

## Choosing an EMV Chip Card

The primary considerations involved in selecting an EMV compliant card are:

- Platform (card operating system)
- Chip Memory Size
- Data Authentication Method

**Platform:** Like any computer, chip cards require an operating system before it can load and use software applications. Applications designed for use in chip cards are written in a particular software language and each application requires an operating system, or “platform”, that understands the application’s language.

There are currently 3 major types of chip card platforms: Proprietary, GlobalPlatform and Multos.

Proprietary chip card platforms are available from individual suppliers, along with applications that are designed specifically for that platform. The platform may be a proprietary operating system that functions on industry standard chips or may be a completely proprietary chip and operating system combination. Typically, applications written for a proprietary platform cannot be used in any other platform or card manufactured by another supplier.

The primary advantage of proprietary platforms is that depending on the vendor and application, they can be less expensive than open environments such as GlobalPlatform or Multos. The primary disadvantages are lack of interoperability and dependency on a single supplier for cards and applications.

Proprietary platforms are best suited to situations characterized by highly focused or special purpose business applications in closed environments, with little or no need for application interoperability; where lowest possible cost is a high priority; and where the issuer is comfortable locking into a long-term relationship with one supplier.

GlobalPlatform is an open card platform that uses JavaCard programming language for application development. GlobalPlatform is the most commonly-used open platform in the world, although most GlobalPlatform applications are used in cellular phone SIM cards rather than debit or credit cards. As this card platform uses a common programming language (Java), applications and development expertise are abundant and readily available.

While GlobalPlatform cards can be more expensive than proprietary environments, they offer issuers the flexibility to choose from numerous card and application suppliers that support GlobalPlatform standards. It should be noted however, that the current lack of official interoperability certification programs to enforce GlobalPlatform compatibility means there is no guarantee that a GlobalPlatform application developed by one supplier will function on all GlobalPlatform cards.

Chip cards that use GlobalPlatform are best suited to issuers that need or desire the ability to change card suppliers with relatively little risk. GlobalPlatform also offers potential opportunities for cost

savings as a competitive bid process for application development would have access to a much wider market than would be possible with proprietary platform cards.

Multos is the other major open card platform and like GlobalPlatform, offers the advantages of open standards and a competitive market environment for the acquisition of cards and applications. Multos also offers the additional benefit of guaranteed interoperability of applications for all Multos cards, due to a strict interoperability certification process that any new Multos application must go through before it may be loaded to any card. Multos also offers a high level of security separating applications so that one application cannot affect/modify/corrupt another Multos application on the same card.

While a full function Multos environment can be more expensive than either proprietary or GlobalPlatform, it is well matched to issuers that require guaranteed application interoperability and the highest level of security along with an open market environment for development and vendor selection. Multos also offers an entry-level product (Multos Step One) without RSA functionality at a reduced cost that is comparable with proprietary platforms.

MasterCard International holds a stake in the MAOSCO Consortium (which holds the rights to the Multos operating system) while Visa International has aligned with Sun Microsystems' Java Card/GlobalPlatform product. Both associations however, recognize the need for issuers to select the operating system that works best for their overall requirements. A MasterCard application will be allowed to run on the GlobalPlatform operating system, as long as there is a version of the MasterCard EMV application (called *M/Chip*<sup>TM</sup>) that is compatible with GlobalPlatform. Conversely, Visa International will work with any issuer who wishes to use the Multos system to run the Visa EMV application (called VSDC – for “Visa Smart Debit and Credit”) as long as it meets the Visa standards.

**Memory Size:** A chip card's memory, also known as EEPROM, dictates the number and complexity of applications that can be used on a single card. In general, the more complex a card's set of applications, the more memory is required. More memory is also required for advanced data authentication methods.

A very basic chip card requires at least 4K of EEPROM to enable a single payment application, although the flexibility and scalability of card applications would be severely restricted. Additional memory is currently priced at approximately \$0.30 per 4K increment, making more powerful cards affordable in most situations.

It should also be noted that the cost of card memory is continually decreasing and it is likely that lower memory costs may justify the purchase of even more powerful cards by the time chip cards are actually introduced to credit union members.

**Data Authentication Method:** The flow of data to and from a chip card is encrypted so that it cannot be intercepted or manipulated in transit by unauthorized parties. There are three methods of data authentication that can be used by parties that process chip card transactions: Static Data Authentication (SDA), Dynamic Data Authentication (DDA) and Combined Dynamic Data Authentication (CDA).

Static Data Authentication uses public key infrastructure (PKI) to verify that a chip card's contents match its digital signature. SDA will identify fake EMV cards that have invalid numbers in any of the critical EMV data elements covered by the card's digital signature. While highly unlikely, a weakness of SDA is that it cannot identify counterfeited EMV cards that have had all of the data from the original card copied to the counterfeit card, i.e., SDA will not detect a "skimmed and counterfeited" EMV card.

Like SDA, Dynamic Data Authentication will verify an EMV card's contents. DDA will also detect if the EMV card has been copied and counterfeited by forcing the card to correctly respond to a card-specific test. Chip cards that support DDA require an additional processor to be on the card and are therefore generally more expensive (by approximately \$0.70) than comparable SDA cards.

Combined Dynamic Data Authentication is the most advanced and secure type of data authentication. CDA is similar to DDA with the additional functionality of verifying the authenticity of the card's application cryptogram, which ensures that the cryptogram has not been corrupted. As CDA cards are more expensive than comparable DDA cards and provide a level of security that exceeds the requirements of most applications, few issuers have chosen to deploy CDA technology.

Interac, Visa, MasterCard and American Express require their issuers to use SDA at a minimum for EMV transactions. All payment associations require their acquirers to support DDA for terminals that will accept offline authorizations.

### **Recommendations:**

1. Selection of one of the open platforms (i.e. GlobalPlatform or Multos). The open platforms offer a greater choice of suppliers and card applications, fewer compatibility or interoperability concerns and greater scalability. Card issuers may also consider aligning their debit card platform choice with the platform used by their credit cards so that both payment cards can be easily integrated into one plastic in the future.
2. Chip cards with at least 8K memory initially. Credit unions that plan on offering more advanced or multiple card applications at or soon after the launch of their chip cards should consider issuing cards with 16K or more in order to enable the greatest flexibility and expandability.
3. SDA is currently the most common and cost effective authentication method and is recommended for initial deployment.