Quick Chip for EMV® and qVSDC — Specification

Version 2.0

July 2017

Visa Public

Important Information on Confidentiality and Copyright

Contents

Tables

Figures

1 About This Specification

This specification introduces modifications to the use of standard processes for contact chip transactions that is compatible with EMV kernels and optimizes processing time by removing or reducing dependencies for chip insertion time in the reader, referred to as Quick Chip.

Version 2 of this specification adds guidance for supporting EMV contactless, i.e., qVSDC (quick Visa Smart Debit Credit), with Quick Chip.

1.1 Scope

This specification is published as a companion document to [AIG], [VIS], and [VCPS]. It defines the modified use of standard EMV processing at the Point of Sale to enable a Quick Chip transaction over the contact interface.

In addition to Quick Chip for contact chip transactions, this specification also provides guidance on supporting qVSDC transactions to achieve a similar user experience. In this document, the contactless version will be referred to as "Quick Contactless".

The Quick Contactless sections are applicable to all qVSDC form factors (e.g. cards, mobile devices, wearables), although the term "card" is used.

Note that MSD processing is out of scope for this document and should not be supported.

1.2 Audience

This document is intended for Visa employees, clients, merchants, regions, and vendors supporting the Quick Chip solution, or supporting contactless transactions.

Quick Chip processing is intended for use at any acceptance point where timeliness (perceived or actual) is critical, such as multi-lane retail, QSR, and Convenience merchants, as well as unattended locations (including ATMs[1]).

[1] ATMs should not perform Quick Chip for EMV processing for PIN management transactions.

1.3 Reference Materials

The following documents are referenced in this specification.

[AIG]	Visa Smart Debit/Credit and Visa payWave U.S. Acquirer Implementation Guide (all active versions).
[EMV]	EMV ICC Specifications for Payment Systems, Version 4.3, November 2011, and all published updates. Integrated Circuit Card Specifications for Payment Systems.
[VCPS]	Visa Contactless Payment Specification, including published updates: • Version 2.1[2], May 2009, or • Version 2.2, January 2016.
[VIS]	Visa Integrated Circuit Card Specification, including published updates: • Version 1.5, June 2009, or • Version 1.6, January 2016.

[2] If using a VCPS 2.1 kernel, MSD should not be supported. This can be accomplished by setting Terminal Transaction Qualifiers byte 1 bit 1 to 0b. All cards in market are qVSDC capable, so there is no additional benefit to supporting MSD.

2 Quick Chip Introduction

The Quick Chip solution allows for early removal of the chip card from the terminal, while relying on standard EMV processing between the card and terminal. It removes the need for EMV processing to wait for the final transaction amount, authorization response, and post-authorization processing (such as script processing and issuer authentication). This functionality is already present in [VCPS], and can be implemented with the configuration as described in section 4 of this document. It is strongly recommended that Quick Chip and Quick Contactless are implemented together.

Quick Chip:

- Significantly reduces time of card in terminal as part of critical path, by eliminating dependencies, allowing for improved throughput.
- Provides the same EMV level of security for online authorizations, including the cryptogram.
- Improves consumer perceived throughput time (particularly important where the cardholder hands over their card to a clerk).
- Lessens cardholder friction by reducing wait time for card removal, consequently also reducing the frequency of cardholders leaving their card behind in the terminal.
- Integrates with US Common Debit AID processing.
- Integrates with VEPS[3] processing.
- Supports all cardholder verification methods.

Quick Contactless:

- Requires a simple tap of the card for improved throughput.
- Provides the same EMV level of security for online authorizations, including the cryptogram.
- Card always remains in the cardholder's possession.
- Similar to Quick Chip processing.

Quick Chip processing has no impact on the EMV kernel or the EMVCo Level 2 approval of the kernel. The timing of when the payment application invokes EMV processing may change, but all necessary EMV processes will be performed (see Table 1 for a comparison of Quick Chip and traditional EMV processing). Quick Chip is a modification to the payment application around the EMV kernel that lessens the time the card remains in the terminal by allowing a contact chip transaction to mimic much

[3] Visa Easy Payment Service (VEPS) allows qualified merchants to process small value transactions without requiring a Cardholder Verification Method or issuing a transaction receipt (unless requested by the cardholder).

of what takes place today on contactless chip transactions, and is based on Visa's best practices for deferred authorization.

Table 1: Comparison of Quick Chip and Traditional EMV Processes

Chip Processing Function	Traditional EMV	Quick Chip
Application Selection	✓	✓
Initiate Application Processing	✓	✓
Read Application Data	✓	✓
Offline Data Authentication	✓	✓
Processing Restrictions	✓	✓
Cardholder Verification	✓	✓
Terminal Risk Management	✓	✓
Terminal Action Analysis	✓	✓
Card Action Analysis	✓	✓
Online Authorization	✓	✓
Completion	✓	✓
Post-Authorization Card Processing	✓	

Traditionally, two factors associated with standard contact chip processing can make the transactions potentially slower than magnetic stripe transactions, while significantly increasing the perception that the transaction is slow:

- The chip terminal waiting for the final amount before completing cardholder verification method processing and requesting data for online authorization from the card.
- The card remaining in the reader until the authorization response is received from the issuer.

Both the Quick Chip solution and Quick Contactless overcome these constraints.

2.1 Quick Chip Processing Overview

Quick Chip transactions are always authorized online. This allows the card to be removed before the online response is returned, while the merchant uses the issuer's online response to determine whether the transaction is approved or declined. As with magnetic stripe processing, the cardholder can dip the card at any time during the check-out process.

The Quick Chip solution works as follows:

1. As soon as the card is inserted into the reader, the Quick Chip transaction may begin. The payment application requests the data to perform an online authorization from the EMV kernel, using either the final transaction amount (if known) or a pre-determined amount (see section 3.1 for further information) as the Amount, Authorized (tag '9F02').

2. The card and EMV kernel perform standard EMV processing to select the application (including cardholder choice or confirmation of the application, if applicable), initiate application processing, read the application data, and perform cardholder verification and other risk management checks. The EMV kernel requests an online authorization cryptogram from the card.

3. The card performs card risk management and either declines the transaction offline (uncommon) or provides to the EMV kernel the data for an online authorization request, including an authorization request cryptogram (ARQC). The EMV kernel provides to the payment application the chip data for an authorization request message.

4. In order to allow the card to be removed from the payment terminal in advance of the authorization response, a Quick Chip transaction is completed as a deferred authorization. The payment application immediately completes the EMV processing. Completing the EMV processing allows for prompting to remove the card from the terminal.

5. Until the final[4] amount is available, the payment application temporarily stores the authorization data from the EMV kernel. Once the final amount is available, the final amount is placed in non-chip data (Field 4) of the authorization message. The EMV data is placed in chip data (Field 55) of the authorization message, where the amount used in step 1 is placed in tag '9F02' of Field 55. The payment application sends the authorization request online.

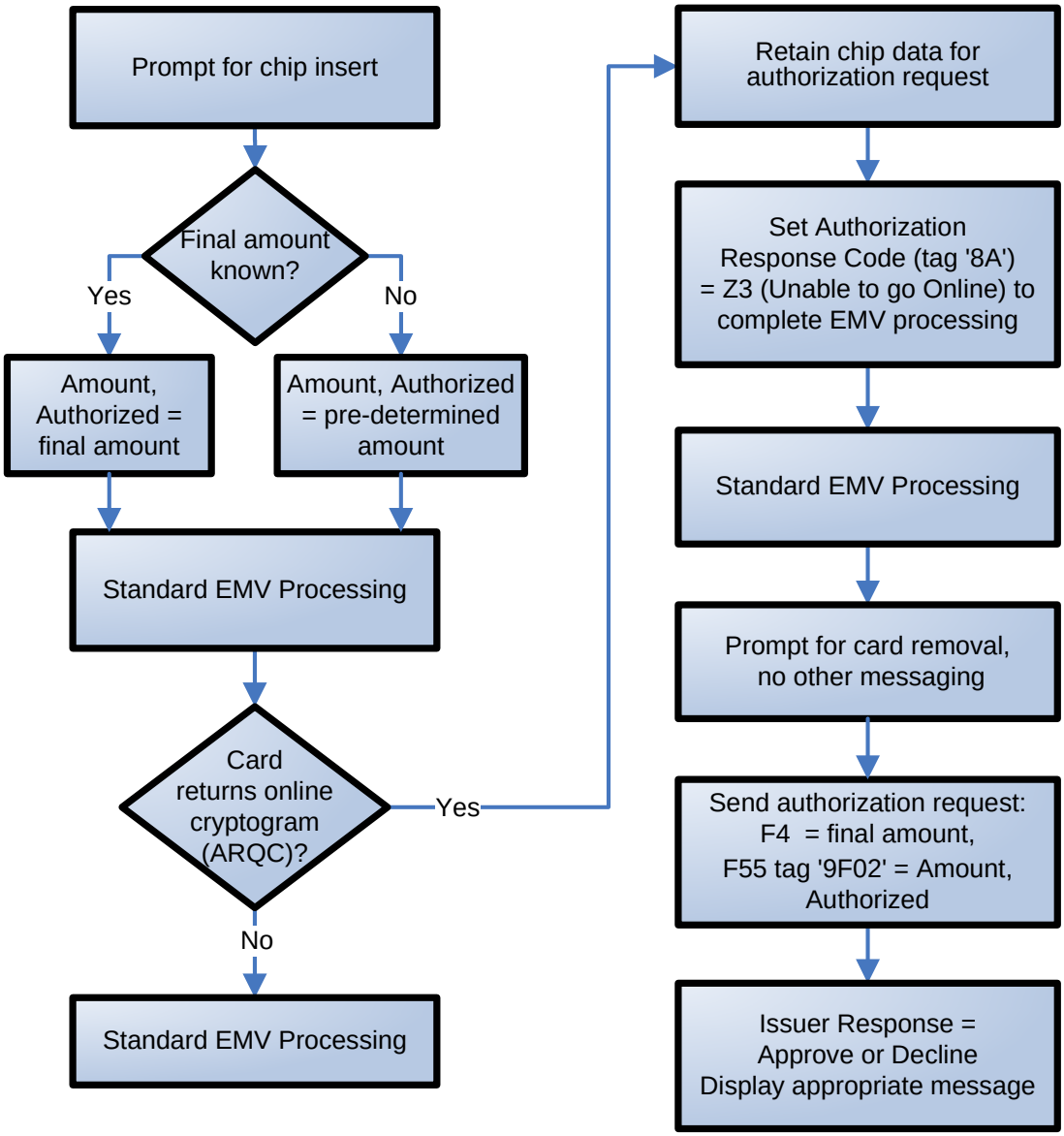
   Note: *Using Quick Chip, the insertion, reading, and subsequent removal of the card may occur while the sales transaction is being rung up; i.e., before the final amount is known.*

[4] Quick Chip does not change the Field 4 amount used for authorization. Merchant segments, such as fuel retailing and T&E, may typically authorize for a nominal amount (e.g., $1) or an estimated amount. These segments should continue to follow current authorization requirements for their segment, if Quick Chip is implemented. Where the nominal or estimated amount is known at the time of card insertion, it can also be used as the final amount for ARQC creation.

6. The issuer host uses Field 4 (Amount, Transaction) as the actual amount to score / approve the transaction while reserving Field 55, tag '9F02' (Amount, Authorized) for cryptogram validation.

7. The online response to the payment application indicates whether the transaction was approved or declined (as is the case today for magnetic stripe). The payment application now displays the appropriate messages to indicate whether the transaction was approved or declined.

Figure 1: Quick Chip Processing Overview



Note: *The processing flow is illustrative. The processing principles can be used to construct any flow that supports business needs.*

2.2 Quick Contactless Processing Overview

Quick Contactless transactions are always authorized online. As with magnetic stripe processing, the cardholder can tap the card at any time during the check-out process.

Note that the Quick Contactless transaction described here simply makes use of a placeholder amount when the final amount is not known. There are no changes to the qVSDC kernel to achieve this transaction experience.

The Quick Contactless solution works as follows:

1. As soon as the card is tapped on the reader, the contactless transaction begins. The payment application requests the data to perform an online authorization from the qVSDC kernel, using either the final transaction amount (if known) or a pre-determined amount (see section 3.1 for further information) as the Amount, Authorized (tag '9F02').

2. The card and qVSDC kernel perform standard processing to select the application, initiate application processing, read the application data, and perform other risk management checks. The qVSDC kernel requests an online authorization cryptogram from the card.

3. The card performs card risk management and provides to the kernel the data for an online authorization request, including an authorization request cryptogram (ARQC). The qVSDC kernel provides to the payment application the chip data for an authorization request message.

4. Until the final[5] amount is available, the payment application temporarily stores the authorization data from the qVSDC kernel. Once the final amount is available, the final amount is placed in non-chip data (Field 4) of the authorization message. The required transaction data is placed in chip data (Field 55) of the authorization message, where the amount used in step 1 is placed in tag '9F02' of Field 55. Lastly, if the amount is above the VEPS limit, Cardholder Verification shall be performed as required in the Card Transaction Qualifiers (CTQ). If the final amount is below the VEPS limit, the payment application may disregard the CVM requirements in the CTQ. The payment application sends the authorization request online.

   Note: *For Quick Contactless, the card tap may be performed before the final amount is known or after, but it should align with contact Quick Chip.*

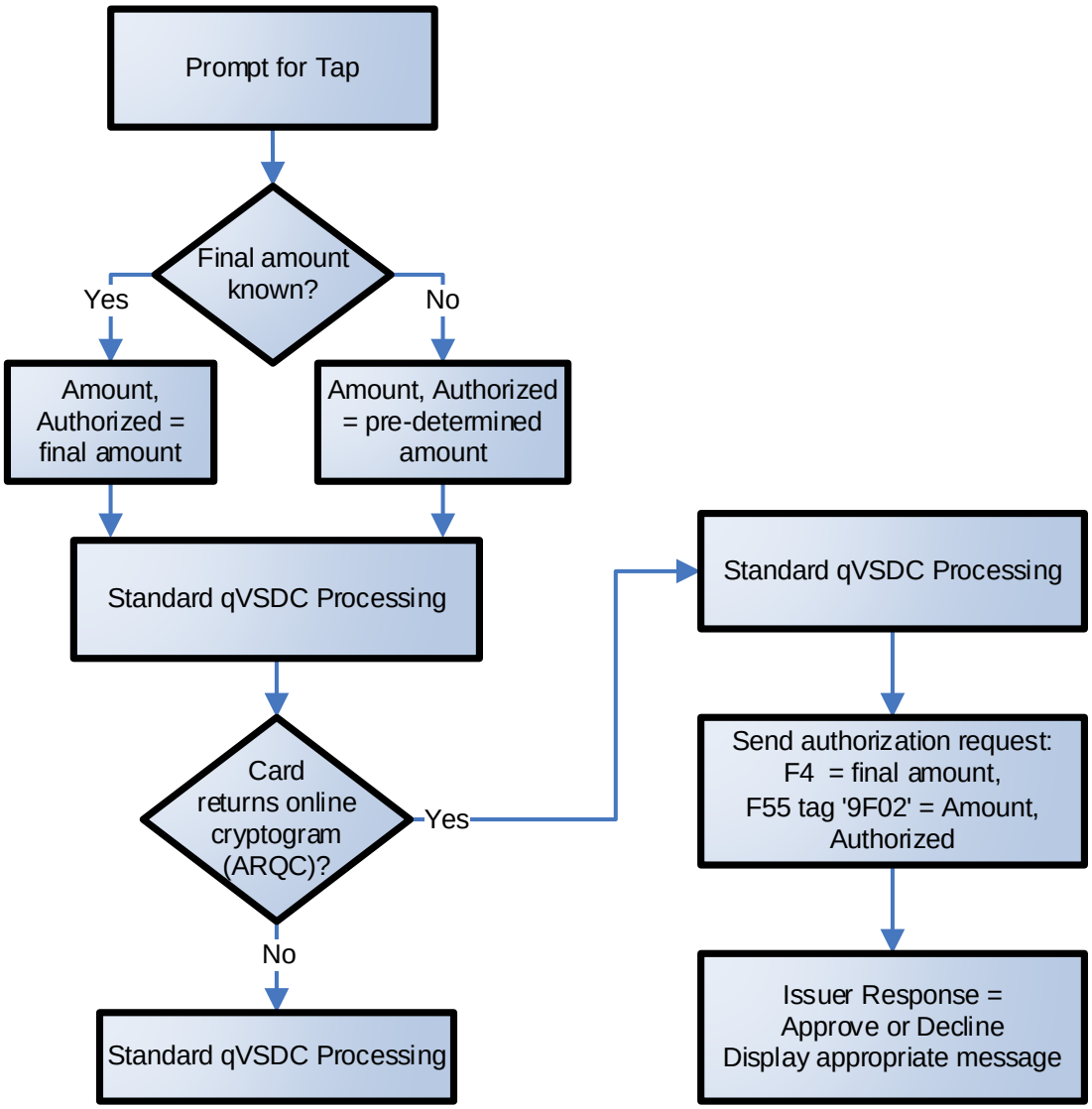
[5] qVSDC does not change the Field 4 amount used for authorization. Merchant segments, such as fuel retailing and T&E, may typically authorize for a nominal amount (e.g., $1) or an estimated amount. These segments should continue to follow current authorization requirements for their segment, when qVSDC is implemented. Where the nominal or estimated amount is known at the time of card insertion, it should be used as the final amount for ARQC creation.

5. The issuer host uses Field 4 (Amount, Transaction) as the actual amount to score / approve the transaction while reserving Field 55, tag '9F02' (Amount, Authorized) for cryptogram validation.

6. The online response to the payment application indicates whether the transaction was approved or declined (as is the case today for magnetic stripe). The payment application now displays the appropriate messages to indicate whether the transaction was approved or declined.

   Note: *For Quick Contactless, Issuer Update Processing, also known as 2-tap, should not be supported.*

Figure 2: Contactless Processing Overview



Note: *The processing flow is illustrative. The processing principles can be used to construct any flow that supports business needs.*

3 Quick Chip Requirements

All Quick Chip transactions must be authorized online. Quick Chip is suitable only for Online Only terminal configurations.

The EMV Terminal Floor Limit shall remain at zero for Quick Chip transactions. This in combination with the TAC-Online Transaction Exceeds Floor Limit (Byte 4, bit 8) = 1 will result in the EMV kernel requesting an Authorization Request Cryptogram (ARQC) from the chip card.

Note: *If the merchant wishes to use Quick Chip processing for only some of their card brands, then the merchant should make sure to enable Quick Chip processing for the AIDs of the brands they wish to support.*

3.1 Quick Chip Amount Considerations

For a Quick Chip transaction, the payment application does not need to wait for the final amount to be known before the EMV processing can take place between the card and terminal. The amount sent to the EMV Kernel is either the final amount (if known), or a pre-determined amount.

- If the final[6] amount of the transaction is known, then the final amount shall be sent to the EMV kernel for tag '9F02' (Amount, Authorized).
- If the final amount is not yet known, then a pre-determined amount shall be sent. The pre-determined amount shall not be zero, but could be any other value consistent with the requirements of the merchant's processing environment. This allows the card and kernel interaction for EMV to begin without waiting for the final amount.

3.2 Quick Chip and Cashback Considerations

Quick Chip processing supports cashback functionality the same way cashback is supported for traditional EMV transactions.

Note: *The terminal may wait until the Application Usage Control (AUC) has been read from the card, to check whether cashback is allowed by the issuer, before offering cashback to the cardholder. If the cardholder has already indicated they want to sign for a debit transaction (by choosing "credit" instead of "debit"), they shall not be offered cashback.*

[6] Actual, nominal, or estimated. See footnote 4.

The terminal may prompt for Online PIN when needed (e.g., for a cashback transaction), even if CVM List processing does not result in the Online PIN being requested as a CVM. In order to ensure the PIN-related indicators are set correctly in the Terminal Verification Results (TVR) before cryptogram generation, the prompt for Online PIN entry shall be performed before completion of the Cardholder Verification phase of the EMV transaction.

If cashback is offered, the cashback amount shall be requested from the cardholder prior to requesting the first Application Cryptogram from the card. The cashback amount shall be sent to the EMV kernel for tag '9F03' (Amount, Other), and is included in the amount sent to the EMV kernel for tag '9F02' (Amount, Authorized).

- If the final amount (actual, nominal, or estimated) of the transaction is known, then the final amount (including the cashback amount) shall be sent to the EMV kernel for tag '9F02' (Amount, Authorized).
- If the final amount is not yet known, then the sum of the pre-determined amount plus the cashback amount shall be sent to the EMV kernel for tag '9F02' (Amount, Authorized).

3.3 Quick Chip CVM Considerations

Quick Chip follows standard CVM List processing. Quick Chip supports Signature, Online PIN, Offline PIN, and No CVM as cardholder verification methods.

For implementations that initiate chip processing when the final amount is not yet known and PIN is the chosen CVM for a transaction, no amount shall be displayed on the PIN entry panel.

Amount confirmation is not recommended for Quick Chip. If implemented, amount confirmation should be performed prior to submitting the authorization request message.

When signature is the selected CVM, printing/displaying the signature panel is normally deferred until the authorization response is received, as is done for non-Quick Chip transactions.

3.4 Quick Chip and VEPS Considerations

Quick Chip is compatible with VEPS.

At a VEPS eligible merchant, where signature is the chosen CVM, the requirements for Quick Chip are the same as for a standard EMV transaction:

- If the final amount is less than or equal to the VEPS limit, a signature is not required to be captured.
- If the final amount is greater than the VEPS limit and the online response is an approval, then a signature shall be captured.

If PIN is the selected CVM, the PIN shall be captured as per standard processing. The Online PIN block can be retained temporarily[7], for inclusion in the authorization message once the final amount is known.

3.5 Quick Chip Authorization Request

For Quick Chip the EMV kernel requests data for an online authorization (ARQC) from the card. The card performs card risk management, and responds with either an offline decline or an online authorization request. For the purposes of this document, the default outcome is an online authorization request.

When the card responds with an ARQC (online authorization request), the payment application shall:

- save the data provided for the online authorization request until the final amount (actual, nominal, or estimated) is known. The data saved for the authorization request is the same as for a standard EMV transaction.
- complete the transaction as a deferred authorization by informing the EMV kernel that the payment application was unable to go online. The Authorization Response Code (tag '8A') may be configured as a default value for the chip terminal or passed as an instruction from the payment application. The Authorization Response Code shall have a value of Z3, indicating the terminal is unable to go online, and completes the EMV processing with an AAC (which is normal procedure for a deferred authorization, and prevents impacting any offline counters on the card). The AAC is **not** an offline decline of the transaction – the transaction outcome for Quick Chip depends only on the Authorization Response Code in the online authorization response. The card will complete standard EMV processing.
- prompt for card removal.
- defer any additional cardholder messaging regarding the outcome of the transaction until after the online authorization response is known.

Meanwhile, once the final transaction amount is known (and if an Online PIN is needed, the Online PIN block is available), the payment application sends the online authorization request message. The data requirements for a Quick Chip transaction are the same as for a standard EMV transaction. The Amount, Authorized that was used to generate the Application Cryptogram shall be sent in tag '9F02' of Field 55, and the final amount is sent in Field 4.

[7] The Online PIN block is only retained in the terminal until it sends the authorization message. This is the same as for any online authorized transaction that contains an Online PIN block, such as a magnetic stripe transaction with Online PIN.

3.6 Completion of the EMV Transaction

Since the EMV transaction is completed as unable to go online, and the card is removed early, the card is not available to perform Issuer Authentication or process Issuer Scripts.

Issuer Authentication is not necessary for Quick Chip transactions, because the transaction is approved or declined based only on the issuer's decision in the authorization response message. Issuer Authentication is also used by some issuers in support of offline transactions, which are not necessary for U.S. transactions. Note that mobile wallets and contactless transactions do not use Issuer Authentication.

For Quick Chip, acquirers may receive Issuer Scripts in the authorization response message and the acquirer may send the scripts to the terminal/device. The payment application shall discard any Issuer Authentication Data or Issuer Scripts in the authorization response.

3.7 Quick Chip Considerations for ATMs

Quick Chip is permitted for use at ATMs. However, issuers should consider the following when deciding whether to support Quick Chip in their ATMs:

- Prompting for and capturing the Online PIN must be performed by the end of the Cardholder Verification function of the Quick Chip transaction, to ensure that TVR and CVR indicators are set correctly for the transaction.
- If the issuer does not support sending issuer scripts to cards, their ATMs could use Quick Chip for all transactions.
- If the issuer needs to support issuer updates to the EMV card (for example, issuer scripts for Offline PIN Management), the updates cannot be performed using Quick Chip, and are instead performed using a traditional EMV transaction flow.
  - The ATM may support Quick Chip for most transactions, only using the traditional EMV flow when the cardholder has chosen a function that requires an issuer script (for example, PIN Change),
  - If the ATM has already performed a Quick Chip transaction before the cardholder chooses the function that requires an issuer update, the ATM initiates a new transaction with the EMV card using the traditional EMV flow. To avoid the cardholder having to select the application a second time, the new transaction shall use the same AID as was chosen for the immediately preceding Quick Chip transaction. Note that unless the card is still present in the chip reader, this will necessitate prompting the cardholder to reinsert their ATM card. Care should be taken to correctly handle the case where a different card is inserted.
  - If this option is selected by the issuer, the ATM will need to support both Quick Chip and traditional EMV transaction flows.

4 Quick Contactless Requirements

As is done with Quick Chip, all Quick Contactless transactions must be authorized online. Quick Contactless is suitable only for Online Only terminal configurations.

Setting the TTQ 'Online cryptogram required' bit (TTQ byte 2 bit 8) to 1b will result in the card returning an Authorization Request Cryptogram (ARQC).

Note: *If the merchant wishes to use Quick Contactless processing for only some of their card brands, then the merchant should make sure to enable Quick Contactless processing only for the contactless kernels and the AIDs of the brands they wish to support.*

4.1 Quick Contactless Amount Considerations

The amount used in the cryptogram generation should be the same as for contact Quick Chip, i.e. whichever amount contact Quick Chip uses, Quick Contactless should use as well.

For example, when the final amount is not known and a placeholder amount is used, the same placeholder amount should be used for both Quick Chip and Quick Contactless transactions.

4.2 Quick Contactless CVM and VEPS Considerations

For implementations that initiate chip processing when the final amount is not yet known, set the TTQ 'CVM required' bit (TTQ byte 2 bit 7) to 1b. If the final amount is lower than the VEPS limit, disregard the CVM requirements in the CTQ. If the final amount is higher than the VEPS limit, capture the CVM as required in the CTQ.

For implementations that initiate chip processing when the final amount is known, set the TTQ 'CVM required' bit (TTQ byte 2 bit 7) to 1b only if the final amount is higher than the VEPS limit, and follow standard qVSDC processing.

A Comparison with Other Brands

Known contact Quick Chip differences with other brand specifications for this functionality:

- MasterCard M/Chip Fast, Version 1.1: None
- Amex Quick Chip Technical Manual, June 2016: No functional difference, except that Quick Chip is not allowed for ATMs.