

## EMV Implementation for Issuers: 7 Decisions You Must Make Before Issuing Your First Chip Card

---

*Even if your organization has been issuing magnetic stripe cards for years, you realize the switch to issuing chip cards (sometimes referred to as EMV cards, ICCs [integrated circuit cards], or smart cards) is much more complicated than simply adding a microchip to your card design specs and choosing a chip card manufacturer to produce the plastics. You realize the move to chip cards will ultimately affect every aspect of your institution, from your branch operations to your payments batch processing. Even so, as a card issuer, focusing first on chip card issuance can be a logical starting point in planning your EMV implementation. This article addresses seven key decisions your organization must make before issuing its first chip card.*

### **1) How will the inclusion of a chip change the graphic design of the card? Where does our logo appear? How do we preserve our brand?**

It's likely that your organization has spent considerable time and devoted resources to developing your unique brand; that is, the "look and feel" of your magnetic stripe cards. Because regulations specify the exact placement of the microchip on your chip cards, you may find you cannot re-use the design of your magnetic stripe cards without relocating graphics or text that will otherwise be displaced by the chip.

Note that in addition to the chip, you will also typically include a magnetic stripe on your new chip cards to enable your cardholders to use their cards at devices that are not chip enabled.

### **2) Which applications will we include on the chip?**

As part of planning your card personalization, in addition to making decisions about the manufacturing of the plastics (embossing, magnetic stripe encoding, and so forth), you must also make decisions about the applications contained on the card's chip. Chip cards can contain multiple applications. For the purposes of our discussion, let's focus on the financial and payments applications on your cards.

Some card applications are associated with a card associations' scheme (such as MasterCard, VISA, American Express). Other applications are associated with financial networks and switches. For your chip cards to be used at a chip-enabled terminal by your cardholders, there must be a match between one of your card applications and one of the applications that the chip-enabled terminal supports.

You may discover that mandates from your card association, regional switch network, or even government may largely determine the applications you must have on your chip cards. If you do have options regarding the applications to include, consider the following.

- If your card issuing organization belongs to a card association (such as MasterCard, Visa, American Express, etc.) or switch network, your organization must work with representatives from those card associations or networks to determine which applications are to be included on chip cards bearing their logos. Card associations and networks typically require formal functional certifications for chip cards, as well as inter-member certifications. Choosing to include an existing, pre-certified application will enable you to get your cards into production faster.
- In addition to any required network-level applications, you may choose to develop your own ICC application. Note, however, that any new application must be based on an existing ICC application and must be certified with the appropriate association (that is, applications based on Visa standards must be certified by Visa, and applications based on MasterCard standards must be approved by MasterCard, and so forth). Achieving that certification may result in substantial delays in getting your cards into production; therefore your organization will need to carefully consider the consequences of developing and certifying a new chip application.
- Card associations have very strict regulations about how cardholder data is to be provided to chip card manufacturers and secured during the card personalization process. Your institution must conform to all of these regulations, in addition to existing [PCI DSS \(Payment Card Industry Data Security Standards\) regulations](#).

### **3) Do we use the same BINs/Prefixes for our chip cards that we used for our magnetic stripe cards, or do we use new BINs/Prefixes? What are the advantages and disadvantages?**

You already have BINs/Prefixes that you use for your mag stripe cards. Your card issuing organization must decide to either issue chip cards using those existing BINs/Prefixes or using a new (never before used) BIN/Prefix. Of course, if you use a new BIN, you must be sure to register that BIN with the appropriate network(s). The new BIN could be either an extended BIN (sharing the first 'n' digits with the existing 'short' BINs owned by the issuer) or a completely new short BIN.

There are advantages and disadvantages to each approach, and your organization should examine both options carefully. For example, using a new extended BIN can enable you to establish host parameters for chip card authorization by BIN, if desired. Similarly, if transaction routing is based on BIN, you can use the extended BIN to identify and route chip transactions to a different endpoint than magnetic stripe transactions. You can also use BINs to distinguish cards by product, service, function, and so forth. Even if

you choose to use your existing BINs to issue your new chip cards, you could still choose to use new PANs for chip cards.

#### **4) How will we handle PIN issuance? Do we automatically issue new PINs?**

In addition to issuing new cards, your organization may also need to reissue PINs. If your institution wishes to allow cardholders to use the PIN from their magnetic stripe cards for their new chip cards, your host system must have a record of (or be able to determine) the existing clear PIN. The clear PIN is then provided to the chip card manufacturer as part of card personalization.

Unfortunately, many organizations do not have a record of the PIN. Instead, functions such as PIN verification rely on a PIN offset (which, depending on the type of card, may also be known as the PVV, or *PIN Verification Value*). The PIN offset can be stored on the magnetic stripe card. Conversely, the chip card has the encrypted PIN stored on the chip. Storing the encrypted PIN within the chip facilitates certain PIN-related functions for chip cards (for example, offline PIN verification at a chip-enabled POS device). Consequently, the track 2 data in the magnetic stripe on a chip card does not contain a PIN offset. (In fact, the Track 2 data within the chip is referred to as the “Track 2 equivalent” [Tag 57] and is slightly different than the Track 2 on a magnetic stripe card.)

#### **5) Will we support the PIN change function on our chip cards?**

You can optionally allow your chip cards to perform a PIN change at chip-enabled ATMs. Alternatively, you might choose to offer PIN changes exclusively at your branch offices via a device in the branch that could send a PIN change script to the chip card. Note, however, that if you choose to support PIN changes at the ATM or branch, your cards and your host system (or a third party, such as a network or switch) will need to contain the keys and programming to support these features.

#### **6) Will we perform the steps needed for chip card authentication, or do we need to rely on a switch, network, or other party to perform it on our behalf?**

To perform chip card authentication, your institution must have an appropriate hardware security module (HSM), as well as the appropriate chip card authentication keys and cryptograms. Chip card authentication is too complex to discuss here at length<sup>1</sup>, but involves steps such as:

- ARQC verification and ARPC generation – Verifying the authorization request cryptogram and generating the corresponding authorization response cryptogram.

---

<sup>1</sup> You can find more information on EMV processing in the Paragon publication [“Beyond Cards and Terminals: Considerations for Testing Host-to-Host EMV Processing”](#).

- TVR/CVR checks – Verifying the Terminal Verification Results (TVR) and Card Verification Results (CVR).
- Fallback checks – Verifying transactions that were processed with a chip card at chip-capable device, but which were completed using a magnetic stripe (typically because of an inability to read the chip). These transactions “fall back” to use of the magnetic stripe to complete transaction processing, and can be indicative of fraud.
- iCVV check – Checking the Card Verification Value contained on the card’s chip.
- ROC check (POS only) –Verifying the Reason Online Code (ROC). The ROC indicates the reason that a POS transaction was forced to go online for authorization rather than being authorized offline at the device, that is, without sending the transaction request to the issuer or authorizer.

If your organization is unable to perform chip card authentication, you may be able to negotiate with a network to perform authentication for you. In that case, all chip transactions destined for your institution must go through this network for authentication. Your organization must provide the appropriate keys and cryptograms to the entity that is performing chip card authentication on your behalf. Your institution would need to discuss the requirements with the network and obtain any updated specifications from the network that explain how authentication will work.

## **7) What functionality can we support for our chip cards that would still allow us to get them into the marketplace in a reasonable timeframe?**

Your organization’s EMV implementation may be regulated by card associations, network mandates, or even government legislation. If your organization can choose its own path, perhaps an ideal EMV implementation would include a chip card that conforms to EMV standards but does not allow offline PIN verification, offline authentication, offline authorization, PIN change at the ATM, or other issuer scripting. Limiting the functions and transactions supported means your cards would not need to contain the keys and programming to support those features.

### **Bonus Question: Will we choose contact or contactless cards?**

One obvious question that we did not include in our seven basic decisions is “Will we choose contact cards or contactless cards?” While this is a fundamental decision, it is also complex, closely linked to your institution’s business alliances and goals—and currently hotly debated in our industry. Basically, there are three chip card options.

- Contact cards are cards with chips that come into physical contact with the device’s chip card reader.

- Contactless cards are cards with chips that can be read by a card reader from a distance using radio frequencies.
- Hybrid cards are dual interface cards that contain both a contact chip and a contactless chip.

As with other decisions in this article, your organization's choice of chip card type may be dictated by its card association membership, network participation, or even government legislation. If not, in addition to the many other business concerns driving your decision, remember to take the following into consideration:

- Availability of devices that can use each chip card type. Determine the percentage of cardholders using your cards locally, regionally, nationally, and internationally; then assess the availability of devices that support each chip card type in each of those regions. Do ATMs support the chip cards you plan to issue? Do merchant terminals? Is your institution comfortable with chip card transactions frequently being presented as magnetic stripe transactions because of limited acceptance of your chosen chip card type by merchants or ATMs? Consider the timeframe in which your chip card type might be commonly supported, and the timeframe in which you typically reissue cards. Would it be feasible to issue one type of card initially, then replace the card with a different chip card type later
- Risk associated with newer technologies. Your organization may want to research the type(s) of chip cards in use (particularly in the geographic area in which your cardholders are currently most active) and try to gauge the success of those programs. Weigh the benefit of gains from being an early adopter of a card type against the risk of using technologies that are not proven in your marketing area.
- Varying costs associated with producing each type of chip card, and with obtaining the devices needed to test them. Card manufacturing costs are of primary importance, but remember that your test labs must also be equipped with ATMs and test terminals that can accept your chip card type.

Although EMV implementation is a complex process that affects your entire organization, you can begin planning EMV implementation by addressing these questions about chip card issuance.

## Can Paragon Help with Your EMV Implementation?

Institutions can use simulators to begin testing EMV processing long before they have EMV devices or chip cards available for testing. Paragon solutions can simulate EMV processing by your host or financial switch, and by ATMs or POS devices. We offer a virtual "soft card" to test the processing of chip cards – including blocked applications and blocked cards – before you have chip cards available for testing. Our solutions can help you build and test ATM loads. Our simulators can also generate sufficient transaction volume to enable you to test batch processing of EMV transactions. In addition, Paragon Professional Services Team offers experienced EMV professionals to provide information and guidance as you develop your EMV implementation plan.

## About Paragon Application Systems

Paragon Application Systems is a leading global provider of ePayment simulation, configuration and testing software solutions to the financial industry. More than 590 financial institutions in over 85 countries use Paragon tools to improve quality and reduce time-to-market. Paragon's broad customer base includes major

interchanges, merchant acquirers, processors, leading software providers, banks and credit unions. Visit Paragon Application Systems at [www.paragonedge.com](http://www.paragonedge.com) or email [info@paragonedge.com](mailto:info@paragonedge.com).

## About the Author

Deborah Spidle, a Senior Business Analyst with Paragon Application Systems, has over 20 years experience in the IT industry, focusing on banking and financial applications. Most recently, Deborah has been working as a business analyst responsible for helping a major national switch, a large bank, and multiple credit unions migrate to EMV. She has worn many hats including: development, business analysis, design engineering, program management, software implementation/installation management, project management, development management, technical writing, software installation, user testing, and client training. Deborah's managerial responsibilities have included the management of personnel across multiple disciplines (engineering, development, testing) as well as management of large, multi-functional project teams. Past clients have included financial institutions in the US, Canada, Brazil, Australia, and England.