Dual-Interface Card Personalization

Version 1.0

Publication Date: September 2018

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

EMV is a trademark owned by EMVCo LLC.

Comments or recommendations for edits or additions to this document should be submitted to: info@uspaymentsforum.org.

Table of Contents

1 Introduction

With the introduction of EMV chip cards in the United States, cardholders are tapping into the power of chip payment technology and the security, value, and convenience it offers to both consumers and businesses. The adoption of dual-interface (EMV contact and contactless chip) technology in the U.S. is important to all stakeholders in the payments industry. Its adoption not only supports the increasing demand for enhanced global acceptance and security through the use of dynamic authentication, it also supports the faster, more convenient "tap and go" experience. Dual-interface card adoption also helps prepare the U.S. payments environment for the arrival of Near Field Communication (NFC)-based mobile payments.

The U.S. has implemented EMV primarily for a zero-floor-limit environment. What this means is that the vast majority of chip transactions are authorized online in real time or use deferred authorization techniques during network outages. As a result, many cards have been issued without support for offline data authentication (ODA),[1] with card authentication instead being solely undertaken as part of the online authorization when a transaction is sent online.

More recently the industry has seen an increased focus on dual-interface cards. These cards support both contact and contactless transactions. One vertical market, the transit industry, is particularly interested in utilizing contactless transactions to manage fares at transit gates. With the speed and throughput requirements of the transit environment, ODA is being considered as a mechanism for quickly determining whether a card is authentic before allowing the cardholder through the transit gate.

The U.S. Payments Forum developed this white paper for the issuing community to provide an educational resource on ODA and to provide recommendations for issuing and personalizing dual-interface cards for the U.S. market.

The document explores dual-interface card personalization guidelines and includes discussion of the use of ODA for transit. There are other uses of ODA and contactless payments in a zero-floor-limit environment, but this white paper focuses on the transit use case.

[1] ODA guidelines may vary by payment network; consult payment network specifications for additional details.

2 What Is a Dual Interface Card and What Does It Mean for Issuers?

This section reviews the differences in hardware and software between dual-interface and contact cards, describes issuer implementation considerations, and outlines market considerations.

2.1 Hardware

2.1.1 Visual Difference from a Contact Card

A dual-interface payment card (also known as a DI card) is visually similar to a typical contact-only payment card. The contact plate (for the contact interface) may have six or eight pins.

A dual-interface card has only one different visual mark, the "Contactless Indicator" (Figure 1), which is licensed by EMVCo. The color of the symbol can be black or white; the color chosen will depend on the color of the card's artwork.[2]

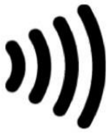


Figure 1. EMVCo Contactless Indicator

During the dual-interface card artwork design phase, issuers should determine where to put the contactless indicator symbol. The symbol should be placed so that it is noticeable to a cardholder since it indicates that the card has the additional contactless interface to communicate with a terminal. Placing the contactless indicator on the front of the card increases awareness. Issuers should consult with payment network guidelines for additional information on placement of the indicator.

Figure 2 shows examples of dual-interface card artwork.

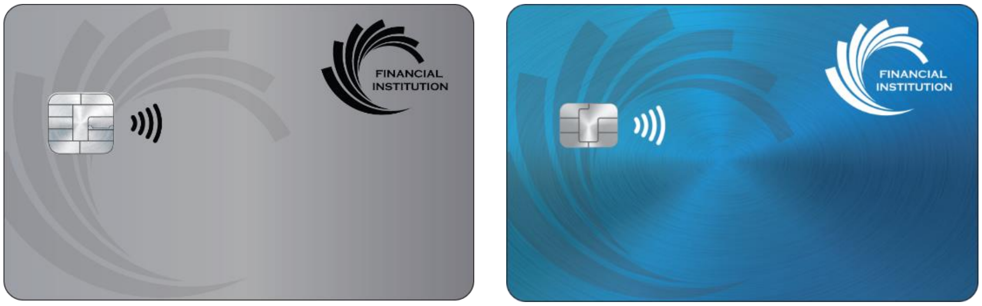


Figure 2. Examples of Dual-Interface Card Artwork with Contactless Indicator

2.1.2 Manufacturing Difference from a Contact Card

The dual-interface card has an embedded antenna in the card body. The antenna is typically invisible to the cardholder. The antenna performs two functions:

[2] See additional information at the EMVCo web site, https://www.emvco.com/about/trademark-centre/.

1. Receives power from the terminal to the chip on the card
2. Transmits transaction data wirelessly between the chip and terminal

The antenna can have either a wired or wireless connection with the chip on the card. The antenna size may differ; there are “full-size,” “3/4-size,” and “half-size” antennas.

If an issuer decides to use embossing on their dual-interface product, it is important to know the size, type and position of the antenna in the card body. The embossing areas should not cross the antenna. The card manufacturer/card vendor can provide issuers/personalizers with a detailed description of the antenna type and size.

Dual-interface card production is more complex than contact card production, due to additional materials (antenna layer), the enhanced chip module with the contactless interface, and additional steps in the card manufacturing process.

Figure 3 provides an illustration of the construction of a dual-interface card.

Figure 4 illustrates two methods for connecting the antenna to the chip on the card – inductive/magnetic coupling and direct connection.

Figure 5-Figure 8 show dual-interface card demonstration samples with different types and sizes of antennae and with embossing.

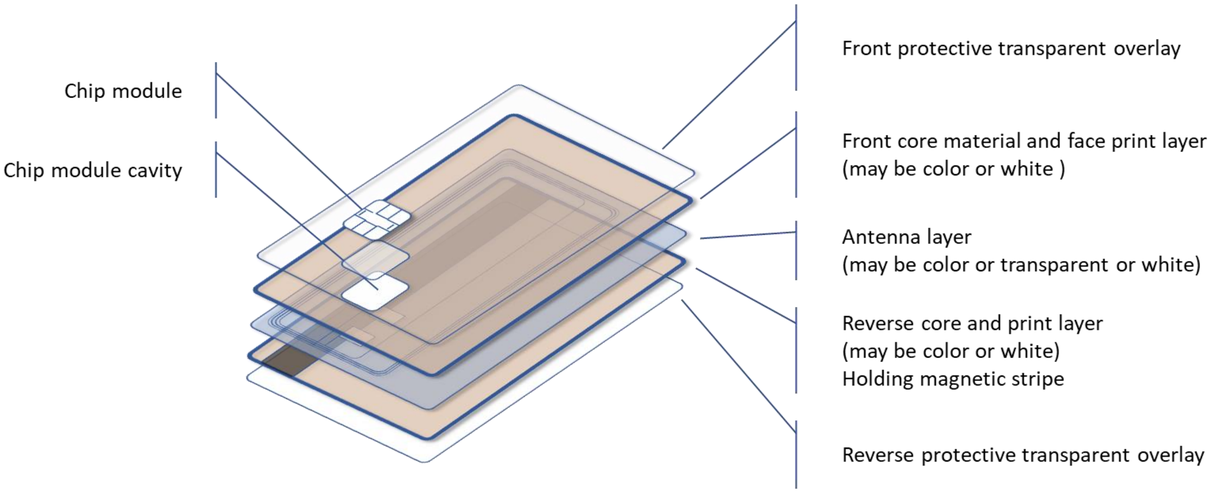

Chip module
Chip module cavity
Front protective transparent overlay
Front core material and face print layer
(may be color or white)
Antenna layer
(may be color or transparent or white)
Reverse core and print layer
(may be color or white)
Holding magnetic stripe
Reverse protective transparent overlay

Figure 3. Dual-Interface Card Construction

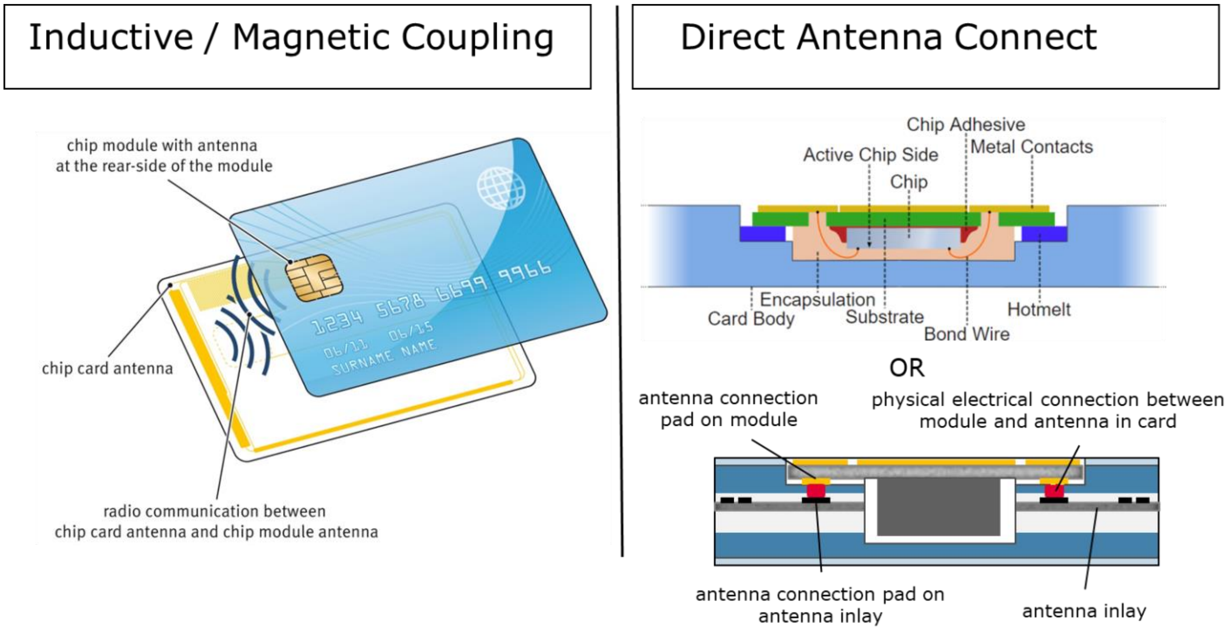


Figure 4. Technologies Used for the Antenna to Chip Connection

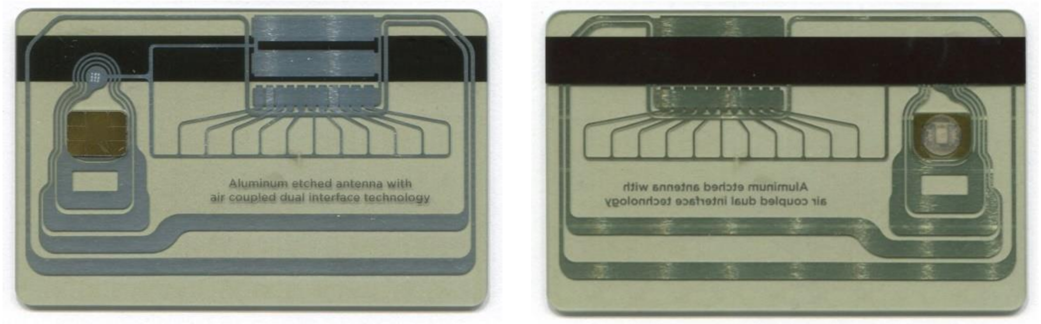

Aluminum etched antenna with
air coupled dual interface technology

Figure 5. Dual-Interface Card Sample with Aluminum-Etched Antenna

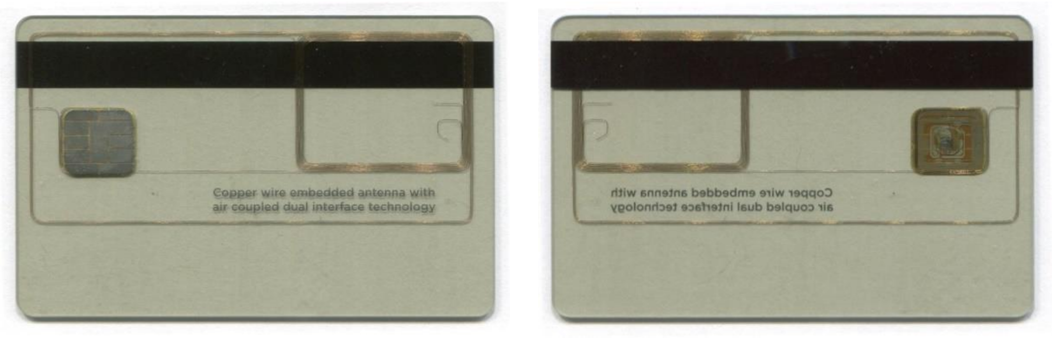

Copper wire embedded antenna with
air coupled dual interface technology

Figure 6. Dual-Interface Card Sample with 3/4-Size Embedded Copper Wire Antenna

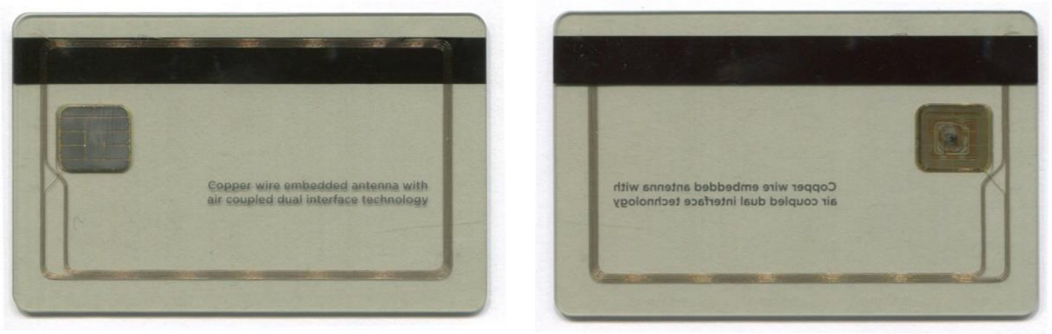

Copper wire embedded antenna with
air coupled dual interface technology

Figure 7. Dual-Interface Card Samples with Full Perimeter Embedded Copper Wire Antenna

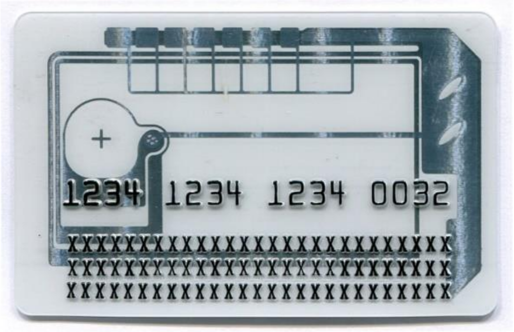


Figure 8. Dual-Interface Card Sample with Embossing and Aluminum-Etched Antenna

2.2 Software

A dual-interface chip, much like a contact only chip, contains a secure chip operating system and a set of one or more payment applications.

2.2.1 Operating System (OS)

The chip is powered and the chip OS functions through either the contact or contactless interface. The chip OS handles the communication between the chip and the terminal using the appropriate communication protocols and security mechanisms.

2.2.2 Payment Application

The payment application functions in compliance to both EMV contact and contactless functional specifications and the specific payment network specifications for the technology.

The following are examples of high-level requirements of these specifications.

- Both contact and contactless interfaces have the same Application Transaction Counter (ATC) that is incremented sequentially regardless of the interface used.[3]
- The contactless interface will not provide access to cardholder data which was only intended for use with the contact interface (e.g. due to security restrictions).

[3] Please consult with the payment networks for guidance on ATC validation on the host. Payment networks are advising that transactions should not be declined based only on the ATC being out of sequence.

- The application may have different cardholder verification method (CVM) requirements when accessed through the contactless interface.
- ODA may be supported on both or only one of the interfaces. Consult with the payment networks for guidance on use of ODA.

The payment application is interface-aware and applies functional and security responses accordingly.

If supported by the payment network application, the same Cryptogram Version Number (CVN) or cryptogram algorithm should be configured for use across both interfaces to simplify host cryptogram verification.

2.2.3 Proximity Payment System Environment (PPSE)

PPSE serves a directory of all AIDs available on the card that the terminal can select over the contactless interface. For debit cards, PPSE would contain two AID entries – the global AID and the U.S. Common Debit AID. PPSE is a mandatory application for fast contactless transaction processing and needs to be personalized and activated on dual-interface cards.

2.3 Issuer Considerations in Implementing Dual-Interface Cards

In the U.S. post-EMV market environment, one of the next issuer considerations is whether or when to begin issuing dual-interface credit and debit cards. The introduction and promotion of the various mobile payment products (e.g., Apple Pay, Google Pay, Samsung Pay) have provided an impetus for issuers to review the opportunity to issue dual-interface cards. While the shift from contact chip interface cards to mobile/virtual cards seems the most efficient route to support contactless transactions, consumers continue to show a preference to use their cards rather than their phones. That said, the speed and efficiency of “tap and go” contactless payment for the consumer are very real benefits, and dual-interface cards are a solid bridge between contact cards and mobile contactless payments.

While the U.S. prepares to adopt contactless payments, dual-interface cards are expected to play a leading role in this transformation. Various market forces appear to be converging to drive the issuance of dual-interface cards, including: mobile payments product introduction and promotion; chip expiration dates on the initial EMV cards issued, with the need to purchase new chips; and lower dual-interface chip costs.

Dual-interface card issuance planning is an opportunity for issuers to segment, innovate and redesign card products while offering cardholders convenience and security.

Noted below are key considerations for issuers in analyzing and defining their issuance strategy.

i. **Dual-interface chip**: Dual-interface chip technology has advanced over the years with the U.S. benefiting from the most advanced chips and payment applications. Choosing the right chip with the maximum expiration option and supporting the latest recommended payment application will benefit long-term issuance planning.

ii. **Card design**: All major payment networks provide design guidelines that include the contactless indicator to physically identify a card capable of contactless transactions. Issuance of dual-interface cards is an opportunity for issuers to redesign the card artwork. Antenna material, such as aluminum or copper, size and shape can serve to complement design and graphical personalization options (e.g., for translucent cards). Card material (e.g., clear, titanium, plastic) should also be considered for the potential impact on acceptance.

iii. **Card manufacturing**: Choosing a partner with expertise in dual-interface card manufacturing is a consideration, in addition to the manufacturer having sustainable manufacturing capacity and strong supply chain. Payment network approval of dual-interface card manufacturing is site-specific.

iv. **Card personalization profiles**: Payment networks have provided recommended personalization profiles that take into consideration the need for fast transactions at the point of sale (POS) and that address new segments for contactless open payments like transit. Card personalization software or personalization service providers' readiness to support these recommended profiles is important in planning issuance. To be backward compatible with POS terminals that support contactless Magnetic Stripe Data (MSD), some personalization profiles may require support for MSD. (See Section 5.2 for additional information on MSD.)

v. **Instant issuance**: If the issuer offers instant issuance of credit or debit cards, the vendor's ability to support dual-interface card personalization with the same profile used for central issuance should be considered in the planning.

vi. **Additional cryptographic keys**: Offline data authentication (ODA) is a feature required by some payment networks and included in the recommended profiles by other payment networks to primarily address the transit segment. To support this functionality, issuers must generate new sets of RSA keys for card personalization. Choosing the right key length for the profile and scheduling key generation sessions are recommended parts of the personalization setup planning. More information on the impact of key length on transaction time is addressed in Section 5. In addition to ODA keys, a new dynamic card security code key is needed when implementing MSD.

vii. **Processor readiness**: Issuer processor services need to support: identification of the POS entry mode (contact or contactless) for a dual-interface card transaction; certified readiness to authenticate a contactless transaction; and management of chosen risk management features. In addition, processor readiness to offer stand-in or other services to identify and authenticate MSD transactions (which uses a specific cryptogram) is a consideration.

viii. **Card issuance planning**: With no deadline set to migrate to dual-interface cards, issuers have the flexibility to segment their card base in planning their issuance strategy. Criteria may include: zip codes with proximity to transit stations; frequent overseas travelers; products that encourage conversion of cash to electronic transactions; choice between credit or debit portfolios or both. Natural reissuance is an option for migrating the wider card base.

ix. **Education**: For a better customer experience, call center employees should be trained to address queries from cardholders related to security, availability of a dual-interface option for the requested product, and transaction details. As proven in other markets, awareness is key to the success of contactless adoption. Industry best practices for cardholder education include: updates to the issuer website with educational information on how to tap to pay with cards; communication material in the card carrier and the card package proactively informing cardholders of the changes.

2.4 Market Considerations

Dual-interface cards have been successful globally, with the UK, Canada and Australia leading in contactless adoption. Experience in countries that have moved to contactless has shown the contactless-capable cards displace cash and drive increased transactions (i.e., "top of wallet" behavior).[4]

As of July 2018, Mastercard and Visa reported the following statistics on contactless acceptance in the U.S.

- 46% of transactions occur at contactless-enabled merchants
- 70% of merchant locations are capable of contactless transactions
- Over 95% of new terminals shipped are contactless capable
- A 10% year-on-year increase in active unique merchant in the U.S has been seen

3 Streamlining the Checkout Process with Dual-Interface Cards

In response to concerns about chip processing speeds raised by various stakeholders, the U.S. payments industry developed a faster, more streamlined processing method at the POS outlined in the U.S. Payments Forum white paper, "Optimizing Transaction Speed at the Point of Sale."[5]

Merchants and cardholders alike have communicated that chip transactions "take a long time to complete" compared to magnetic stripe transactions. Contactless transactions typically take less than 0.4 seconds for card and terminal interaction, with faster speeds typically required for transit.

In reality, a chip transaction conducted on a fast network connection is only marginally slower than an equivalent transaction conducted using a magnetic stripe card. There are, however, two requirements for chip processing that do make contact transactions take longer to complete. These requirements, combined with an unfamiliar experience, heighten the perception that the transaction is "slow."

Traditional EMV processing:

1. Requires that the final tally or total amount be available prior to building the authorization message.
2. Typically requires that the card remain in the reader until the authorization response is received from the issuer.

Neither of the above is true for magnetic stripe transactions.

Contactless transactions don't have the second requirement for the chip to remain in the terminal until transaction completion; however traditional contactless EMV transaction processing may require the final amount to be known before card is tapped.

[4] "Contactless Payments: Proposed Implementation Recommendations," Secure Technology Alliance Payments Council white paper, January 2018, https://www.securetechalliance.org/publications-contactless-payments-proposed-implementation-recommendations/.

[5] http://www.uspaymentsforum.org/optimizing-transaction-speed-at-the-point-of-sale/

In order to address these (real and perceived) issues, the U.S. payment networks developed "Faster EMV"[6] (also known as Amex Quick Chip, Discover Quick Chip, Mastercard M/Chip Fast, and Visa Quick Chip) solutions that mitigate the impact of both of these requirements, thus addressing both problems relating to transaction speed.[7] The Faster EMV solutions in a contactless environment allow the cardholder to tap the contactless payment device at any point during the checkout process. This additional function is established at the terminal and is not impacted by dual-interface card personalization.

Furthermore, to provide a more convenient and streamlined payment experience, some payment networks have established transaction dollar amount thresholds, under which terminals may not require cardholder verification (such as asking for PIN or signature). These limits are set at the terminal and are generally not impacted by dual-interface card personalization.

3.1 Dual-Interface Personalization Considerations for Faster EMV

Contactless transactions are like Faster EMV contact transactions in that they don't support the Authorization Response Cryptogram (ARPC) and issuer scripting. Considerations that should be taken into account during personalization include whether the card supports offline transactions and/or offline PIN. Issuers may decide to use different parameters for the contact and contactless card interfaces (e.g., for offline PIN).

In addition, issuers are encouraged to support quad-speed cards, as described in the U.S. Payments Forum Faster EMV white paper, to ensure fast transactions across both interfaces.

[6] "Faster EMV" is an umbrella term to describe the optimized online-only EMV transaction processing solutions announced separately by American Express, Discover, MasterCard, and Visa. These solutions retain the security features of EMV, while removing dependencies that can negatively influence the cardholder perception of transaction time.

[7] Additional details on Faster EMV can be found in the U.S. Payments Forum white paper, "Optimizing Transaction Speed at the POS," available at http://www.uspaymentsforum.org/optimizing-transaction-speed-at-the-point-of-sale/.

4 Offline Data Authentication (ODA)

An important consideration in the issuance of dual-interface cards is the inclusion of ODA – allowing the terminal to authenticate the card offline. In the U.S., support for ODA is supported primarily to address requirements for the transit vertical; however, other uses of ODA are possible for some payment networks. ODA relies on a public key infrastructure (PKI) that enables terminals to authenticate cards, and in the case of a transit gate, to allow the cardholder to enter a train station or board a bus.

It is important to distinguish between online and offline authentication. Online authentication is the process of validating the Authorization Request Cryptogram (ARQC) by the issuer's host systems during authorization processing.

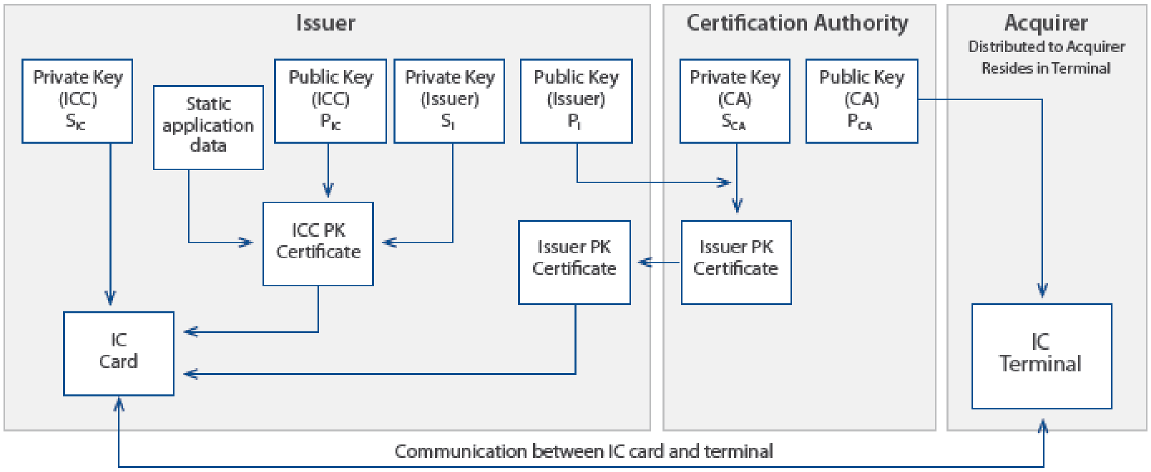
With ODA, a set of data is sent to the card to be digitally signed by the card private key; the signed data is sent back to the terminal. The terminal uses the card public key to validate the card's digital signature which authenticates the card.

Both the personalization process and the authentication process are impacted in implementing ODA.

There are different methods of ODA – Dynamic Data Authentication (DDA), Combined DDA/Application Cryptogram (CDA) and Static Data Authentication (no longer used). This white paper describes DDA processes. Issuers should check with their payment networks about ODA requirements and select the appropriate ODA method for their cards.

4.1 Personalization of the Card for the ODA Process

During the personalization process, the relevant keys and certificates are personalized onto the card and the terminal is loaded with a key, as shown in the diagram in Figure 9.



Card provides to Terminal:

- Issuer PK Certificate (P_I signed by the CA S_{CA})
- ICC PK Certificate (P_{IC} and static application data signed by issuer S_I)
- Card and terminal dynamic data and digitial signature (dynamic data signed by Card S_{IC})

Terminal:

- Uses P_{CA} to verify that the issuer's P_I was signed by CA
- Uses P_I to verify that Card P_{IC} and static application data were signed by issuer
- Uses P_{IC} to verify the card's signature on the dynamic data

Figure 9. Offline Data Authentication for DDA

The card is personalized with:

- Card Private Key (This key is stored securely and never leaves the card.)
- Card Public Key Certificate (This is sent to the terminal during a transaction.)
- Issuer Public Key Certificate (This is sent to the terminal during a transaction.)

The terminal is also loaded with:

- The Certificate Authority (CA) Public Key (Generally the CA is the payment network.)

These keys and certificates are used in the process to authenticate the card.

4.2 Authentication of the Card using the ODA Process

The following ODA process is used during a transaction to authenticate a card.

- The card is sent dynamic application data and a random number generated by the terminal. The card signs this data with its internal Card Private Key and it returns the signed dynamic application data to the terminal.
- The terminal recovers the Issuer Public Key using the CA Public Key.
- The terminal recovers the Card Public Key using the Issuer Public Key.
- The terminal uses the Card Public Key to validate the dynamic signature.

4.3 Chain of Trust

For ODA, trust works on an implicit or indirect trust. (See Figure 10 and Figure 11.)

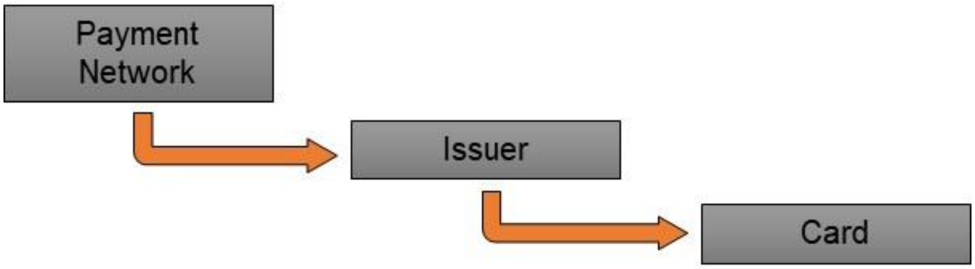


Figure 10. Chain of Trust with ODA

The acquirer trusts the payment networks and loads the CA public keys on their terminals.

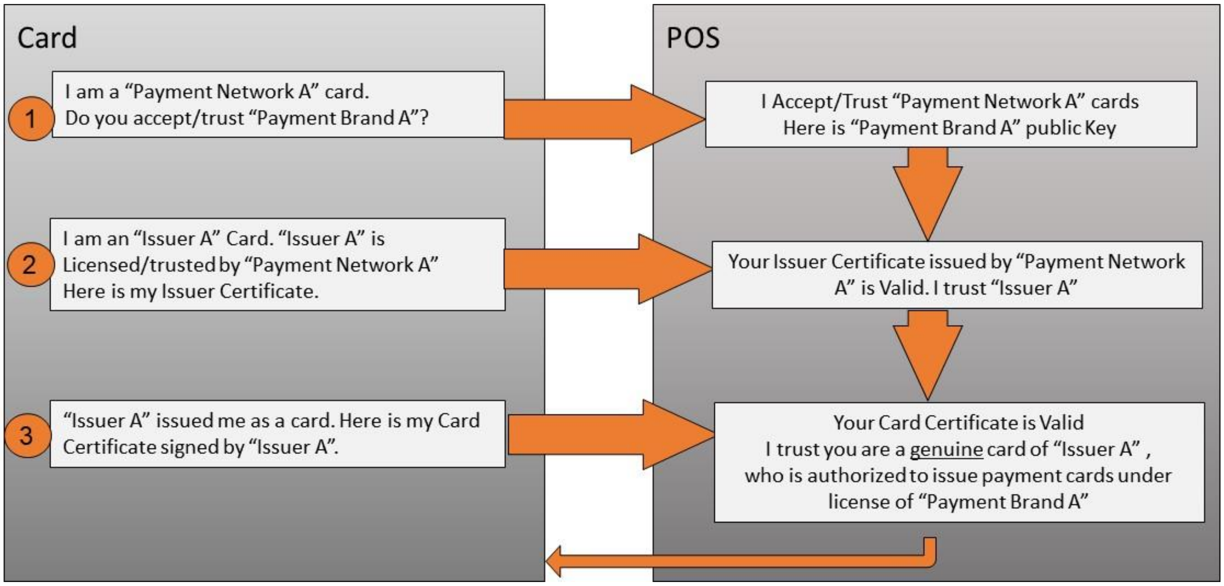
The payment network's CA signs the Issuer Public Key and creates the Issuer Public Key (IPK) Certificate that is loaded on the card.

Since the payment network is trusted, the payment network's CA public key is used to validate the IPK certificate that was loaded on the card and the IPK Public Key is extracted. The issuer of the card is now trusted.

The validated Issuer Public Key is used to validate the Integrated Circuit Card (ICC) Public Key Certificate and extract the ICC Public Key. The card is now trusted.

The validated ICC Public Key is used to validate information between the terminal and the chip.

What results is a chain of trust that originates from the trusted payment network's CA.



Card

1 I am a “Payment Network A” card. Do you accept/trust “Payment Brand A”?

2 I am an “Issuer A” Card. “Issuer A” is Licensed/trusted by “Payment Network A” Here is my Issuer Certificate.

3 “Issuer A” issued me as a card. Here is my Card Certificate signed by “Issuer A”.

POS

I Accept/Trust “Payment Network A” cards Here is “Payment Brand A” public Key

Your Issuer Certificate issued by “Payment Network A” is Valid. I trust “Issuer A”

Your Card Certificate is Valid I trust you are a genuine card of “Issuer A” , who is authorized to issue payment cards under license of “Payment Brand A”

Figure 11. Chain of Trust in Straightforward Language

5 Card and Personalization Recommendations

The EMV specifications are designed to facilitate both offline and online card authentication. Issuers are encouraged to understand the advantages and disadvantages of using online and/or offline authentication, as well as understanding network requirements and recommendations for card personalization.

5.1 ODA Personalization

Most of the initial EMV specifications were designed to facilitate offline authorized transactions to address the lack of online infrastructure that was the case for many countries at the time. In the U.S., which has an online infrastructure, payment networks recommend online authorization when implementing ODA.

5.1.1 Requesting Issuer Certificates

Issuer certificates are generated by payment network CAs based on the keys generated by the issuers.

The issuer generates the Issuer Public/Private Key Pair. The issuer will store the Issuer Private Key securely and send the Issuer Public key (IPK) to the CA. The CA signs the IPK with the CA Private Key to create the IPK certificate. This certificate is made available to the issuer.

The typical process is as follows:

- The issuer generates Issuer Public/Private Key Pair.
- The issuer selects the CA key length with the corresponding expiration date to be used for the issuer certificate. The issuer should seek payment network guidance for selecting the key length.
- The issuer may need to generate a tracking number and a serial number based on CA requirements.
- The issuer (or its agent) creates a certificate request file with the Issuer Public Key. The file must be in the format specified in the CA’s technical requirements.
- The issuer sends the certificate request file to the CA.
- The issuer picks the CA keys to be used to sign the Issuer Public Key.
    - The issuer must ensure that the requested key can be used. In all cases, the length of the CA key must be equal to or greater than the length of the issuer's key being signed.
    - The issuer must ensure that the corresponding CA key expiration date exceeds the intended expiration date of the cards issued.
- The request is reviewed by the CA and feedback is provided to the issuer.
- The CA generates the issuer certificate.

5.1.2 Obtaining Issuer Certificates

The CA provides the certificate response to the security officer(s) of the issuer (either internal or delegated party). This delivery may take different forms, such as email or download from a web site.

Each CA may have different rules for distribution of certificates and the party that can request and receive certificates. Issuers should check with the appropriate CA for details of the process.

5.1.3 Delegating the Issuer Certificate Request

The issuer may choose to delegate the issuer certificate request process to its personalization or technology service provider.

Due to the nature of public key cryptography – which is performed between the card and the terminal – the required keys and certificate do not need to reside at the issuing host and are only needed during the card personalization process.

The delegation process is well defined by each CA. The authorized business and/or security contact at the issuer will need to complete and authorize a certificate request authorization form and submit it via an established channel – either an original paper form or, if supported, a digitally-signed electronic document. The service provider who will be requesting the certificates on behalf of the issuer must have registered at least two security officers who have the authority and the necessary tools to:

- Generate and submit security issuer certificate requests
- Receive and import the CA certificate response files
- Receive and import the issuer certificate response files

5.1.4 Key and Data Generation for ODA

Personalization of dual-interface cards with ODA support will require several key and data generation steps.

5.1.4.1 Issuer Private/Public Key Pair Generation

Before requesting an issuer certificate from the CA (see Section 5.1.1), the issuer (or the delegated party) generates a unique Issuer Public/Private Key pair. Typically, the key pair is unique for each BIN. The key management system used to generate the key pair must be also able to generate an issuer certificate request file per the CA specification. This file, although it contains only the Issuer Public Key, is still submitted securely to the CA to ensure the integrity of the process.

The Issuer Private Key is used subsequently to generate a certificate for each individual card during the card data generation process.

The CA may have certain requirements for the length of the issuer key. Table 1 shows the issuer key maximum length, as defined by the EMV specifications. Issuers should consult with the payment networks for additional information on key length. The CA key that is signing the request determines the maximum expiration date of a resulting signed certificate.

CA Key Length	Maximum Issuer Key Length
1984	1976
1408	1408

Table 1. CA and Issuer Key Length

For issuers supporting both central and instant issuance, it is recommended that each service provider (if different) generates additional Issuer Private/Public Key Pairs to avoid exchanging keys between different parties. The issuer may delegate the certificate request to only one entity who would submit the requests to the CA. Note that the certificate requests contain only the public part of the key. Issuers should consult with their technology providers for more details.

5.1.4.2 ICC (Card)-Unique Private/Public Key Pair Generation

Every EMV card issued with ODA support will have a unique card key pair. The ICC key length is based on issuer choice with guidance from the payment networks.

The card key is shorter than the issuer key. Check with the payment networks for specific recommendations for key length. Generating card-unique RSA key pairs is an intensive cryptographic function performed for each personalization record. Some personalization systems are able to pre-generate and encrypt card RSA key pairs ahead of time and use them during the personalization process. This may improve the data generation and personalization timing. If the personalization system has adequately powerful hardware security modules (HSMs), this process may also occur in-line with the personalization process with minimal timing impact.

5.2 Personalization of Cards Supporting Contactless MSD

5.2.1 Why Support Contactless MSD?

Contactless payments relying on magnetic stripe data (MSD) have been available since 2005.

While EMV-enabled POS terminals include EMV contactless capability, legacy MSD contactless terminals still represent a meaningful percentage of the contactless POS infrastructure in the U.S. To provide cardholders with the best user experience, issuers should work with the payment networks and card or device personalization vendors to ensure that all EMV dual-interface cards and EMV contactless-capable form factors are backward compatible with contactless MSD terminals.

5.2.2 Key and Data Generation for Contactless MSD

When implementing MSD support for contactless a new key may or may not be required. This key may be called the Dynamic Card Verification Key (CVK), depending on the payment network. This key is diversified for each card and encoded in the chip, similar to the other EMV application keys. The key is used to generate a dynamic card security code (e.g., CVV/CVC) value or MSD cryptogram during a contactless MSD transaction. Issuers should consider managing this key in the same way as they currently manage other symmetric card keys.

5.3 Personalization of Contactless-Relevant Data Elements

5.3.1 PPSE Personalization

The Proximity Payment System Environment (PPSE) is required by all payment networks and used as the selection mechanism for the required application. For multi-network acceptance, PPSE allows a POS terminal to quickly obtain all the available payment networks and applications with a single command and to make an immediate choice based on application identifier (AID) and/or priority and kernel availability.

The PPSE includes the application data for the terminal to quickly identify the applications on the card. The PPSE includes: application identifier (AID), label, priority indicator, and any payment-network-specific tags.

5.3.2 Contactless Data Elements

Any AID application having access to the contactless interface, in addition to the contact interface, will require extra data be personalized in the card.

Some data are defined in the EMV specifications; other data are defined by the payment network specifications.

Examples of typical data (not exhaustive) required for a contactless interface are shown below:

- Contactless Select
    - Application Label, Priority Indicator, Language Preference, Issuer Discretionary Data, plus other data
- Contactless GPO (answer to Get Processing Option)
    - Application contactless capabilities (MSD and EMV may be different)
    - Contactless application data directory
- Contactless card risk management
    - Velocity checks, limits, CVM, other behaviors
- Contactless readable data
    - Primary account number (PAN), dates, Application Usage Control (AUC), Issuer Action Codes (IACs), CVM, Track2 equivalent data
- Contactless application keys
    - MSD key for dynamic CVC/CVV generation
    - EMV keys for contactless cryptogram generation
    - ICC Private Key
- Additional data based on payments networks and specifications

5.4 Personalization Time Duration/Efficiency

Dual-interface card personalization may be done via the contact or contactless interface; however, it is usually done through the contact interface, so personalization equipment does not need to be changed.[8] It is recommended that a quality assurance (QA) test be performed for the contactless interface at the end of the personalization process.

Compared with contact-only profiles that may not support ODA, the personalization time of dual-Interface ODA profiles may be longer due to the larger amount of data that must be personalized (e.g., PPSE data which is mandatory for contactless cards, ICC RSA key pair, certificates required for ODA).

The personalization time also depends on the following parameters:

- EMV profile
- Personalization environment: When personalization data (with keys and certificates) is generated prior to personalization, personalization time is only for loading data to the chip; whereas, when data generation is done along with personalization, personalization time could be longer because it includes data generation (e.g., in the instant issuance use case).
    - Contributing parameter differences:
        - Central issuance vs. instant issuance at branch
        - ‘One step’ mode (data preparation and encoding performed together) vs. personalization only (data preparation done offline in batch mode)

[8] Payment networks also advise using the contact interface for in-branch personalization for security reasons. If using the contactless interface, it is recommended that full data encryption be enabled for all personalization commands.

- Chip capability to support the increase in baud rate and clock speed: If contact baud rate/clock speed increase is not supported, the contactless interface is typically capable of faster personalization, although this may require equipment updates.
- Key size
- Cryptographic equipment performance (especially for an on-the-fly mode as the ICC RSA key pair is generated at personalization time)
- Communication speed: Using high communication speed for personalization will greatly reduce the personalization time. Consult with the chip vendor and the personalization solution provider for the possibility of supporting high communication speed.

Note that because of the antenna, dual-interface cards are more sensitive to electromagnetic interference and electrostatic discharge. Consult with the service or equipment provider on how to address these potential issues.

The following are recommended best practices:

- Invest in a key management system that:
  - Is ready to support the certificate request to the financial payment network CA.
  - Is scalable to add more HSMs to manage the additional cryptography requirement.
- For central issuance, perform an inline QA for the contactless interface.
- Dual-interface card personalization takes longer, so more couplers may be needed.

5.5 Shipment of Dual-Interface Cards

It is recommended that dual-interface cards be sent to the cardholder inactive and require activation prior to first usage, as done for contact-only cards. This activation may be done through the usual channels.

Although contactless transactions are protected by strong encryption and one-time values specific to each transaction, some card data is available through the contactless interface when it’s active. As a result, it may be possible that some card data (the card number and expiration date) can be collected from the card during shipment by tapping the envelope to a reader without opening the envelope. Data collected with this tap would be very limited; however, issuers may consider further precautions to prevent unwanted collection of card data prior to cardholder activation.

The following measures may be considered for this purpose:

- Use a protective sleeve/envelope for dual-interface card shipment. Such sleeves and envelopes can prevent contactless data access while the card is in the sleeve/envelope.
- Ship cards with the contactless interface disabled and require an initial contact chip transaction to enable the card’s contactless interface. Availability and specific operation of enabling the contactless interface function depend on the payment network application specifications being used. Enabling may be automatically triggered by the card itself with the first contact transaction or require issuer scripting. Issuers should consult with their payment networks and card vendors for further guidance. It’s recommended that issuers enabling the contactless interface in this way clearly communicate this activation process to the cardholders, since cardholders will not be able to use the contactless interface until it’s enabled.

5.6 Recommended Card Profiles

Table 2 includes the global payment network recommended card profiles for dual-interface cards. Please note:

- Recommend card profiles provided are for U.S.-issued cards.
- Exceptions to the network requirements may be granted upon issuer request.

Payment Networks	Standard Profiles (Y/N)	ODA Required (Y/N)	Online Authorization Only (Y/N)	EMV Contactless Support	MSD Support	U.S. Debit Contactless	ODA Support on U.S. Common AID
American Express	Y	Y	N	Required for all dual-interface cards	Required for all dual-interface cards	N/A	N/A
Discover	Y	Required for contactless; optional for contact interface	N	Required	MSD with dCVV only (Zip)	U.S. Common AID required on contactless interface	Y
Mastercard	Y	Y	N (online required, but offline supported)	Required	MSD	U.S. Common AID required on contactless interface	Y
UnionPay	Y	Y	Y	Required	N/A	U.S. Common AID required on contactless interface	Y
Visa	Y – Processor Express	ODA on contactless interface only	Y	Required	MSD with dCVV only	U.S. Common AID required on contactless interface	N*

**Technically possible, but separate contactless certificate must be created and provisioned. Please contact the debit payment networks for more information.*

Table 2. Recommended Card Profiles

6 Use Case: Transit Vertical

The transit industry has long used contactless technology for fare collection to provide a significant improvement over magnetic stripe tickets and tokens. However, transit closed-loop contactless card-based systems have been costly to operate and maintain due to the systems' card-centric nature. In addition, since each transit system has a unique fare collection system, customers need to learn how the fare and ticketing systems work for each city they visit. Then, customers must convert "real money" into "transit money" on the closed-loop card, causing queues and frustration at various pinch points in transit locations.

The introduction of bank-issued contactless payment cards using open standards has been seen as an opportunity to reduce costs and improve the customer proposition for transit. Rather than transit agencies operating their own card issuance systems, they simply deploy a system that can accept the cards customers already have. This can help reduce costs and barriers to system entry, and can improve the customer experience by allowing them to take transit as soon as they arrive in a city.

The need to move so many people around a city presents some unique challenges for transit operators when implementing contactless open payment cards. Many transit systems still use station infrastructure built in the early 1900s and passenger safety and movement are key requirements. To handle rider volume, the transit industry requires transaction time at the transit gate of 500ms or less. As a result, there is not enough time to seek an online issuer authorization for transactions. Instead, two key risk management features, described in this section, may be used for transit.

6.1 ODA with Online Authorization

As already defined, ODA relies on a PKI that enables terminals to authenticate cards, and in the case of a transit gate, will allow the cardholder to enter the train station or board a bus with the transit agency knowing that the card is genuine.

For the transit environment, transit terminals should be set up with ODA followed by an online authorization. Consult with the payment network specifications for additional information on how this is supported. For non-transit environments, requirements supporting ODA may differ based on the payment network.

Figure 12 describes an example of the flow of an online authorized transaction with ODA for transit.

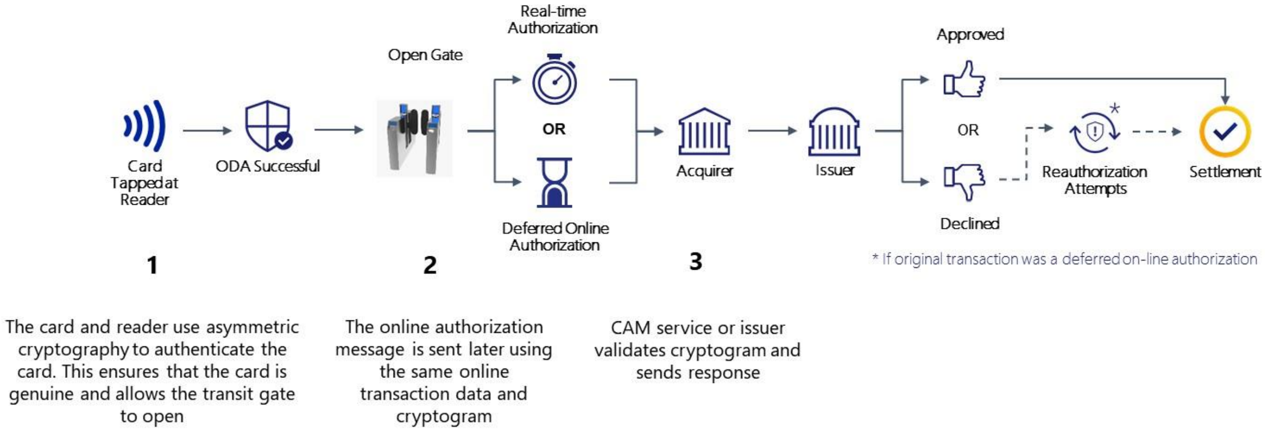

Card Tapped at Reader
ODA Successful
Open Gate
Real-time Authorization
OR
Deferred Online Authorization
Acquirer
Issuer
Approved
OR
Declined
Reauthorization Attempts
*
Settlement
* If original transaction was a deferred on-line authorization
1
The card and reader use asymmetric cryptography to authenticate the card. This ensures that the card is genuine and allows the transit gate to open
2
The online authorization message is sent later using the same online transaction data and cryptogram
3
CAM service or issuer validates cryptogram and sends response

Figure 12. Online Authorization Including ODA for Transit

The most critical piece of any chip transaction is the dynamic cryptogram used in online authorization. In transit, ODA is used to authenticate the card so that the transit gate opens and the transit agency knows the card is not counterfeit. Later in the day, the actual payment transaction occurs, and online authorization occurs. This authorization checks for lost and stolen cards and performs other risk management checks. The transaction information is sent to the issuer, along with a transaction-specific cryptogram, and the issuer either approves or declines the transaction.

To support transit, contactless payment devices should be personalized with ODA support in order to process transactions that required offline authentication with online authorization. See additional information on personalization in Section 5.

In the event of a failed authentication or authorization decline, one optional control available to transit agencies is a "risk list." For a complete discussion on the use of list options (white or black lists), please see the U.S. Payments Forum white paper, "Transit Contactless Open Payments: Technical Solution for Pay As You Go."

Additional information on the implementation of transit contactless open payments acceptance can be found in the U.S. Payments Forum transit use case white paper.[9]

[9] "Transit Contactless Open Payments: Technical Solution for Pay As You Go," Version 2.0, Sept. 2018, http://www.uspaymentsforum.org/working-committees-sigs/transit-contactless-open-payments-working-committee/

7 Testing and Certification

7.1 Personalization Validation Testing

Similar to contact-only cards, payment networks have personalization validation testing requirements for dual-interface cards. These processes help to ensure the card personalization has been performed successfully, and to mitigate the risk of interoperability issues.

The payment networks are requiring or recommending support of ODA with the contactless interface. ODA support adds some additional complexity, as the certificates must be validated in addition to the other data on the card. In particular, because the issuer certificate may be dependent on the BIN, each BIN should be tested. Issuers should consult with the individual payment networks for further information on personalization validation testing requirements.

The payment networks may have programs that allow simpler contact and contactless card validation. These programs allow the use of standard profiles to go through a full certification once per profile, after which an issuer onboarding on the same profile may be possible, without having to open a new testing project with the payment network. To simplify contactless deployment, issuers should consult with their technology providers or payment networks for further information on how to take advantage of the programs where supported.

7.2 Online-Only Testing and Certification

The same set of testing is currently done for both contact and contactless interfaces on EMV chip cards. Note that there may be differences in testing requirements across payment networks.

If the contact chip card was previously tested, the payment networks typically require the following to be tested:

- Purchases
- Reversals
- Refunds
- Online PIN validation
- Card Authentication Method (CAM) validation
  - Online cryptogram validation by the issuer
  - Stand-in validation of the cryptogram if supported for issuer
- Deferred authorization
- Transit transaction

In addition, if MSD is personalized on the card, payment networks require that the MSD application also be validated.

Payment networks typically include positive and negative transactions to ensure correct handling of declined transactions. These include but are not limited to:

- CAM failure
- Online PIN failure
- Deferred authorization
- Transit-specific failures (see Section 7.3)

Payment networks typically require transaction testing to be performed for both POS and ATM channels, depending on card support.

Contact the payment networks for additional details on testing and certification.

7.3 Transit Testing and Certification

Payment networks may require additional acquirer and issuer testing for transit implementation. Consult with each payment network for their requirements

7.3.1 Acquirer / Transit Agency / Merchant Testing

The following testing may be required to be performed by the acquirer and transit agency. Consult with each payment network for their requirements.

- Transit terminal testing – validating ODA and/or deny list check for opening the transit gate
- Back-end testing and certification to correctly handle various transit models and rules for different payment networks
    - Known-fare model
    - Mass Transit Transaction (MTT) – including aggregation

7.3.2 Issuer Testing

The following testing may be required to be performed by the issuer. Consult with each payment network for their requirements.

- Issuer host system testing for Mass Transit Transaction (MTT) certification
    - **Recognizing transaction data fields:** Issuers should use the key field values unique to MTT.
    - **Application Transaction Counter (ATC) processing:** Issuers that validate the ATC in authorization messages should be aware that the use of deferred authorization might cause ATCs in authorization requests to arrive out of order. Out of sequence ATC values (especially from transit merchants) do not necessarily indicate fraud and issuers should take this into account in their authorization decisions.
    - **Card issuance and personalization:** All cards and devices that issuers wish to enable for use in domestic or global transit environments should be personalized to support ODA for deferred online authorization.
    - **Merchant Initiated Transactions (MIT):** Issuers should expect to see system-generated merchant-initiated debt recovery transactions performed using the MIT framework, and must not decline an MTT based solely on a missing card security code.
    - **Cardholder Verification Limit (CVL)**: As the final fare of an MTT is not known at the time a card is presented to a reader, if the accumulated charge at the end of the day results in a transaction higher than the CVL, a valid CVM will still not be captured in the transaction. Therefore, Issuers should not decline an MTT based solely on a missing CVM.
    - **Issuer host system MTT certification**: Certification must be performed and include the following:
        - Deferred Authorizations: Issuers must be able to process deferred authorization transactions correctly. Correct processing can help to improve approval rates for

token-based and card-PAN-based payments originating from transit operators. Out of sequence ATC issues are believed to be the single biggest cause for unnecessary declines of MTTs; ensuring issuers manage ATC out-of-synchronization scenarios in transit transactions accordingly for any deferred authorization transit transactions is crucial.

- Handling shared risk, chargebacks and aggregation correctly
- Recognizing that the amount in Field 4 and tag 9F02 in Field 55 (used for the cryptogram) may not match
- Recognizing that the transaction must have been initiated from an Unattended Cardholder Activated Terminal (UCAT)
- Recognizing that the transaction must have been initiated by a contactless reader only
- Checking that the Merchant Category Code (MCC) code is one of the Transit MCCs

8 Conclusions

The U.S. Payments Forum developed this white paper to provide an educational resource for issuers and the issuing community, as a result of increased interest In dual-interface card issuance. A prominent use case for dual-interface cards globally is supporting their use in open-loop payment in transit systems.

The information presented in this white paper is intended to provide an overview of the differences between EMV contact and dual-Interface card personalization, the process for personalizing cards to support ODA, and the ODA transaction process. Issuers should consult their payment networks for additional details on personalizing dual-Interface cards and supporting ODA use cases.

9 Legal Notice

While great effort has been made to ensure that the information in this document is accurate and current, this information does not constitute legal advice and should not be relied on for any purpose, whether legal, statutory, regulatory, contractual or otherwise. All warranties of any kind are disclaimed, including all warranties relating to or arising in connection with the use of or reliance on the information set forth herein. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk.

It is important to note that the information provided in this document is necessarily limited in various respects. Among other things, it is limited to the information received from the payment networks and others that participated in developing this white paper. Where specific payment network positions are referenced, it should be noted that each payment network determines its own rules, requirements, policies and procedures, all of which are subject to change.

Prior to implementation, merchants, issuers, acquirers, processors and others interested in dual-interface card personalization and related implementation efforts are therefore strongly encouraged to consult with all applicable stakeholders regarding associated rules, requirements, policies and procedures, including but not limited to their respective payment networks and testing and certification entities, as well as state and local requirements.