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 data exchange 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.

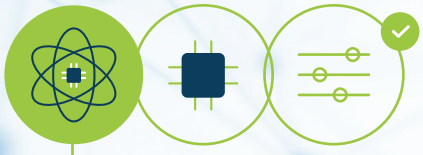
A one-time use security code is produced for every EMV transaction.

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.

Cybersecurity collaboration

EMVCo is a global body with a proven capability and framework to promote cybersecurity during a payment transaction. Its work is used by others to fight cyber threats, including local and global payment systems.

Its dedicated security group performs continuous monitoring of attacks and security developments to keep pace with currently known vulnerabilities and threats and undertakes the required updates to ensure the integrity of EMV Specifications.

EMVCo works closely with researchers, academics and global technical bodies, including the Payment Card Industry Security Standards Council (PCI SSC), World Wide Web Consortium (W3C), Fast IDentity Online (FIDO) Alliance and GlobalPlatform.

Did you know?

EMVCo's dedicated security group supports the work of the Joint Hardware Attack Subgroup (JHAS), which consults on cyber-attack rating methodology and its interpretation. The JHAS group, which is a component of the European Common Criteria-based cybersecurity certification scheme (EUCC), is currently migrating to an Information Sharing Analysis Centre (ISAC) to continue to support the developing European Union (EU) cybersecurity infrastructure.

"EMVCo's commitment in addressing cybersecurity for more than 20 years has been essential to achieve payments trust as new products and ways to pay come to market. This experience has made EMVCo a valuable contributor to the work of JHAS, generously sharing vast experience and real-world insights with the group to progress our collective cybersecurity efforts.

Through this collaboration, EMVCo not only integrates the latest advancements in attack methodologies into its own framework, but also plays a crucial role in reducing the fragmentation of cybersecurity requirements across the industry."

***Sebastien Colle** Chair of JHAS*

How does EMVCo deliver security?

EMVCo produces specifications that are available royalty-free and used by all EMV stakeholders to facilitate consistent and secure technical interaction between the payment device and acceptance terminal.

EMVCo Security Evaluations are a suite of industry requirements and tests that build on this market knowledge. Evaluations are performed by a network of EMVCo recognised laboratories. They confirm that a payment product or solution has been assessed against the EMVCo security evaluation methodology.

Where applicable, EMVCo evaluation methodology includes mechanisms and protections to reach **a 'High' level of resistance** to 'withstand known attacks', as defined in JIL Application of Attack Potential to Smart Cards (JIL AP).

Successfully evaluated products are listed on the EMVCo website.

What products does EMVCo evaluate?

Card

900+

EMVCo evaluated

Mobile

190+

EMVCo evaluated

How does EMVCo manage the process?

Information and forms about the EMVCo approval process can be downloaded from the **Approved and Evaluated section on the EMVCo website.** Once the full evaluation process is successfully completed, a solution or product provider receives a security evaluation certificate, which is published at www.emvco.com. Through its maintenance and renewal process, EMVCo requires products to be reviewed regularly to ensure they meet the latest threats, before receiving extended certificates.

EMVCo has issued more than

2,300

cybersecurity evaluation certificates

14

independent laboratories are recognised by EMVCo to deliver testing

12 are based within the EU

The EMVCo evaluation process has received **ISO/IEC 17065** accreditation

Impartial / Quality

About EMVCo

EMV technology enables billions of card-based payments to be made **seamlessly** and **securely** worldwide.

No matter where you are in the world or what you're buying, you expect your payment card to work.

For in-store, e-commerce or remote transactions, the process needs to be familiar, convenient and **reliable.**

EMV technology helps make this possible.

EMVCo is the global technical body for the EMV payment community and offers a proven, effective forum to create, evolve and promote payment **consistency, security** and **innovation.**

Banks, merchants, technology providers and other industry stakeholders all provide expert input into EMVCo.