Quick Chip for EMV® — Specification

Version 1.2

August 2016

Visa Public

Important Information on Confidentiality and Copyright

THIS DOCUMENT IS PROVIDED ON AN "AS IS”, “WHERE IS”, BASIS, “WITH ALL FAULTS” KNOWN AND UNKNOWN. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VISA EXPLICITLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE LICENSED WORK AND TITLES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

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.

1.1 Scope

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

1.2 Audience

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

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]).

1.3 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. Integrated Circuit Card Specifications for Payment Systems.

[VIS] Visa Integrated Circuit Card Specification:

- Version 1.5, June 2009, or
- Version 1.6, January 2016.

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

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).

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[2] processing.
- Supports all cardholder verification methods.

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

[2] 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).

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.

The Quick Chip solution overcomes both of 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.

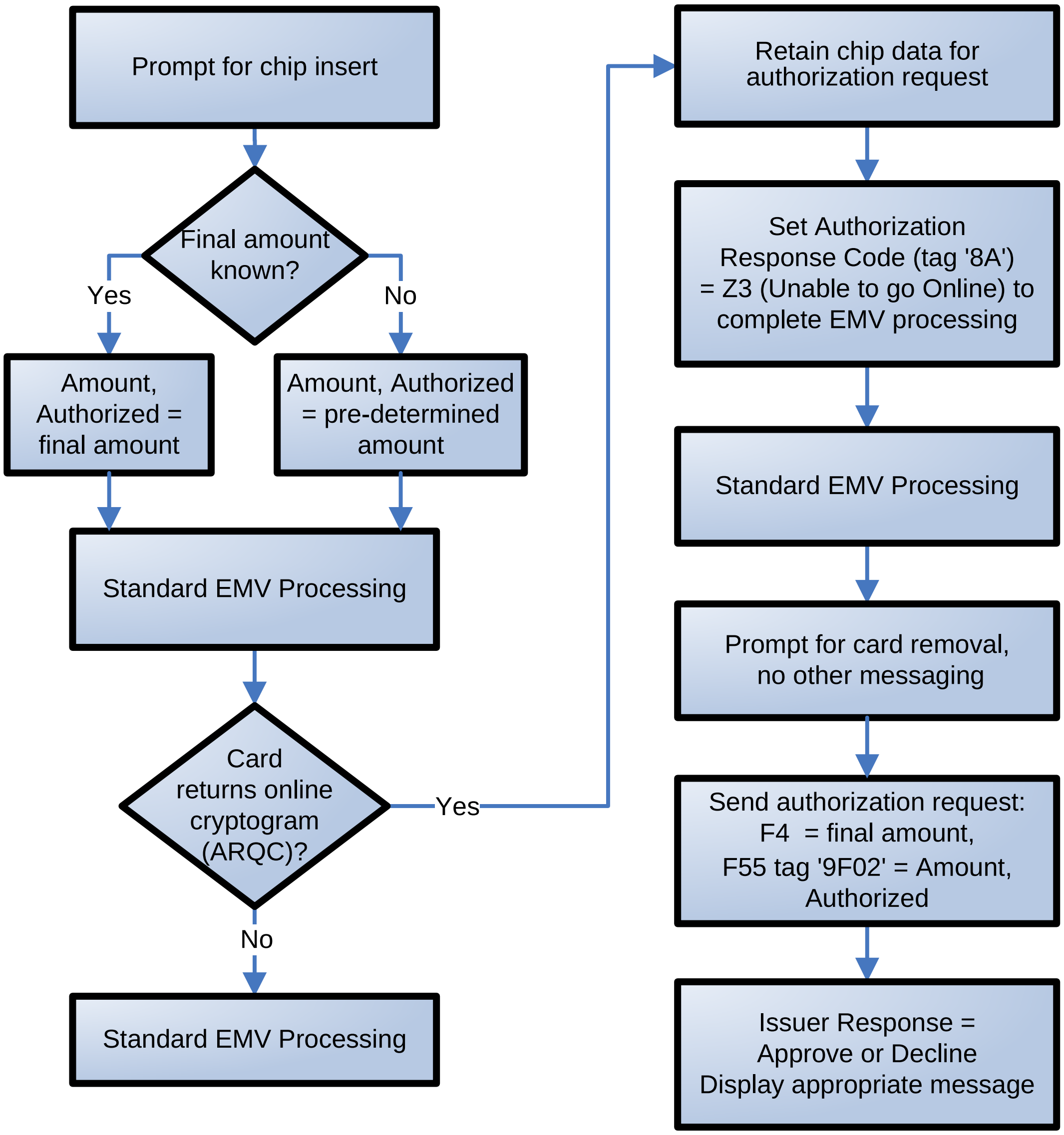
5. Until the final amount is available, the payment application temporarily stores the authorization data from the EMV kernel. Once the final amount is available, the final amount is placed in non-chip data (Field 4) of the authorization message. The EMV data is placed in chip data (Field 55) of the 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.*

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


Prompt for chip insert
Final amount known?
Yes
No
Amount, Authorized = final amount
Amount, Authorized = pre-determined amount
Standard EMV Processing
Card returns online cryptogram (ARQC)?
Yes
No
Standard EMV Processing
Retain chip data for authorization request
Set Authorization Response Code (tag '8A') = Z3 (Unable to go Online) to complete EMV processing
Standard EMV Processing
Prompt for card removal, no other messaging
Send authorization request: F4 = final amount, F55 tag '9F02' = Amount, Authorized
Issuer Response = Approve or Decline Display appropriate message

***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, and are 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 with which they do wish to use Quick Chip processing (e.g., the Visa Debit/Credit AID, the U.S. Common Debit AID).*

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 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.*

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 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 processing follows standard CVM List processing, allowing 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, for inclusion in the authorization message once the final amount is known.

3.5 Quick Chip Authorization Request

Unless EMV Terminal Action Analysis requires an offline decline, 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:

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 is known. The data saved for a Quick Chip 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.

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 process Issuer Authentication (ARPC) or 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, and failure to receive the ARPC will only result in the card being required to go online the next time it is used. Note that mobile wallets and contactless transactions do not use Issuer Authentication.

Issuer scripts are not recommended by Visa for U.S. transactions and are already not supported for mobile wallets and contactless transactions globally.

The payment application shall discard any Issuer Authentication Data or Issuer Scripts in the authorization response.

The Authorization Response shall determine the outcome for the transaction.

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.

A Comparison with Other Brands

Known 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.