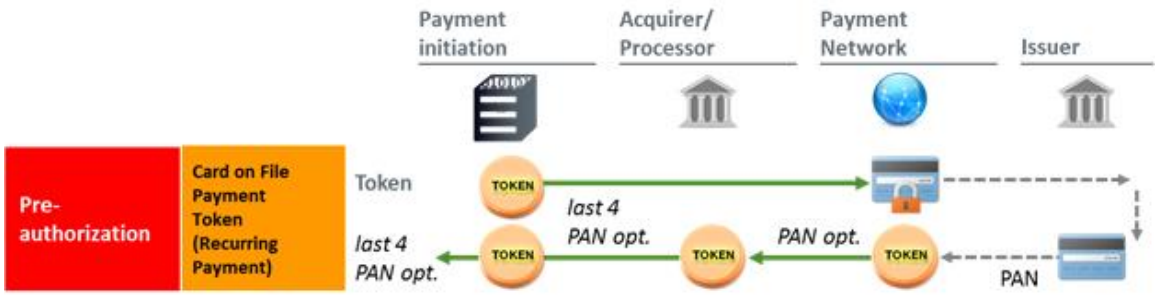
PAYMENT TOKENS (USING THE ABOVE ILLUSTRATION):

Payment is initiated by the cardholder who has received their card credentials in digitized format such as a payment token. The payment token is presented by the cardholder to a terminal, such as through NFC. The tokenized data is sent through the ecosystem where it remains tokenized until it is detokenized into account data (PAN and SAD) within a secured token vault and forwarded to the issuer for authorization.

PCI SCOPE

In this scenario, original PAN or its equivalent data is limited to the closed environment that exists between the payment network or a Token Service Provider and issuer. When payment tokens are used for transactional processing, PCI scope can be significantly reduced; if segmentation exists between payment tokens and clear text account data (PAN and SAD) during processing, storage or transmission. In other words, scope reduction can be recognized if segmentation is in place that segregates clear text account and payment token data. In fact, the PCI Council excludes payment tokens from being in scope for assessments. However, like acquiring tokens if other clear text payment acceptance channels exist then those channels and associated systems that process, store, or transmit data must remain in the PCI DSS scope.

CARD ON FILE



PAYMENT TOKEN (USING THE ABOVE ILLUSTRATION):

In most cases, a Card on File (CoF) is used for consumer convenience or recurring payments. At first purchase, a CoF merchant receives a cardholder's PAN and requests a payment token from a token vault (such as MDES). The merchant stores the payment token instead of the PAN to conduct future payment transactions. Future transactions are initiated using the payment token that is stored in the merchant's database.

PCI SCOPE

Like the card present scenario, original PAN or its equivalent data is limited to the closed environment that exists between the payment network or a Token Service Provider and issuer. When payment tokens are used in a Card on File scenario for transactional processing, PCI scope can be significantly reduced; however, anywhere there is clear text PAN present, PCI compliance must exist.

SUMMARY

Using and implementing acquiring and payment tokens provides entities the opportunity to reduce their risks and PCI DSS scope. Entities that store cardholder data, such as card on file, can significantly reduce their risk posture if cardholder data is replaced with acquiring tokens which in essence removes cardholder data from their environment. Furthermore, entities that choose to implement and segment payment token acceptance channels receive maximum PCI DSS scope relief since payment tokens are considered out of scope for PCI DSS assessments (see table below).

The following table provides a high-level overview of some of the key similarities and differences between Acquiring tokens and Payment tokens.

	Acquiring Tokens	Payment Tokens
FUNCTION	▪ Replaces sensitive card data (PAN) with a surrogate value ▪ Value created after cardholder presents card	▪ Replaces sensitive card data (PAN) with a surrogate value ▪ Value created before cardholder presents card
PCI DSS SCOPE	▪ Reduces PCI DSS compliance scope ▪ Proper segmentation must exist between tokenized and account data	▪ Maximizes PCI DSS compliance scope ▪ Payment tokens are considered out of scope for PCI DSS compliance when used with dynamic cryptograms/domain controls
BENEFITS	▪ Makes transactions more secure ▪ Reduces the risk of counterfeit fraud	▪ Enables digital payments ▪ Makes transactions more secure ▪ Reduces the risk of counterfeit fraud

BY LARRY NEWELL, CISSP, CISM, CISA MASTERCARD

For more information on MasterCard PCI 360 education resources, please visit www.mastercard.com/pci360 or www.mastercard.com/sdp