EMV Certification

EMV Certification Services Team

For a FREE consultation with EMV experts and how to propel your company into the future, click the link below.

https://www.omniintegrate.com/contact-us/

OMNI INTEGRATION

U.S merchants are increasingly implementing the EMV Smart Card standard in their consumer card-present payment environments. EMV technology is gaining adoption amongst U.S. merchants since a card industry mandated liability shift for general retailers took place in October of 2015. Card issuers, acquirers, banks, and merchants are investing heavily in modifying and upgrading their payment technology infrastructures to keep up with the evolving standards and technologies involved with EMV payment processing. While large merchants extensively plan this transition towards secure payment processing guidelines, many other merchants are reliant on industry service providers to facilitate and manage the regulatory compliance involved with this transition. Omni Integration provides EMV compliance and certification (L3) solutions that are cost effective and mitigate unknowns and bottlenecks from a typical EMV merchant transition cycle. By leveraging the expertise and efficiency of Omni Integration's managed solutions, merchants and payment service providers can keep up with the evolving landscape of smarter and more secure payment transaction processing.

TERMS USED IN THIS DOCUMENT

EMV: EMV stands for Europay, MasterCard, Visa. "EMV" is a global standard term used for chip-based Debit and Credit Card transactions.

It is a joint effort between Europay, MasterCard and Visa to ensure security and global acceptance of consumer payment cards.

EMVCo: EMVCo, LLC is a technical body that facilitates the worldwide interoperability and acceptance of secure payment transactions by standardizing EMV processing specifications as well as related testing processes. For more information please visit: https://www.emvco.com

EMV Level 3 Certification: EMV L3 certification is related to the software application running on a device and its connection to the acquirer. During this certification process, specific test script must be successfully completed for each EMV card brand to receive Level 3 certification compliance approval (LOA) from each brand.

Acquirer: An acquirer is an organization licensed as a member of major card brand networks as an affiliated bank or is part of a bank/processor alliance in the business of processing transactions for businesses (acceptors) and acquiring new merchants.

US Common AID & Global AID: U.S. Common and Global AIDs represent a standard for debit-based payment card transactions. Common AID is to ensure Regulation II compliance and can be utilized by all ATM acquirers and merchants, allowing transactions to be routed to a network available on the card. Global AID is for international use.

MSR Card: A magnetic stripe card, also called "swipe card" or "magstripe card", is a type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on the card's magnetic band. The stripe works by the payment terminal reading data when a magnetic strip is swiped past a reading head.

Chip & PIN Card: EMV cards are also called chip cards as they have a small microprocessor built in. Data on the chip can be accessed interactively, and requires specific responses from a card terminal to reveal the information available on the card. Once the terminal has read financial and identity data, the card is considered "Chip & PIN". This process of inputting a PIN at the time of chip read is also known as two-factor authentication.

Hardware security module (HSM): This is a specialized hardware computing device that safeguards and manages digital cryptographic keys and provides the encryption and decryption of cryptographically managed data.

Merchant Identification Number (MID): The MID is generated by a processor or acquirer. Each MID is specific to each individual merchant location. MID number helps identifying the merchant during processing of daily transactions, rejections, adjustments, chargebacks, end-of-month processing fees, and more.

Payment Account Number (PAN): This number is an identifier for an account held at a financial institution. The most common usage of a PAN is a credit card number. The PAN does not include other potential identifying information such as CVV or cardholder name.

Point of Sale (POS): A software application that manages inventory, pricing, and other elements of a retail transaction. The POS typically initiates a payment transaction involving card reader and terminal hardware.

Point of Interaction (POI): POI is a (hardware and/or software) component in point of sale equipment (e.g. a magnetic card reader) that enables a consumer to use a credit card to make and complete a payment transaction. The POI terminal may be attended or unattended.

INTENDED AUDIENCE

This technical document is prepared for the merchants and system implementers looking for the best-practice and approach for EMV L3 Certification.

INTRODUCTION

The U.S. is the largest and most structured market to adopt chip technology with no central body guiding or mandating the migration compared to other countries. This, coupled with the vast number of card issuers, acquirers, payment processors, gateway operators and numerous regional debit networks, makes introducing EMV contact and contactless technologies to the U.S. extremely complex and difficult to coordinate. This is especially true for the acceptance (merchant/acquirer) side of the migration and, adding to the complexity, this segment has thousands of value-added resellers (VARs), independent sales organizations (ISOs) and independent software vendors (ISVs) that deal with payment acceptance in the U.S.

While the fraud liability shift has passed for the retail segment, there are many small and medium-sized merchants, VARs, ISOs and ISVs that are only starting to learn about EMV Certification and implementation project plans. This white paper aims to help the community understand the EMV L3 certification process along with its complexities.

This document offers advice on technology development costs containment by understanding which functional and security standards are stipulated by the secure chip payment industry.

An appreciation of the certification process will result in shorter time to market and ensure no unforeseen delays are incurred during the final stages. Brand certification is the last step of an acquirer's EMV migration and POI development process. EMV brand certification consists of three key stages: Test Preparation (scoping and preparation), Test Execution and Test Validation. The assumption that certification is a massive and costly undertaking should be challenged with the following:

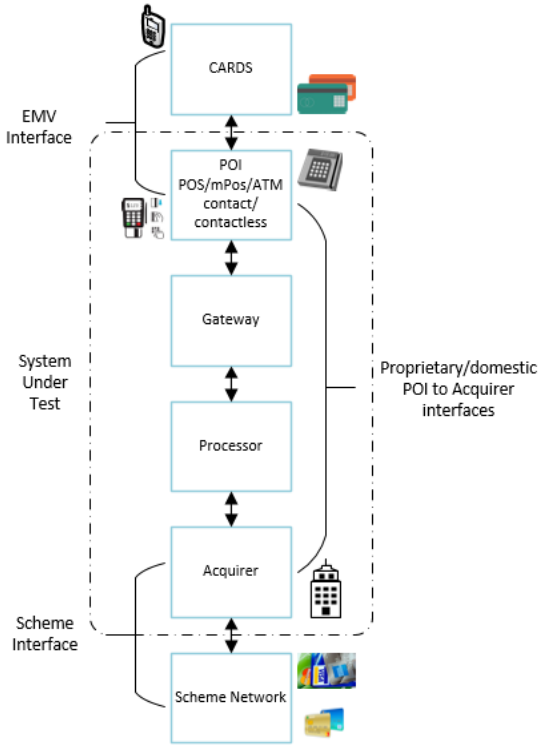
- What is EMV?

- EMV certification levels.

- EMV certification road blocks

We will elaborate on the above points and conclude this document with a concise assessment on process improvements by leveraging a systematic certification effort. A typical picture of the System Under Test – POI implementation below, including the adjacent interfaces:

Figure 1: General EMV Certification frame work



WHAT IS EMV?

Due to incremental growth in card payment fraud, major credit card companies have implemented a new set of security standards called EMV; this includes cards that store user information on a chip rather than a magnetic strip, as well as integration of cryptographic components into the payment transaction flow. EMV is an abbreviation for Europay, MasterCard, Visa. It is the global standard for chip-based card transactions.

Visa, MasterCard, American Express, Discover, and others have mandated that issuers and merchants that do not support chip technology will be held liable for counterfeit fraud. The process to support chip technology is referred to as “EMV Certification”. There are different levels of EMV Certification.

POIs use card acceptance devices that ship from manufacturers with EMVCo Level 1 card readers and one or more Level 2 certified kernels. A processor or acquirer must develop the POI Level 3 application, qualify the system, and perform Level 3 acquirer integration end-to end testing to receive certification required prior to operational acceptance in merchant environments.

EMV CERTIFICATION LEVELS

EMV Level 1 certification ensures the device (also: terminal) meets the lower level voltage and communication protocol requirements. Essentially, it certifies the hardware requirement of a terminal device.

EMV Level 2 certification focuses on the validation of the software that implements the payment functionality running on the Level 1-certified device. This software is called as payment kernel.

EMV Level 3 certification, or brand certification, ensures that the configuration of software on the devices, POI, or other infrastructure meets the brand processing requirements. In the case, multiple payment brands are to be supported, all respective Level 3 certifications must be performed.

EMV CERTIFICATION ROADBLOCKS

The top five biggest obstacles likely preventing merchants from becoming fully EMV-compliant are:

Costs - The price of switching over to new hardware can be huge for larger businesses who may have hundreds of locations across the nation. To reduce costs, enterprises should re-examine their business operations to identify whether they can streamline their processes, or if they already have chip-enabled devices and may only need new software. In such cases, it is more efficient to invest in software development to upgrade existing systems to meet the specific needs of the business.

Incomplete Certification - POS terminals and software are updated before the deadline by the merchants but they may still be unable to accept EMV card payments due to pending certification from issuing banks/brands and payment processors. Due to this a backlog of requests, retailers trying to get the certified do not have the sufficient resources to handle the growing number of cases in an organized manner. This has caused many merchants to seek other alternatives and hold off on purchasing new EMV terminals until they achieve the certification.

Untrained Store Staff - Every new piece of equipment implemented into a business operation requires training for the staff members, to learn how to easily operate the new hardware and handle any situations concerning these new technologies. Depending on the size of the business, merchants may not have the manpower or resources to provide training to every employee. In most of these cases, it is often preferred to bring in experts who understand the equipment to educate staff on proper use.

Concerns with Transaction Speed - As merchants become EMV-compliant, consumers are growing accustomed to using Chip and PIN payment methods. A large concern for the speed of transactions remain for retailers and customers alike. EMV smart cards must be "dipped" into the POS terminal rather than swiped and must remain in the slot for data to transfer properly and allow for a unique transaction code to be generated. Though this process is more secure than traditional methods, it can take anywhere from a few seconds to a full minute depending on the

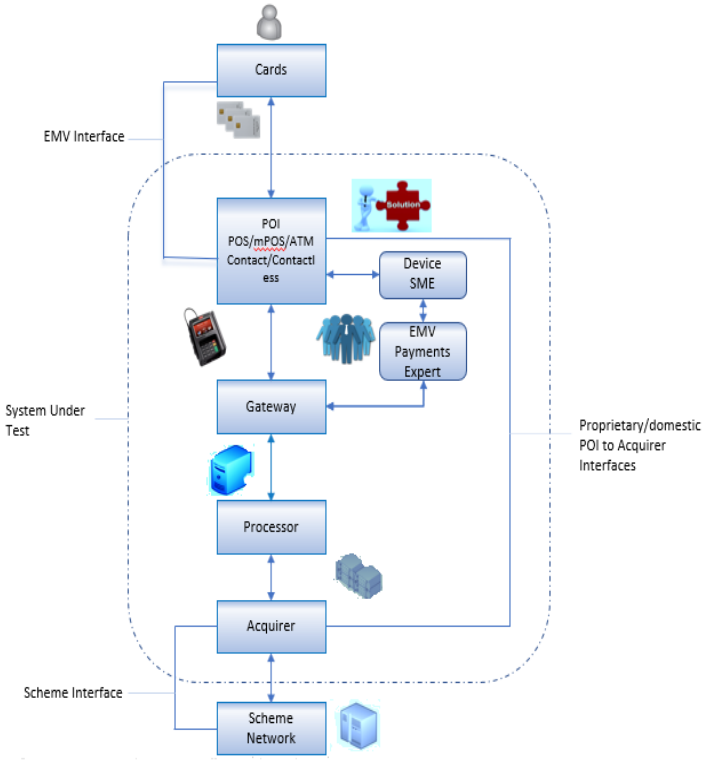
vendor's software, which can lead to an increase in customer complaints and ultimately result in a lesser capacity for transaction processing. To remedy this situation, the card brands have identified new technology options such as Quick Chip and Contactless EMV features to processors who can then offer these streamlined processing flows to merchants.

Indifference to Liability Risks - Merchants who have yet to become EMV-compliant face the risk of being held liable for fraudulent transactions that occur as a result of a swiped EMV smart card transaction. Many small businesses believe they have a low risk of fraud due to the low number of transactions they process; therefore, the cost of upgrading entire systems outweighs the risk of possible fraud. Most large chain stores have already implemented EMV POS systems to deter fraud. Individuals seeking to perform fraudulent transactions have moved on to targeting small businesses and merchants who have not adopted EMV.

OMNI DRIVEN EMV CERTIFICATION

EMV Level 3 Certification would need resources such as testing tools, device experts, payment domain, and EMV knowledge to roll out a production-ready implementation within a single iteration. This white paper offers insight on how technological development and certification costs can be contained by understanding the functional and security standards stipulated by the secure chip payment industry.

Figure 2: Omni Driven EMV Certification frame work



Subject Matter Experts (SME) support for EMV and device configurations during the certification process result in a shorter time to market, and ensures no unforeseen delays are incurred during the final stages of product development.

It has been observed from several years of experience that the EMV certification period becomes stretched with issues pertaining to devices and lack of EMV knowledge as quality assurance teams are performing certification test executions. Though AID preference configuration is performed in coordination with merchant requirements. Omni Integration provides expertise on U.S. specific requirements and U.S. Common Debit AID support for major card brand schemes.

Omni Integration leverages its continuously improving areas of expertise to deliver on shorter certification cycles. The success metrics of the “one and done” approach is greatly increased by dry run and pre-cert test cycles which are performed prior to the final brand certification cycle.

Figure 3: Pre-Cert

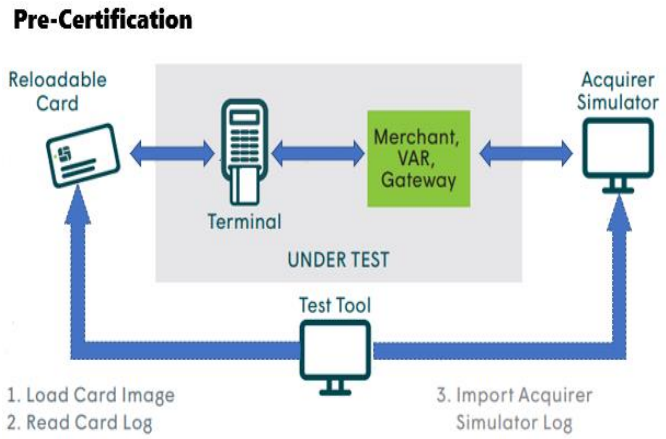
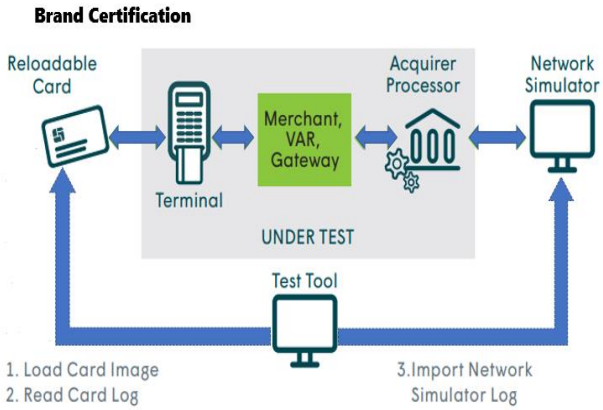
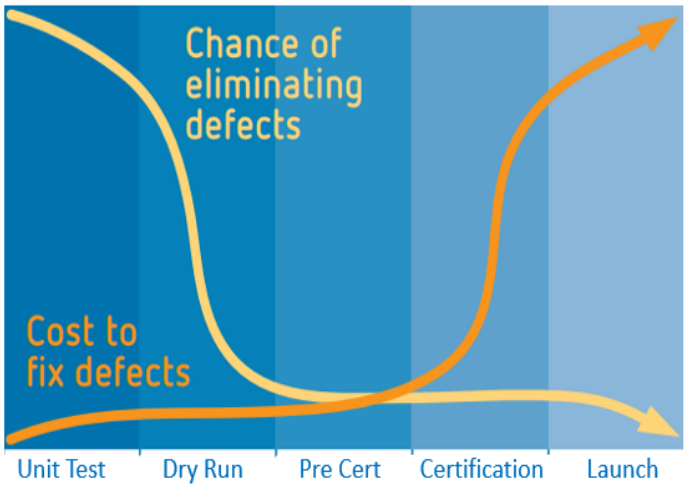


Figure 4: Brand Certification



Omni adds even greater value to the certification stream by providing state of the art infrastructure and resources to roll out production-ready EMV certified terminals to the market within 3 months including quick chip, EMV Contact, and EMV Contactless transaction set support. By identifying and correcting all the environment, terminal application and acquirer issues during the dry run and pre-cert scenarios, Omni Integration can significantly streamline and reduce costs associated with a typical certification effort.

Figure 5: Defect Fix Cost



Exception testing is performed by well-trained technical EMV staff at Omni. Exception testing relies on knowledge and expertise to create negative tests. It also requires a testing platform with two key features. Firstly, the platform must be able to deploy rapidly and to manage the expected volume of test cases in a scalable fashion. Secondly, the platform should replicate the payment chain so that test cases can be run in various environmental configurations.

Omni can also provide training to the store/operating staff in handling EMV transactions, settlements, and chargebacks etc. This training would help merchants to remain EMV capable post certification and better utilize the EMV payment transaction system.

FINAL WORDS

Migrating to and remaining compliant with the EMV standard can seem like a daunting process, although it doesn't need to be if an efficient and streamlined approach is taken. There are opportunities to optimize the process without compromising quality. All solutions referenced in this document contribute to reducing efforts and costs in an EMV migration scenario. However, to successfully reduce the expected costs and workload, a mix of solutions is recommended.

For the U.S. market, the biggest challenges are coping with the complexity of the market and the lack of standardization.

While lowering the amount of test cases or complexity of a testing effort may not be a feasible approach, a broader perspective which involves the optimal sequencing of certification events,

along with a comprehensive testing strategy can greatly improve challenging certification efforts.

Omni Integration offers a balanced solution which can lower costs, reduce certification cycles, and greatly improve time to market, with a strategic approach to leverage the best of people, processes, and planning.

ABOUT US

Omni Integration is a solution provider specializing in payment applications and payment platforms for the Retail, Specialty Retail, Hospitality, Petroleum, and Insurance Industries. We have provided innovative enterprise payment solutions to Fortune 100 organizations around the world. Let our team of experts provide solutions for you.

Omni Integration has a dedicated team of engineers and technical support resources available to strategically deliver projects large and small. Our team of seasoned IT and project experts have thousands of hours of combined service delivery expertise. We lower the rework and gap burden by leveraging industry-standard engagement models and real-life validated implementation and design patterns.

Omni Integration solutions are deployed in several countries. Solutions provided for our clients have reached out to many end-users. This level of market saturation allows Omni Integration to be a true partner for mobile enablement without all the guesswork of technology or industry trends. We support a productivity-driven SDLC approach. From project start to delivery, we ensure maximum transparency and velocity with our fully integrated project support model.

We help our customers accomplish their business targets by reducing exposure to areas outside of their core competence.

By this approach our customers may pursue innovation in their business procedures, functions, and technology of value-adds. We are specialized in diverse technologies & domains like Custom Software Development, QA & Software Testing Solutions, Mobile App Development, B2B Applications, B2C Applications, Web Design & Development Services, Enterprise Business Solutions, eCommerce Solutions and Next-Gen Payment Technology Solutions for our partners and customers.

Omni Integration is driven by its client satisfaction, transparency, work excellence, reliable and on time delivery, passion for new technology, and flexibility in our approaches. Omni believes strongly in a R&D investment strategy, designed to enable and improve modern-day payment solutions worldwide.