The Future of Payments is Now: Advancing EMV® Technology

Wednesday 17 September 2025

Oliver Manahan, Director of Engagement and Operations

About EMVCo

EMVCo enables card-based payments to work seamlessly and securely worldwide

Mission

To facilitate the worldwide interoperability of secure payment transactions by developing and publishing the EMV® Specifications and their related testing processes

- Specifications
- Approvals and Evaluations
- EMVCo Marks
- Industry Engagement and Collaboration

EMVCo In Numbers

Worldwide EMV® Deployment Statistics

14.7bn
EMV Chip payment cards in global circulation
(as of December 2024)

of all issued cards globally are EMV
(as of December 2024)

of all card-present transactions globally were EMV Chip
(as of December 2024)

Industry Engagement

79
Associates

359
Subscribers

11,000+
Approved and Evaluated products

178
Qualified test tools

20
Working Groups and Task Forces

82
Recognised laboratories

Current EMVCo Associates

*Participation as of June 2025

Industry Engagement

Key Initiatives

EMV® Technology Initiatives

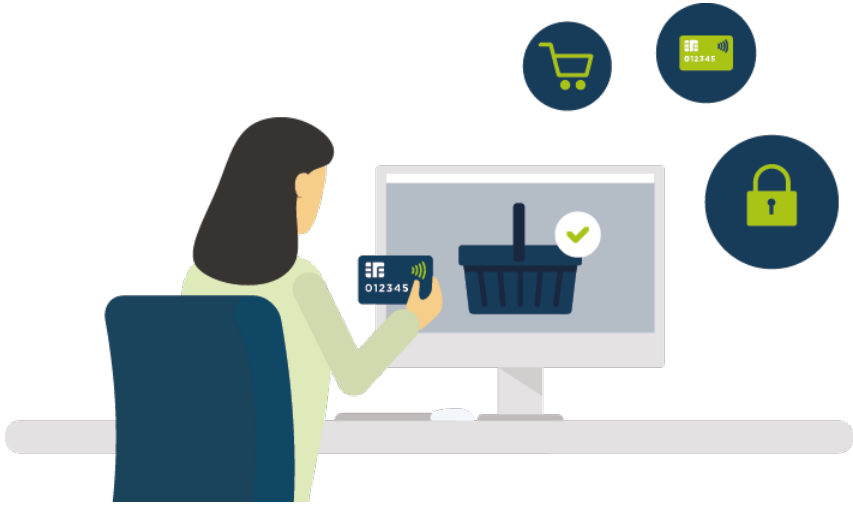
EMV® Contact and Contactless Chip

- Reduced Range Approval Process
- EMV Contactless Kernel Approval Process
- EMV Contact Chip Features Sunsetting
- New POI Information Identifier for Transit Operators
- EMV Level 3 (L3) Testing Framework – Participant Systems Guidelines

EMV® Technology Initiatives

EMV® 3-D Secure

- Guidance on Use of FIDO with EMV 3DS
- EMV 3DS White Paper: Frictionless Flow, Out-of-Band and Recurring Transaction Use Cases
- EMV 3DS Attribute Verification Message Extension
- EMV 3DS Wrapped SDK Best Practices
- Exploring the Use of the European Union Digital Identity Wallet (EUDI) in EMV 3DS



EMV® Technology Initiatives

EMV® Security

- Biometric on Card Security Guidelines
- Software-Based Mobile Payments (SBMP) Security Evaluation Methodology and Security Evaluation Guidance
- Quantum Computer Position Paper
- Annual RSA and ECC Key Lengths Assessment

Quick Resource Guide: EMV® Security


EMVCo

EMV® Security

Promoting cybersecurity in payments

Ensuring payment transaction security is a shared responsibility across all stakeholders. When payments don't work and security is compromised, everyone within the payments community is impacted.

For more than 20 years, EMV® technology has provided guidance on the appropriate level of security requirements to enable safe and reliable payments globally.

What is EMV security?

EMV Chip technology secures the communication channel between the payment device (card/smartphone/wearable) and the payment terminal.

An EMV transaction integrates security features such as cardholder verification, localised card and terminal risk management, as well as card and transaction data authentication ensuring integrity of the payment process.

The merchant terminal cryptographically authenticates the payment device and its data by verifying digital signatures that have been generated by the payment device, its issuer and the payment system.

A one-time use security code is produced for every EMV transaction.

How does EMV secure a payment transaction?

During a transaction the cardholder's payment device responds to an unpredictable number from the terminal to create two types of cryptograms: an offline cryptogram that can be verified locally by the terminal, and an online cryptogram that can be verified remotely by the issuer.

- **Public key cryptography** is used for local authentication: the payment device uses its private key to authenticate itself and the transaction data to the terminal locally. This avoids the payment device and terminal sharing secret keys.
- **Symmetric cryptography** is used for remote authentication: the payment device uses its secret session key to authenticate itself and transaction data to the issuer directly.

EMV supports the use of RSA (Rivest, Shamir and Adleman) and Triple DES (Data Encryption Standard), as well as ECC (Elliptic Curve Cryptography) and AES (Advanced Encryption Standard).

The potential impact of **quantum computing** is nuanced regarding EMV Chip cryptography as payment data is processed and managed in real time and not stored long-term. EMVCo is continually monitoring and analysing quantum advances to ensure adjustments are considered and implemented when relevant.

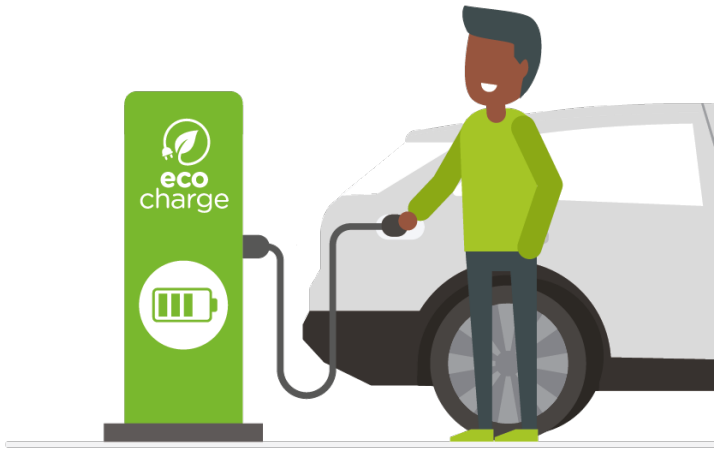
Video: Cryptography in EMV® Chip Payment Security

EMV Insights: How is EMV® Chip Addressing Cybersecurity in Payments?

EMV® Technology Initiatives

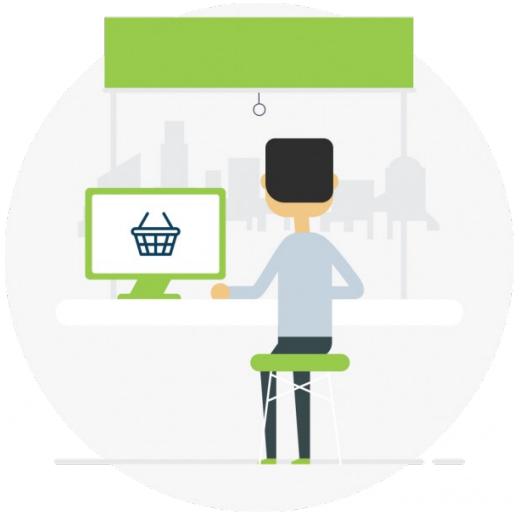
Electric Vehicle Open Payments (EVOP)

- Exploring approaches to enable a card-based open payment experience for EV drivers across charging networks



EMV® SRC

- EMVCo launched EMV SRC – Click to Pay CX Guidelines for merchants, payment service providers, product owners, developers and CX designers



Enhancing Seamless and Secure Payments in 2025

- Addressing new trends in payment initiation and authentication
- Continued collaboration on EV open payments
- Improving access to EMV® Publications
- Optimising EMVCo Approvals and Evaluations
- Evolving cryptography in EMV® Chip payments security

What is EMV® 3-D Secure?

"Solutions like EMV 3-D Secure are being more widely adopted to combat e-commerce fraud risks without adding friction to the checkout process."

U.S. Payments Forum

- EMV® 3-D Secure (EMV 3DS) helps payment card issuers and merchants around the world prevent card-not-present (CNP) fraud and increase the security of e-commerce payments.
- The EMV 3DS Specifications provide a common set of requirements that product providers can use to integrate this technology into their solutions to support seamless and secure e-commerce payments.
- EMVCo maintains the EMV 3DS Specifications and supporting approval processes, and collaborates with the PCI Security Standards Council on the security evaluation of EMV 3DS solutions.

The EMV® 3DS White Paper

The EMV 3DS White Paper is available in both an interactive online format and as a PDF.

It provides industry participants with an accessible, easy-to-use resource that aims to promote a better understanding of the EMV 3DS Specifications.

The White Paper takes industry's business use cases as the foundation and focuses on ways to implement 3DS technical features to better support those use cases.

Version 1.0 published in April 2024 included:

- Frictionless
- Challenge Flow/Improved Out-of-Band (OOB)
- Recurring and Instalment Transactions

Version 2.0 includes updates covering:

- WebAuthn and Secure Payment Confirmation (SPC)
- 3DS Requestor Initiated (3RI)
- Split-SDK
- Message Extension Implementation
- Delegated Authentication
- … and more

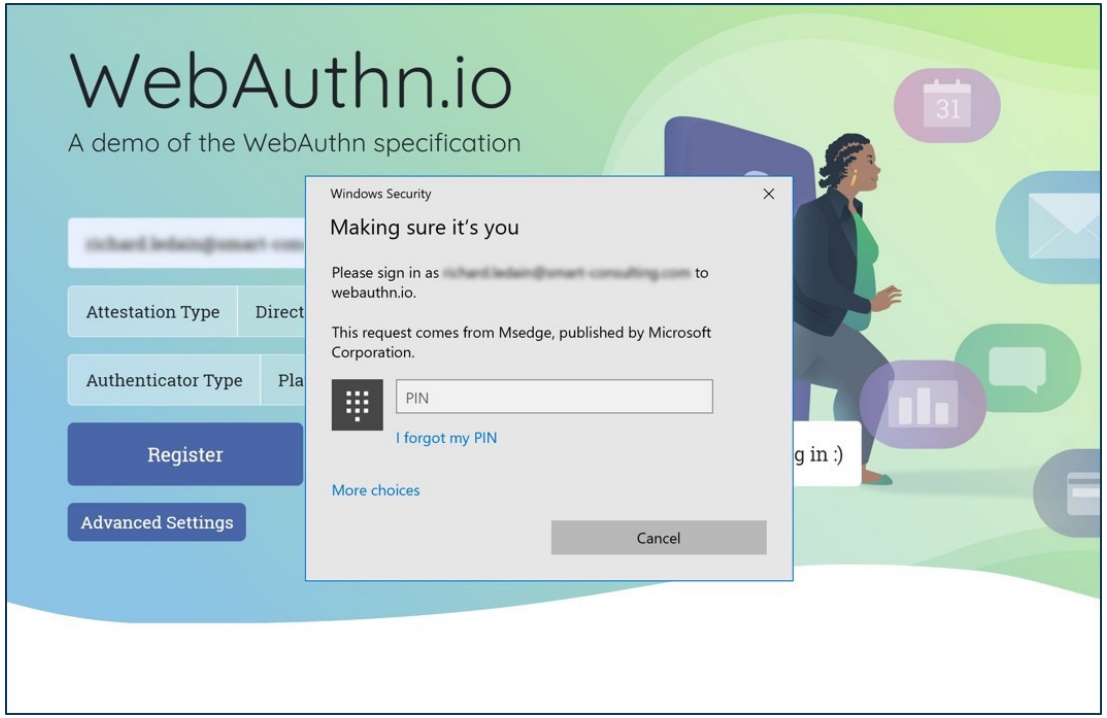
The white paper is also available in an interactive web format

https://www.emvco.com/whitepapers/emv-3-d-secure-whitepaper/

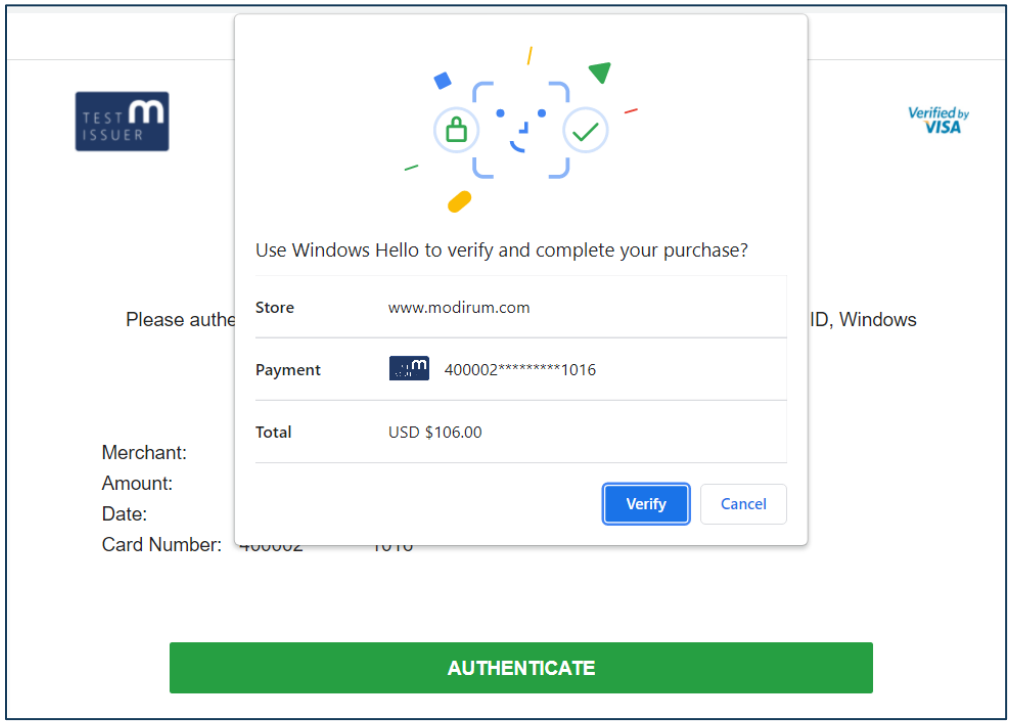
EMV® 3DS Supports Both WebAuthn and SPC

Issuers and merchants can use FIDO-based WebAuthn and SPC within the EMV® 3DS flow to better determine the legitimacy of a transaction in order to reduce the risk of fraud

WebAuthn



SPC



Evolution of Consumer Card Acceptance Devices

Dedicated devices were used for all acceptance environments to ensure:

- Interoperability
- Security
- A great user experience

Even in the most demanding acceptance environments, such as transit and retail.

Small businesses started using consumer mobile phones for payment, enabled through dedicated accessories embedding:

- Magstripe
- Contact
- And contactless readers

These accessories allow full compliance with EMV® Specifications (and PCI requirements).

Even more recently, NFC enabled devices are used for contactless card acceptance.

These devices can be:

- Off-the-shelf mobile phones
- Devices designed for professionals with payment in mind (but not as primary/sole use case)

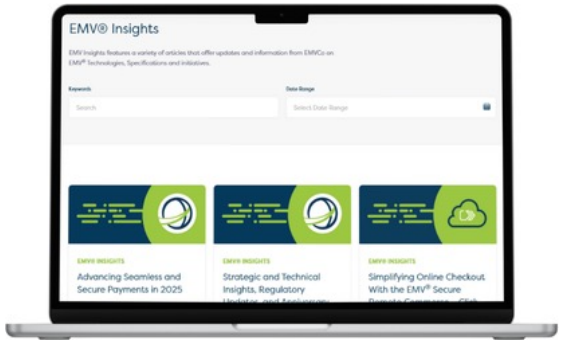
What is TapToMobile?

- EMVCo released the TapToMobile User Experience Guidelines in August 2021, focusing on the user experience aspects of Mobile Devices:
  - Where do I tap?
  - Point to tap may be on the reverse side of the screen
  - No fallback to chip or magstripe
- EMVCo launched its COTS (Consumer Off The Shelf) **Early Adopter Programme** in October 2020, which ran until April 2022.
- A number of NFC-enabled devices were evaluated with respect to their 'compatibility' with EMV® compliant cards and mobiles.
- One of the major findings is that user experience on these devices depends mainly on their NFC strength or 'read range'.

TapToMobile specifically allows merchants to accept contactless payments directly on NFC-enabled consumer mobile devices (such as smartphones, phones or tablets) with no need for an additional connected device, dongle or attachment.

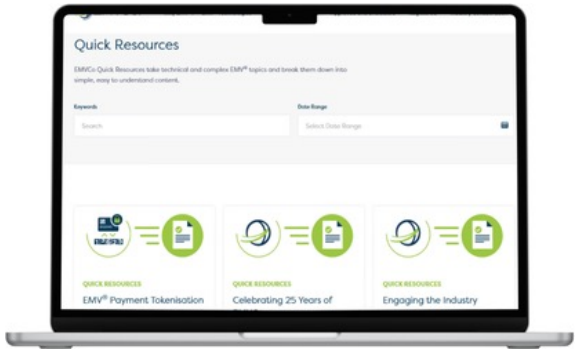
Knowledge Hub

EMVCo has a variety of educational channels and resources to connect with the wider payment community. This includes:

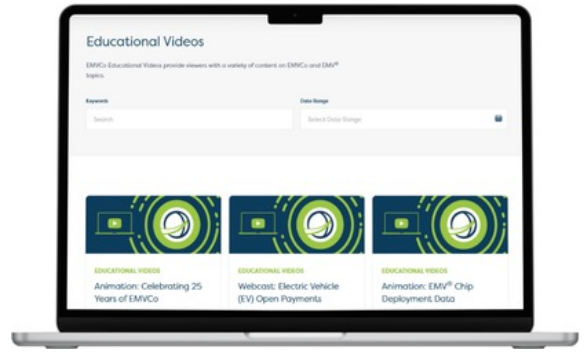


EMV® Insights

Annual Report



Quick Resource Guides



Educational Videos

Stay informed:

- Join us on LinkedIn
- Sign-up to EMVCo bulletins

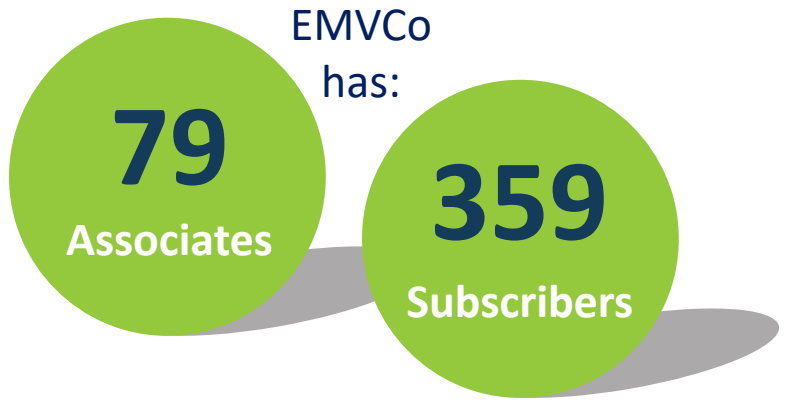
Industry Participation: Shaping the future of EMV® Specifications

Associates:
EMVCo Associates play an active role in EMVCo's strategic and technical direction and contribute their knowledge and expertise to shape the development of EMV® Specifications

Industry stakeholders across the globe, including merchants, banks and technology providers participate as EMVCo Associates to advance seamless and secure payments worldwide

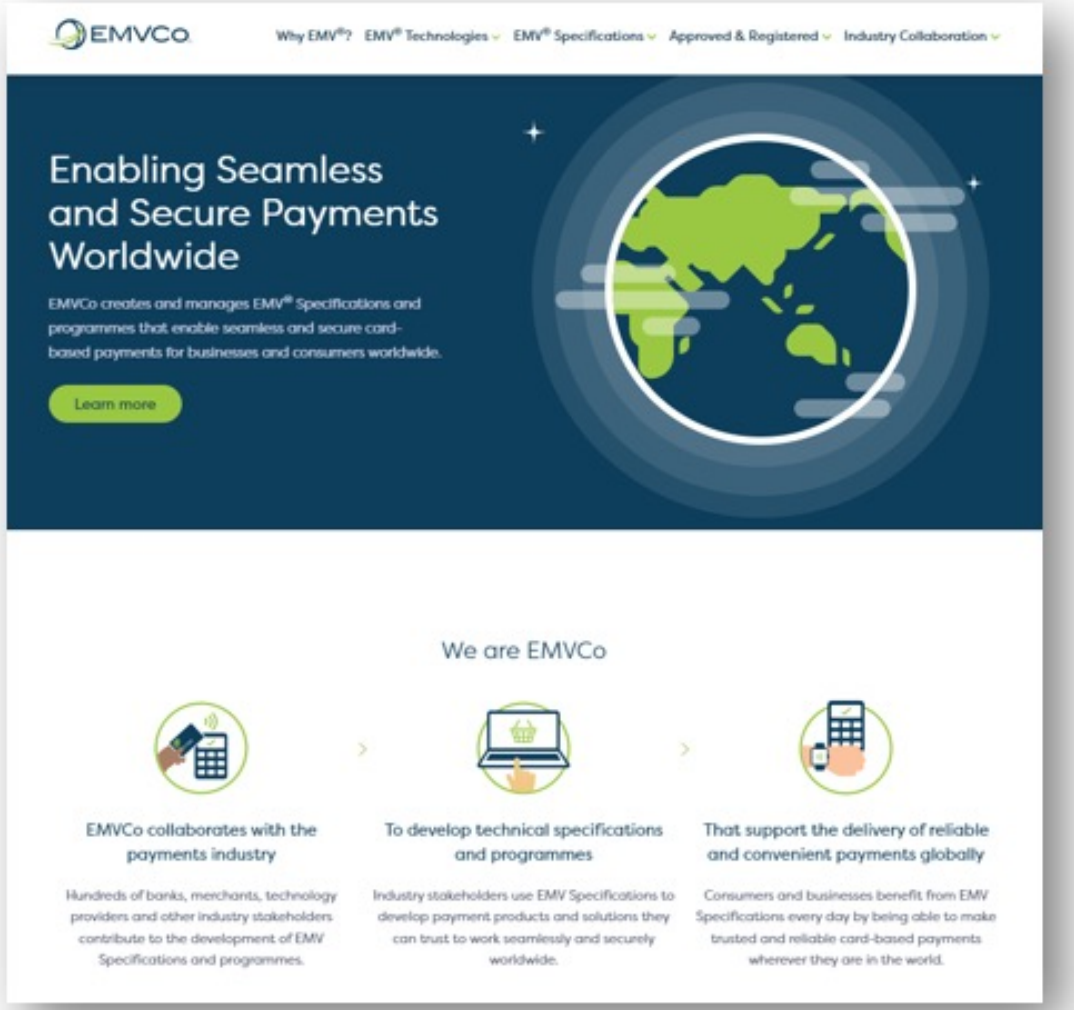
Subscribers:
Hundreds of industry stakeholders around the world participate as EMVCo Subscribers to receive advance insights on EMV Specifications and provide direct feedback

Any interested party can become an EMVCo Subscriber



To become an Associate or Subscriber visit: https://www.emvco.com/industry-collaboration/ways-to-participate/

Thank you



Visit www.emvco.com to access our Quick Resource Guides

Join us on **LinkedIn:** linkedin.com/company/emvco

Subscribe to **EMV® Insights**: emvco.com/emv-insights/

Watch more on **YouTube.** Search: EMVCo Videos

Subscribe to our **Podcast:** Talking Payments with EMVCo

PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING