MagTek EMV Common Kernel a Faster Path to EMV L3 Certification

DEVELOPER GUIDE: Learn how common kernels and thoughtful discovery, build better applications faster.

Initial Considerations

Understand the difference between a typical EMV L3 certification process compared to one using a common kernel.

Secondary Considerations

Determine the best EMV L3 certification strategy and discovery questions to reduce costs, expedite approvals, and get your payment solution deployed.

CONTACT US

Where hardware and services meet.

MAGTEK®

INITIAL CONSIDERATIONS

A Typical EMV L3 Certification Experience

The EMV L3 certification process evaluates and confirms that an EMV-compliant payment acceptance device and its payment application work together properly to deliver a reliable end-to-end transaction process with the merchant and bank payment systems. This testing helps to ensure that a new (or upgraded) payment acceptance device meets the requirements of the individual payment systems before deployment. This test and certification process is managed by the payment processors and/or financial institutions that a merchant selects for payment processing. An L3 certification is required for each new (or modified) payment device that a merchant selects, and requires a complex sequence of paperwork, scheduling, testing, analysis, test reports, and if needed, remediation and retest before achieving an L3 certification. Typically, this process takes 6 to 8 months to complete. Therefore, if a merchant desires to support multiple payment devices (e.g., countertop terminal, kiosk reader, and mobile reader), this process becomes redundant, lengthy, and expensive.

A Better Way... EMV Common Kernel

To simplify and expedite the EMV L3 certification process it is recommended to select payment devices that share an EMV Common Kernel. A payment kernel is a set of software functions that manage data exchanges between an EMV chip/ NFC contactless payment card and a payment acceptance device in reference to verification, authentication, and encryption requirements. When multiple payment acceptance devices share the same payment kernel, it can be stated that they have a “common kernel” and communicate in the same manner. The primary advantage of this strategy is that once a device using a common kernel is L3 certified, then all the other devices using that common kernel are also certified. Using this strategy provides merchants with flexibility to add different types of payment devices and functionality to their solution platform without incurring the additional time and costs to certify each individual device.

Initial Decisions

Planning the L3 Certification Strategy

Time to market matters. The faster that payment device(s) and applications are EMV L3 certified, the faster that revenue generation starts. With that in mind, it's imperative to start with an initial planning and scoping phase to evaluate both short and long-term objectives.

The following are critical discovery questions that merchants and payment application developers/ISVs need to consider upfront when creating their roadmap for EMV L3 certifications:

1. WHAT TYPES OF PAYMENT USE-CASES AND ENVIRONMENTS SHOULD I CONSIDER?

Understanding use-cases and payment environments is critical as it will substantially impact the types of payment functionality and capabilities your payment solution provides initially and into the future.

Related discovery questions must consider where and how the payment transactions will occur, and under what environments:

- Will the payment solution occur at a counter, kiosk, mobile device, online, or all the above?
- Do you anticipate transactions only happening at a central location?
- Will you offer table-side, line-busting, or curb-side mobile solutions?
- Do you envision stand-alone, unattended, or semi-attended kiosks for faster check-out?
- Will there be a need for eCommerce and online transactions?
- Where and how will customers interact with the software?

2. WHAT ABOUT POS APPLICATION SOFTWARE AND OS?

Selection of the POS software application, its OS platform, and integration model are also important considerations.

Further discovery questions should answer the following questions:

- What POS software application will be used?
- What operating system(s) will the POS Host use?
- Will the Payment Application be "integrated" or "semi-integrated"?
- Can the Payment Application be leveraged across multiple payment devices and use-cases?

SECONDARY CONSIDERATIONS

Vendor Selection for Hardware and Payment Services

After determining the overall scope and objectives of your EMV L3 payment platform, the next step is to make specific determinations of the hardware and payment service vendors you will need to partner with to achieve those objectives.

3. WHAT PAYMENT METHODS AND BRANDS SHOULD I SUPPORT?

It is important to ask what types of payment methods and payment brands you want to accept and then select payment gateways and processors that can accommodate them. It is recommended to select payment devices that support a full range of payment methods (e.g. MSR, EMV Chip, EMV NFC, QR Codes, PIN). Doing so ensures maximum flexibility to accommodate various payment methods both now and into the future.

The supported EMV payment brands are VISA, MasterCard, Amex, Discover, CUP, JCB, and Interac. Depending on your targeted operational region(s) you may need to support all of them or just a subset.

- Related discovery questions should include:
    - What card brands will you accept?
    - Will you accept gift cards or store branded cards?
    - Do you need to accept HSA, FSA, or IAAP payments?
    - Do you want to accept mobile wallets like Apple Pay or Google Pay in-app, in-web, or in-person?
    - Do you want to support payment loyalty programs such as Apple VAS or Google SmartTap?
    - Will you offer an eCommerce component?
    - Will you want to send a QR Code for invoicing or read from digital wallets for couponing?
    - Do you need to offer subscriptions, rewards, or loyalty?
    - Do you need to accept debit cards?
    - Do you want to accept PIN?
    - Do you need to accept signatures?
    - Are signatures required for returns?
    - Do tax or tip calculations need to be accommodated?
    - What information do you need when processing returns or chargebacks?
    - How do most customers pay today and how may that change?

4. HOW TO SELECT THE RIGHT PAYMENT PROCESSOR(S)?

Not all processors are built the same and their services can vary significantly in terms of costs, performance, and scope. Be certain to select a processor that handles the types of transactions you want to accept in the environment where your application will be used. For example, there are regulations and requirements that must be met in petrol that vary from hospitality, and not all processors can handle contactless and touch free payments. It is important to understand these differences and to align your payment solution requirements with a processor that meets your specific needs.

When selecting a processor, it is important to ask the following questions:

- What industries and payment types do they typically work with? (e.g. Retail, Food Service, Lodging, Petrol, Medical…)
- What is their chargeback policy?
- Do they allow tip and tax options?
- Can they support contactless transactions?
- What is the transaction flow?
- What is the cost per transaction?
- What additional service fees will a user have?
- How quickly do they fund merchant accounts?

5. HOW TO SELECT THE RIGHT PAYMENT GATEWAY(S)?

Although optional, a Payment Gateway can provide a merchant with many more options to connect with various processors, gain access to specific transaction types, provide the flexibility to use multiple processors, and have the capabilities to provide feature-rich services that are custom-tailored to a merchant's needs.

When selecting a gateway, it is important to ask the following questions:

- Is it an established and trusted company?
- Does it provide access to numerous payment processors and transaction types?
- Are their data decryption services PCI-DSS and PCI P2PE validated?
- Do they support TDES, AES-128, and AES-256 decryption?
- Do they provide simplified developer integration resources?
- What are their fees?
- Do they provide an omni-channel solution (in-person, online, and in-app)?

6. HOW TO SELECT THE RIGHT PAYMENT DEVICE HARDWARE VENDOR?

It is recommended to select payment devices that support a full range of payment methods (e.g. MSR, Chip, NFC Contactless, QR Codes, PIN, Signature, Manual Entry) and share an EMV common kernel. In doing so, it ensures that you have options to expand support for multiple payment methods as needed and will be able to expedite L3 certification timelines and reduce costs.

This strategic model is typically implemented via a “family” of payment devices that share the same microcontroller, firmware, command set, and EMV payment kernels. By selecting a payment device family that shares an EMV common kernel platform, developers will gain a significant advantage in that once an L3 certification is successfully completed for one member of the product family, then all other products within that family are also included as L3 certified.

Therefore, it is beneficial to select hardware payment devices from a single vendor that provides the range of devices and functionality needed. If you select devices from multiple hardware vendors, you will not gain the benefit of a common kernel since they will not be in the same family, and you will need to certify each product type individually.

CONCLUSION

Minimizing time-to-market for EMV L3 certifications requires a plan and trusted partners. MagTek and Magensa have a complete solution of integrated hardware, services, and support to simplify and expedite the EMV L3 certification process.

MagTek Dyna Devices are PCI PTS 6.x rated and share a Common EMV Kernel. This platform ensures simplified L3 certifications and allows flexibility to mix and match devices and payment methods in your payment solution as needed.

Magensa Cloud Services are EMV certified with leading payment processors including FIS (WorldPay), Fiserv (First Data), TSYS, Heartland, NAB (EPX), Elavon, and Chase. Magensa's Payment Gateway, Unigate, and Tokenization Services are an extensive set of web services used by integrators and software developers to secure point-of-sale (POS) systems and other sensitive data in mobile, eCommerce, and traditional brick-and-mortar settings. Magensa gateway services provide ISVs/developers with a PCI-DSS certified environment for securely processing payment transactions. Retail, restaurant, fuel, gift/loyalty cards, and healthcare FSA/HSA/IIAS application certifications are supported by some or all processors.

One integration with Magensa provides tremendous flexibility to ISVs, VARs, ISOs, and system integrators in terms of product solutions and processor options. The L3 certifications include Quick Chip technology, which improves transaction speed and reduces complexity. Magensa's Decrypt and Forward service allows our clients to hit any processor or gateway's front end without PCI data exposure, limiting PCI scope and economizing the development of a client certified solution.

Partner with MagTek and Magensa today and let us show you how making use of an "EMV Common Kernel" provides a better and faster way to attain EMV L3 certifications, add flexibility to expand and enhance your payment solutions, and ensure maximum data protection for your customers and your business.

About MagTek

Founded in 1972, MagTek is a leading manufacturer of electronic systems for the reliable issuance, reading, transmission, and security of cards, barcodes, checks, PINs, and identification documents. Leading with innovation and engineering excellence, MagTek is known for quality and dependability. Our hardware products include secure card reader/authenticators, Qwantum secure cards, token generators; EMV Contact Chip, EMV Contactless, barcode and NFC reading devices; encrypting check scanners, PIN pads, and credential personalization systems. These products all connect to Magensa, a MagTek owned gateway that offers businesses the ability to securely process transactions using authentication, encryption, tokenization, and non-static data.

MagTek is headquartered in Seal Beach, CA, please visit www.magtek.com to learn more or contact us at www.magtek.com/contactus.