



# FAQs for Developers



## What is the difference between being “EMV ready” and “EMV capable”?

When a merchant is using a device that has been through Level 1 and 2 certifications, it is *EMV ready*. Once that device and the payment applications and systems that it is connected to have completed a Level 3 certification, the POS solution becomes *EMV capable*.

## What are the three levels of EMV certification?

There are three levels of EMV certification that a solution must undergo before it can be deployed. Level 1 and Level 2 certifications pertain to the terminal device and are the responsibility of the point of entry device manufacturer. The POS developer must then undergo a Level 3 certification for the complete solution.

**Level 1 certification** addresses the mechanical and electrical protocols used for transferring data between the terminal and the payment card.

**Level 2 certification** is the device manufacturer's responsibility, which addresses the software application residing inside the device (firmware) that performs EMV processing. Once the manufacturer has achieved both Level 1 and Level 2 certification, a POS developer can then use the certified device to create an EMV solution for its POS system.

**Level 3 certification**, also called network certification, tests each unique EMV path to the networks. The testing flow is as follows: Level 1 and 2 certified device, the POS application, any middleware or gateway in use, the processor, and finally out to the card brands. Each card brand has a set of defined EMV test cases that must be run to satisfy their EMV certification requirements.

In addition, each processor may have their own test cases that they want POS developers to run as part of their host message certification. This process must be completed individually for each device the POS is using.

## What are the requirements for a Level 3 certification?

Each unique transaction path has to be certified to each network individually, and if any part of the path changes, a new certification is needed. Examples of changes requiring a new certification include: the terminal/point of entry devices, the processor/merchant acquirer, and any middleware or gateway that is involved.

**Example** - A POS provider wants to certify with two different devices and currently works with four different processors:

- At a minimum of 2 terminals x 4 processors x 4 card brands = A total of 32 card brand certifications will be needed
- Each card brand certification could have around 200 test cases. In addition to any cases specific to the processor's own host message certification requirements.

### When would a direct integration to EMV be most suitable?

This option enables the greatest degree of customization, allowing developers to choose which device you want to take through certification and how you want to configure terminal transaction flows. The drawbacks include having the longest time to market and the highest degree of complexity. It also comes with a high cost, both from development and QA resource time, as well as the purchase of the necessary test cards, kits, and tools needed to complete the certifications. We anticipate that many tier 1 retailers will look to complete direct EMV certifications to support their unique POS environments and in store business process flows.

### What is a "semi-integrated" approach?

In this case, the POS is integrated to the payment application, but is removed from most of the EMV transaction flow and the complicated integration and interaction between the EMV device and chip card. In an EMV out of scope solution the transaction process flow is simplified for the POS developer. The POS initiates the transaction request and passes the purchase amount and other basic information such as the merchant credentials, to a payment application running on the POS. That payment application then communicates with the EMV device, which actually handles the transaction, then returns the necessary information back to the POS for printing an EMV compliant receipt, and for reporting purposes.

### What are the advantages of a semi-integrated approach?

There are many benefits to the EMV out of scope solution for POS developers. Most importantly, it puts the burden of the Level 3 certification on the payment application provider. It is up to the EMV out of scope solution provider to take each device through certification with the various processors and networks. It will also speed up the time to market for POS providers, as integrating to the EMV out of scope solution is similar to the payment integration process they are familiar with. It is also cost effective for the POS developer because the cost of EMV device integration is taken on by the EMV out of scope solution provider. However, minor tradeoffs include lack of customization in terms of the EMV devices available and a limited amount of terminal screen flows that come with EMV.

### How does this solution compare to a stand-alone solution?

Stand-alone terminal EMV solutions are already on the market today because they are the simplest to deliver, both from a functionality and certification standpoint. The transaction path from the terminal application to the processor is shortened, which reduces the complexity of the Level 3 certification. This simplicity, however, comes with a loss of business functionality. Without integrated payments, transaction reconciliation becomes challenging, as payments capabilities are removed from the POS. Merchants may also be taking a step back from an overall security perspective if they choose an EMV capable terminal that is not capable of end-to-end encryption. Where they may benefit from the card authentication that EMV provides, they lose the benefit of protecting data in flight.

### **Are others going to market with stand-alone terminals?**

In Canada, at first many developers offered stand-alone EMV terminals. They later came back to offer an integrated solution, because stand-alone wasn't meeting their needs. The feedback we heard from merchants was that they were dissatisfied with the stand-alone terminals because the payment process was not integrated to the rest of their business and caused a lot of extra work.

### **As a developer, would we have any liability if our product does not support EMV by October 1, 2015?**

In Canada, at first many developers offered stand-alone EMV terminals. They later came back to offer an integrated solution, because stand-alone wasn't meeting their needs. The feedback we heard from merchants was that they were dissatisfied with the stand-alone terminals because the payment process was not integrated to the rest of their business and caused a lot of extra work.

### **Is EMV compatible with preauthorization? For example in hospitality, you have to preauthorize at check in and you capture at check out.**

Per the EMV standards today, no, the concept of preauthorization does not exist in an EMV implementation. Each transaction is a one-time event, driven by the cryptographic validation that occurs between the chip and the terminal. EMV will impact the way that certain verticals, like lodging and restaurants, handle their transaction processing and interactions with cardholders. We will cover this in much more detail in future communications.

### **I already have E2E encryption, do I have to implement EMV?**

There is no mandate to implement EMV, but EMV is an important part of a card security solution. Coupling EMV with E2E encryption can provide a merchant with the benefits of both the liability shift that EMV brings, along with PCI scope reduction when using E2E encryption. EMV will add another level of security with card authentication, protecting against counterfeit card fraud. Think of it this way: E2E encryption protects the card data once a transaction is initiated, EMV makes sure that the card initiating the transaction is valid.

*EMV and EMVCo are registered or unregistered marks belonging to one or more unaffiliated third parties that do not endorse or sponsor Mercury Payment Systems, LLC.*