An Introduction to: EMVCo Approvals and Evaluations for In-Person Payments

Billions of card-based payments are made and accepted daily. Whatever you are buying, wherever you are in the world, you expect your payment to be familiar, convenient, secure and reliable.

EMV® Specifications and the related testing processes help make this possible.

This eBook explores the testing processes, collectively referred to as EMVCo Approval and Evaluations, and the role they play in enabling seamless and secure in-person payments across the globe.

Contents

What are EMVCo Approvals and Evaluations?

As a global technical body, EMVCo develops EMV Specifications, EMVCo functional requirements, and EMVCo security requirements and guidelines.

These specifications, requirements and guidelines provide a technical baseline, enabling any party to develop and deploy products and solutions that support the delivery of safe, reliable payments.

EMVCo Approvals and Evaluations collectively refer to various testing processes that confirm products meet the technical baseline for security, performance and compatibility when deployed:

- **EMVCo Functional Approvals** assess whether payment products meet EMV Specifications and requirements for performance and compatibility.
- **EMVCo Security Evaluations** assess whether payment products meet EMV Specifications, requirements and guidelines for security.

What are EMVCo Functional Requirements?

Requirements relating to a product's performance and compatibility.

What are EMVCo Security Requirements and Guidelines?

Approaches, mechanisms and protections to resist attacks.

Are EMVCo Approvals and Evaluations mandated?

No. EMVCo does not mandate the use of EMV Specifications or require that products or solutions conform with the EMV Specifications. However, other entities may require conformance.

For definitions of all terms used within this eBook, view the Glossary section.

What are the Benefits of EMVCo Approvals and Evaluations?

Reliability and Global Interoperability

EMVCo Approvals and Evaluations verify that payment products and solutions meet EMV Specifications for security, performance and compatibility when deployed, so they can work anywhere in the world.

Trust

EMVCo Approvals and Evaluations promote trust, confidence and transparency across the payments ecosystem, providing publicly available listings of products and providers. This is supported by EMVCo Marks, which are easy-to-recognise symbols at the point-of-payment providing consistency and familiarity to the payment experience and inspiring consumer confidence during the checkout process.

Efficiency

EMVCo Approvals and Evaluations generate significant efficiencies, as they enable payments systems to use the same fundamental testing processes. This supports the accelerated deployment of products into marketplaces across the world.

An Accredited ISO/IEC 17065 Certification Body

EMVCo has received ISO/IEC 17065 accreditation for its security evaluation processes. This recognises the value and quality of EMVCo security product evaluations in enabling the deployment of safe and secure payment solutions.

What Payment Products Do EMVCo Approvals and Evaluations Support?

EMV Technologies are the suite of payment technologies that EMV Specifications support.

Various EMVCo Approval and Evaluation testing processes have been defined for specific payment product categories.

For in-person payments, these are:

- **EMV acceptance devices**
- **EMV Chip cards**
- **Mobile payment form factors**

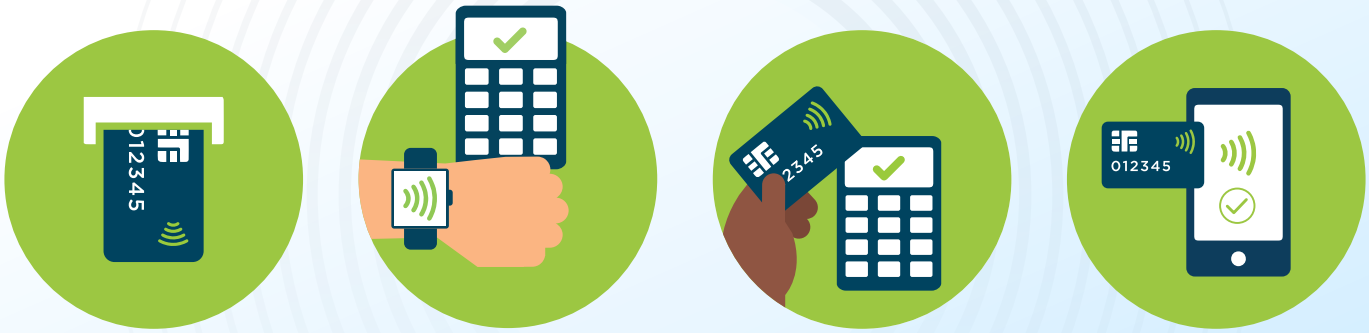
Before exploring the different processes for EMV acceptance devices, EMV chip cards and mobile payment form factors, it is firstly important to understand the concepts of EMV Level 1 and EMV Level 2.

What is EMV Level 1?

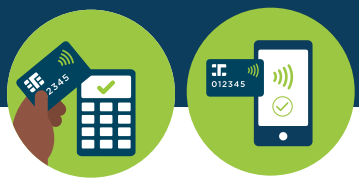
EMV Level 1 (L1) refers to the communication protocols that enable the exchange of data between the payment instrument and acceptance device. This includes the mechanical, electrical and radio frequency (RF) interfaces.

What is EMV Level 2?

EMV Level 2 (L2) refers to the software component, commonly known as the 'kernel' or 'payment application', that resides on an acceptance device or card and mobile respectively. This software contains the set of functions that provide the processing logic along with necessary data to perform an EMV contact or contactless transaction.



EMV Acceptance Devices



EMV acceptance devices are products that enable merchants to accept EMV contact or contactless payments. These include traditional Point of Sale (POS) terminals and also TapToMobile devices, which enable merchants to accept contactless payments directly using near field communication (NFC)-enabled devices, such as smartphones, without the need for an additional connected device, dongle or attachment.

EMVCo Functional Approvals

EMV L1 Testing

EMV L1 testing assesses the compliance of the acceptance device with the communication protocols defined within the EMV Chip and Contactless Specifications. These cover the transfer of data between the acceptance device and the payment instrument (such as chip cards, smartphones, and smartwatches).

The specific components of the payment acceptance device assessed during L1 testing are the Interface Module (IFM) for contact and the Proximity Coupling Device (PCD) for contactless:

Interface Module (IFM)
The component of a chip reader that supports the protocol communication with the consumer's EMV Chip card to enable an EMV contact transaction.

Proximity Coupling Device (PCD)
The component of a contactless reader that supports the protocol communication with the consumer's payment instrument to enable an EMV contactless transaction.

Reduced Range Approvals

EMV L1 includes tests to confirm how close the payment instrument needs to be to the acceptance device to enable the successful exchange of payment data for a contactless transaction. To support emerging payment acceptance form factors such as TapToMobile, EMVCo has published a dedicated Reduced Range approval process.

EMV L2 Testing

EMV L2 testing assesses the compliance of the acceptance device with the software features defined within the EMV Chip and Contactless Specifications.

EMVCo has defined the Contact Kernel **approval process** for contact.

The combination of EMVCo Functional Approvals for EMV acceptance devices is known as **Terminal Type Approval.**

EMV Acceptance Devices

For contactless transactions, EMVCo has launched an **approval process** for the new EMV Contactless Kernel (EMV Contactless Specifications for Payment Systems: Book C-8 – Kernel 8 Specification) which was published in 2022 to support the evolution of contactless and mobile payments and simplify global acceptance.

EMV Contactless Kernel Testing

The EMV Contactless Kernel addresses industry demand for a contactless kernel that can be used by all stakeholders globally. Over time, this can help reduce the number of contactless kernels that stakeholders need to support and maintain – creating opportunities for merchants, solution providers and payment systems to reduce costs and improve time to market. It can be used with the existing terminal infrastructure, can co-exist with existing contactless kernels, and has a flexible split architecture that supports physical or cloud implementations. It also brings advanced security features, including Secure Channel, Blinded Diffie-Hellman (BDH), and Elliptic Curve Cryptography (ECC).

To ease the transition for stakeholders deploying the new EMV Contactless Kernel, the approval process supports two approaches. The EMV Contactless Kernel can be tested as a full contactless acceptance device, which reflects the approach currently used for other available contactless kernels. Additionally, EMVCo has introduced standalone testing of the EMV Contactless Kernel itself to support different deployment options for products in the field that are already approved.

Importantly, the EMV Contactless Kernel Specification is flexible to support different implementation options. For example, the EMV Contactless Kernel supports a split architecture that allows processing and functions to be performed in different locations. However, the EMVCo approval process does not change regardless of whether this functionality is implemented.

Family of Products

To increase efficiency, EMVCo has also defined the concept of a ‘Family of Products’. This allows multiple contactless acceptance products from the same manufacturer to be grouped under the same ‘family’ if they share identical hardware and communication configurations. A product ‘family’ may include different L1-approved PCDs and L2-approved software packages. If an PCD or software package has already been tested and approved within a family, it can be used in other family members without requiring additional testing.

EMV Chip Cards

EMV Chip cards are payment cards embedded with a secure chip containing applications that enable consumers to make EMV contact or contactless payments.

EMVCo Functional Approvals

EMV L1 Testing

EMV L1 testing assesses whether a card product sufficiently conforms to the protocols defined within the EMV® Common Core Definition (CCD) Specification and EMV® Common Payment Application (CPA) Specifications – which form part of the EMV Chip Specifications.

EMV L2 Testing

EMV L2 testing assesses whether a card application sufficiently conforms to the EMV CCD and EMV CPA Specifications.

The combination of EMVCo Functional Approvals and Security Evaluations for EMV Chip card products is known as **Card Type Approval.**

EMVCo Security Evaluations

EMVCo Security Evaluations assess the security of the chip and platform (the combination of chip and operating system [OS]) used in EMV Chip card products.

Biometric on Card

As adoption of biometric payments cards increases, there is growing industry consensus around the benefits that could be realised by promoting increased consistency and alignment across the performance and testing requirements.

EMVCo launched its Biometric on Card initiative to help balance convenience and security, while addressing the unique considerations for biometric payment cards.

As part of this initiative, dedicated security requirements have been defined and incorporated into the chip security guidelines and evaluation process.

EMVCo has also defined performance requirements for the fingerprint sensors on biometric payment cards and is developing a dedicated supporting performance testing approval process.

Mobile Payment Form Factors

NFC-enabled mobile devices such as smartphones, tablets and smartwatches – as well as other form factors such as rings and bands – can be used to perform EMV contactless transactions in-store.

EMVCo Functional Approvals

EMV L1 Testing

EMVCo has defined dedicated L1 testing processes to promote a good consumer experience when NFC-enabled smartphones and wearables are used to make contactless payments.

EMV L2 Testing

EMVCo has developed specific L2 testing processes for the selection of payment applications within the Proximity Payment System Environment (PPSE) on consumer mobile devices.

EMVCo Security Evaluations

EMVCo Security Evaluations assess the security of the chip and platform used in mobile payment form factors.

In addition, the continued growth of mobile payments has increased the number of solutions deployed that use software applications to enable consumers to pay in-store. As these Software-Based Mobile Payment (SBMP) solutions operate in the more vulnerable consumer device environment, mobile wallet providers use a layered security approach comprising various software and device components to combat threats.

To support this layered security approach while ensuring flexibility and efficiencies, EMVCo introduced a dedicated Security Evaluation Process for SBMP. This includes Software Development Kits (SDK), Trusted Execution Environments (TEE), White Box Cryptography (WBC), Multi-Factor Authentication (MFA) solutions, Consumer Device Cardholder Verification Methods (CDCVM) such as biometrics / authenticators, Attestation mechanisms, and Software Protection Tools (SPT). Full mobile payment applications comprising various individual components can also be evaluated.

The combination of EMVCo Functional Approvals and Security Evaluations for mobile payment products is known as **Mobile Type Approval.**

How do EMVCo Approvals and Evaluations Work?

EMVCo is responsible for defining the various product approval and evaluation processes, but it does not perform any testing 'in-house'. This activity is delivered by specialist independent, recognised testing laboratories using qualified test tools.

To support this activity, EMVCo acts as a trusted authority. This gives product and solution providers confidence when engaging third parties to test their products:

Laboratories

EMVCo develops and administers processes for independent laboratories.

Functional Test Tools and Platforms

EMVCo develops and administers qualification processes for test tools and platforms to validate that they can test in accordance with EMVCo functional requirements. Test tool vendors may use the 'EMVCo Qualified Mark' in connection with tools that have been qualified by EMVCo.

Auditors

EMVCo develops and administers qualification processes for laboratory auditors.

All qualified tools and recognised laboratories are listed on the EMVCo website.

EMV Level 3 Testing

In addition to functional approvals and security evaluations, EMVCo also supports EMV Level 3 (L3) testing.

EMV L3 testing aims to validate the integration of an EMV acceptance device with its acceptance infrastructure to help ensure the interoperability of an end-to-end EMV transaction.

Unlike EMV L1 and L2 testing, the L3 test plans are provided by the Participant Systems. This term refers to payment systems and other entities that elect to use the EMV L3 Testing Framework and qualified L3 test tools.

While EMV L3 testing is defined by each Participant System's policies, EMVCo supports this by defining a set of standardised L3 test tool technical components – the EMV L3 Testing Framework – and a streamlined qualification process for L3 test tools.

Find out more

EMVCo Approval and Evaluation Processes

Functional Approvals

1. EMVCo develops a functional test plan that outlines the test strategy and objectives.
2. The product or solution provider engages a recognised laboratory and/or service provider to test the product or solution with a qualified test tool.
3. The recognised laboratory and/or service provider tests the product and provides a report to EMVCo.
4. EMVCo reviews the report and – if the requirements have been met – issues a Letter of Approval to the product provider confirming the product as meeting EMV Specifications for performance and compatibility.
5. The 'EMVCo Approved Mark' may be used in connection with products or solutions that have been approved by EMVCo.

Security Evaluations

1. EMVCo develops security requirements, guidelines and evaluation methodologies.
2. EMVCo audits and recognises laboratories as following the EMVCo process to deliver security evaluation services.
3. The product / solution provider engages a recognised laboratory, which tests the product and creates a security evaluation report.
4. EMVCo reviews the report and – if the evaluation requirements have been met – issues an evaluation certificate or security certificate to the product provider.
5. An 'EMVCo Evaluated Mark' is available specifically for use by product providers in connection with SBMP solutions or components.

It should be noted that the above represents a simplified process flow.
For complete details of all respective processes, visit the EMVCo website.

Renewals

As all approved and evaluated products have an expiry date, EMVCo has defined renewal processes, when relevant, to ensure that products are not outdated and meet the latest requirements for performance, interoperability and security.

What about Registered Identifiers?

In addition to Approvals and Evaluations, EMVCo also issues identifiers (IDs) to designated payment systems and providers. The types of identifiers and respective registration processes **are detailed on the EMVCo website.**

How is EMVCo Advancing Approvals and Evaluations?

- EMV Specifications have an important role to play in providing a common and flexible foundation for the delivery of new payment methods and options.
- Advancing the supporting testing processes and infrastructure in parallel with these specification developments helps enable consistent, convenient and secure payment experiences worldwide.
- This is why EMVCo works closely with EMVCo Associates, Subscribers and industry partners to streamline, enhance and optimise Approval and Evaluation activities as specifications evolve and potential efficiencies are identified.
- Broad industry engagement also promotes approval and evaluation processes that are agile and reactive to address new payment methods.

Click here to learn more about how you can get involved. →

Glossary

Card Type Approval	The combination of EMVCo Functional Approvals and Security Evaluations for EMV Chip card products.
EMV Level 1	EMV Level 1 refers to the communication protocols that enable the exchange of data between the payment instrument and acceptance device. This includes the mechanical, electrical and radio frequency (RF) interfaces.
EMV Level 2	EMV Level 2 refers to the software component, commonly known as the 'kernel' or 'payment application', that resides on an acceptance device or card and mobile respectively. This software contains the set of functions that provide the processing logic along with necessary data to perform an EMV contact or contactless transaction.
EMV Level 3	EMV Level 3 testing aims to validate the integration of an EMV acceptance device with its acceptance infrastructure to help ensure the interoperability of an end-to-end EMV transaction.
Interface Module (IFM)	The component of a chip reader that supports the protocol communication with the consumer's EMV payment card to enable an EMV contact transaction.
Mobile Type Approval	The combination of EMVCo Functional Approvals and Security Evaluations for mobile payment products.
Proximity Coupling Device (PCD)	The component of a contactless reader that supports the protocol communication with the consumer's payment instrument.
Software-Based Mobile Payments (SBMP)	Mobile payment solutions that use software applications to enable consumers to pay in-store
Terminal Type Approval	The combination of EMVCo Functional Approvals for EMV acceptance devices.

About EMVCo

EMVCo creates and manages EMV Specifications and programmes that enable seamless and secure card-based payments for businesses and consumers worldwide.

EMV Specifications support technologies including EMV Contact Chip, EMV Contactless Chip, EMV Mobile, EMV QR Codes, EMV Secure Remote Commerce (EMV SRC), EMV 3-D Secure (EMV 3DS) and EMV Payment Tokenisation and are widely used by the payments industry to develop products and services that deliver trusted and convenient in-store, online and remote card-based payments.

As a global technical body, EMVCo is collectively owned by American Express, Discover, JCB, Mastercard, UnionPay and Visa. Hundreds of payments stakeholders, including merchants, banks and technology providers, participate as EMVCo Associates and Subscribers to develop, evolve and enhance flexible EMV Specifications that support innovation and address marketplace needs. All EMV Specifications are available royalty free on the EMVCo website.

Connect with EMVCo

www.emvco.com | EMV® Insights | LinkedIn | Quick Resources