EMV®
Migration Forum
WHITE PAPER

AN EMV MIGRATION FORUM WHITE PAPER

Implementing EMV in the U.S.: Best Practices in Support of EMV Instant Issuance

Version 1.0

Date: October 2015

EMV Migration Forum

191 Clarksville Rd.
Princeton Junction, NJ 08550

www.emv-connection.com

About the EMV Migration Forum

The EMV Migration Forum is a cross-industry body focused on supporting the EMV implementation steps required for global and regional payment networks, issuers, processors, merchants, and consumers to help ensure a successful introduction of more secure EMV chip technology in the United States. The focus of the Forum is to address topics that require some level of industry cooperation and/or coordination to migrate successfully to EMV technology in the United States. For more information on the EMV Migration Forum, please visit http://www.emv-connection.com/emv-migration-forum/.

EMV is a trademark owned by EMVCo LLC.

The EMV Migration Forum has used best efforts to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. The EMV Migration Forum disclaims all warranties as to the accuracy, completeness or adequacy of information in this document. Comments or recommendations for edits or additions to this document should be submitted to: pin-bypass@us-emvforum.org.

EMV®
Migration Forum

Table of Contents

1 Introduction

As financial institutions continue to transition to new models of card issuance, the financial industry has developed solutions to personalize these cards in-branch. With the global adoption of EMV chip technology, chip cards are significantly more expensive, and the personalization of chip cards has become more complex. It is no longer a simple process of embossing characters on the front face of the card, printing data on the back of the card, encoding the magnetic stripe with static track 1 and track 2 data, applying tipping foil to the embossed characters and, in some cases, using a four-color printing process to apply images to the front face of the card.

Issuing an EMV chip card involves the enrichment and preparation of chip data as well as cryptographic functions utilizing a series of keys essential to the authentication, verification, and authorization capabilities enabled by EMV. In order to support this added complexity instant issuance systems must be upgraded to support the specific data requirements of the chip card, its operating system, and the applicable loaded applications.

This paper summarizes industry-recommended best practices when transitioning a financial institution's existing instant issuance solution to an EMV chip instant issuance program. Key risks and suggested risk mitigation steps are also outlined. During each of the planning, development and go live phases, the primary stakeholders and key considerations of the project are noted and expanded upon.

Additional benefits of an instant issuance solution include the in-person customer experience which enables the customer service representative to further engage the cardmember, add value-added products, as well as cross sell opportunities for revenue generation.

2 Risks and Solutions

In order to maintain a proper control environment that meets the rigor of a given financial institution's global security policies, there are additional and more robust processes, controls and procedures that must be taught and adopted by the customer service representatives working at facilities where chip cards are stored and personalized to minimize the risks associated with EMV instant issuance.

2.1 Risks

- Access to (or unauthorized use of) personalization and issuer master keys.
- Eavesdropping during the personalization process of dual interface cards if secure encryption is not utilized.
- Use of unsecured session keys to potentially expose personalization data.
- Potential interoperability issues from using multiple or varying card profiles.

2.2 Solutions

Payment networks have developed specifications, operating requirements and recommendations associated with instant issuance to mitigate these risks. Some of these specifications and requirements are below:

- The keys are to be managed in a particular way, and they shall be unique to both the BIN owner/sponsor and each financial institution.
- To avoid potential eavesdropping, per the EMV and GlobalPlatform mandate, strong encryption protocols should be used while personalizing over the faster contactless interface.
- Ensure physical and logical security.
    - Session keys are necessary to avoid personalization scripts being replayed on unauthorized card stock. (See section on key management). In addition to using a virtual private network (VPN), a secure connection between the hardware security module (HSM) and chip is recommended to ensure the desktop device is secure.
    - There should be an implementation of a set of card inventory management procedures. These inventory management procedures ultimately are designed to assure the logical and physical security of blank payment network-branded payment cards.
    - The payment networks include a series of recommendations that include, and are not limited to, the use of serial numbers, either inside the chip or printed on the card itself, which ultimately could be used during a forensic investigation to identify points of compromise.
    - Unless the card profile is strictly managed, controlled and maintained, the risk of producing cards with interoperability issues in the field is high. Even if a standard profile is used, the card validation process begins again if that profile is revised (reference section 4.3).

The core value of EMV is the security it provides. Therefore the creation, use and management of the keys, identified above, are essential to ensure the integrity of a card program. Instant issuance is a particular use case associated with the provisioning of devices that affect payments secured by EMV.

This commercial framework does not imply nor define by whom or how these keys are generated, controlled, managed, distributed, employed or otherwise used. Therefore, this document assumes that any party may be the responsible party and assumes they are able to identify: who will generate these keys; with whom these keys can be shared; and who will be the "system of record" for these keys.

3 Planning Phase

3.1 Project Team Stakeholders

Below is a list of common participants in an instant issuance EMV chip project. Not all stakeholders are applicable in every case.

- EMV chip card manufacturer
- Instant issuance hardware vendor
- Instant issuance software vendor
- Issuer
- Issuing processor
- Payment network
- Personalization bureau
- Personalization certification laboratory
- Third-party agent

It is integral to initiate an instant issuance EMV chip project kick-off meeting with the key stakeholders. There are many implementation variations with an instant issuance solution; therefore, to ensure operability, it is key to understand each stakeholder's readiness and capability to implement such a project.

3.2 Cost Considerations

Even though a magnetic stripe instant issuance solution is already live, it is still important to evaluate the solution for its EMV chip capability. Depending on the age of hardware, physical adjustments such as replacing an encoding module or updating firmware may be needed to ensure operability. In some instances, purchasing new hardware or updating software may be required. Issuers often use EMV implementations as an opportunity to evaluate their current and future instant issuance capabilities to determine if new technology (such as a new fleet of hardware and software) would better suit the organization's needs and should be implemented as part of the EMV chip conversion project.

In addition, the purchase of EMV chip ready and PCI compliant peripherals, such as external PIN pads, may be needed to support customer PIN options. For example, a PIN offset validates that a cardholder's PIN is correct without having to store the PIN itself; however, if a financial institution wishes to provide customers with the ability to change their PIN in-branch, they may need to purchase a different peripheral and related software.

A critical component to instantly issuing EMV chip cards is the card personalization software. To support EMV, software will need to be updated or migrated to the most up-to-date version, which includes critical features such as data security patches and updates, detailed reporting (including card stock management ordering and destruction), PIN capture and PIN change capabilities, as well as personalization profile compatibility. To comply with payment network security standards, a certified hardware security module is required for the high-performance symmetric and asymmetric cryptographic operations needed in EMV personalization.

EMV cards include complex operating systems and applications adhering to the payment network specification, and require the design of scripts capable of loading the essential keys, parameters and associated data. In some cases these scripts may be part of the instant issuance system vendor's library. In other cases these will require licensing use of the personalization specification and development of the personalization scripts.

EMV education courses, implementation, project management and consulting services are often available for purchase or offered by some suppliers, which may increase the cost associated with implementing an EMV instant issuance project. At a minimum, issuers should become familiar with the information available at the Smart Card Alliance and EMV Migration Forum websites.

Additional expenses to consider include peripherals needed for in-branch card testing (though some issuers may choose to utilize the personalization bureau or issuer processor for this validation), as well as any incremental expense for service and maintenance agreements.

When using an issuer processor, additional costs for transmitting data, card validation, key creation and implementation may be charged. A processor may conduct testing to ensure the EMV keys used to personalize cards can be authenticated. Typically, an instant issuance vendor will assist in printing test cards as part of a scheduled installation. Test cards with the exact same configuration as those planned to issue will need to be obtained from the card manufactuer.

3.3 Card Ordering and Inventory Monitoring

There are a number of decisions required regarding the ordering of EMV chip cards. A financial institution's chip card and central issuance vendors may offer pre-defined EMV chip personalization profiles typically specified by the payment networks to ensure compatibility and seamless integration between instant issuance and central issuance.

To instantly issue cards in branch, there must be an order and inventory maintenance of EMV chip cards. If a central issuance bureau is used for portions of the card portfolio, or for reissues, the bureau may recommend that the instant issue stock and central issuance stock be the same in order to ensure the cards are produced identically.

Cards used for instant issuance will tie to an issuer-specific transport key (KMC) which locks the chips for transport to the issuer. In addition to the keys utilized for a magnetic stripe transaction (e.g., Card Verification Value (CVV) and PIN Encryption Key), there are additional keys for EMV chip transactions (e.g., Master Derivation Key (MDK)) that support the creation of the EMV cryptogram that is authenticated in the transaction process to offer greater security. The keys will need to be loaded by the instant issuance vendor, who will need to be used to create unique EMV keys for each card. The KMC/Personalization Secret Key (PSK) used for central and instant issuance may or may not be the same. The instant issuance vendor can assist in printing test cards required for card personalization validation of instantly issued EMV chip cards.

Another requirement is to develop a process to monitor inventory supply as well as the chip expiration date(s). Chip cards can only be issued to cardholders if the card stock has a valid chip card product Letter of Approval (LOA).

Instant issuance printers can accommodate various EMV cards including pre-printed plastic (custom lithography) or white plastic. Some issuers may choose print-on-demand technology which issues a card with a custom design, but without the need for unique custom lithography cards. The design can be printed on a white EMV lithography card at the time of card personalization using retransfer or direct to card print technology.

3.4 Profile Determination

The profile that is selected to be personalized at the issuer's branch locations should be identical to the profile the issuer has defined for use at their central issuance location. Even employing the exact same profile, when any profile, system, hardware or chip card solution changes, the issuer will need to manage the change through both systems and it is recommended that card validation testing is performed. If the issuer is new to (or is concurrently working on) implementing an EMV program, it is recommended that the issuer work with their applicable payment network to select and define their profile.

3.5 Logical Security

There are several critical recommendations to help ensure risks are minimized and the likelihood of improperly personalized cards is reduced.

Recommended risk mitigation include the following:

- The set of card profile(s) and personalization data elements are fixed, well-tested in the marketplace and cannot be changed by branch personnel.
    - When a profile is changed, the new profile must be thoroughly tested before being redeployed in the instant issuance environment.
- The cards most recommended are open standard cards.
    - For ease of use, it is recommended that the same operating system and version of the chip application should be used across all environments.
- The cards are single or multi-application payment cards, including single application multi-access cards for U.S.-issued debit and prepaid products.
- Random personalization validation checks should be implemented for both quality and accuracy of the data and card personalization.

3.6 Server Updates

Issuers should reach out to their processing vendor to confirm the status of instant issue support with their preferred instant issuance vendor. Due to the lead-time necessary to enable support between the parties involved, issuers should allow several months before implementations are complete. Once a relationship and project has been initiated between the processor and instant issue vendor, further discussions can begin.

Issuers will also need to confirm that their instant issuance vendor can support the card profile chosen. (Issuers may choose a different card type than what is used by the central issuance processor.) When placing card orders/reorders, financial institutions must ensure their processor is ready to support the payment network application and cryptogram version resident and selected on the chip (e.g., VIS 1.4, VIS 1.5, M/Chip 4 Select, M/Chip Advance, AEIPS v4.2).

3.7 Processor Update (Card Management System)

The card management system (CMS) is the system used by issuers to manage card-related data. With the differences identified between magnetic stripe and EMV instant issuance, it is imperative that financial institutions make this a part of their initial evaluation process. Card management might be a back office process or managed by the issuer’s core processor and may be integrated with the issuer’s card authorization system. The CMS might connect all vendors in the card issuance process.

Issuers should validate with their existing vendors (e.g., core processor, payment processors, central issuance bureau, instant issue vendor) that this software/process will continue with instant issue of EMV or if additional development may be needed or enhanced. It is possible that support with their existing vendor may not be immediately available for EMV.

An added complexity briefly identified in this white paper is data preparation. Data preparation produces the cryptographic data and prepares EMV data necessary for personalizing the EMV chip embdedd in the card. Issuers should evaluate all of the options once the key stakeholders involved in their EMV instant issuance project are identified. Options for data preparation might include an in-house or centrally hosted solution where the HSM used to house and manage the EMV keys and perform the data preparation might reside in either a branch location or with a vendor, depending on the choice of product and support.

The management of the cryptographic processes is inherently complex and requires special consideration relative to the security of the systems and keys employed. Involve security and compliance officers and consult with the various stakeholders, including the payment networks to determine the most secure approach to addressing the management of the various cryptographic keys used during the personalization of a chip card within the branch environment. Exposure of any of these keys or the process of generating the unique keys created for each card can put the issuing organization at serious risk

Not all core and issuer processors will support all types of connections with instant issuance vendors, so it is important to engage stakeholders for both short term and possible future solutions to make the most economical decision for the financial institution.

4 Development Phase

4.1 Issuer Preparation

Issuing EMV chip cards will impact almost every area of an organization. It is critical to identify and engage critical business, marketing, and product operational areas that will be impacted and begin dialog regarding the migration to chip technology. Having the support of the organization at the on-set of the project will assist in program success. Proper planning will go a long way with a project of this magnitude. Dedicated technology resources will be needed throughout the project, and smaller organizations may consider seeking third party consultative support. Early in the project, it will become obvious that certain support areas within an organization may need additional staffing to support either the influx of cardholder inquiries or changes to current procedures (e.g., security, risk, fraud and call centers and Reg E disputes environments).

When embarking on such a large project as EMV instant issuance, a close partnership must exist between the issuer, data processor and chip card manufacturer. Utilizing these two or three external resources will better position the program for a successful launch. Only with this partnership can a comprehensive and complete list of business and technical requirements be made available, which will become the basis of the project. Requirement sessions should include all of the organization's impacted areas and external partners (where permitted). Specific requirements will depend on the organization; however, at a minimum, requirements should include resolving the following questions:

- What payment network card product is being offered?
- What cardholder base is being targeted?
- What is the reissuance strategy?
- What chip operating system will be used?
- Which payment application will be used?
- Who will be supplying the cards and chips?
- Has the payment application been certified by the payment network?
- Who will perform the chip certification?
- What are the Cardholder Verification Methods (CVMs)?
- Will the card be single or dual interface?
- Will the product be PIN or signature?
- Do cardholders select the PIN?
- What supporting products are being used that may require enhancements to work with chip transactions?
- From whom will the card and application keys be generated and received?

Throughout the project, there will be several key decision points that will need to be resolved, often requiring separate work-streams to run concurrently. These decision points will require input from internal support teams and may be better managed by departmental subject matter experts. Decision points will include the following; however, many more may exist:

- Card expiry term
- Card design
- Cardholder communication
- Internal communications and training
- External marketing plan
- Cardholder experience

To better position the program for success, a strict adherence to regularly scheduled project meetings, a clear project scope/structure, and identification of limitations are necessary. Utilizing resources from a project management office (PMO) to manage a project of this size is highly recommended.

4.2 Issuer Implementation

Prior to a full EMV product launch, steps should be taken to ensure all aspects of the EMV chip card are working as planned. It is highly recommended that issuers perform a limited pilot at selected branches. The length of the pilot is not as important as the cards included in the pilot. The pilot does not need to be lengthy; however, it should include every BIN from which chip cards are or will be issued. Specific testing scripts are recommended to capture the user's interactions and perceptions at the moment of usage.

Not only will these testing results indicate possible failure points, it will identify areas of cardholder confusion, which can be addressed in customer-facing marketing materials, internal training materials, and care center/branch scripting.

The cardholder will look to the issuer as the owner of his/her customer experience regardless of whether the issuer is at fault or not. Preparing front-line associates with updated training and communication is the best option available. As EMV is rolled out across the U.S., issuer, merchant, and cardholder confusion is certain; how the issuer owns the cardholder experience will only strengthen the relationship between cardholder and issuer.

4.3 Payment Network Certification

Certification is required to provide assurance that a chip card personalized with issuer-defined parameters will be compliant with the network's chip-related payment product requirements and best practices.

The primary certification steps include:

- Define the card design according to payment network's published card design standards.
- Obtain card design and artwork approval when existing card designs will be used for the first time using instant issuance card personalization or if a new card or form factor design will be used.
- Follow the card artwork approval process as per the payment network card design standards.
    - Prepaid cards issued through an issuer's instant issuance program may replace the cardholder name with a program name.
    - Existing (already approved) chip card or form factor designs require no additional design approval.
    - Certification is required for each EMV instant issuance card even if the profile is being used in central issuance.
- Select a chip card application (e.g., VSDC, M/Chip, AIEPS (contact, dual interface (contactless)) that can be personalized through the instant issuance platform or through the batch personalization process.
- Complete the sample card profile personalization documentation with the chip card product details.
- If supported by the brand, have the card personalization vendors and/or issuer processors submit an XML image of the test card to be verified prior to the actual test card validation.
- Submit sample test card(s) for Card Personalization Validation (CPV) certification from each of the instant issuance environments (i.e., instant issuance platform and equipment (branch) and batch issuance and platform and equipment (re-issue process)).
- Get an official CPV certification approval report from the payment network.

4.4 Key Management

In addition to the keys utilized for a magnetic stripe transaction (e.g., CVV), there are additional keys for EMV transactions (e.g., MDK) that support the creation of the EMV cryptogram that is authenticated in the transaction process to offer greater security from counterfeit fraud. For those that seek to support Offline Data Authentication there is also a unique pair of public and secret keys that must be established and signed by the payment networks certificate authority.

Instant issuance hardware vendors will require the keys to lock and unlock the chip on the card, prior to in-branch personalization of an EMV chip card registered by key custodians (issuer or delegated to issuer processor or personalization vendor).

Key management requirements include the following:

- Use the payment network provided tools to request Issuer Public Key (IPK) certificates from the brand certificate authority if an offline capable card profile is required.
- Generate set of issuer master keys to personalize onto the cards.
- Perform end-to-end testing.
- Use live card (form factor) artwork, with live keys and live data as part of the live environment testing.
- Enable end-to-end key and lifecycle management.
- Refer to the payment network's guides and references for more details.

5 Go Live Phase

5.1 Key Exchange/Key Ceremony

In addition to the logical security recommendations listed above, proper key management and related processes are needed to ensure the security of the personalization process over the chip interface. In particular, care must be taken to prevent eavesdropping on the communication between the card and the device. The following minimum requirements are necessary:

- All keys and key management systems should be host-based. The HSMs should be housed at the issuer back office facility and managed according to industry practices. For more details, refer to the payment network risk management documentation found in section 7.
- All communication between the desktop personalization device and the issuer host systems must be secured by either a dedicated circuit or IPSEC tunnel.
- Ensure card personalization data is transmitted over secure protocol between the data preparation system and each chip card.
- The host-based data preparation system also houses the EMV Master Derivation Keys for that particular issuer BIN and is able to derive the Unique Derived Keys (UDK) from the primary account number of the card that is to be personalized.
- These keys, together with the chip data elements, are sent encrypted directly to the card, under the secure channel established with the initial Issuer Master Key.

Work with the processor, card manufacturer and instant issuance vendor to identify the appropriate secure protocol to be employed.

5.2 Implementation (Hardware, Software and Configuration)

Issuers must complete applicable physical hardware (e.g., printer and peripherals) and software installation. Some updates may apply to the physical hardware itself, and some may be executed remotely, such as firmware updates. In some cases there may be need for a field services technician (may be an internal IT resource or hired third-party). Install an HSM if being maintained onsite with the financial institution.

Please note: an HSM is required to support instant issuance, but onsite HSM installation is not necessary if using a centrally hosted solution, or if keys are managed by a service provider (e.g., data enrichment service provider or personalization provider).

5.3 Card Validation

It is recommended to perform card validation on all cards produced in the branch. If this is not possible, the best practice is to implement regular random personalization validation checks. These should implemented at high volume branches, or systematic personalization validation checks should be performed from time to time on all cards. Branches with lower card volumes may find that sending test cards in from the branches to a centralized location is more effective for managing time and expense.

A Personalization Validation Tool (PVT) tests the card prior to releasing the product to the cardholder. The PVT should check the following:

- Chip personalization elements are correct. All PVTs must be configured to the EMV profile being issued.
- A known PAN should be used to check the magnetic stripe content as well as CVV2.

- The card must be capable of conducting a transaction successfully.

Several personalization validation tools are available inline as part of the instant issuance hardware, or as standalone/handheld tools. The PVT can also be leveraged as a customer service tool. Depending on the PVT chosen, additional costs may be incurred, and equipment/software may need to be installed within the branch, central location, processor, payment network, or qualified personalization facility.

5.4 Consumer Education and Employee Training

There are some best practices for educating customers when EMV chip cards begin to be instantly issued in-branch. These include adding education about EMV to the company website, displaying educational signage in branch, or including information in the card fulfillment carrier or inset. Email campaigns are also effective modes of communication in order to let cardholders know why their cards have a chip.

It is also important to inform and educate managers, personal bankers, tellers and customer service representatives so that they are prepared to answer questions from cardholders. They should be able to explain to cardholders what EMV is, and why cards now contain a chip. Internal training sessions can be helpful, and a frequently-asked-questions reference sheet should also be available to managers, personal bankers, and tellers.

An instant issuance vendor can assist in providing staff with detailed training on how to personalize an EMV instant issue chip card, and how the process differs from the personalization of magnetic stripe cards. It is recommended that all procedures be documented and field tested prior to deployment.

5.5 Processes and Maintenance

Instant issuance solutions require regular maintenance and upkeep to ensure quality output and maximize optimization. There are not incremental hardware maintenance procedures related to EMV chip card production specifically, beyond the manufacturer’s current cleaning and servicing guidelines. Most instant issuance solution providers have included, or make available for an additional cost, an annual maintenance agreement that typically covers hardware maintenance and necessary software updates to ensure the instant issuance solution is current.

In an instant issuance environment, there should be a plan to monitor inventory supply and the chip “end of life” process. EMV chip card products are evaluated and approved by the payment networks. A product is typically approved for three years. The issuer can ask their card manufacturer and the payment networks about the validity of any of their chip card products. Chip cards do not stop working when the approval expires; however, it is a date that must be tracked in order to comply with payment network policies to restrict the procurement and issuance of unapproved chip products.

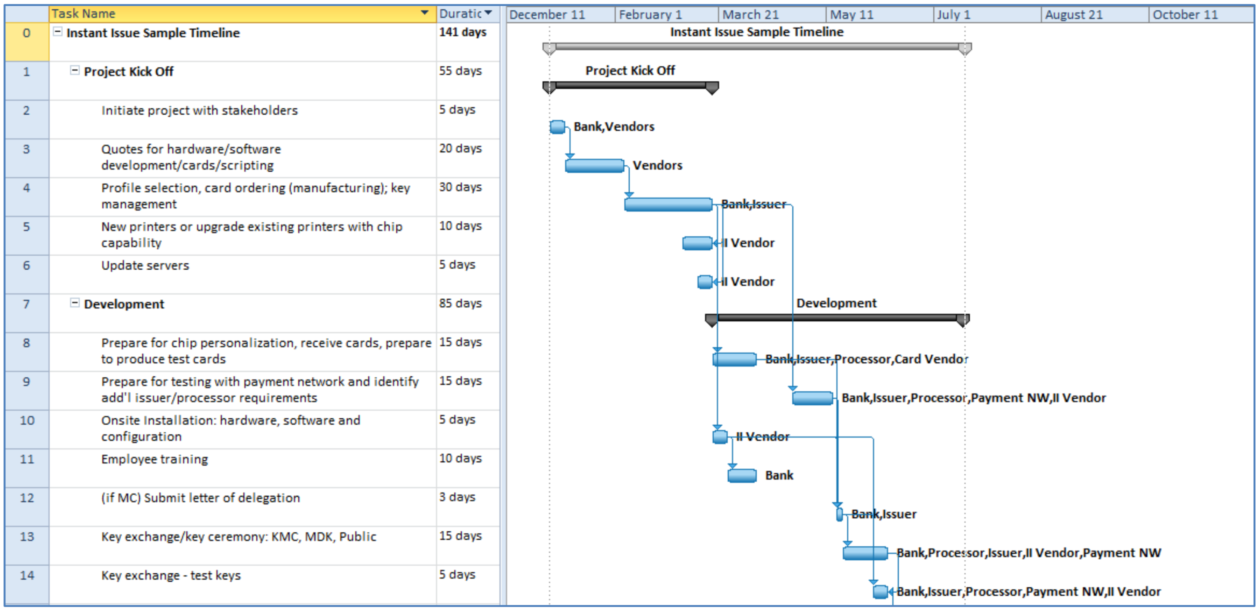
Card personalization bureaus may provide assistance for managing chip expiration dates due to using the same stock in central issuance, or as part of the procurement process. These procedures can be done with internal resources as well, but it is important that issuers manage cardholder reissuance cycles to keep track of chip expiration dates.

6 Conclusion

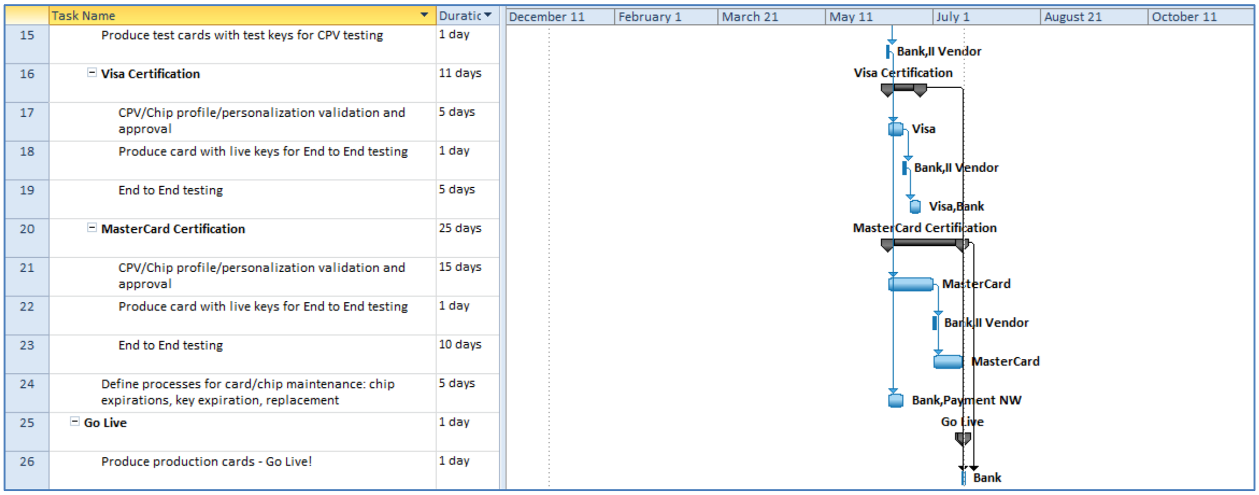
The transition of an existing instant issuance program to an EMV-enabled instant issuance program is complex. There are risks to mitigate specific to data preparation, migration of data, and the industry-mandated security requirements. Financial institutions must also implement organizational changes in handling card stock, as well as training customer service representatives and other branch-level employees on the best practices of EMV chip migration. This paper has focused on summarizing best practices, as well as providing a detailed look at the process of changing to an EMV instant issuance program. In order to further ensure program success, working with trusted vendor partners can alleviate some of the transition difficulty. Ultimately, in following the best practices and implementation steps listed here, financial institutions can successfully develop an EMV capable instant issuance program.

7 References

7.1 Sample timeline


December 11
February 1
March 21
May 11
July 1
August 21
October 11
Instant Issue Sample Timeline
Project Kick Off
Bank,Vendors
Vendors
Bank,Issuer
II Vendor
II Vendor
Development
Bank,Issuer,Processor,Card Vendor
Bank,Issuer,Processor,Payment NW,II Vendor
II Vendor
Bank
Bank,Issuer
Bank,Processor,Issuer,II Vendor,Payment NW
Bank,Issuer,Processor,Payment NW,II Vendor

	Task Name	Duratic
0	Instant Issue Sample Timeline	141 days
1	Project Kick Off	55 days
2	Initiate project with stakeholders	5 days
3	Quotes for hardware/software development/cards/scripting	20 days
4	Profile selection, card ordering (manufacturing); key management	30 days
5	New printers or upgrade existing printers with chip capability	10 days
6	Update servers	5 days
7	Development	85 days
8	Prepare for chip personalization, receive cards, prepare to produce test cards	15 days
9	Prepare for testing with payment network and identify add'l issuer/processor requirements	15 days
10	Onsite Installation: hardware, software and configuration	5 days
11	Employee training	10 days
12	(if MC) Submit letter of delegation	3 days
13	Key exchange/key ceremony: KMC, MDK, Public	15 days
14	Key exchange - test keys	5 days



	Task Name	Duratic
15	Produce test cards with test keys for CPV testing	1 day
16	Visa Certification	11 days
17	CPV/Chip profile/personalization validation and approval	5 days
18	Produce card with live keys for End to End testing	1 day
19	End to End testing	5 days
20	MasterCard Certification	25 days
21	CPV/Chip profile/personalization validation and approval	15 days
22	Produce card with live keys for End to End testing	1 day
23	End to End testing	10 days
24	Define processes for card/chip maintenance: chip expirations, key expiration, replacement	5 days
25	Go Live	1 day
26	Produce production cards - Go Live!	1 day

7.2 References

- EMVCo: EMV Card Personalization Specification
- EMV Migration Forum: Standardization of Terminology
- Visa Global Instant Card Personalization Issuance Security Standards: explains the instant issuance program and issuer responsibilities and provides a baseline of due care for any issuer contemplating the personalization and instant issuance of Visa card products at a branch, remote branch or third-party locations. To access, please log into www.visaonline.com and search by the document name.
- Visa Product Brand Standards: provides brand standards for Visa cards and other payment devices, use of marks and names, personalization specifications, service logos and marks downloads. To access, please log into www.visaonline.com and on the home page, click on the "Marketing" tab, then click on "Product Brand Standards"
- MasterCard Security Guidelines for Instant Card Issuance and Instant Card Personalization. To access, please log into www.MasterCardConnect.com, the Library Publications section.
- American Express Personalization requirements and guidelines: GNSweb can be accessed at https://network.americanexpress.com/en/globalnetwork/gnsweb/
- American Express Guidelines for instant Card Issuance: provided upon request. Please contact the American Express Account Manager for all EMV issuing documents.

7.3 Out of Scope Definition

This paper assumes the financial institution has an existing instant issuance system installed and operational as well as the related application processing and account management integrations.

8 Publication Acknowledgements

This white paper was developed by the EMV Migration Forum to provide an educational resource for issuers that documents the best practices for transitioning an existing instant issuance solution to support the issuance of EMV chip cards.

Publication of this document by the EMV Migration Forum does not imply the endorsement of any of the member organizations of the Forum.

The EMV Migration Forum wishes to thank the instant issuance project team members for their contributions to the white paper. Special thanks go to Phillip Andreae, Oberthur Technologies, and Jennifer Cristallo, Entrust Datacard, for leading this project.

The following members participated in the development of the white paper:

- Philip Andreae, Oberthur Technologies
- Alyssa Arredondo, Entrust Datacard
- Charl Botes, MasterCard
- Chole Casber, The Members Group
- Jeffery Comi, PNC
- Keri Crane, JHA Payment Processing Solutions
- Jennifer Cristallo, Entrust Datacard
- Jim Ellis, ABnote
- Kevin Emery, Discover Financial Services
- Dave Ewald, B2PS
- Tanya Fillmore, JHA Payment Processing Solutions
- Mke Gorski, Visa Inc.
- Arthur Harper, PSCU
- Kirsty Haugh, Oberthur Technologies
- Peg Haustetter, SEI – Cincinnati (for Vantiv)
- Simon Hurry, Visa Inc.
- Mansour Karimzadeh, Smart Commerce International Ltd. (SCIL)
- Greg Kuyava, Harland Clarke
- Liza Mackinnon, Magtek
- Mina Malek, Giesecke & Devrient
- Jason Muncey, American Express
- Sharon Pazlar, Fiserv
- Joe Segal, American Express
- Jonathan Taylor, JPMorgan Chase
- Dean Vance, First Data
- Kelly Witteride, Vantiv
- David Worthington, Bell ID

Trademark Notice