EMV Specifications provide foundational requirements for developing products that support seamless and secure in-store, online and remote card-based payments.

EMV 3-D Secure (EMV 3DS), EMV Secure Remote Commerce (EMV SRC) and EMV Payment Tokenisation support the global adoption of secure technologies that fight fraud and enable convenient and reliable payments across all online commerce channels and connected devices.

By offering convenience and confidence, these specifications help deliver a consistent and trusted payments experience for e-commerce merchants and their customers.

DID YOU KNOW?

EMV SRC, 3DS and Payment Tokenisation Specifications enable the consistent use of these fraud fighting technologies, which can be used together or separately to deliver a safe and convenient payment experience. EMVCo also works closely with organizations including FIDO Alliance and the World Wide Web Consortium (W3C) to promote industry-wide compatibility.

The airline industry has always looked to prevent fraud and better protect its customers. The EMV 3DS protocol helps make internet card payments more secure, while achieving a better balance between security and customer convenience by letting the card issuer know more details about the intended purchase.

For more information on EMVCo please visit: www.emvco.com

EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.
In today's connected world, protecting data can be challenging. A particularly sensitive piece of payment data when shopping online is the primary account number (PAN) – the number on payment cards that is used to make purchases. EMV Payment Tokenisation provides a technology solution for protecting the PAN and securing digital and online payments.

EMV Payment Tokenisation is the process of replacing a consumer's PAN with a unique, payment token. Importantly, a payment token can be restricted in how it can be used. For example, a payment token may only be used on a specific device or merchant website. This enhances the underlying security of digital and online payments by limiting the risk of the PAN being compromised or used fraudulently / without authorisation. It also reduces potential disruption for both consumers and merchants if a payment card is lost or stolen.

Complexity and unwanted friction are key challenges for e-commerce merchants and consumers. The EMV SRC Specifications enable a common consumer e-checkout, Click to Pay, and provide the opportunity for all merchants globally, regardless of size, to offer trusted, safe and convenient card-based payments to consumers shopping online. By enabling a common experience across online commerce sites, EMV SRC removes barriers to the purchasing process that can lead to abandonment, such as entering card and shipping information.

EMV 3-D Secure (EMV 3DS) helps prevent the unauthorised use of a card online and provides consumers and merchants with the confidence that they are protected from fraud, while also supporting an easy and convenient purchasing experience that reduces the number of declined transactions.

For transactions that are higher risk, EMV 3DS provides an additional layer of security to validate that the individual making the purchase is the legitimate cardholder.

What are examples of high risk transactions?

- Transactions made from a new device
- Transactions made for an unusually large amount
- Unexpected transaction types

EMV 3DS is designed to support many authentication methods. This provides flexibility to the issuing banks, which ultimately decide how the cardholder should be authenticated.

- One-time-passcodes
- Knowledge-based questions
- Biometrics

*The Payment Tokenisation Specification provides an interoperable Technical Framework.