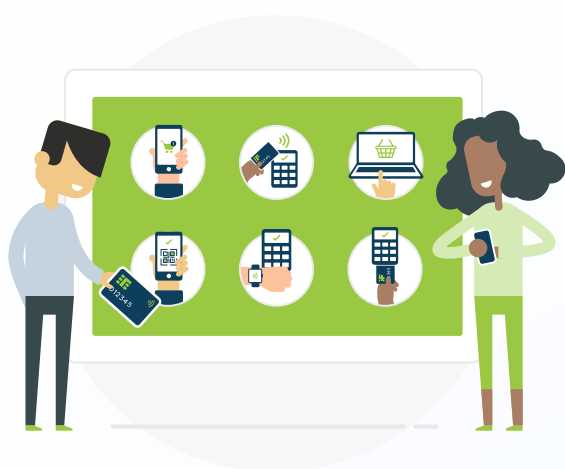


EMV® Payment Tokenisation

Transactions have historically been initiated using the primary account number (PAN) associated with a payment card. If the PAN is compromised, it leads to fraud and customer disruption. EMV® Payment Tokenisation mitigates these risks by providing additional controls that limit the risk typically associated with compromised, unauthorised or fraudulent use of PANs both in-store and online.



Why is EMV Payment Tokenisation needed?

- ✓ Payment technologies must be secure and convenient.
- ✓ Consumers are increasingly paying in new ways both in-store and online.
- ✓ Protecting payment data in transit and at rest is fundamental.
- ✓ Reducing the value and limiting the use of compromised payment information is critical to protect consumers and businesses.

How does EMV Payment Tokenisation work?

EMV Payment Tokenisation enhances in-store and remote transaction security by removing the most valuable data to a fraudster within a transaction, the PAN, and replacing it with a unique alternative value, an EMV Payment Token.

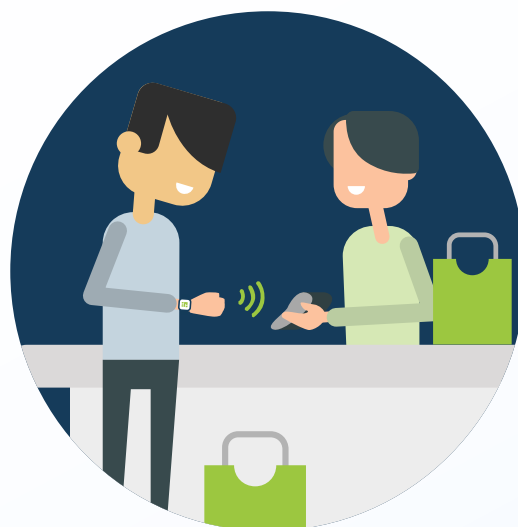
EMV Payment Tokens are by design constrained in how and where they are used to prevent their use outside of specific defined parameters. For example, an EMV Payment Token can be provisioned to a specific device, merchant, or for a specific use case. This reduces the value of payment information stolen in the event of a data compromise.

More than just a PAN replacement

The presence and application of Token Domain Restriction Controls (TDRC) is unique to EMV Payment Tokens and critical to transaction integrity and fraud prevention. They enable the constraint of an EMV Payment Token to its intended use case(s) or domain(s).

How does EMV Payment Tokenisation differ from other forms of tokenisation?

Other forms of tokenisation typically do not pass across payment networks and can happen at different points within the payment process. In the merchant environment, for example, tokenisation can happen between the merchant and the acquirer. In contrast, EMV Payment Tokenisation provides end-to-end tokenisation throughout the transaction, from the cardholder interaction with the merchant to the issuer.



How are EMV Payment Tokens managed throughout their lifecycle?

Common interfaces ensure that an EMV Payment Token is affiliated with the correct PAN and can be appropriately managed throughout the lifecycle of both elements. This enables the PAN and EMV Payment Token to be managed interdependently to minimise disruption to the cardholder if either needs to be updated.



The cardholder uses a mobile payment application and their device is lost / stolen. The EMV Payment Token associated with the PAN can be deleted and a replacement EMV Payment Token issued to a new device without the need to change the PAN or issue a replacement payment card.



The cardholder has a card saved 'on file' with a number of merchants and the underlying PAN is updated. The payment token associated with the PAN at each merchant can be linked to the new PAN without any cardholder input.



Benefits of EMV Payment Tokenisation

EMV Payment Tokenisation offers consumers and merchants the ability to protect payment data throughout a transaction to support security. This means that all parties within the payment community can realise the benefits of this technology.



Enhanced Security

Reduces the value of stolen or compromised payments information. Merchants have reduced the likelihood of being targeted by criminals and potentially have reduced costs associated with storing payment data. Issuers have fewer card replacements.



Enables Innovation

Enables the development of new payment technology and scenarios, without impacting security, or adding cardholder friction. Consumers and merchants benefit from the convenience provided by the ability to support high value transactions.



User Convenience

Uses the existing familiar, convenient and seamless payment infrastructure to improve security and support innovative new ways to pay. Consumer behaviour does not need to change.



Compatibility

Provides compatibility with and allows the use of other forms of tokenisation such as acquirer and/or security tokens.



Flexibility

Supports all use cases which traditionally have used a PAN.

How can the payment community use EMV Payment Tokenisation?

Technical documents and use case examples provide a common foundation that can be adapted to regional or country-specific implementation requirements. They are available, royalty-free from the [EMVCo website](https://www.emvco.com). EMV Payment Tokens can co-exist with other forms of tokenisation, support many use cases and are applicable in any environment which traditionally have used a PAN.



What is EMVCo's role in EMV Payment Tokenisation?

EMVCo publishes the EMV Payment Tokenisation technical documentation and maintains the registry of Token Service Providers and Bank Identification Number (BIN) Controllers. Product or solution implementation is beyond EMVCo's remit.

Learn more - visit the EMVCo Website:

www.emvco.com 