CHIP ADVISORY #20, JANUARY 10TH, 2012

# Visa Recommended Practices for EMV Chip Implementation in the U.S.


## Summary

As issuers, acquirers, merchants, processors and vendors plan and begin programs to adopt chip technologies, Visa has developed recommended practices to provide guidance on the implementation choices that seem most appropriate for the U.S. market and facilitate reduced complexity, cost and time to market.


- ☒ Issuer
- ☒ Acquirer
- ☒ Chip Vendors
- ☒ Chip Card Vendors
- ☒ Chip Terminal Vendors
- ☒ Chip Card Personalization Bureaus
- ☐ Other

## Overview

On 9 August 2011, Visa announced plans to accelerate contact and contactless EMV chip technology migration in the U.S., and provided a roadmap to help guide industry investments in payment infrastructure. Investments in chip technology will accelerate the adoption of mobile payments, enhance international card acceptance and improve security through the use of dynamic authentication elements.

## Overview of Recommended Practices

EMV, a globally interoperable industry standard for chip payments, is a flexible platform designed to meet the diverse needs of stakeholders worldwide. To provide guidance and help reduce complexity, cost and time-to-market, Visa has developed a set of recommended practices for issuers, acquirers, merchants, processors and vendors in the process of planning, adopting and implementing chip technology programs in the U.S.

Visa's guidance for chip implementation in the U.S. includes:

- **Always Online:** All chip transactions should leverage the robust, real-time, online infrastructure for authorization and authentication. The U.S. has a zero floor limit; therefore, nearly 100 percent of all transactions are authorized online in real time. Also, many U.S. issuers use host-based fraud mitigation tools enabled by online, real-time authorization. The existing online infrastructure should be used to optimize chip transaction processing in the U.S.

- **Flexible Cardholder Verification Methods:** Visa will continue to support a range of cardholder verification methods (CVMs) including signature, online PIN and no signature for low-value, low-risk transactions. Visa will not require a "chip-and-PIN" approach in the U.S.; instead, stakeholders will have the flexibility to choose which CVMs to support.

Visa's recommended practices follow the global EMV specification and have been tailored to be specific to the functionality that is appropriate for the U.S. (There are many options for additional complex functionality in the EMV specification, including offline authentication, offline cardholder verification and offline authorization, which are not necessary for chip technology implementation in the U.S.)

These recommended practices provide guidance on the EMV implementation options best suited for U.S. issuers and acquirers. **Note:** While these recommendations are appropriate for most issuers and acquirers, individual needs may vary. These suggestions are not prescriptive, but are meant to provide guidance to U.S. issuers, merchants and processors as they become more familiar with EMV specifications.[1]

[1] These recommendations are intended for informational purposes only and should not be relied upon for marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, clients should consult with legal counsel to determine what laws and regulations may apply to specific circumstances. The actual costs, savings and benefits of a chip card program may vary based upon a client's specific business needs and program requirements. Visa makes no representations and warranties as to the information contained herein; clients are solely responsible for any use of the information in this presentation in connection with their card programs.

## Recommended Acceptance Practices for Acquirers, Acquiring Processors and Merchants

Host System Chip Support

- **Be an early adopter of chip technology.**

  In anticipation of merchant demand, acquirers should consider updating their systems and becoming certified well in advance of the 1 April 2013 requirement to support full chip data using Field 55.

- **Ensure that merchants are able to send full chip data to acquirers.**

  The merchant's terminal and the acquirer must be able to transmit full chip data to each other and, prior to a terminal's deployment, the entire transaction flow must be successfully tested by the Visa Acquirer Device Validation Toolkit (ADVT). Acquirers and merchants should contact their terminal vendors to ensure this requirement has been taken into consideration.

  Visa recommends that chip data be carried in Field 55 (which is a flexible format) to help ensure extensibility and future proofing.

Chip Terminal Deployment

- **Deploy chip-enabled, dual-interface terminals that support contact chip, Visa payWave and magnetic-stripe interfaces.**

  Merchants that deploy dual-interface terminals are preparing their point-of-sale (POS) environments for mobile payments and other emerging payment technologies. **Note:** For a merchant to qualify for participation in the Technology Innovation Program (TIP), at least 75 percent of the merchant's transactions must originate from chip-enabled, dual-interface terminals.

  Using these terminals provides protection under the counterfeit fraud liability shift, which will become effective in the U.S. in October 2015 (October 2017 for Automated Fuel Dispensers (AFDs)).

- **Deploy the latest version of the Visa Contactless Payment Specification (VCPS); enable quick VSDC (qVSDC) and Magnetic-Stripe Data (MSD) features.**

  The latest version of VCPS, which is Version 2.1.1, supports functionality specific to mobile proximity payments. To minimize problems related to interoperability and prolong the longevity of the terminal and the contactless reader base, acquirers and merchants should ensure that their contactless readers:

  - Support the most current version of the specification
  - Are approved by EMVCo and Visa

  **Note:** To qualify for participation in the TIP, merchants must deploy VCPS, Version 2.1.1 (or a subsequent version).

  Visa is in the process of phasing out MSD contactless; however, MSD-only cards still exist. During this migration phase, acquirers of chip and contactless transactions should support both qVSDC and MSD to ensure interoperability.

  Acquirers and merchants accepting contactless transactions must support qVSDC when their infrastructure is capable of transmitting full chip data; they also have the option to support MSD.

- **Support the ADVT, the ADVT qVSDC Device Module and the Contactless Device Evaluation Toolkit (CDET).**

  Visa requires that clients and merchants use the ADVT prior to deploying contact chip terminals and the ADVT qVSDC Device Module prior to deploying qVSDC-capable contactless readers. Visa strongly recommends that clients use the CDET.

  Chip acquirers can also use the Web-based Visa Chip Compliance Reporting Tool (CCRT) to streamline ADVT results reporting.

- **Prioritize deployment of chip-enabled, dual-interface terminals by using a targeted approach.**

  Prioritizing the deployment of chip-enabled devices helps minimize potential declines and protects against counterfeit fraud. For example, larger retailers with multiple locations might first deploy in locations with high international acceptance, high overall volume or high counterfeit fraud concentrations.

  Prioritized deployment may expedite a merchant's eligibility for the TIP and may help provide protection under the 2015 counterfeit fraud liability shift (which will occur in 2017 for AFDs).

EMV Chip Terminal Configuration

- **Configure EMV chip terminals to support online options only.[2]**

  EMV chip terminals can support a variety of offline functionality (e.g., offline data authentication, offline cardholder verification and offline transaction authorization). However, because the U.S. has a zero floor limit, there is no practical need to support these offline functionalities, which can introduce unnecessary complexity into configuring and maintaining a terminal. Also, supporting only online authorization can simplify ongoing EMV compliance.

- **Implement a POS environment that supports online PIN verification. (This recommendation applies to merchants that choose to support PIN in addition to other CVMs.)**

  Merchants that support PIN in addition to other CVMs (e.g., signature) should support online PIN only. There is no need to support offline PIN verification in the U.S.

  Acquirers and merchants deploying new terminals that support online PIN should ensure that the PIN-entry devices are Payment Card Industry PIN Transaction Security (PCI-PTS) compliant. **Note:** EMV chip cards from outside the U.S. that support offline PIN can also support signature at the POS and online PIN at the ATM.

[2] If an online connection fails or is unavailable, the merchant can create a batch file for transactions that took place while the connection was offline and submit them later for online authorization.

## Recommended Practices for Issuers

Transaction Authorization

- **Personalize chip cards and mobile applications to support online authorization only.**

  An online authorization is sent from the merchant's terminal to the issuer via VisaNet.[3] Based on the issuer's host-based risk management parameters, the issuer will send either an approval or a decline response to the merchant's terminal. Visa recommends using online authorization in the U.S. because it leverages the "always online" infrastructure and enables issuers to use their host-based fraud detection tools to manage risk in real time.[4] Online authorization also provides a more streamlined personalization approach, reducing cost and time-to-market. **Note:** Online-only Visa chip cards work in terminals worldwide.[5]

  Offline authorization decisions are made by the chip card using data from the card and the terminal only. Using offline card authorization in the U.S. introduces unnecessary complexity and cost to the personalization processes. Also, an issuer that uses offline authorization loses some of its ability to manage fraud and credit risk at the transaction level because it has less real-time visibility into payment activity.

Card Authentication Methods

- **Personalize chip cards or mobile applications to only support online card authentication (i.e., online cryptograms) rather than offline data authentication.**

  Card authentication methods help ensure that transactions are made using a valid card.

[3] See note 2, above.
[4] Once a chip program is launched, the issuer should review its online fraud monitoring tools and risk management practices, making adjustments as appropriate to accommodate changes in fraud patterns (e.g., adjusting risk rules for chip transactions with dynamic authentication elements).
[5] Issuers considering support of transit system use with their contactless or mobile applications should contact Visa for additional information regarding authorization practices and requirements outside of the U.S., where acceptance may be limited to domestic cards and mobile applications.

Online card authentication takes data from the chip card and the terminal and inputs it into an algorithm that generates a dynamic, unique cryptogram for each transaction. This cryptogram is validated by the issuer's host system (or by Visa on behalf of the issuer) as part of the real-time authorization process.[6]

Offline data authentication uses data from the card to allow the terminal to authenticate the card:

- **Offline Static Data Authentication (SDA)** uses the same data for all transactions and is sent to the terminal for validation (rather than the issuer host). SDA ensures that the data provided by the card has not been altered since personalization; however, due to its static nature, SDA provides only limited protection against copying and reuse.

- **Offline Dynamic Data Authentication (DDA) and offline Combined DDA (CDA)** both take dynamic data from the chip card and the terminal as input into a public key-based algorithm performed by the chip that, unlike SDA, provides protection against copying and reuse. For both DDA and CDA, the terminal authenticates the card offline (rather than the issuer host). Cards that **do not** support DDA or CDA are generally less costly and make chip issuance faster and easier.

Offline data authentication was developed when telecommunications were expensive, slow and/or unreliable. Because the U.S. has a reliable, cost efficient, real-time communications infrastructure, using offline data authentication introduces unnecessary complexity and costs to the personalization and transaction processes.

## Chip Transaction Processing

- **Leverage Visa Chip Services.**

  Visa Chip Services, a turnkey chip transaction processing solution for issuers, reduces costs and time-to-market associated with developing full chip data processing functionality in an issuer's systems.

  Once Visa Chip Services receives an authorization message containing full chip data, it validates the cryptogram and submits the authorization message to the issuer without additional chip fields. Issuers just have to be able to accommodate additional values in the existing authorization message fields.

  Visa plans to develop additional services to further streamline chip implementation for issuers.

[6] Issuers should consider successful validation of the online cryptogram to be a trustworthy indication of a valid card, and should ensure that authorization systems do not decline a transaction because the integrated Circuit Card Verification Value (iCVV) failed when the online card authentication method passed.

Cardholder Verification Methods

- **When deciding whether to support offline PIN, consider where cards are most likely to be used.**

  U.S. issuers should carefully consider the implications of supporting offline PIN. In the U.S., offline PIN support is not required by EMV or by Visa and is not needed for interoperability at most global acceptance points. Offline PIN verification methods introduce unnecessary complexity and costs to the personalization and transaction processes. For example, compared to online PIN, which is managed centrally on the host management server, offline PIN also resides on the chip card and requires remote PIN management.[7]

Chip Interface Options (Contact and Contactless)

- **Issue dual-interface cards (supporting both contact chip and Visa payWave).**

  To maximize the benefits of U.S. chip migration and take full advantage of the speed and convenience of Visa payWave, Visa recommends issuing either a dual-interface card or a contact chip card with a companion mobile application. **Note:** Magnetic stripe continues to be the required baseline card-reading format, and must be supported on both contact-only and dual-interface cards.

- **Use VCPS, Version 2.1.1 (or the mobile equivalent) and support both qVSDC and MSD.**

  To maximize the most current functionality and reduce problems with interoperability, issuers migrating away from the MSD, Version 1.4.2 specification and contactless-only cards should consider dual-interface VCPS, Version 2.1.1 cards or mobile applications that support Visa Mobile Contactless Payment Specification (VMCPS) Version 1.4.

- **Do not issue "contactless-only" chip cards.**

  To derive the most benefit from EMV chip card issuance and to optimize the cardholder's experience, Visa recommends issuing either a dual-interface card or a contact chip card with a companion mobile application.

[7] Issuers targeting chip cards to international travelers should contact Visa for additional information regarding offline PIN implementation.

## Personalization Profile

The following table shows a chip card personalization profile according to Visa's recommended practices.

| Category | Profile | Comments |
|---|---|---|
| **Card Authentication** | Always online | No offline data authentication (e.g., SDA, DDA) |
| **CVM List** | Signature, online PIN and no CVM | No offline PIN[8] |
| **Chip Interface** | Dual-interface (contact and contactless) **or** contact chip card with companion contactless mobile application | No contactless-only cards |

[8] See footnote 7

## Glossary of Terms

**ADVT** – Acquirer Device Validation Toolkit. A Visa toolkit mandated for use prior to deployment of contact chip or dual interface terminals. Designed to check for known interoperability issues and provide acquirers with additional assurance that a terminal has been correctly configured.

**ADVT qVSDC Device Module** – A module addition to the ADVT, mandated for use prior to deployment of dual interface terminals that support the quick Visa Smart Debit / Credit (qVSDC) transaction path. Designed to help ensure that the qVSDC reader is configured correctly prior to deployment.

**AFD** – Automated Fuel Dispenser.

**Online CAM** – Online Card Authentication Method. The online cryptogram generated by a card and sent to the issuer (or to VisaNet) for validation. Successful validation confirms a non-counterfeit card.

**CCRT** – Chip Compliance Report Tool. A web-based Visa tool that enables chip acquirers to streamline ADVT reporting results. **Note**: Visa only accepts ADVT results via CCRT.

**CDA** – Combined Dynamic Data Authentication. A dynamic method of offline data authentication. Offline data authentication is not required in the U.S. and adds significant cost and complexity to chip implementation.

**CDET** – Contactless Device Evaluation Toolkit. Toolkit recommended for use prior to deployment of any Visa payWave program. Designed to check for known interoperability issues and provide acquirers with additional assurance that a terminal has been correctly configured.

**CVM** – Cardholder Verification Method. A contact chip card's prioritized list of CVMs with the CVMs' associated conditions for execution.

**CVV** – Card Verification Value. A unique check value encoded on the magnetic stripe of every card (magnetic stripe only, contact chip and dual interface). Used to validate magnetic-stripe data during the authorization process of a magnetic-stripe transaction and to detect counterfeit cards. CVV is calculated from data encoded on the magnetic stripe using a secure cryptographic process.

**DDA** – Dynamic Data Authentication. A dynamic method of offline data authentication. Offline data authentication is not required in the U.S. and adds significant cost and complexity to chip implementation. **Note**: DDA should not be confused with Dynamic Authentication which, per Visa's authentication strategy, addresses dynamic authentication systems.

**Dual-interface terminal or card** – A terminal or card that supports contact chip, Visa payWave and magnetic stripe.

**EMV** –The industry-recognized specification that forms the basis of chip deployments around the world. Originally created by Europay, MasterCard and Visa.

**EMV Liability Shift** – Once the liability shift goes into effect, responsibility for counterfeit transactions at the point of sale (excluding ATMs) will reside with the non-chip party for both domestic and inter-regional transactions.

**EMVCo** – The governing body that manages the EMV specification.

**Field 55** – A flexible format (tag, length, value) that carries chip and supplemental data from the acquirer's host to VisaNet and on to the issuer.

**Full chip data** – The ability to send, receive and act on (as applicable) all data elements associated with chip. Acquirers are required to be full chip data certified by April 2013. Issuers may optionally develop full chip data functionality within their systems or opt to take advantage of Visa Chip Services, which will carry out validation on behalf of the issuer.

**iCVV** – integrated Circuit Card Verification Value. The iCVV value replaces CVV in the magnetic-stripe image on the chip and differs from the CVV value on the physical magnetic stripe. iCVV protects against the copying of magnetic-stripe data from the chip and using it to create counterfeit magnetic-stripe cards.

**MSD** – Magnetic Stripe Data. This element of the VCPS specification is backward compatible to the MSD 1.4.2 specification currently deployed in the U.S. The MSD path of VCPS 2.1.1 includes a limited set of chip data that is passed to the issuer (or to VisaNet) for authentication.

**PCI-PTS** – Payment Card Industry PIN Transaction Security. This framework supports the evaluation and approval of payment security devices. PCI-PTS compliant PIN-entry devices are listed on the PCI Security Standards Council website at https://www.pcisecuritystandards.org.

**qVSDC** – quick Visa Smart Debit / Credit. This element of the VCPS specification is the EMV-based transaction path for Visa payWave transactions. When a card / mobile phone personalized to support qVSDC is waved near a qVSDC reader, chip data is passed to the issuer (or to VisaNet) for authentication.

**SDA** – Static Data Authentication. A type of offline data authentication. Offline data authentication is not required in the U.S and adds significant cost and complexity to chip implementation.

**TIP** – Technology Innovation Program. Visa program that waives the annual PCI DSS validation exercise for merchants meeting certain qualification criteria. In addition to meeting other program requirements, to qualify, merchants must apply through their acquirer and must have at least 75 percent of transactions originating from an EMV-enabled dual-interface terminal.

**VCPS, Version 2.1.1** – Visa Contactless Payment Specification (most current version). Defines the functionality needed to implement a Visa payWave program and contains additional considerations related to Mobile Visa payWave.

**Visa Chip Services** – Validates chip data on behalf of the issuer. The issuer does not have to be able to act on any new fields in the authorization message, it only needs to recognize new values in existing fields, bringing the benefit of chip to the issuer while simplifying implementation.

**VMCPS, Version 1.4** – Visa Mobile Contactless Payment Specification (most current version). Defines the functionality needed to implement a Visa payWave program on a mobile phone.