Visa Fleet and Automatic Fuel Dispenser Recommendations

Introduction

Intended Audience

This document is intended for U.S. retail petroleum merchants, acquirers, processors and terminal providers who are planning deployments of EMV chip terminals in the U.S., as well as issuers and processors who are planning to issue fleet chip cards.

As the U.S. market prepares for the 2020 Automatic Fuel Dispenser (AFD) EMV® counterfeit liability shift, many stakeholders ask: "What are Visa's recommendations for migrating from magnetic stripe to EMV in the petroleum retail market in the U.S.?"

Visa's U.S. migration strategy for the point of sale has been to focus on a very simple, online only acceptance, leveraging existing online magnetic-stripe infrastructure which is robust, real-time, and always online for authorization and authentication. The petroleum retail industry is no different. 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.

Fleet card issuance follows a similar approach. Visa recommends leveraging the existing infrastructure to ensure a smooth transition to chip, by using an online only chip card profile with the fleet service indicators in the Track 2 Equivalent Data on the chip. This approach reduces complexity in personalization and host development.

The balance of this paper is divided into two parts. Part one focuses on U.S. chip card issuance in the context of fleet, while part 2 focuses on Visa's Online Only AFD configuration in the context of the U.S. market.

Because the U.S. is a zero-floor limit country, all transactions must go online for authorization. Therefore, any offline functionality on the chip card is highly discouraged, as is scripting and issuer authentication. Additionally, due to the

EMV is a registered trademark or trademark of EMVCo LLC in the United States and other countries.

© 2020 Visa. All Rights Reserved.

presence of both magnetic stripe and chip terminals in the market place over the next few years, as well of the lack of a fully agreed industry standard, the fleet service indicators should be kept in Track 2 Equivalent Data on the chip.

Online Only AFD terminals always send a transaction online for authorization. If PIN support is needed, 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.

To ease implementation and testing, Visa has developed the Quick Chip specifications, which are recommended for any online-only implementation, and strongly recommended for AFDs.

Considerations for Fleet Card Issuance

Chip Card Personalization – Online Only

Personalizing a chip card as online only is significantly simpler than adding any offline functionality. There are no requirements for certificates, nor are there any requirements to update the issuer's host system to add offline risk parameters. Furthermore, because there is no need for issuer authentication and scripting, this functionality also doesn't need to be developed for issuer host systems.

Fleet Service Indicators

Due to the co-existence of magnetic stripe and chip terminals, the simplest way to incorporate fleet prompts is to mirror the process as it is done for the magnetic stripe today, by adding the Fleet Service Indicators in Track 2 Equivalent Data (tag '57') on the chip. The Fleet Service Indicators are in the last 3 positions of field 57, as defined below:

Field Position	Field Name	Possible Values
1	Reserved	Reserved for future use; the default value is 0 (zero)
2	Service Enhancement Indicator	0 = Fleet, No Restriction (fuel, maintenance, and non-fuel purchases) 1 = Fleet (fuel- and maintenance-only purchases) 2 = Fleet/Fuel Only (fuel-only purchases) 3-9 = Reserved
3	Service Prompt	0 = Reserved (no prompt required) 1 = Identification (ID) and odometer reading 2 = Vehicle ID and odometer reading 3 = Driver ID and odometer reading 4 = Odometer reading 5 = No prompt 6 = ID[1]

Application Interchange Profile – Online Only

The Application Interchange Profile (tag '82') is a list of capabilities the card sends to the terminal stating what the card is able to do. The simple Online Only value is '18 00', which corresponds to no Offline Data Authentication and no Issuer Authentication.

Cardholder Verification Method List (CVM)

The Cardholder Verification Method List (tag '8E') is a list of Cardholder Verification Methods supported by the card. Visa's standard CVM List for fleet is '0000 0000 0000 0000 0201 1E04 0005 5E00 1F00'. This corresponds to a simple signature-preferring card, with No CVM at unattended devices (which include AFDs), as well as Online PIN for ATM access.

[1] After prompt for ID, the cardholder enters the six-digit numeric vehicle, driver, or generic ID.

© 2020 Visa. All Rights Reserved.

Issuer Action Codes

An EMV terminal will determine how to direct a transaction (online, offline, or decline) by comparing the Terminal Verification Results (tag '95') with Terminal Action Codes (TACs) and Issuer Action Codes (IACs). The TVR is a 5-byte bit map that tracks specific transaction events and the Action Codes share that same 5-byte bitmap. The terminal compares the Action Codes in pairs against the TVR as follows:

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.

Visa's recommended Issuer Action Codes for U.S. fleet cards are the following values:

Issuer Action Code – Denial = '00 00 00 00 00'
Issuer Action Code – Online = 'FC 70 BC 98 00'
Issuer Action Code – Default = 'FC 50 AC 88 00'

Quick Chip

Quick Chip is an enhanced implementation of the standard EMV flow, which allows for early removal of the card, without waiting for the issuer response, similar to how the magnetic stripe works today. Quick Chip additionally allows for a much simpler testing suite. Since it removes the possibility for Issuer Authentication and scripting at the terminal, testing for those possibilities has also been removed. For more information please refer to Quick Chip for EMV Specification (www.visachip.com, under "Quick Chip for EMV") regarding how to implement Quick Chip.

Considerations for EMV Acceptance at Petroleum Retail Merchants

Authorization and Clearing Considerations

In-store transactions follow the standard EMV processing flow used for general retail transactions.

There are three acceptable ways to process AFD authorizations:

- The cardholder may determine an exact amount to be authorized and dispensed. The AFD generates an authorization for the exact amount, and a clearing record (TC05) for the exact amount is generated later.
- The cardholder does not know the final amount of purchase. The AFD sends a pre-authorization request for $1. This type of pre-authorization request is known as a "status check."[2] An AFD Confirmation Advice (0120 non-financial message) containing the actual amount is generated within two hours of the status check authorization. A clearing record (TC05) is generated for the actual purchase amount.
- The cardholder does not know the final amount of purchase. If the merchant and acquirer participate in the Real Time Clearing program, the AFD sends an estimated pre-authorization request. The pre-authorization amount is a good faith estimate based on spending patterns at the merchant and can be up to US $500. A real-time clearing record (0220 Acquirer Financial Advice) is generated for the actual purchase amount.

In each case, the chip data, including the cryptogram, will be included in the authorization/pre-authorization message (0100). For contact or contactless chip transactions, the chip cryptogram amount should be whatever amount is contained in the authorization message.

No chip data is required in the clearing/advice (TC05/0220) or the final amount notification (0120) from the dispenser as long as the transaction is online authorized.

Terminal Type – Online Only

A terminal configuration is essentially a collection of parameters that drive specific behavior associated with a chip transaction. It also determines the EMV testing that is performed by the accredited laboratory. Visa does not require that specific terminal configurations (i.e., Terminal Types) be used in production, but does require that the EMV kernel always requests an online configuration. (Always asks for an ARQC at 1st Gen AC, unless a product restriction is in place.)

[2] A status check provides authorization protection up to a certain value depending on card type. Please see "Visa Payment Acceptance Best Practices for U.S. Retail Petroleum Merchants" for more information.

© 2020 Visa. All Rights Reserved.

The first parameter considered when setting-up an Online Only terminal is Terminal Type (tag '9F35'). The Fleet Terminal Type value for Visa's U.S. Online Only configuration is '24' – Online Only, Unattended Merchant (POS). However, other Terminal Types may be used for AFDs as long as the Level 2 configuration effectively acts as an Online Only Unattended terminal.

While the Terminal Type data object is important in expressing the device capabilities, alone it is not sufficient to ensure that the terminal will always attempt to go online. The Terminal Floor Limit (tag '9F1B') must be set to zero ('00 00 00 00') and the Terminal Action Code – Online byte 4, bit 8 is set to 1.

Note: If 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 comparison of IAC/TACs vs. TVR is described under Issuer Action Codes above, and is called Terminal Action Analysis. An Online Only terminal may forgo the normal Terminal Action Analysis and always request to go online.[3]

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 is set to zero, this forces the setting of TVR byte 4, bit 8 = 1. Therefore, if a terminal has not already determined a condition to decline the transaction, the transaction will be forced online based on the process described above.

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

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 in an Online Only AFD 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 credit transactions)
Interlink (Optional)	–	'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) – 'A0 00 00 00 98 08 40'

Terminal Capabilities & Additional Terminal Capabilities

Terminal Capabilities (tag '9F33') and Additional Terminal Capabilities (tag '9F40') will also carry specific settings for an Online Only AFD. These data objects are both formatted as binary bitmaps and their settings are expressed as such. For a Visa U.S. Online Only AFD, 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
Byte 2, bit 4	–	No CVM Required

[3] See EMV v4.3 Book 3, Section 10.7 for a summary of special Online Only kernel options associated with Terminal Action Analysis.

© 2020 Visa. All Rights Reserved.

Additional Terminal Capabilities (tag '9F 40')

Byte 1, bit 7 – Goods

Byte 1, bit 6 – Services

Byte 4, bit 7 – Printer, cardholder

Byte 4, bit 5 – Cardholder display

Final Contact Chip Terminal 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 AFD 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. 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 No CVM, allowing for traditional acceptance in the U.S. market.

U.S. EMV Fleet cards (as described in this paper) and Online Only terminals 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.

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 and the mandatory Terminal Action Codes. However, when implementing Deferred Authorization 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[4], 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.

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 checking. 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 the 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.

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.

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**. This means that in the U.S. these merchant and acquirer interfaces remain largely unchanged.

[4] 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.

© 2020 Visa. All Rights Reserved.

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, this table is an extraction from the EMV application kernel Implementation Conformance Statement (ICS). This extraction summarizes the necessary options for a Visa Online Only AFD; 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	Online Only
Magnetic Stripe	Required
IC with Contacts	Yes
Online Enciphered PIN	Optional
No CVM	Required
Transaction Type – Goods	Yes
Transaction Type – Services	Yes
Print, Cardholder	Yes
Display, Cardholder	Yes
Partial AID Selection	Yes
Common Character Set	Yes
Fail CVM	Yes
Floor limit checking	Yes
Terminal Risk Management irrespective of AIP setting	Online Only

Contactless Considerations

Older versions of Visa contactless supported two different transaction flows: legacy Magstripe Data (MSD) that passes over the RF interface track 1 & track 2 data along with a dynamic CVV, and a Quick Visa Smart Debit Credit (qVSDC) flow that passes over the RF interface with full cryptographic data. Globally, merchant terminals should now be designed to support only qVSDC transaction flows. Issuer cards may still be designed to support both the MSD and qVSDC transaction flows, which ensures that any contactless form factor can be accepted at any merchant terminal.

Note: Fleet card cannot support MSD contactless and should be issued as supporting qVSDC only. This is due to the ATC counter value in the MSD track layout that is in the same position as Fleet Service Indicators, that will cause incorrect prompting at Fleet Terminals.

With the global migration to full chip processing now underway, the need for terminal support of the legacy MSD transaction flow is redundant and should be avoided as:

- Visa Approval Services no longer accepts contactless terminals/readers supporting MSD only
- All issuer products minimally support qVSDC
- Development, certification, and integration efforts are essentially doubled when supporting both MSD & qVSDC
- Terminals supporting both MSD & qVSDC will never process the MSD flow as qVSDC has priority irrespective of AIP setting.

Supporting the qVSDC path alone, and removing MSD support, from contactless reader development or integration requirements is the streamlined approach to contactless acceptance.

Streamlined qVSDC Configuration

Support of contactless acceptance is not required, however if supported, the qVSDC reader/terminal configuration can be significantly simplified by following this streamlined qVSDC Configuration.

- Terminal Transaction Qualifiers (tag '9F66')
  - AFDs must minimally support qVSDC, CDCVM, and require an online cryptogram ('20 80 40 00')
  - Optionally, add support for Online PIN ('24 80 40 00')
- Reader Contactless Floor Limit (terminal proprietary data object) = $0 - as the U.S. is a zero floor limit country, does not preclude Store & Forward/Deferred Authorization integrations
- Reader Contactless Transaction Limit (terminal proprietary data object) = maximum or null value - allows for a contactless transaction of any amount (per Visa Rules, this limit must not be set)
- Reader CVM Required Limit (terminal proprietary data object) = $0

© 2020 Visa. All Rights Reserved.

Additional Reading for Acquirers

The following resources are available via acquirer licensing:

- Visa Payment Acceptance Best Practices for U.S. Retail Petroleum Merchants
- Visa Smart Debit/Credit (VSDC) and Visa payWave U.S. Acquirer Implementation Guide (www.visachip.com) – 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's Transaction Acceptance Device Guide (www.visachip.com) – Overview of terminal chip acceptance.
- Visa Transaction Acceptance Device Requirements – Summary of Visa acceptance business rules.
- Quick Chip for EMV Specification (www.visachip.com, under "Quick Chip for EMV") – Specification regarding how to implement Quick Chip.

Additional Reading for Issuers

The following resources are available via issuer licensing:

- Visa Smart Debit/Credit (VSDC) U.S. Issuer Implementation Guide – Issuer guidance for contact chip issuance.
- Visa Smart Debit/Credit Personalization Requirements for U.S. Implementations – Issuer guidance for chip personalization.
- VCPS U.S. Issuer Implementation Guide – Issuer guidance for contactless issuance.

© 2020 Visa. All Rights Reserved. 20.DEC.19