Visa Minimum U.S. Online Only Terminal Configuration

Introduction

Intended Audience

This document is intended for U.S. merchants, acquirers, processors and terminal providers who are planning deployments of EMV chip terminals in the U.S.

As U.S. merchants, acquirers, and processors begin planning for the October 2015 EMV® counterfeit liability shift, many stakeholders ask: "What are Visa's minimum requirements for a chip terminal in the U.S.?"

Visa's U.S. market strategy is to focus on online only acceptance, leveraging existing online magnetic-stripe infrastructure which is robust, real-time, and always online for authorization and authentication. The primary goal of this strategy is to limit disruption by simplifying implementation.

Chip terminal implementations are more complex when compared against their magnetic-stripe counterparts. However, Online Only chip terminals are significantly less complex when compared to offline capable solutions. Finally, the scope and effort associated with testing an Online Only chip terminal is significantly reduced when compared against all other terminal configurations.

The balance of this paper focuses on Visa's Online Only terminal configuration in the context of the U.S. market.

Online Only terminals always send a transaction online for authorization and when supporting face-to-face transactions will provide for signature support, as well as for cardholder receipts. If PIN support is needed (e.g. PIN debit) a PIN pad is added to the hardware configuration.

Merchants are encouraged to work directly with their acquirer and/or terminal deployer to determine the approved EMVCo terminal configurations offered that satisfy Visa's U.S. Online Only terminal requirements. Approved EMVCo terminal configurations (chip reader and chip software) are a global industry requirement, and the U.S. is no exception.

EMV is a registered trademark or trademark of EMVCo LLC in the United States and other countries.
© 2016 Visa. All Rights Reserved.

Terminal Type – Online Only

A terminal configuration is essentially a collection of parameters that drive specific behavior associated with a chip transaction. The first parameter considered when setting-up an Online Only terminal is Terminal Type (tag '9F 35'). Possible Terminal Type values for Visa's U.S. Online Only configuration are:

'21'	– Online Only, Attended Merchant (POS)
'24'	– Online Only, Unattended Merchant (POS)
'14'	– Online Only, Unattended Financial Institution (ATM)

Online Only chip implementations are significantly less complex when compared against offline capable solutions.

While the Terminal Type data object is important in expressing the device capabilities, alone it is not sufficient to ensure that terminal will always attempt to go online. The Terminal Floor Limit (tag '9F 1B') must be set to zero ('00 00 00 00') and the Terminal Action Code – Online byte 4, bit 8 set to 1. (Note: When the Level 2 configuration supports a Terminal Type of Offline w/Online Capability these can easily be deployed as Online Only configurations by ensuring the Terminal Floor Limit and TAC values are configured as defined in this document.)

During an EMV transaction the Floor Limit is compared against the transaction amount. When the transaction amount is greater than or equal to the Floor Limit, the terminal sets an indicator in Terminal Verification Results (tag '95'). The Terminal Verification Results (TVR) is a 5 byte, bit map which tracks specific transaction events.

An EMV terminal will determine how to direct a transaction (online, offline, or decline) by comparing the TVR with Terminal Action Codes (TACs) and Issuer Action Codes (IACs). These action codes share the same 5 byte, bit map format as the TVR. The terminal compares the Action Codes in pairs against the TVR as follows:[1]

1. **TAC/IAC – Denial**, any match vs. TVR results in decline request. Card must respond with decline cryptogram.
2. **TAC/IAC – Online**, any match vs. TVR results in online request. Card must respond with online cryptogram or decline cryptogram.
3. **TAC/IAC – Default**, only if terminal cannot go online, any match vs. TVR results in decline request. Card must respond with decline cryptogram.

Minimally, Visa's (POS) Terminal Action Codes must carry the following values:

Terminal Action Code – Denial	=	'00 10 00 00 00'
Terminal Action Code – Online	=	'58 40 04 F8 00'
Terminal Action Code – Default	=	'58 40 00 A8 00'

An Online Only device must configure Terminal Action Code – Online byte 4, bit 8 = 1. As the Terminal Floor Limit has been set at zero, this forces the setting of TVR byte 4, bit 8. Meaning if a terminal has not already determined a condition to decline the transaction it shall be forced online, based on the process described above.

[1] See EMV v4.3 Book 3, Section 10.7 for a summary of special Online Only kernel options associated with Terminal Action Analysis. In summary, an Online Only terminal may forgo the normal Terminal Action Analysis and always request to go online.

© 2016 Visa. All Rights Reserved.

Application AIDs

Visa Application Identifiers (AIDs) allow the terminal to recognize and interact with Visa's payment applications on the chip. The Visa AIDs that must be programed to an Online Only terminal are:

Visa Credit/Debit (Required)	– 'A0 00 00 00 03 10 10'
Visa Electron (Required)	– 'A0 00 00 00 03 20 10'(processed in the U.S. as Visa transactions)
Plus (Required - ATM Only)	– 'A0 00 00 00 03 80 10'
Interlink (Optional - POS Only)	– 'A0 00 00 00 03 30 10'

The Visa U.S. Common Debit AID may be added to support debit routing arrangements:

Visa U.S. Common Debit AID (optional – POS and ATM)	– 'A0 00 00 00 98 08 40'

Terminal Capabilities & Additional Terminal Capabilities

Terminal Capabilities (tag '9F 33') and Additional Terminal Capabilities (tag '9F 40') will also carry specific settings for an Online Only terminal. These data objects are both formatted as binary, bit maps and their settings are expressed as such. For a Visa U.S. Online Only terminal the minimum settings are as follows:

Terminal Capabilities (tag '9F 33')

Byte 1, bit 7	–	Magnetic stripe (when the chip terminal integrates such hardware)
Byte 1, bit 6	–	IC with contacts
Byte 2, bit 7	–	Online Enciphered PIN when Terminal Type is ATM
Byte 2, bit 6	–	Signature when Terminal Type is POS

Additional Terminal Capabilities (tag '9F 40')

Byte 1, bit 8	–	Cash must be set when Terminal Type is ATM
Byte 1, bit 7	–	Goods must be set when Terminal Type is POS
Byte 1, bit 6	–	Services must be set when Terminal Type is POS
Byte 4, bit 8 or bit 7	–	Printer attendant or printer cardholder

Final Considerations

Readers familiar with EMV terminal configurations will note that features common in other regions of the world are not expected in Visa's U.S. Online Only terminal configuration. In particular, no Offline Data Authentication (ODA) is specified in the Terminal Capabilities. Online Only devices are not required to support ODA features, reducing the need for EMV terminal key management. Additionally, a PIN Pad need not be supported by Visa's U.S. Online Only POS terminal thereby reducing Payment Card Industry (PCI) scope.

PIN pads remain a requirement for ATMs and POS terminals that process debit transactions via Interlink. It is recommended that when accepting online PIN for magnetic-stripe debit, chip debit also be accepted with online PIN. Support for offline PIN is not required when supporting online PIN, as those offline PIN preferring cards from foreign markets are also required to support Signature allowing for traditional acceptance in the U.S. market. Finally, if a merchant does not support PIN today then there is no Visa requirement to support PIN on chip in any format.

U.S. EMV cards and Online Only terminals typically do not support offline approvals, meaning merchants/acquirers with temporary network connectivity issues should consider adopting a Deferred Authorization approach. This Deferred Authorization approach, sometimes called Store & Forward, is common in many magnetic stripe environments and is equally suited to Online Only EMV environments. Such an approach addresses network latency issues for EMV without the cost, development, and complexity of a fully offline capable EMV solution.

All Visa U.S. EMV transactions will initially attempt to go online (i.e. GenAC 1 = ARQC). When a host connection is unavailable the card/terminal will typically perform an EMV offline decline (i.e. GenAC 2 = AAC) due to the Zero Floor Limit, the card's ability to support offline transactions, and the mandatory Terminal Action Codes. When implementing Deferred Authorization, however, the terminal may approve the transaction and delay or defer the GenAC 1 ARQC authorization request until the network connection is restored.

No special terminal logic is needed to determine if a Deferred Authorization is allowed, such as checks on TVR or TSI , which could override the card decision to initially send the transaction online. In the U.S. chip data in clearing is optional for Visa. However, if the merchant chooses to include chip data in the clearing record, the GenAC 1 ARQC, and not the GenAC 2 AAC, should be included assuming an approval was received. In the event the Deferred Authorization request was declined that transaction must not be cleared or settled.

[2] As most TVR and TSI settings are primarily relevant to offline functionality, and most U.S. cards do not support offline functionality, it is strongly recommended that TVR and TSI settings not be used to filter transactions for eligibility for Deferred Authorization.

© 2016 Visa. All Rights Reserved.

In a Deferred Authorization environment the merchant must consider the risk of completing a local approval and implement appropriate risk management such as velocity checking and total cumulative amount. Deferred Authorization risk management for EMV is identical to magnetic stripe situations, carrying the same open to buy risk, meaning an issuer could decline for insufficient funds and merchants would absorb such a loss should this occur. However, such exposure is typically small and can be sized by evaluating the current overall decline rate, applying the likely number and value of transactions that would occur during a host outage. Visa's Acceptance Solutions team can help evaluate the financial impact of a Deferred Authorization approach.

Merchants/acquirers participating in the **Visa Easy Payment Service Program** (VEPS) will require a Selectable Kernel allowing for the dynamic programing of the Terminal Capabilities based on transaction parameters. When a transaction qualifies for VEPS, the Terminal Capabilities (tag '9F 33') must be configured to include only: No CVM Required (byte 2, bit 4) for attended devices. Unattended devices must always support No CVM Required (byte 2, bit 4).

Merchant/acquirers who also wish to participate in the **TIP program** to reduce their PCI audit, must deploy a dual-interface terminal which supports both EMV contact chip and contactless chip transactions. Visa's U.S. contactless reader configuration is not addressed in this paper.

Finally, while chip data is required to be included in the authorization request and authorization response messages: **there are no requirements to carry chip data in the clearing and settlement messages, or returns**. This means, that in the U.S. these merchant and acquirer interfaces remain largely unchanged.

EMV Configuration

EMV terminal providers will be intimately familiar with the configuration options associated with their particular device and will provide guidance on satisfying Visa's Online Only requirements. However, to facilitate discussions with terminal providers the table to the right is an extraction from the EMV application kernel Implementation Conformance Statement (ICS). This extraction summarizes the necessary options for a Visa Online Only terminal; these features are also expressed on the EMV Letter of Approval.

Other brands may have other requirements which are outside the scope of this paper.

Feature	Setting
Terminal Type	'21', '24', or '14'
…	
Magnetic Stripe	Conditional
IC with Contacts	Yes
…	
Online Enciphered PIN	Conditional
Signature (paper)	Conditional
…	
No CVM	Conditional
…	
Transaction Type – Cash	Conditional
Transaction Type – Goods	Conditional
Transaction Type – Services	Conditional
…	
Print, Attendant	Conditional
Print, Cardholder	Conditional
Display, Attendant	Conditional
Display, Cardholder	Conditional
…	
Partial AID Selection	Yes
…	
Common Character Set	Yes
…	
Fail CVM	Yes
…	
Floor limit checking	Yes
…	
Terminal Risk Management irrespective of AIP setting	Conditional
…	

Additional Reading

The following resources are available via acquirer licensing:

- **Visa Smart Debit/Credit (VSDC) and Visa payWave U.S. Acquirer Implementation Guide** – Acquirer guidance for chip acceptance.
- **EMV in the U.S.: Simplifying Deployment in a Zero Floor Limit Environment** – Detailed review of the Visa online only strategy.
- **Visa U.S. Merchant EMV Chip Acceptance Readiness Guide: 10 Steps to Planning Chip Implementation for Contact and Contactless Transactions**
- **Visa's Transaction Acceptance Device Guide** (www.visa.com/tadg) – Overview of terminal chip acceptance.
- **Visa Transaction Acceptance Device Requirements** – Summary of Visa acceptance business rules.

[3] VEPS allows merchants the capability to accept Visa cards without requiring a signature or PIN for transactions under $25 or $50, depending on merchant category. A customer receipt is also not required, unless requested by the cardholder. VEPS helps to make the payment process easier and more convenient for both the merchant and cardholder.

© 2016 Visa. All Rights Reserved. VBS 06.JUL.16