Heartland

Understand your software vendors'/POS developers' EMV strategy to build your own

Your clients view you as a reliable industry consultant. Now more than ever, with the launch of EMV in the U.S., they will be looking to you for guidance. However, you may be facing a great deal of uncertainty—particularly when you are not in control of the development roadmap for the products you sell.

We've provided some questions and topics that you can pose to your software vendor to help you understand their EMV strategy and begin to form your own, as well as the background you need to put the topics in context.

Are you planning on supporting EMV? If no, what is the rationale? Do your customers typically operate in a lower fraud environment?

Make sure your ISV understands that fraud will eventually migrate to the weakest point—merchants who only support magstripe. Even if the liability impact is minimal, many merchants will want to upgrade in order to ensure they have the latest security technology. Lastly, ensure that the ISV is not reacting to any EMV myths. If the decision to not support is final, consider how to adapt your marketing strategies around security, such as emphasizing encryption and tokenization for your clients' security needs.

Are you going to develop a full EMV integration and certify that interface directly with the card brands? What are the timelines for EMV card brand certification with your most used processors?

Many acquirers are already establishing EMV certification queues, and the card brand testing itself has inherent lead times. Additionally, many ISVs are not aware of the increased complexity around chip card development and certifications or the hard costs involved.

Are you investigating out-of-scope options to accelerate EMV availability? Is the out-of-scope solution middleware-based or peripheral-based?

In general, peripheral-based out-of-scope solutions may have certain constraints for multilane environments if they lack a centralized server component—such as tips needing to be edited on the originating device/workstation. Make sure you understand these use cases and how they impact you and your customers.

RSPA

Heartland

What devices are you planning on supporting? Are they networked peripherals, or USB/serial?

Different out-of-scope offerings may opt to manage devices from a centralized server or have them connected directly to a workstation.

What changes are needed for your current installation and/or support workflows to accommodate your selected EMV solution? How does this solution handle EMV parameter downloads?

EMV parameters include things such as Certificate Authority Public Keys, which should get pushed to the device when updates are available. The parameter management approach may require the VAR to deal with a terminal management system (TMS), but ideally the POS developer will be able to build in parameter download support as part of the EMV transaction workflow. Heartland supports this approach and incorporates parameter updates directly into our EMV APIs.

Are you considering all of the different customer environments that may be relevant, such as counter service, kiosk, tablet, etc.? Are you going to support multiple kernel configurations (either as part of a fully integrated or out-of-scope solution) to account for these environments? What about "selectable kernels" so the supported CVMs may be edited on the fly to support "QPS – no signature required?"

A device's "kernel configuration" refers to the capabilities that device has enabled or disabled, mostly due to the merchant environment. When software is certified for EMV (either an ISV's direct solution or a third party's out-of-scope solution), it is required to be certified for each specific configuration that will be employed. For instance, if a restaurant does not want Pay-at-the-Table, they can select a configuration which disables Online PIN and Offline PIN (note that in this scenario they would still be susceptible to liability for lost/stolen fraud with MasterCard, American Express and Discover).

What is your Pay-at-the-Table strategy (if applicable)? Have you surveyed major clients/users on Pay-at-the-Table?

There are multiple Pay-at-the-Table options—kiosk at the table, purpose-built mobile devices, phone/tablet sleds, etc.—each with varying costs and implementation considerations. Table service merchants may also opt to continue the bill presenter model by selecting a solution with a "no PIN" configuration.

What is your roadmap for EMV solutions with all currently supported processors? Are there differences between implementations for each processor (e.g., some full integrations, some out of scope)? Do any of the processors or out-of-scope solutions impose arbitrary limitations on EMV functionality (e.g., not allowing PIN bypass or not supporting kernel configurations with chip and signature)? How does that impact your merchant training and support tasks?

All U.S. acquirers are mandated to support EMV on their processing hosts, but the time and costs involved in full integration and certification can be daunting for an ISV. Additionally, some processors have announced their own policies in terms of certain EMV functionality that they are choosing to limit, which may impact your merchants.

RSPA