Optimizing Transaction Speed at the POS

Version 3.0

Date: October 2017

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

EMV is a trademark owned by EMVCo LLC.

Table of Contents

1. Introduction

With the U.S. payments industry's ongoing migration to EMV chip technology for more secure payments, the U.S. Payments Forum continues to identify and provide guidance on the areas essential to improving and optimizing secure EMV transactions.

As chip cards continue to be issued and chip-enabled terminals continue to appear at merchant locations across the U.S., many cardholders and merchants are having varied responses to their chip transaction experiences. A common response heard across the industry is the inconsistent speed observed during an EMV transaction, where a chip transaction might take a couple seconds at one merchant but 20 or more seconds at another.

Any payment transaction can pass through several distinct networks and stakeholders in the payment ecosystem, and stakeholders can optimize each segment for maximum speed throughput. This payment system complexity is especially pronounced in the U.S. and is causing inconsistent experiences at the point-of-sale (POS) which directly impact cardholders and merchants.

This white paper focuses on several categories of approaches to help speed transactions and discusses their potential impacts for each stakeholder group in the U.S. payments ecosystem: "Faster EMV" solutions for terminals, faster card-terminal communication speeds, contactless/Near Field Communication (NFC) solutions, and EMV checkout optimization practices. For each category, a detailed description and analysis are presented, including considerations and implications for various stakeholder groups.

- Faster EMV Solutions. "Faster EMV" is an umbrella term used in this white paper to describe the optimized online-only EMV transaction processing solutions announced separately by American Express, Discover, MasterCard, and Visa. These solutions retain the security features of EMV, while removing dependencies that can negatively influence the cardholder perception of transaction time.
- Faster Card-Reader Communication Speeds. In conjunction with Faster EMV, a section is included on faster card-terminal communication speeds, which allows cards to operate at higher transmission speeds. When combined with "Faster EMV" significant improvements to the card's time-in-terminal may be achieved. However, issuers that adopt this option are advised to consult with their card vendor, payment network and EMVCo standards for additional guidance.
- Contactless/NFC Transactions. The adoption of contactless transactions in the U.S. can greatly improve the cardholder experience. Cardholders benefit from being able to tap and quickly put away the contactless-enabled payment device. Merchants and cardholders benefit from both perceived and actual reduced transaction time compared to contact methods.
- EMV Checkout Optimization. Both merchants and issuers can implement tactics that can help to optimize the EMV checkout experience. In the course of implementing EMV support, merchants have worked to provide an efficient checkout process for cardholder interaction with the terminal and for system processing time. Different techniques may offer benefits in various checkout scenarios. These techniques arise from both new learnings in implementing EMV, and from traditional approaches to optimizing checkout throughput.

The goal of the white paper is to educate payments industry stakeholders and offer a sufficient level of detail about each set of solutions to provide the reader with a starting point for pursuing one or more of

these solutions. The solutions described are generally compatible with each other and this white paper can be considered a primer for different optional techniques that may be used to speed the EMV transaction process at the POS. In particular, merchants that choose to adopt Faster EMV in conjunction with contactless transactions should adapt their checkout flow to allow for a uniform cardholder experience regardless of whether the card is tapped, inserted or swiped.

2. Faster EMV Solutions[1]

Faster EMV processing solutions have been announced by the payment networks noted in this paper, under the names of Amex Quick Chip, Discover Quick Chip, M/Chip Fast, and Visa Quick Chip.

These chip processing solutions are specifically designed for environments where faster transaction times, in addition to security, are particularly important. Each prioritizes the parts of the EMV transaction that provide protection against counterfeit fraud and omits certain other EMV features.

As with traditional EMV, counterfeit protection is central to the Faster EMV transaction and is accomplished through the generation of a unique one-time cryptogram. Once this cryptogram has been generated by the card and delivered to the terminal, Faster EMV allows completion of EMV processing to be initiated, and the card can be removed from the reader. This improves the cardholder perception of the time it takes to perform the overall payment process.

Faster EMV solutions are defined as online-authorization-only processing scenarios (also referred to as "online-only"). By definition, EMV offline chip-based authorization[2] is not supported. Other options discussed in the U.S. Payments Forum white paper, "Merchant Processing during Communications Disruptions,"[3] still apply.

Currently, these Faster EMV solutions are only approved for implementation in the U.S. American Express, Discover, and MasterCard do not allow for Faster EMV processing at the ATM.

2.1 Faster EMV Processing Overview

The Faster EMV solutions allow the card data to be retrieved and, if applicable, the PIN to be entered and validated, before the scanning of goods has been completed and the final transaction amount has been determined.

Traditional EMV Processing

During traditional EMV processing, the card remains in the reader until the final amount is known, and the online cryptogram (the Authorization Request Cryptogram (ARQC)) can be generated using the final amount as one of the cryptogram data elements. An online authorization request is built using the ARQC, and sent to the issuer. The card remains in the reader until the authorization response is processed, issuer authentication is (optionally) performed, and any issuer scripts are sent to the card and processed.

Faster EMV Processing

Faster EMV solutions are based on two fundamental processes: optional use of a pre-determined, or "placeholder," amount to obtain the ARQC prior to determination of the final transaction amount; and the request for a termination cryptogram (Application Authentication Cryptogram (AAC)) to complete EMV processing before the authorization response is received by the terminal. The flow is discussed in more detail in this section with flow diagram in Figure 1.

---

[1] Additional information can be found in Section 7, "Appendix: Faster EMV Questions and Answers."

[2] U.S. Payments Forum, "Merchant Processing during Communications Disruptions," April 2016, http://www.emv-connection.com/merchant-processing-during-communications-disruption/

[3] Ibid.

The card reader performs the traditional EMV flow up to and including the processing of the first Generate AC command, using a predetermined amount in place of the final transaction amount if the final transaction amount is not yet known. The standard flow includes application selection, cardholder verification, and terminal risk management. Offline card authentication may also be performed.

When the card provides an ARQC, the terminal does not immediately attempt to go online. Instead the card reader completes the EMV processing through a second Generate AC command indicating that the terminal is unable to go online (request for AAC).

These modifications to the transaction flow mean that the reader interacts with the card for only for a short period of time – typically two to three seconds.

Following completion of EMV processing, and once the final transaction amount is known, the terminal authorizes the transaction online. The authorization request includes the final transaction amount in DE4[4] and the full chip data (including the amount used to generate the ARQC – either the placeholder amount or the final transaction amount) in DE55. The terminal indicates approval or decline of the transaction according to the issuer's decision, and captures the cardholder's signature if necessary.

Note that the difference between the amounts in DE4 and DE55 is not new to issuers, as this can occur in various acceptance environments (for example, loyalty-based discounting and transit) today.

By eliminating the wait times associated with determination of the final amount (such as when a basket of goods is being scanned) and authorization response processing, the time that the card resides in the reader can be greatly reduced. Eliminating the dependencies associated with these wait times also allows for more flexibility in the cardholder interface. For example, card insertion can now be allowed at the beginning of the retail transaction. Elimination of the wait times can result in a significant reduction in the cardholder-*perceived* transaction time, as the time that the chip card is in the reader is reduced. Faster EMV also eliminates some traditional EMV processing time, such as for issuer authentication and issuer script processing functions. While this can result in *actual* reductions in processing time, the reduction depends on the efficiency of the current implementation, and may be negligible.

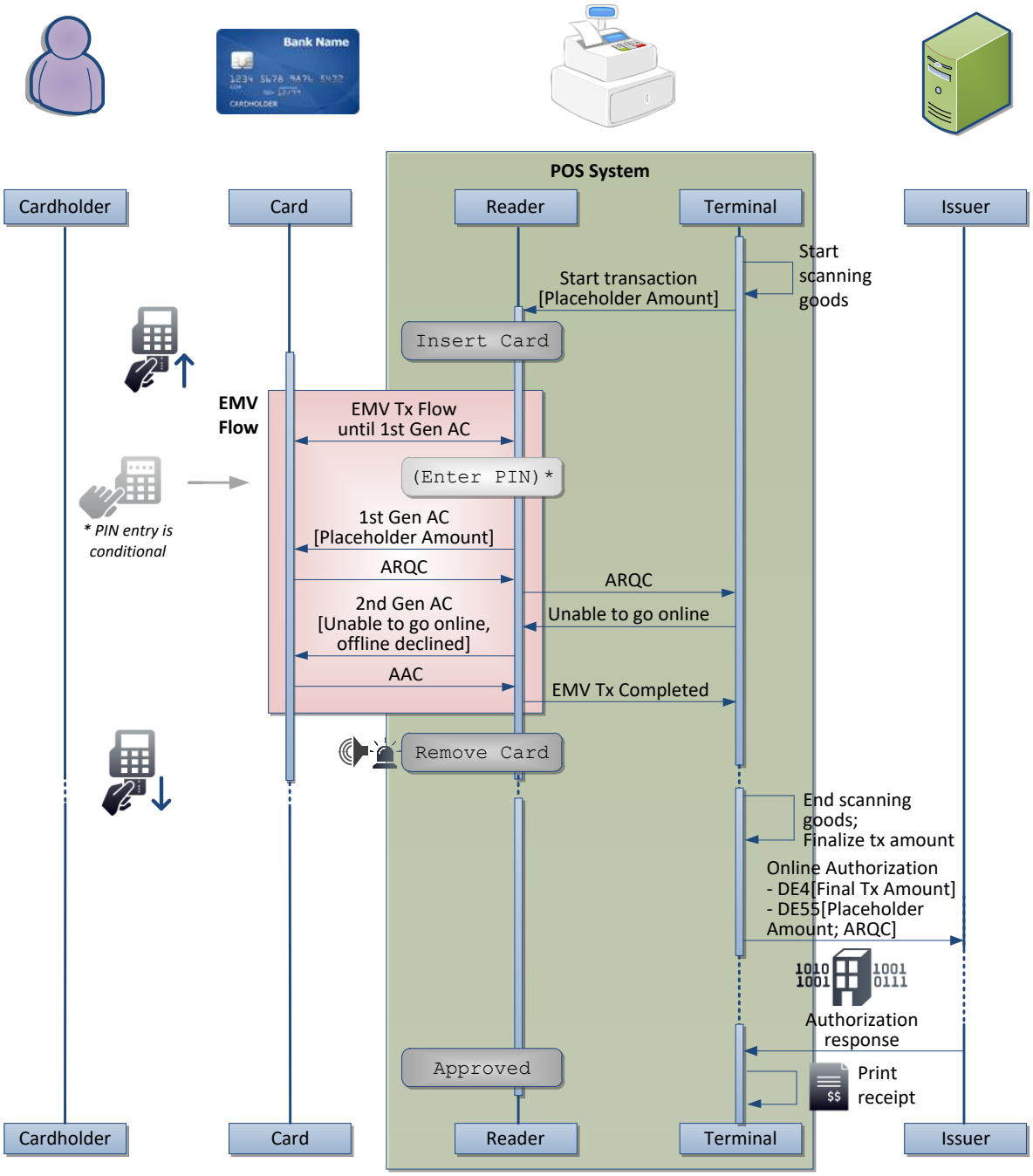
The Faster EMV solutions provide the same level of protection against counterfeit fraud as conventional EMV processing flows.

2.2 Transaction Flow

The different steps of the modified Faster EMV processing flow are shown in Figure 1 and described below. The flow assumes that the terminal controls the messages displayed to the cardholder.

[4] "DE" is an abbreviation for "Data Element" and is commonly used when referring to fields in an ISO/IEC 8583-based message format. Thus, "DE4" is the identifier of the fourth data element in an authorization request based on ISO/IEC 8583. "Data elements" may also be referred to as "fields." DE4 is defined as the "Transaction Amount;" DE55 Tag 9F02 is defined as "Amount, Authorized" within the cryptogram data. ISO/IEC 8583 is a common base for payment network messaging; however other message formats, such as proprietary device-to-server message formats, may be based on other specifications. Nevertheless, all formats will contain equivalent fields.

Figure 1. Faster EMV Transaction Flow



These following steps are illustrative and aim to show how an existing terminal-reader configuration can be adjusted for Faster EMV.

1. The terminal may activate the reader as soon as the scanning of goods starts. If the final amount is not known yet, the terminal includes a placeholder amount in the activation request. The placeholder amount is a non-zero amount. The merchant may select any non-zero value[5].
2. Depending on the acceptance environment, the terminal may be configured to select a placeholder amount that does not exceed the Cardholder Verification Method (CVM) limit (if the terminal is configured to perform No CVM processing and to submit the transaction without PIN or signature).
3. The cardholder is invited to insert their card. The placeholder amount of the transaction is not shown to the cardholder.
4. Application selection, transaction initiation and reading of the card data is performed as per traditional EMV (through the Select, Get Processing Options and Read Record commands). Faster EMV supports standard application selection processes, whether Cardholder Selection, Application Priority Selection, or customized application selection.
5. If supported by the card and the terminal, offline data authentication is performed as per traditional EMV. (This may involve additional commands, such as Internal Authenticate.)
6. If the transaction amount exceeds the CVM limit and if PIN is the selected CVM, the cardholder is invited to enter the PIN.[6]
    a. If offline PIN is the selected CVM, the cardholder is informed of the result (through the Verify PIN command and potentially the Get Challenge command for encrypted offline PIN).
    b. If online PIN is the selected CVM, the PIN is encrypted into a PIN block.
    c. If signature is the selected CVM, it is not captured at this point but at the end of the transaction following receipt of the issuer approval.
7. The reader requests an online cryptogram (ARQC) from the card.
8. Unless the transaction is terminated when the online cryptogram is requested (i.e., AAC returned), the reader receives an ARQC from the card and returns the ARQC together with the other chip data to the terminal.
9. The terminal stores the ARQC and the associated chip data for the later authorization request.
10. The reader completes EMV processing by sending a second Generate AC command with an Authorization Response Code 'Unable to go online, offline declined' (value 'Z3') to request an AAC, and upon receipt of the card's response, informs the terminal that the EMV processing is completed. (In this scenario, requesting a "decline" cryptogram is used only to complete EMV processing, and does not determine transaction disposition. Disposition is determined by the issuer response.) The cardholder is prompted to remove their card.

[5] Please refer to payment network documentation for variances when performing No CVM transactions.

[6] Assuming that the kernel configuration supports PIN.

11. When the final transaction amount is known, the terminal sends an authorization request to the issuer with the final amount in DE4, the ARQC and chip data in DE55, and if applicable, the online PIN block; the transaction amount in DE55 (with tag '9F02') is the amount used to generate the ARQC, in this example, the placeholder amount. The authorization request amount (DE4) may vary from the cryptogram amount (DE55 Tag "9F02").
12. The payment process is completed according to the issuer response (approve or decline) and the cardholder is informed of the outcome. If the transaction is approved and signature was the chosen CVM, the signature can be captured on a sales receipt or signature capture device.

2.3 Implications for Cardholders

The cardholder only needs to put the card in the reader for a short time before withdrawing it, creating a fast cardholder experience that is similar to swiping a magnetic-stripe card. This also means less risk of the cardholder accidentally leaving their card in the reader after the transaction.

Cardholders will likely continue to have different experiences at different locations since implementations will differ and some merchants may not choose to implement Faster EMV solutions.

Although Faster EMV allows the total time of the card in the reader to be reduced, the overall flow will still be familiar to both U.S. and international cardholders. The acceptance device should continue to prompt for the cardholder to insert the card, to leave the card in the reader, and to remove the card. This will maintain the cardholder experience of "following the prompts."

2.4 Implications for Issuers

The issuer still receives the benefit of chip as the authorization request includes the ARQC (and the associated chip data needed for ARQC validation). This allows the issuer to check that the card is genuine and provides counterfeit fraud protection.

The issuer will need to ensure that the authorization request amount (DE4), which is the actual transaction amount, is used for the authorization decision; the cryptogram amount (DE55 Tag '9F02') is used solely for cryptogram validation, since the amount in DE55 may be the placeholder amount.

As with traditional EMV processing, a PIN can be obtained providing merchants with lost/stolen fraud protection where the lost/stolen liability is shifted under payment network rules. If offline PIN was performed during the EMV transaction, the PIN verification result is included in the chip data. If online PIN was performed, the issuer receives the PIN Block in the authorization request message.

If chip data is provided in clearing, the cryptogram will be an ARQC, rather than a Transaction Certificate (TC). Issuers also receive ARQCs in clearing when deferred authorizations are performed, as well as for certain host-capture configurations.

Scripting will not be performed for Faster EMV transactions. Issuers should review their scripting processes to ensure scripts are re-tried until successful (or canceled).

2.5 Implications for Merchants

Cardholders may perceive traditional EMV processing as time-consuming if the card remains in the reader during scanning of multiple goods. Merchants wishing to provide improved cardholder

perception of transaction time may wish to implement Faster EMV processing. Faster EMV processing may modestly affect overall actual processing time, depending on the specific implementation.

In a magnetic stripe environment, some merchants in the United States support a process that allows the cardholder to swipe their card prior to the final amount being known – either at the start of the transaction or during the transaction process. Merchants have deployed these solutions to improve the perceived and/or actual transaction time at their point of sale. In an EMV environment, the Faster EMV solutions will offer the merchant a similar opportunity to allow the cardholder to insert and remove their card in contact transactions prior to the final amount being known, using a placeholder value for the final amount.

Currently, for contact transactions, a terminal is implemented with either Faster EMV or traditional EMV. In order to support the Faster EMV process, the POS application software vendors will need to make changes to the POS application software if their merchant customers want to implement Faster EMV.

With Faster EMV processing, the overall transaction flow can be:

- Insert card
- Read the chip data
- Enter the PIN (as applicable)
- Remove card[7]
- Present cardholder with total (optional)[7]
- Get issuer authorization
- Obtain signature (dependent on processing; may be optional)

The merchant may still support any combination of the standard chip CVMs[8]: offline and online PIN, signature and No CVM. Offline data authentication (Dynamic Data Authentication (DDA), Combined DDA/Application Cryptogram (CDA)) can be supported.

Merchants should carefully consider their strategy for CVM processing with a Faster EMV implementation, because the lost/stolen liability shift remains in place for Faster EMV transactions. This is especially important if merchants use a placeholder amount for Faster EMV transactions. Merchants participating in small ticket "signature/PIN not required (No CVM)" programs should be aware that the application logic inherent in these programs complicates the logic for implementing Faster EMV. This is because for No CVM programs, the final amount must be known in order to prevent the prompt for PIN or signature, and the final amount may not be known at the point in the transaction where CVM is prompted.

Where a merchant supports multiple kernel configurations, additional care should be used to select the appropriate one for the desired condition. When a predetermined value is used for cryptogram creation for Faster EMV transactions, this value is also used for the kernel selection. Thus, the initial selection of the kernel will apply regardless of the final transaction amount. Examples include the following:

---

[7] This may take place in parallel with the issuer authorization.

[8] PINs will be obtained while the card is in the reader. Signature can continue to be obtained once the authorization response is returned.

- If a merchant desires to capture a PIN for the transaction, the kernel supporting all CVMs should be considered. For PIN-preferring cards, this selection will result in a PIN being collected regardless of transaction amount.
- If the merchant wishes to use a No CVM kernel, then all transactions will be performed without a PIN. If desired and available from its solution provider, the merchant may configure its software to capture a signature for transactions over the relevant network's No CVM limit for chargeback purposes.

Merchants should also review their strategy and logic for supporting transactions when communications are disrupted.[9] If a merchant supports EMV offline authorization, they should be aware that a TC is not possible with Faster EMV. If a merchant supports deferred authorization, Faster EMV may fit well with this strategy. If a merchant supports force post for communication disruptions, they should review their logic to see if changes to processing are needed.

Application selection, including support for U.S. Common Debit AID, will function normally, including selection of U.S. Common Debit AIDs. Cardholder selection for support of multi-account cards can be offered.

Scripting will not be performed for Faster EMV transactions.

Reduced time of the card in the reader also means less risk of the cardholder accidentally leaving their card in the reader after the transaction.

As of September 2016, Faster EMV production implementations are limited, so merchant learnings and considerations are still being developed.

2.5.1 Merchant Segments Where Approach May Be Relevant

The relevance of a Faster EMV solution as opposed to a full traditional EMV implementation will vary by merchant. Faster EMV is geared towards merchants where cardholder perception of speed is critical. To assess whether Faster EMV implementations are relevant to specific merchant scenarios, merchants are encouraged to discuss feasibility and availability with their payment network and processing partners.

All liability shift policies still apply to Faster EMV implementations.

2.6 Implications for Acquirers

There should be no transaction flow impact on the acquirer, as the authorization request message is the same as a traditional EMV authorization request message. In particular, there is no impact on U.S. Common Debit AID routing.

Acquirer testing and certification requirements will need to be updated to incorporate the Faster EMV requirements.

[9] U.S. Payments Forum, "Merchant Processing during Communications Disruptions," April 2016, http://www.emv-connection.com/merchant-processing-during-communications-disruption/

2.7 Implications for Terminal and POS Application Providers

Depending on the payment application architecture, Faster EMV functions can either be implemented in the terminal or in the POS application. Typically, the payment application will implement the functionality by invoking APIs into the kernel to execute the desired EMV function.

Terminal vendors may choose to implement Faster EMV functions on a per-AID basis to allow flexibility of implementation between different payment networks. However, the Faster EMV solutions currently announced are all compatible, and there is no inherent reason not to implement these solutions for all payment networks.

2.8 Implications for Testing and Certification

Faster EMV functions can be implemented without impacting the EMVCo Level 2 approval of the kernel.

For point-of-sale solutions that *have* been Level 3 EMV certified through the payment networks and wish to enable Faster EMV transactions, all payment networks have recommended regression test cases that can be performed internally to validate Faster EMV functionality. Additional Level 3 certification is not currently required. American Express will provide an amendment to the existing American Express Letter of Approval (LOA) upon attestation that inclusion of Quick Chip was the only change made.

For new point-of-sale solutions that *have not* been Level 3 EMV certified through the payment networks, test plans have been updated to reflect Faster EMV acceptance when requested. For new certifications, all payment networks require a streamlined testing approach (subset of test cases) versus a standard full EMV certification. Refer to each payment network's current processes and programs for specifics on requirements.

Additional information on the payment networks' testing and certification requirements can be found in the U.S. Payments Forum white paper, "EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community."[10]

[10] U.S. Payments Forum, "EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community," http://www.emv-connection.com/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/

3. Faster Card-Terminal Communication Speeds

Following the initial publication of the U.S. Payments Forum "Optimizing Transaction Speed at the POS" white paper, various stakeholders have been looking for ways to further optimize transaction speed. Some POS suppliers have been converting traditional EMV implementations to use Faster EMV, or starting their EMV migration with Faster EMV, to improve the transaction speed. However, there are also ways that issuers can enhance their customer experience by adjusting settings on their EMV chip cards.

The data transmission speed determines the rate at which data can be exchanged between the card and the EMV payment terminal. Card vendors and card personalization services may be able to set the data transmission speeds when producing cards, as permitted by the product approval process defined by each payment network. In many cases, current card platforms are available in configurations that can operate at data transmission speeds two or four times the default rate. Increasing the data transmission speed can have a noticeable impact on total contact EMV transaction time, particularly when the card contains significant amounts of data. EMV testing for terminals has included testing for functionality at the default rate, the doubled rate, and the quadrupled rate. (No changes are required to terminals tested since EMV2000 Version 4.0 in order to support the higher data transmission speeds.)

This optimization is only applicable for cards that have not been initialized or personalized. Issuers should check with their card vendors to see if their cards support the faster speed. This change only impacts initialization and does not impact personalization profiles.

This optimization is most beneficial for transactions involving signature or no CVM on a terminal supporting Faster EMV. If the cardholder is required to enter a PIN or if the terminal doesn't support Faster EMV, the speed improvement may be less significant.

3.1 Faster Card-Terminal Communication Speeds within the EMV Specs

The section below is highly technical and included for completeness; it is based on the existing EMV specifications. Please refer to EMVCo for any future updates on low level card-terminal protocols and communication speeds.

Issuers considering chip cards for their EMV implementation, whether a new implementation or reissuance, should note that support for higher data transmission speeds may differ among available cards. In many cases, current card platforms will have a variant that can support data transmission speeds double or quadruple the default rate.

This section includes the specific technical details for how to implement the faster card-terminal communication speeds; see the EMVCo specifications for details on how the card-to-terminal communications occur.

Figure 2 shows the transaction flow for the card to reader communication to enable faster communications speed.

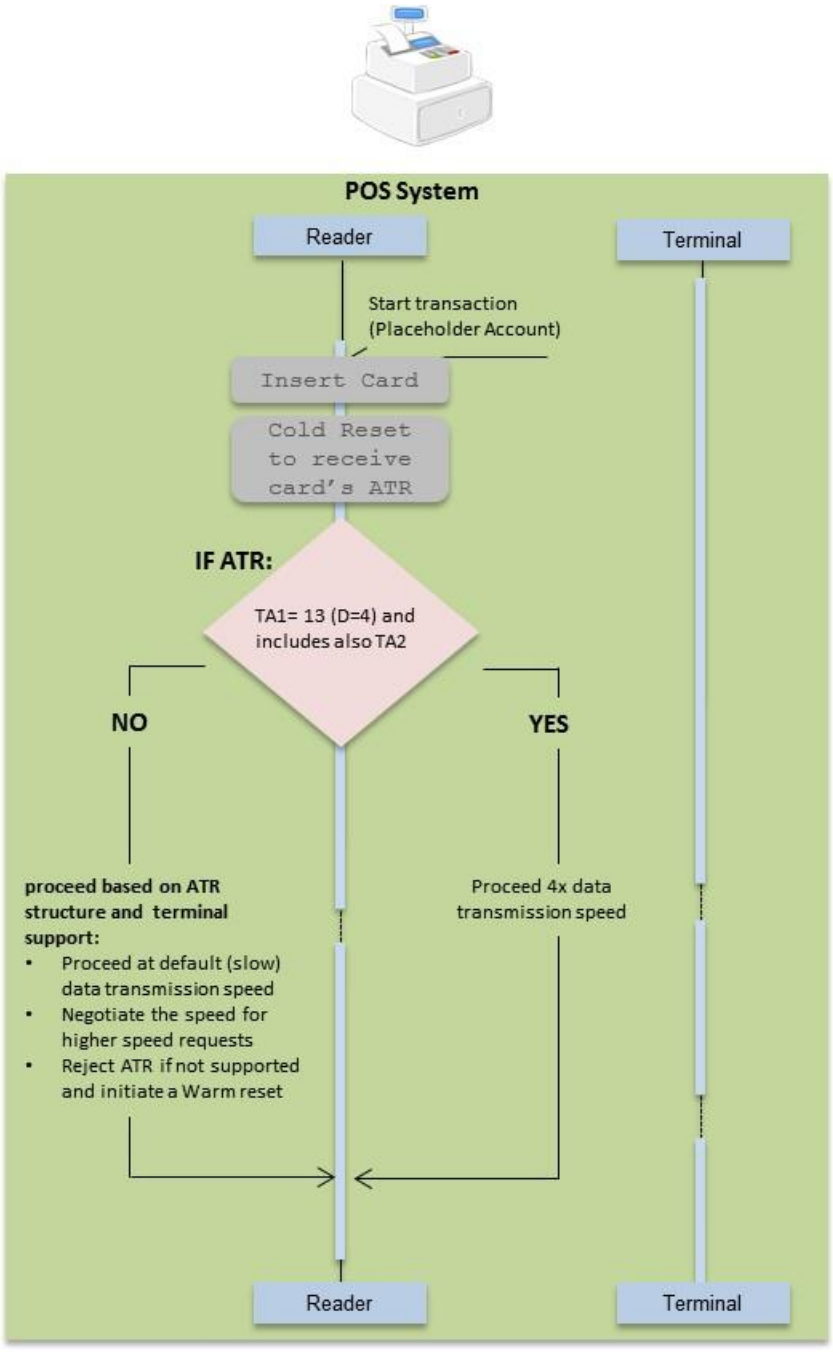


Figure 2. Card to Reader Communication for Faster Data Transmission Speed

Two options are available for implementation – T=0 or T=1 – described below; issuers are advised to consult their card supplier in order to select the appropriate approaches.

The solution implements EMV compliant COLD and WARM ATRs for T = 0 and T = 1 as indicated below:

3.1.1 T=0 Implementation

T = 0: COLD ATR (non-basic):

- TA1= 13 (referring Di=3 and D=4)
- TC1= 'FF' or '00' (extra guard time not required)
- TA2 shall be contained in ATR to ensure specific mode with the values below:
  - TA2 the least significant nibble is also the first indicated protocol in the ATR which is T=00 protocol (bit 4-1 = 0000)
  - TA2 bit 5 = 0
  - TA2 bit 7-6 = 00 (RFU)

For the rest of the parameters/characters used in ATR please refer to *EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements Version 4.3, November 2011,* Section 8.

T = 0: WARM ATR (basic): EMV Basic ATR as indicated in *EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements Version 4.3, November 2011*, Section 8.2, Table 15 – Basic ATR for T=0 only.

3.1.2 T=1 Implementation

T = 1: COLD ATR (non-basic):

- TA1= 13 (referring Di=3 and D=4)
- TC1= 'FF' (referring special meaning with N=-1 for Extra Guard Time for T=1 protocol)
- TA2 shall be contained in ATR to ensure specific mode with the values below:
  - TA2 the least significant nibble is also the first indicated protocol in the ATR which is T=1 protocol (bit 4-1 = 0001)
  - TA2 bit 5 = 0
  - TA2 bit 7-6 = 00 (RFU)
- TB3 = '20' with the meaning of:
  - Most significant nibble BWI = '2' for Block Waiting Time integer
  - Least significant nibble CWI = '0' for minimum Character Waiting Time integer (TC1 above must be 'FF' for this value to prevent conflict)

If any of the values for CWI=0 in TB3 OR TC1='FF' changed to a different one than the recommended values above, the new values will need to be re-evaluated to prevent a conflict. A conflict in these values may cause ATR to be invalid. Please refer to *EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements Version 4.3, November 2011,* Section 8.3.3.10, including the "Note."

For the rest of the parameters/characters used in ATR please refer to *EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements Version 4.3, November 2011,* Section 8.

T = 1: WARM ATR (basic): EMV Basic ATR as indicated in *EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements Version 4.3, November 2011*, Section 8.2, Table 16 – Basic ATR for T=1 only.

With the combination above, the terminal is expected to switch to quadruple speed as soon as the COLD ATR received. In rare cases, if the terminal is a legacy version (below EMV version 4.0), the COLD ATR will be rejected. In such a scenario the legacy terminal would initiate a WARM ATR. As WARM ATR is EMV basic, it is accepted and the transaction continues at a default speed.

3.1.3 Considerations for Cardholders

- Cardholder prompting is unchanged.
- The cardholder may experience faster transaction times.

3.1.4 Considerations for Issuers and Issuer Processors

- Issuers may wish to consider issuing dual-interface cards since all dual-interface cards already have been certified and support the faster communications speed over the contactless interface. Dual-interface cards comply with timing performance requirements defined by the payment networks. Typically, a tap-and-go transaction can be processed in less than half a second (i.e., less than 500ms), giving the fastest cardholder experience. (See Section 4 for information on contactless/NFC.)
- Improvements on faster bus speeds apply to new card production only. Issuers should be aware that their current card stock may not support higher speeds.
- Issuers must contact their card manufacturer, card personalization bureau and instant issuance provider for information on support for faster bus speeds.
- Issuer processors may need to contact their module supplier.
- Card manufacturers may need to contact their module supplier.
- Issuers will need to check with their card suppliers for whether their products have payment network/brand approval. Issuers should be aware that payment network product approval may take time, as it will depend on the card vendor product roadmap and availability of the testing process at payment networks and laboratories.
- Issuers will need to check with their card supplier and personalization partners if faster cards need to be re-tested as per the card personalization validation processes.

3.1.5 Considerations for Merchants

- Merchants are encouraged to test cards with faster bus speeds in their environment.
- POS terminals after EMV Specification Version 4.1 (January 31, 2002) automatically support the faster bus speed. These terminals were tested based on the test plan, “EMVCo Type Approval Terminal Level 1, Test Cases, Version 2.0, January 31st, 2002,” ensuring faster bus speed support up to quadruple speed. For such terminals and after, no additional testing and certification will be required to support high bit rates.

3.1.6 Considerations for Acquirers

- Acquirers are encouraged to test cards with faster bus speeds in their terminal population.
- POS terminals after EMV specification Version 4.1 (January 31, 2002) automatically support the faster bus speed. These terminals were tested based on the test plan, "EMVCo Type Approval Terminal Level 1, Test Cases, Version 2.0, January 31st, 2002," ensuring faster bus speed support up to quadruple speed. For such terminals and after, no additional testing and certification will be required to support high bit rates.

3.1.7 Considerations for Terminal and POS Application Providers

- Terminal and POS application providers are encouraged to test cards with faster bus speeds in their terminal population.
- POS terminals after EMV specification Version 4.1 (January 31, 2002) automatically support the faster bus speed with no additional testing and certification.

3.1.8 Considerations for Testing and Certification

- For POS terminals after EMV specification Version 4.1, no additional testing and certification is required if the specifications outlined in Section 3.1 are followed.
- Issuers and issuer processors should consult with their network and card vendors on any additional testing and certification required; this should be done for each product and card profile.
- No additional certification is required for dual-interface card products.
- Card vendors should check if their contact-only products support higher speeds and contact their payment network approval service team for product re-certification and testing plan availability. Note that depending on card vendor strategies and payment network testing policies, this can be a lengthy process.

3.1.9 Considerations for Personalization Services – Centralized and Branch/Instant Issuance

- Personalization vendors should determine how to manage the card profile to support the enhanced ATR (e.g., during personalization or during initialization).
- Personalization providers and/or module suppliers must ensure that the chosen ATR matches the Letter of Approval ATR values.
- Personalization providers may use quadruple speed for their own benefit to improve the time of personalization.

4. Contactless/NFC

4.1 Contactless Description

Contactless is a payment method that enables cardholders to make payments by tapping their contactless-enabled payment device (e.g., dual-interface card, NFC-enabled mobile phone, wearable) onto a contactless-enabled POS device rather than swiping or inserting a payment card. The chip and antenna in the payment device securely transmits payment details wirelessly to a contactless reader, either integrated within or connected to a merchant's POS system. The transaction details are sent online for authorization via the merchant/acquirer authorization interface and are subsequently cleared through the same acceptance network used for traditional payment card transactions.

Embedded inside the contactless-enabled payment device is an antenna that typically runs around its perimeter. Contactless payment uses radio frequencies (RF) and can power payment to be made with many types of form factors.

The discussion and diagram in this section cover EMV contactless implementations. The EMV contactless transaction flow utilizes all of the key principles of EMV – application selection (Proximity Payment System Environment (PPSE)), terminal risk management, offline card authentication, cardholder verification – until the contactless device generates the Authorization Request Cryptogram (ARQC). The full transaction is then concluded after the device is removed from the RF field. The merchant and their acquirer will then populate the authorization message with the appropriate data element information to request an online authorization.

The interaction between the EMV contactless-enabled payment device and contactless reader is targeted to take place in less than half a second.

Contactless capability is denoted by the universal **Contactless Indicator** which should be present on all contactless cards and form factors or displayed on the screen of contactless mobile devices. (See Figure 3.) A **Contactless Symbol** should be present on all contactless readers to indicate compliance with the EMV Contactless Communication Protocol, and the Contactless Symbol must be used to indicate the "read area" on the reader where the payment device should be tapped. Any payment device with a Contactless Indicator should work on any reader with a Contactless Symbol.

Figure 3. Contactless Indicator and Contactless Symbol

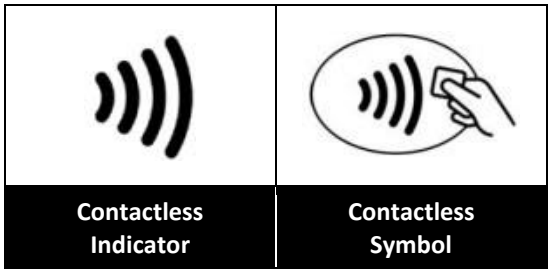
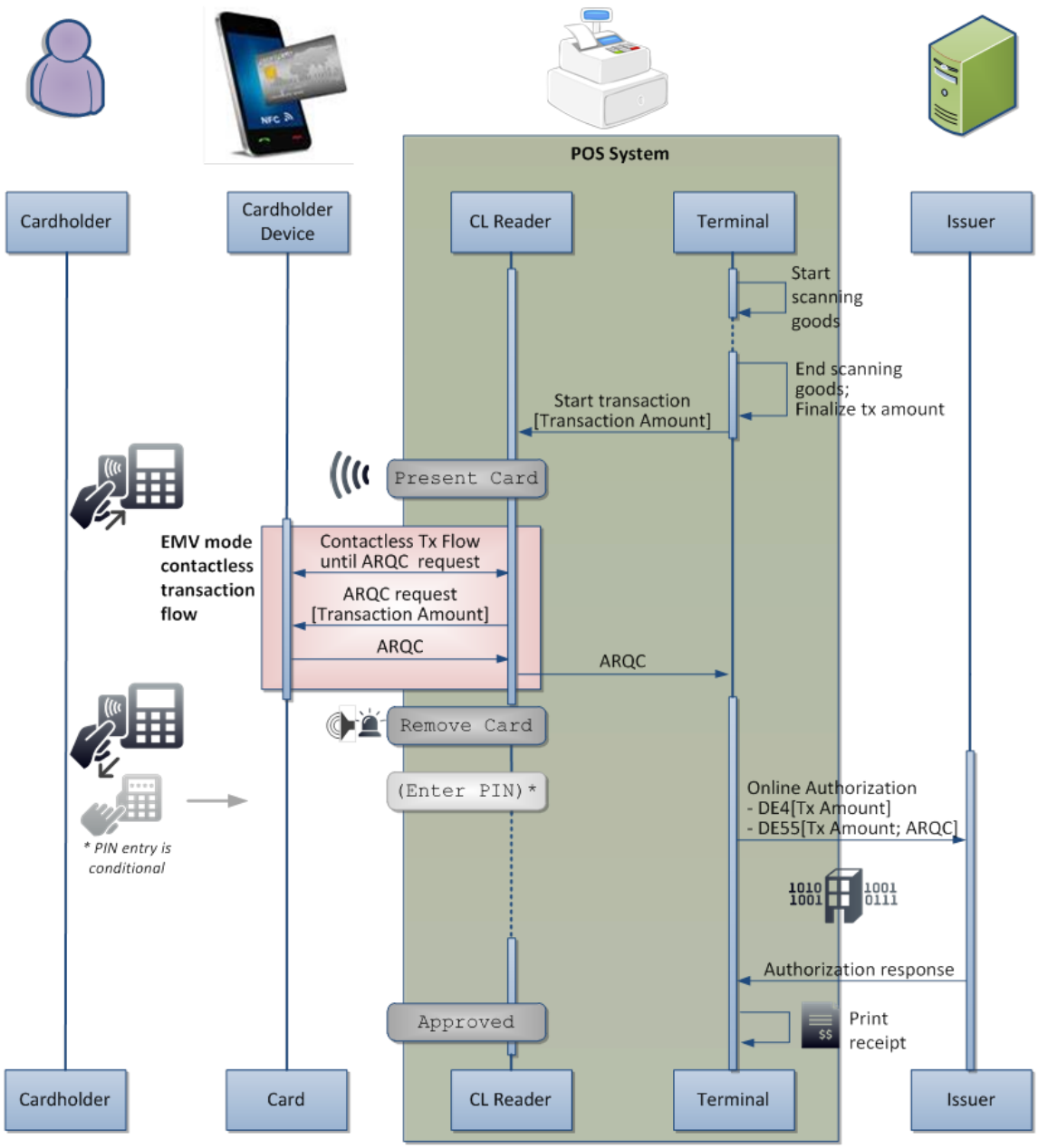


Figure 4 illustrates the EMV contactless transaction flow.

Figure 4. EMV Contactless Transaction Flow for Online Transactions



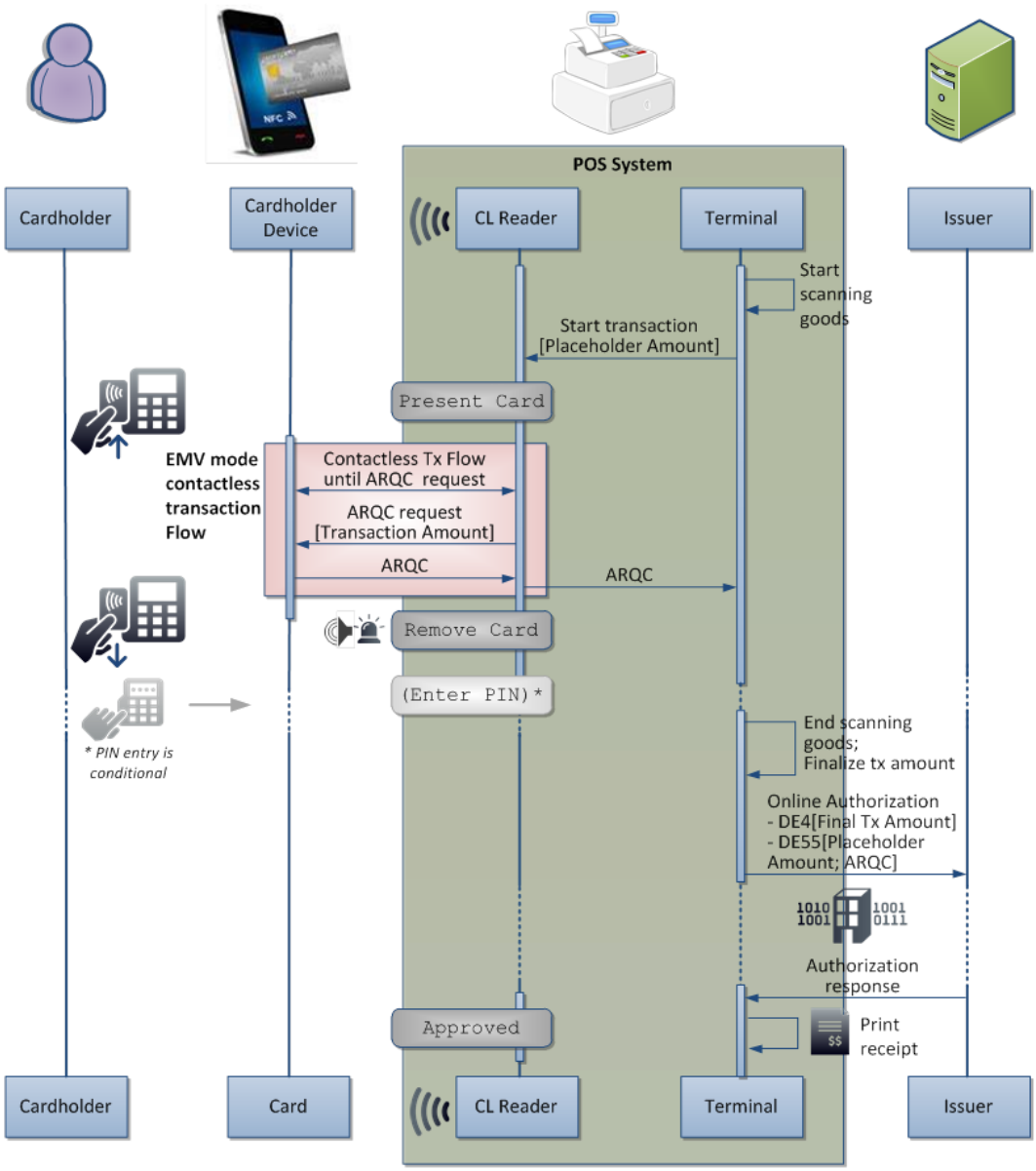
4.2 Contactless Pre-Tap Description

While a basic contactless transaction described in the previous section requires the total amount to be known prior to the cardholder tapping their contactless-enabled payment device, many payment networks support a “pre-tap” capability for online transactions which allows the cardholder to tap a contactless-enabled payment device prior to the total amount being known. (See Figure 5.) If enabled by a merchant/terminal provider, the contactless reader on the POS device becomes active when the clerk begins scanning items. Upon tapping a payment device prior to the total amount being known, the terminal generates an ARQC using a placeholder amount. When the total amount becomes known, the

total amount is included in the authorization request, while the placeholder amount is included in the accompanying cryptogram data along with the ARQC. The issuer validates the cryptogram using the placeholder amount. The other elements of the transaction proceed as outlined in the previous section and diagram.

At the time of publication of this document, American Express, Discover, MasterCard, and Visa support a contactless pre-tap capability; contact the relevant payment network for information on their support for contactless pre-tap.

Figure 5. EMV Contactless Pre-Tap Transaction Flow for Online Transactions



4.3 Functionality Supported and Not Supported

The following functions are supported in contactless form factors:

- Application Selection
  - PPSE, which facilitates the selection of the highest priority payment application that is mutually supported by the card and terminal
  - U.S. Common Debit AID for Durbin routing, available from POS terminal providers[11,12]
- Data authentication – online (ARQC or TC) and offline card authentication
- CVMs: Online PIN, No CVM, Signature, Consumer Device CVM (CDCVM)/On-Device CVM (ODCVM)[13]
- Authorization – online (ARQC) and offline (TC)

The following functions are not supported in contactless form factors:

- Authorization Response Cryptogram (ARPC)
- Offline PIN CVM
- Issuer scripting (e.g., for offline card risk management controls, PIN change, PIN management, PIN lock)

4.4 Implications for Cardholders

In a contactless payment transaction, the dual-interface (contact and contactless) card or NFC-enabled mobile device never leaves the consumer's hand, making the consumer payment experience simple and quick, especially when the issuer/merchant allows the use of "No CVM" to complete the transaction below the contactless CVM limit. For contactless cards, the consumer retaining possession of the card also reduces the likelihood of a cardholder leaving a card behind.

As consumers become increasingly comfortable with using one contactless-enabled payment device, they may desire a similar contactless experience with additional form factors. Contactless payment devices create the opportunity for cardholders to obtain a form factor(s) most conducive to their lifestyle (e.g., card, mobile device, key fob, sticker, wristband, watch).

4.5 Implications for Issuers

Issuers benefit from the use of contactless products because cardholders are more likely to develop the habit of using their contactless payment devices for small dollar transactions where they might normally have used cash. Also, contactless products allow issuers to offer unique differentiated payment products for their cardholders (including cards, mobile devices, key fobs, stickers, wristbands, watches), which increases the opportunity to secure top-of-wallet status.

Because contactless products are not expected to remain in close proximity to the POS device during a transaction, issuers must defer the ability to use issuer authentication (ARPC). Issuers will also defer the

---

[11] The terminal logic to support the Common AID for the contactless interface is different from the terminal logic to support it for the contact interface.

[12] Merchants are advised to contact the acquirer/processor for additional information.

[13] Note that not all CVMs are supported for all AIDs. For network CVM support, contact the acquirer/processor for specific information.

ability to use scripting to complete certain actions that may be available for contact transactions, including updating offline card risk management controls, offline PIN management, and application blocking. (In some cases, issuers may be able to force a transaction to be processed using the contact chip.) Scripting actions must be deferred until a contact transaction is performed at a device supporting scripting, such as one that does not support Faster EMV. Also, contactless products are typically more costly to issue than traditional contact products (for example, due to the antenna inlay and additional data elements required).

4.6 Implications for Merchants

The primary benefit to merchants is that contactless transactions can improve transaction speed so that queues are faster at the POS. Additionally, there is reduced chance for a mechanical error in the POS device and reduced opportunity for cardholders to leave their contactless-enabled payment devices behind. Most issuers allow a contactless-friendly CVM with contactless devices, including "No CVM" or CDCVM/ODCVM, which simplify the cardholder verification process for some Application Identifiers (AIDs).[14]

Contactless products, like all electronic payment methods, have shown increased cardholder spend.[15] Contactless products may be useful for acceptance devices in environmentally-challenging situations, such as those situated in outdoor environments. Lastly, some cardholders attribute a "cool" factor to merchants who accept payments through a contactless interface, since the cardholder has more freedom to make a payment using a variety of form factors.[16]

There is potentially an incremental expense for merchants to acquire and maintain a terminal that is enabled to accept contactless payments. Many EMV-capable terminals available in the U.S. are also capable of accepting contactless payments if the merchant chooses to enable the contactless feature. For those merchants that develop their own terminal application, impacts to that software for both credit and debit transactions should be anticipated.

Merchants should also be aware that some contactless-enabled payment devices (e.g., mobile phones) use a token value in place of the primary account number (PAN) for security purposes. Merchants should consider the impact of token values to loyalty and reward programs, since the token value may not be recognized in connection with a PAN value.

Merchants should be aware that when a terminal is enabled for NFC, any device with NFC payment capability will be accepted. While the devices presented may have different security, cost or data use policies, they will all be accepted based on how the technology works. In addition, U.S. payment networks may have "honor all wallets" or "honor all devices" policies which may require merchants to accept mobile wallets that support cards on any network accepted by the merchant, which may be challenging to implement. Networks may also have data sharing requirements and end-user experience

[14] Note that not all CVMs are supported for all AIDs. For network CVM support, contact the acquirer/processor for specific information.

[15] MasterCard, "New MasterCard Advisors Study on Contactless Payments Shows Almost 30% Lift in Total Spend Within First Year of Adoption," May 2012, http://newsroom.mastercard.com/press-releases/new-mastercard-advisors-study-on-contactless-payments-shows-almost-30-lift-in-total-spend-within-first-year-of-adoption/

[16] Smart Card Alliance, "Contactless EMV Payments: Benefits for Consumers, Merchants and Issuers," June 2016, http://www.smartcardalliance.org/publications-contactless-emv-payments-benefits-for-consumers-merchants-and-issuers/

options which should be taken into consideration by merchants that want to enable acceptance of contactless-enabled payment devices.

If support for the contactless pre-tap capability is desired, merchants should ensure that the POS device selected is enabled and certified to support that capability or work with their terminal provider(s) to meet the necessary network requirements.

4.6.1 Merchant Segments Where Approach May Be Relevant

Contactless acceptance appeals to merchants where support for mobile payments is desired and speed and convenience are valued. It is also geared toward those merchant categories where cash is currently the dominant payment method, such as supermarkets, quick-service restaurants (QSRs), drive-throughs, convenience stores, daily-use retail, vending machines, toll booths, taxis, parking venues, fuel pumps and public transport. Secure contactless payments are recognized as the only realistic option for ticketless mass transit systems.

4.7 Implications for Acquirers

Most acquirers are capable today of processing authorization messages that contain EMV contactless payment data. Thus, the implication for acquirers and their associated technology partners is to continue to support the contactless elements of current and future EMV specifications for all supported payment networks.

If the contactless pre-tap capability is offered to merchants, acquirers are strongly encouraged to ensure that the POS devices are enabled and certified to support that capability, and work with terminal provider(s) to meet the necessary network requirements.

4.8 Implications for Terminal and POS Application Providers

Many terminal and POS application providers are capable today of providing terminals that are compliant with each payment networks' contactless terminal reader specifications. The implication for this stakeholder group is to maintain support and ensure their terminals remain compliant and certificated to future versions of the relevant networks' specifications.

Global payment network terminal specifications as of the publication of this document (September 2016) are as follows:[17]

- American Express Expresspay Terminal Specification; EMV Book C-4
- China Union Pay QuickPass; EMV Book C-7
- Discover Contactless D-PAS; EMV Book C-6
- JCB QUICpay; EMV Book C-5
- MasterCard Contactless; EMV Book C-2
- Visa Contactless Payment Specification; EMV Book C-3

POS application providers need to integrate the contactless reader application software into their merchant POS software and configure the contactless reader and POS software with the specific device

[17] Check with payment networks for current version of specifications.

(e.g., card, mobile phone) and payment networks' functional requirements. This includes support for the contactless pre-tap capability if a terminal provider chooses to offer that capability to its customers.

At the time of publication of this document, American Express, Discover, MasterCard, and Visa support a contactless pre-tap capability; contact the relevant payment network for information on their support for contactless pre-tap. For further understanding about the implementation of this capability, terminal and POS application providers should work with acquirers to define requirements that will ensure a favorable cardholder experience at the point-of-sale.

4.9 Implications for Testing and Certification

Testing and certification for contactless-enabled cards and terminals are required today for all payment networks. Many testing and certification tools are currently available to make contactless and contactless pre-tap enablement as convenient as possible for all stakeholders.

Contactless implementation may have implications for existing contact EMV approvals and certifications. Check with the acquirer/processor for additional information.

4.10 Other Considerations

While impossible to articulate every issue at every stakeholder's system involved in a contactless EMV transaction, some examples of additional things to consider are as follows: chip capability; data personalization method; hardware and composite material design of the payment device (card, fob or mobile); design of the device antenna (if contactless); the telecom network (fiber or wireless); and the number of unique firewalls and level and methods of encryption (point-to-point encryption (P2PE) or end-to-end encryption (E2EE)) or other security measures utilized, such as tokenization.

5. EMV Checkout Optimization

Faster EMV and contactless/NFC are two transaction processing methods that can reduce the cardholder interaction time with the terminal. There are also many other considerations, both for merchants and issuers, to help foster an efficient checkout process in terms of both the cardholder interaction with the terminal and the system processing time.

The goal of this section is to describe various additional approaches that have been used successfully to improve checkout time for an EMV transaction. There are likely other ideas not represented here. Please note that there may be many business factors to consider for these approaches beyond speed impacts. Some of these factors include cardholder experience considerations, technical feasibility for the business, availability from suppliers, and broad cost implications including both business and technical costs, and applicable industry rules and requirements.

Approaches reflected throughout this paper should be evaluated against overall business needs, requirements and strategies to determine relevance. Some of these approaches reflect merchant learnings while implementing EMV, while others are based on historical learnings in optimizing the checkout experience.

Finally, availability of some of the approaches in this section may differ by network. Please consult with acquiring processors and/or networks to understand relevant requirements.

5.1 Merchant Business Tactics to Optimize the EMV Checkout Experience

5.1.1 Consider Customer Options

When looking to optimize the EMV checkout process, consider the impact of customer options at the point of sale. A few examples of customer options during checkout include cash back, dynamic currency conversion, loyalty programs and receipt delivery options. While additional options can add value, they also may contribute to time in lane. As always, benefits should be weighed against costs. Review business requirements and check default settings on devices and software configurations to determine that appropriate options match business requirements.

Cash back may be an option for debit and certain credit transactions. Supporting cash back can complicate the payment sequence, lengthening in-lane transaction time.

Offering customers the option to pay in their home currency can also add steps during the checkout process. Consider the frequency of cross-border transactions to determine if dynamic currency conversion is an appropriate or necessary option.

Loyalty information collection and loyalty redemption may take place during the checkout process. If this is desired, merchants may wish to consider optimizing the transaction flow in order to reduce the impact on overall transaction processing time.

Moving receipt delivery to electronic methods reduces one point of customer interaction during checkout. In some cases, a customer may be able to opt out of a receipt entirely. Alternatively, offering customers the option to receive receipts via email or text message may reduce customer interaction and receipt printing time for subsequent transactions. Please consult legal partners regarding requirements for receipt delivery changes or opt-in/opt-out choices.

5.1.2 Ensure Efficiency of Prompts

Prompting optimization at the point of sale for both the customer and sales associate can result in a smoother payment experience. Consider where prompting is required while minimizing additional choices or options that may confuse a customer or slow the experience.

Prompting can potentially be removed or reduced in some cases. For example, there are opportunities to optimize prompting during CVM handling, around the "Total" screen, and during application selection.

Related to CVM optimization, supporting a "No CVM" kernel for low-value transactions may reduce customer interaction time. If No CVM is supported, a customer may not be required to sign or enter a PIN below a specified threshold in certain circumstances. Note: Refer to network specifications and work with the processor/acquirer to determine the appropriate No CVM threshold and additional certifications that may apply.

Where PIN is selected for processing by the chip card, review the PIN-related screen prompts. Screens like "Would you like to enter PIN? Y/N" can add time and confusion. Consider a PIN entry prompt process, especially for payment types with high PIN usage like debit. PIN bypass can also be supported from this screen for customers wishing to sign for their transactions. Where signature capture is prompted, consider prompting immediately, concurrent with EMV processing.

Review the screen flow and consider where combining or eliminating screens may be appropriate. Removal of unneeded screens can reduce both system processing time and customer interaction time. For example, many payment networks do not require the "Total" amount to be displayed for the customer before authorization. Where "Total" is required before authorization, consider adding the "Total" to the PIN prompt or signature screen (if signature is before authorization).

Understand the various methods used to support application selection, especially for U.S. debit cards. Currently in the U.S., there are two primary methods for debit prompting: PIN prompting and customer selection, each of which can be optimized.[18]

- PIN Prompting: With this implementation method, the merchant chooses the AID for processing and moves directly into EMV processing. For U.S. debit cards, Online PIN is the first CVM on the U.S. Common Debit AID, so this is often referred to as PIN prompting. Depending upon the screen flow design, moving directly into EMV processing, particularly for U.S. debit cards, can streamline the customer interaction and system processing time.
- Customer Selection: While prompting of AIDs for customer selection may be required for cards where multiple AIDs represent unique funding accounts[19], it is not required for cards containing only two AIDs pointing to the same funding account, such as for U.S. debit cards.[20,21] When

[18] For additional information on PIN bypass, see the U.S. Payments Forum white paper, "PIN Bypass in the U.S. Market," http://www.emv-connection.com/pin-bypass-in-the-u-s-market/.

[19] Contact the acquirer/processor for additional information on whether cardholder selection of AIDs is required.

[20] Application selection processes can be combined to optimize the cardholder experience. For example, the global AID can be removed from a "debit pair" (global debit AID linked to same source of funding as an associated U.S. Common Debit AID) before offering cardholder choice (EMV "Cardholder Selection") between a credit AID and a debit AID.

[21] For U.S. debit cards, the U.S. Common Debit AID accesses all networks available on the card for routing purposes; the global AID accesses only one network on the card.

choosing to implement customer selection, ensure that the screen prompt makes sense to the customer. Many implementations include the AID Labels or Application Preferred Names. These are programmed on the card by the issuer, but in some cases may not be helpful to the customer. Consider adding language on the screen to ensure the customer understands their choice.

While it may seem counterintuitive, in some cases, transaction timing may be improved by adding instructional prompting to the payment device. For example, consider prompting the customer to pre-insert once item scanning has begun. This allows the customer to find and insert the card into the terminal prior to completion of scanning. Similarly, if cash back is supported, prompting for cash back amounts prior to the total can reduce overall transaction time.

Processing errors can also be reduced by adding instructional prompts, especially at unattended terminals. Prompts such as "Please do not remove card" (once card is inserted) can minimize re-starts and reversals, which can improve transaction speed in aggregate and improve the customer experience. Similarly, adding language to help customers understand that PIN must be entered for cash back can reduce customer confusion and foster effective transaction completion. Finally, prompts can speed the transaction by assisting the customer with pre-programmed choices. For example, providing pre-programmed tipping amounts or percentages or cash back amount options may speed transaction time and increase convenience for the customer.

5.1.3 Educate to Foster Effective Checkout Experience

Well-trained sales associates improve customer satisfaction overall, while also reducing transaction time. Training associates on key elements of EMV transactions can proactively reduce frustration for customers, increase approval rates, improve in-lane transaction speed, and enhance the customer experience. Some EMV elements which may cause confusion include: premature card removal, improper insertion technique, and unavailable CVM options. Customer-facing infographics showing the steps of an EMV transaction can also foster efficient transactions and reduce customer confusion, particularly at unattended terminals.

5.2 Merchant Technical Approaches to Optimize the EMV Checkout Experience

5.2.1 Streamline Systems Processing

There are ways that merchants can optimize transaction processing times by streamlining systems processing. For starters, they can look at implementing parallel processing to perform authorization and non-authorization functions (e.g., loyalty) at the same time. Merchants can also look at the number of hand-offs between the card and their software applications, as the transaction process can slow whenever a new service or application is called. In addition, many applications perform health checks. These checks can be performed in ways that do not impact transaction speeds.

The terminal has a list containing the Application Identifier (AID) of every EMV application that it is configured to support. Once communication with the chip card is established, the terminal will begin to build the "candidate list" of applications that are supported by both the card and the terminal. The terminal may build the candidate list by querying the card to determine support for each individual AID in the terminal's AID list.

Alternatively, the terminal may attempt to request the Payment System Environment (PSE) from the card, which is a listing of all applications supported by the card. Requesting the PSE is optional for the terminal and supporting a PSE is optional for the card. If the PSE is supported by both card and terminal, this can greatly reduce the time necessary to build the candidate list by eliminating excessive queries to the card. This reduction in time can be noticeable where the terminal supports many AIDs. A typical U.S. terminal is likely to support at least six AIDs and quite possibly 10 or more. Therefore, merchants should consider supporting Application Selection using PSEs.

5.2.2 Optimize Network Communication

The packet size of an EMV transaction is typically larger than magnetic stripe and key-entered transactions, due the additional data elements being sent. To keep the POS environment optimized, merchants can evaluate their in-store network connectivity as well as connections to external service providers. In the petroleum space, this includes connectivity between the automated fuel dispensers (AFDs) and in-store environments. It is helpful to have an internal network engineer or third party networking consultant be involved in the review to determine any necessary additional bandwidth requirements. Merchants may also want to work with their payments solution and service providers to perform peak load testing to determine capacity of their network, and make sure it can handle the load of high volume transaction times.

Lastly, merchants using a dial-up connection as their primary or backup connectivity option can evaluate the connection's capability to handle the load of an EMV transaction efficiently. Certain baud rates may be able to handle a transaction size better than others. Pre-dial may also make overall transaction time via dial-up connection faster by overlapping processing functions. Merchants may also want to explore other backup connectivity options for wired or wireless implementations, including broadband, integrated services digital network (ISDN) and 4G-enabled routers.

5.2.3 Simplify Architecture

Another area that can impact the speed of transaction processing is the merchant's POS and payment architecture. This would include the number of connections, gateways, or "hops," it takes to get from the EMV reader to the card-issuing bank. Typically, the more hops added to the round trip of a transaction, the longer that trip will take. Simplified payment architectures may have the additional benefit of speeding up the EMV certification process, simplifying ongoing re-certification of the POS/payment solution, and limiting the scope of Payment Card Industry Data Security Standard (PCI DSS) audits.

In addition, it is important to set appropriate timeout settings for each internal and external connection in order to both make sure there is enough time to traverse the route and also to quickly identify when processes or connections are non-responsive. Nesting the timer values and late response reversal processes appropriately between processing connections and internal processes can also remove the opportunity for late system responses to impact processing.

5.3 Issuer Business Tactics to Optimize the EMV Checkout Experience

5.3.1 Consider Card Configurations and Functionality

There are several steps issuers/card bureaus can take in setting up EMV cards that can help in streamlining the interaction between the terminal and the card. The more records that have to be read

from the card, the more interactions that are needed between the card and the terminal, which could result in increased checkout time. Examples of card optimization include streamlining how the Application Elementary Files (AEFs) are set up and using the PSE file.

AEFs are typically the files and associated records that are defined within the Application File Locator which the terminal uses to read data from the card. Issuers should consider setting up the AEF information in as streamlined fashion as possible. This includes, but is not limited to:

- Avoid unnecessarily separating data into separate records. The terminal uses a separate command to read each record in each file, and the overhead for each command increases the time it takes to read the data. Grouping the data into fewer records will enable the terminal to read the data as efficiently as possible, improving the cardholder experience.
- Organize data by grouping related items together. This can include:
    - If using Dynamic Data Authentication (DDA) and/or Combined DDA/Application Cryptogram (CDA) Generation, organize information together such as issuer public key certificates, remainders, exponents and key indices
    - Organize ICC public key certificates, remainders and exponents together
    - Try to keep all data used for signing in a single record and avoid having multiple file records that will be signed

Issuers who are defining offline data authentication (DDA and/or CDA) on their cards may wish to consider the RSA key lengths being used. Longer RSA keys may negatively impact speed of both the terminal and the card, so issuers may wish to consider using key lengths that best represent key management policies of their institution. RSA keys should be long enough to enhance security without creating a burden on processing time. Note that decisions regarding key length must comply with applicable industry and/or legal rules and requirements.

There are two ways to support offline enciphered PIN. For optimizing transaction speed, issuers can consider using the ICC Public Key for PIN encryption rather than defining a separate ICC PIN Encipherment Public Key for this purpose. Defining the ICC PIN Encipherment Key adds additional processing on the terminal and also adds additional data records that must be read by the terminal.

The length used for the exponent component of RSA keys can significantly impact the overall processing time at both the card and the terminal. Longer exponent lengths should be evaluated to assess whether they measurably add to the strength of the RSA algorithm. EMV defines two values that may be used for the exponent value, 3 and 2^16+1. Issuers may wish to consider using the smaller of the two exponents “3,” when implementing RSA functionality for offline data authentication and/or offline PIN encryption on their cards. In addition, issuers may wish to consider using payment network certificate authority (CA) keys that utilize the smaller of the two defined exponent lengths when requesting the signing of their issuer public keys.

Issuers may want to consider the established baud rate (bps) personalized on the card. This establishes the maximum communication speed for data to be transmitted between the terminal and the card. Traditionally, cards were setup with a communication speed of 9600 bps; cards can now be configured to allow faster communications (at least double or 19.2 Kbps). Issuers and/or their card bureaus should

validate what communication speeds the chip has been set up for and evaluate whether or not this can be increased.[22]

Another consideration from an issuing perspective is the use of the PSE to help streamline the checkout process. The terminal can request the PSE from the card, which is a listing of all applications supported by the card. If the PSE is supported by both card and terminal, this can greatly reduce the time necessary to build the candidate list by eliminating excessive queries to the card.

EMV allows issuers to offer new card products personalized with multiple funding accounts such as debit, credit and prepaid. Using such cards may add more time to the card and terminal interaction, as cardholders may have to choose the "product" they want to perform the transaction. Issuers wanting to implement such cards may wish to consider the implications to the cardholder experience and how best to ensure that the cardholder understands what will be displayed to them on the terminal screen, and what implications there will be for the cardholder choice.

Finally, when issuing U.S. debit cards, appropriate naming of AID Labels and Application Preferred Names may help to reduce transaction time. These are programmed on the card by the issuer, but may also be presented to the cardholder during the checkout process if the merchant uses Cardholder Selection to select the AID the transaction will use. Appropriate labels are helpful to the cardholder and should convey enough information so that the cardholder understands their choice.

5.3.2 Offer Cardholder-Selected PIN

To foster effective PIN use at the ATM and in the checkout process, issuers may allow the cardholder to select their own PIN. This enhances the ability for the cardholder to remember the PIN and input it accurately. To foster effective management of the PIN lifecycle, other PIN functions such as PIN reminder, PIN reset and PIN change can be used wherever the cardholder is allowed to select the PIN.

5.3.3 Educate to Foster Efficient and Informed Card Usage

Effective cardholder education can be a factor in improving the efficiency of the checkout process. Purposeful, appropriately timed messaging may be especially useful. Especially when cardholder action is needed, construct communication based on the cardholder's point of view. To meet the cardholder where they are, consider presenting desired messages in all channels where direct cardholder engagement is supported.

There are three key phases to cardholder communication: before issuance, at issuance and after issuance. The messages shared during each of these times may be different. The U.S. Payments Forum resource, Recommended Communication Best Practices,[23] suggests the following focus at each phase:

1. Prior to card issuance: focus on awareness
2. At the time the card is issued: focus on activation, security benefits and use of the card
3. On an ongoing basis after the card is issued: focus on continual education

[22] Older terminals may not support higher communication speeds, but will process these cards at the highest rate at which they are capable.

[23] http://www.emv-connection.com/recommended-communications-best-practices/

To foster efficient card use during checkout, provide information about the checkout at POS from the cardholder's perspective. Items which may be helpful to highlight regarding using the card at an EMV payment terminal include: (1) that the card is inserted rather than swiped; (2) that PIN entry or signature may be requested based on the card's profile; and (3) that the card should remain in the terminal until the terminal presents messaging to remove the card. Especially during the EMV migration in the U.S., it may also be helpful to note that the card will still be accepted by using the magnetic stripe if the payment terminal at the merchant is not EMV capable.

6. Conclusion

Thus far, the primary focus of the EMV migration in the U.S. has been on stakeholders becoming EMV enabled to prevent card-present fraud. Now that the industry is seeing increasing volumes of chip-on-chip transactions, the U.S. Payments Forum leveraged feedback from cardholders and merchants to identify themes and pain points. This publication was produced in response to one of the loudest pain points – EMV transaction speed at the point-of-sale terminal.

Four general solutions are put forth in this document for stakeholders to consider to improve transaction times at the point-of-sale: Faster EMV, faster card-terminal transmission speeds, contactless/NFC, and EMV checkout optimization. These approaches are based on best practices from EMV migrations in many other large countries, best practices from the U.S. EMV migration, and a new capability to improve the point-of-sale experience in response to this issue in the U.S. Some of these approaches reduce the cardholder-perceived transaction time, improving the cardholder experience with little impact on the overall transaction time, while others reduce the actual transaction time. When designing a comprehensive merchant checkout experience, it is important to take all of these factors into account.

The specific approaches presented in this document may not be appropriate for every payment scenario in the U.S. Each stakeholder should consider available options and corresponding implications in light of its respective cost-benefit analysis and customer experience goals. The U.S. Payments Forum also encourages ongoing conversation between each stakeholder and its partners to ensure the details of each approach are understood and considered.

7. Legal Notice

While great effort has been made to ensure that the information in this document is accurate and current, this information does not constitute legal advice and should not be relied on for any legal purpose, whether statutory, regulatory, contractual or otherwise. All warranties of any kind are expressly disclaimed, including all warranties relating to or arising in connection with the use of or reliance on the information set forth herein. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk.

Without limiting the foregoing, it is important to note that the information provided in this document is limited to the specific approaches, payment networks and other factors as expressly described herein, and that applicable rules, requirements, configurations and transaction processes may impact or be impacted by the specific circumstances of a given implementation and related results and/or liabilities.

Additionally, note that specific payment networks and/or acquirers/processors determine their own respective rules, requirements, policies and procedures for transaction processing, liability and other matters, all of which are subject to change.

Merchants, issuers, acquirers, processors and others implementing EMV chip technology in the U.S. are therefore strongly encouraged to consult with their respective payment networks, acquirers/processors, and appropriate professional and legal advisors regarding all aspects of implementation, including but not limited to applicable rules, requirements, policies and procedures.

Nothing in this document constitutes or should be construed to constitute an endorsement or recommendation of any particular approach, service or provider, and all implementation decisions and activities should be properly reviewed in light of applicable business needs, strategies, requirements, industry rules, and laws.

8. Appendix: Faster EMV Questions and Answers

In the course of the development of this white paper, many questions about Faster EMV arose from industry participants in the U.S. Payments Forum. All efforts were made to address those questions within the Faster EMV section of the white paper. This appendix consists of those questions that did not fit directly within the structure of the white paper. Note that questions submitted may have been combined for clarity and brevity.

Additional information on testing and certification is discussed in more detail in the U.S. Payments Forum white paper, "EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community."[24]

General Questions

Q1. Who are the best candidates to implement Faster EMV?

A. Merchants and deployers will need to determine whether Faster EMV meets their business needs based on the descriptions and considerations provided in the white paper, "Optimizing Transaction Speed at the POS."

Q2. What is the impact of Faster EMV to merchant's/acquirer's batch settlement processes? Would this code change impact settlement certification?

A. Because no Transaction Certificate (TC) was generated, the ARQC and associated data elements should be used for settlement where chip data is required. This is the same process used when clearing deferred authorizations. If deferred authorizations are not currently supported, then changes may be required to the settlement process. No requirements for settlement re-testing have been announced. Note that the AAC generated by the terminal during Faster EMV processing is not a "decline" from a business process standpoint. This AAC should not be returned in clearing, but rather the ARQC (with associated data elements) should be used, as is done when clearing deferred authorizations.

Q3. Are there implications for chargeback exposure with Faster EMV processes?

A. Faster EMV processing is intended for online-only environments. Faster EMV transactions receive the same chargeback protection as traditional EMV with online authorization. The same fraud liability shift applies for Faster EMV transactions; merchants therefore should ensure they obtain the appropriate CVM to protect themselves from the lost/stolen liability shift.

Q4. Can Faster EMV be used in store-and-forward mode?

A: Faster EMV is a very similar process to Deferred Authorization as discussed in the U.S. Payments Forum white paper, "Merchant Processing during Communications Disruption," available at http://www.emv-connection.com/merchant-processing-during-communications-disruption/. Cryptograms obtained during a Faster EMV process can be used for a deferred authorization.

[24] U.S. Payments Forum, "EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community," December 2016, http://www.emv-connection.com/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/

Q5. Are there implications for offline approval processing with Faster EMV processes?

A. Faster EMV processing is intended for online-only environments. Within those environments, there are no such implications. When an EMV card is used in an offline-capable environment, normal offline controls apply (assuming the card supports offline approval processes).

Q6. When would the Last Online Application Transaction Counter (ATC) increment during a Faster EMV transaction?

A. The Last Online ATC would not increment until the next transaction where the online response goes back to the card (i.e., the next traditional EMV transaction).

Q7. Does a Faster EMV transaction register as an offline transaction for the counter on the chip? If so, are there implications with Lower Consecutive Online Limit (LCOL)/Upper Consecutive Online Limit (UCOL)?

A. It depends on card personalization, but generally, issuers do not personalize cards to consider "declines" (AAC) when counting offline transactions, meaning counters and amount accumulators would not increment; therefore, Faster EMV transactions would not register as offline transactions.

Q8. Will offline counters on the chip ever be reset in a Faster EMV transaction?

A. No. Counters are only reset when the card is used in a traditional EMV transaction. Note that there are no implications when the card is being used in an online-only environment.

Q9. Are there certain offline-preferring merchant categories (e.g., transit and airplane terminals) where there are challenges with accepting cards that have been used previously in Faster EMV transactions?

A. If a merchant attempts an offline authorization, previous Faster EMV transactions will not impact the current state of the card accumulators. If PIN management scripting (PIN Change, PIN reset) was attempted during the prior Faster EMV transaction, the scripts would not have applied to the card and this may impact the PIN functionality during the attempted offline transaction. Deferred authorization transactions may also be available in these environments.[25]

Q10. Do the Card Verification Results (CVRs) display the same result with Faster EMV as they do with traditional EMV?

A. The CVRs using Faster EMV will still display the same information as they do for traditional EMV transactions.

Q11. What happens with Issuer Authentication failure on last online transaction or Issuer Authentication not performed when Issuer Authentication is mandatory?

A. With a Faster EMV process, the EMV processing will be completed with no expectation of Issuer Authentication processing, since the transaction is completed as unable to go online, with an AAC request. Refer to the payment network specifications for additional details.

[25] Additional information can be found in the white paper, "Merchant Processing during Communications Disruption," available at: http://www.emv-connection.com/merchant-processing-during-communications-disruption/.

Q12. Does Faster EMV impact clearing for the issuer?

A. Faster EMV transactions will be cleared using the ARQC (and associated data elements), rather than a TC. This is the same process followed for clearing deferred authorization transactions, as well as for 'online data capture' (i.e., single message) transactions.

Q13. How would offline PIN management be conducted for a Faster EMV transaction?

A. Offline PIN as a Cardholder Verification Method (CVM) works with Faster EMV transactions. Offline PIN management actions (i.e., PIN change, or PIN Unblock) will not occur in a Faster EMV transaction. To provide a consistent consumer experience, issuers may prefer to use ATMs or the branch infrastructure, if available, to manage issuer scripting messages to cards to synchronize offline PINs with the online PIN on the host, or to reset offline PINs.

Q14. Are there recommendations for incremental controls being added to EMV contact cards that may encounter Faster EMV merchants?

A. There are no additional controls recommended for contact chip cards that may encounter a merchant that has implemented Faster EMV. Faster EMV is simply a variant of an always-online merchant.

Q15. What are the implications for application blocking if scripting is no longer possible?

A. Application blocking is intended to prevent a chip card application from being used for offline approvals. Application blocking is not needed in an online-only environment.

Q16. How will cash back processing work with Faster EMV?

A. Cash back can be implemented in the same way as in a traditional EMV environment provided the cash back amount is known once the AID has been selected at the beginning of the EMV transaction. If the transaction is to be processed as Faster EMV, the Amount, Authorized field (tag 9F02) should be populated with the sum of the placeholder amount and the cash back amount. All other amount fields should be populated as for a traditional EMV cash back transaction.

Q17. How will No CVM offerings work with these solutions?

A. No CVM processing with Faster EMV is available, either through use of a predetermined amount for the cryptogram or by implementing Faster EMV using the final transaction amount for the cryptogram.

For merchants choosing to use the final amount for the cryptogram, the implementation of No CVM is similar to traditional EMV. The merchant can leverage the No CVM kernel configuration for transactions under the network rule No CVM limits, and capture the applicable CVM for transaction amounts over the No CVM limit.

For merchants choosing to use a predetermined amount for the cryptogram, care should be given to the selection of the predetermined amount. Different predetermined amounts will yield different customer experiences and may have liability implications for certain transactions. Merchants setting their Faster EMV predetermined amount based on the desire to have No CVM as the primary CVM for transactions must understand that their Faster EMV terminal will not prompt for PIN or signature, regardless of the actual transaction amount. Although a signature may be obtained out of band should the amount exceed the merchant's

established NO CVM limit, failure to capture a PIN could open the merchant to chargebacks on PIN-preferring lost or stolen cards on transactions over the amount of the network rule limits.

Some options to mitigate this chargeback exposure may include the following. All options may not be available on all payment networks.

a. Capturing a signature for signature-preferring credit-based transactions over the network rule No CVM limits,

b. Capturing an online PIN (outside of EMV processing) to include in the authorization request message for U.S. debit transactions over the network rule No CVM limits,

c. Using another processing method for high dollar transactions (NFC, traditional EMV, using the final amount method for Faster EMV). This option may include use of a differently programmed payment terminal, or

d. Setting the placeholder amount to an amount that is greater than the No CVM limit and applying the CVM logic while the card is in the terminal, but only request an online PIN or signature if the final amount is greater than the CVM limit.

The extent to which these measures reduce chargeback risk vary. Merchants should contact their acquirer to understand the details of each network's specification, liability shift, and other chargeback exposure.

Q18. Are there guidelines for the placeholder amount? Do these vary by merchant category?

A. There is no guidance on how to choose the placeholder amount as this is determined by each merchant. In some environments the actual amount will be available earlier in the process and this amount can be used instead of the placeholder amount. For these environments, the benefit of Faster EMV is being able to withdraw the card from the reader while the authorization message is sent to the issuer. Where a placeholder amount is used, its value must be greater than zero. Placeholder amounts for No CVM environments are discussed above.

Q19. Are there any data indicators in the authorization message that let the acquirer/issuer know that the transaction is a Faster EMV transaction?

A. Faster EMV transactions are processed identically to deferred authorization transactions, and contain no special indicators.

Q20. Can Faster EMV support merchant routing choice for debit transactions?

A. Faster EMV for debit supports merchant choice using the principles outlined in the EMV Migration Forum white paper, U.S. Debit EMV Technical Proposal.[26] Merchants and acquirers should consult with their existing and prospective debit network relationships to determine the manner in which Faster EMV is deployed and supported, as well as the operating rules that govern its support and what it means to them.

[26] http://www.emv-connection.com/u-s-debit-emv-technical-proposal/

Q21. Does Faster EMV work with PINless debit?

A. Faster EMV is compatible with PINless debit. Merchants and acquirers should consult with their existing and prospective debit network relationships to determine the manner in which Faster EMV is deployed and supported, as well as the operating rules that govern its support and what it means to them.

Q22. Are there considerations for unattended devices when implementing Faster EMV?

A. Unattended POS devices may have different abilities (such as extended support for No CVM transactions) or restrictions (such as lack of support for signature as a CVM), when compared to attended POS. These abilities and constraints remain in place with Faster EMV implementations. Implementation of Faster EMV should still adhere to the fundamental business requirements for unattended devices. Please contact the relevant payment networks for information on specific requirements for unattended devices.

Q23. What certifications are required for Faster EMV? Have the payment networks and acquirers determined whether recertification will always be required? Never required? If it depends, what are the criteria?

A. Testing and certification for Faster EMV implementations are discussed in the updated white paper, "EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community," available at http://www.emv-connection.com/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/.

Q24. What are the time savings using Faster EMV? A couple of retailers reportedly have implemented it – what efficiencies are they seeing?

A. Since Faster EMV implementations are relatively new, there are currently no baselines for comparisons.

Petro/Automated Fuel Dispenser (AFD) Q&A

Q25. If implementing Faster EMV (inside or outside at a petro merchant), what dollar amount should be used to create the cryptogram? The pre-authorization amount? The maximum sale amount? A different amount?

A. There are no changes to the payment networks requirements for fuel transaction processing when implementing Faster EMV solutions. Typically, retail fuel purchases use preset preauthorization amounts (either a single dollar or a preset estimated amount). These amounts can be used for the cryptogram amount. In other cases, the actual transaction amount is known when the cardholder specifies a particular amount to purchase. In these cases, the actual amount can be used for the cryptogram amount. Contact the acquirer or payment network for more details how Faster EMV works with AFDs.

Q26. When creating the cryptogram for Faster EMV, are there amounts that should not be used (e.g., the standard amounts that payment networks use for automatic fuel dispenser (AFD) pre-authorizations)?

A. Each payment network's specifications indicate that a zero-dollar amount should be avoided.

Q27. Can a petro merchant store use "traditional EMV" inside and Faster EMV outside or vice versa?

A. From a processing standpoint, there is no connection between using traditional EMV at one device and Faster EMV at another. Using both forms of processing will have implications for testing and certification. See the white paper, "EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community," available at http://www.emv-connection.com/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/.

Q28. What is the recommended prompting sequence at the pump when using Faster EMV?

A. It is recommended that merchants and their developers provide logical prompts to guide the consumer through making the payment. Changes to accommodate traditional EMV may be amended to address the Faster EMV transaction sequence of the process. The Forum recommends, however, that petro merchants contact their acquirers and the payment networks to discuss their unique implementations of Faster EMV.

Q29. Does car wash payment at the pump impact ability to use Faster EMV?

A. The current process for supporting car wash payments should not be affected by Faster EMV. The amount of the car wash will be included in the final transaction amount. If the car wash amount is not included currently in the authorization amount, there is no change for a Faster EMV transaction.

Legal Notices

All answers in this Appendix were prepared and validated by the members of the "Optimizing Transaction Speed at the POS" white paper project team, including but not limited to representatives of member acquirers, issuers, payment networks and other stakeholder groups.

While great effort has been made to ensure that the information in this document is accurate and current as of the publication date, this information does not constitute legal advice and should not be relied on for any legal purpose, whether statutory, regulatory, contractual or otherwise. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk. All warranties of any kind, whether express or implied, relating to this document, the information set forth or otherwise referenced herein or the use thereof are expressly disclaimed, including but not limited to all warranties relating to or arising in connection with the use of or reliance on the information set forth herein, all warranties as to the accuracy, completeness or adequacy of such information, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement.

Without limiting the foregoing, it is important to note that the information provided in this document is limited to the specific approaches, payment networks and other factors as expressly described herein, and that applicable rules, requirements, configurations and transaction processes may impact or be impacted by the specific circumstances of a given implementation and related results and/or liabilities.

Additionally, note that specific payment networks and/or acquirers/processors determine their own respective rules, requirements, policies and procedures for transaction processing, liability and other matters, all of which are subject to change.

Merchants, issuers, acquirers, processors and others implementing EMV chip technology in the U.S. therefore are strongly encouraged to consult with their respective payment networks,

acquirers/processors, and appropriate professional and legal advisors regarding all aspects of implementation, including but not limited to applicable rules, requirements, policies and procedures.

Nothing in this document constitutes or should be construed to constitute an endorsement or recommendation of any particular approach, service or provider, and all implementation decisions and activities should be properly reviewed in light of applicable business needs, strategies, requirements, industry rules, and laws.

Comments or recommendations for edits or additions to this document should be submitted to: transaction-speed@uspaymentsforum.org.