A US PAYMENTS FORUM WHITE PAPER

Contactless Adoption at the ATM

Version 1.0

May 2024

U.S. Payments Forum
544 Hillside Road
Redwood City, CA 94062

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body that brings stakeholders together on neutral ground to enable efficient, timely and effective implementation of emerging and existing payment technologies. This is achieved through education, guidance and alternative paths to adoption. The Forum is the only non-profit organization whose membership includes the whole 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. The organization operates within the Secure Technology Alliance, an association that encompasses all aspects of secure digital technologies. Additional information can be found at http://www.uspaymentsforum.org.

Table of Contents

Executive Summary

In the past few years, contactless payment using Near Field Communication (NFC)-enabled EMV chip cards and mobile devices has emerged as a popular method for consumers to make and retailers to accept transactions securely and conveniently. Contactless technology provides an excellent opportunity for ATM owners to offer improved convenience for consumers with the same level of transaction security and integrity as contact EMV transactions. A contactless ATM platform also delivers the ability to implement advanced ATM features and protects against traditional card skimming. This white paper provides information for ATM owners who are planning to implement contactless EMV; it does not cover other forms of touchless payments (e.g., using QR codes).

When adding contactless to ATMs, ATM owners need to understand the differences between the transaction types. While contact EMV transactions require a payment card to be inserted into a terminal, contactless EMV transactions use radio frequencies (RF) to transmit payment information wirelessly. While both rely on technical EMV specifications that are defined and managed by EMVCo, they use different communication protocols and different transaction processes. In addition, transactions from NFC-enabled mobile devices (e.g., mobile phone, wearable) use a tokenized primary account number (PAN), replacing the PAN with a surrogate number.

Consumers are already using contactless payment at many retailers and are familiar with the EMV Contactless Symbol that indicates contactless acceptance. ATM owners should include the symbol on their ATMs when contactless EMV payment cards and NFC-enabled mobile devices are accepted and ensure the placement is in the area with the strongest signal.

As with all new payment technologies, implementers will find challenges with upgrading infrastructure, ensuring security, complying with industry standards and regulations, integrating with legacy systems, and testing the system end-to-end. To ensure interoperability, EMVCo and the payment networks have rigorous certification programs for both payment system components and end-to-end testing. In addition, ATM owners should evaluate the differences in software and hardware when choosing suppliers and are advised to establish collaborative relationships with trusted vendors who can provide guidance and support through implementation.

Through careful planning and implementation with trusted partners, ATM owners can provide consumers with convenient, secure contactless EMV transactions and a better customer experience.

1. Introduction

In recent years banks and ATMs have seen a dramatic shift in how consumers transact – from physical cash to digital transactions. As technology has advanced, many consumers now choose contactless payments as an alternative.

The trend to contactless transactions is increasing rapidly, making it a very exciting time for banking and retail organizations. The adoption of such convenient technology at the ATM has proven to be a great opportunity to improve the consumer experience, potentially reduce operational costs, and increase customer loyalty.

Contactless transaction adoption at the ATM is becoming increasingly popular as more and more people prefer their convenience and security. Contactless transactions can be completed with just a tap of a card or a tap of a mobile phone or wearable device, providing customers with a secure and efficient way to access their funds. By using contactless transactions at the ATM, consumers can save time and enhance their overall experience.

The main advantage of contactless transactions is convenience. Contactless is easy and intuitive to use so is an appealing choice for consumers.

Unlike contact transactions that require a consumer to insert the payment card into a terminal, contactless payments do not require any physical contact between the consumer and the terminal. This saves time and reduces wear and tear on payment equipment. Overall, the convenience advantages of contactless transactions make them an increasingly popular and desirable option for consumers.

As a result, an increasing number of financial and retail institutions are rolling out contactless payment technologies in their cash machines. In addition, with more banks taking advantage of these technologies, the future of contactless payments looks brighter than ever for consumers and organizations alike.

The objectives of this white paper, “Contactless Adoption at the ATM,” are to provide information for operators planning to adopt contactless acceptance at the ATM, and to suggest best practices for contactless transaction interoperability for all ATM providers.

The U.S. Payments Forum ATM Working Committee understands that multiple definitions of “contactless” transaction are used in the market. This white paper focuses on contactless EMV transactions completed with Near Field Communication (NFC)-enabled digital wallets and contactless-enabled EMV chip cards.[1]

Issuers work with the ATM networks to enable contactless transactions. Issuers must provide the BINs that participate in contactless transactions and ensure that the BIN tables are updated accordingly. Each network may have internal configurations that need to be switched on for enablement. The networks publish up-to-date BIN tables that the acquirers adopt to provision all contactless card transactions to allow for acceptance across all ATMs. Implementers are advised to check the payment network recommendations for chip provisioning.

This document is not intended to be a comprehensive textbook or step-by-step instruction manual. It is focused only on U.S. transactions and does not cover other transaction types (such as QR codes). In addition, magnetic stripe data (MSD) contactless transactions, using any form factor, are out of scope.

[1] The term “contactless transaction,” as used in this white paper, specifically means “contactless EMV transaction.”

The white paper also does not discuss contactless transaction security.[2] Where relevant, the paper provides implementation information and suggests industry contacts with whom to engage to help implement contactless transactions successfully.

This document provides information primarily intended for ATM providers, acquirers, processors, and vendors who are preparing to implement contactless EMV transactions at their ATMs in the United States. The white paper also highlights how contactless EMV transactions differ from contact-based EMV transactions and covers contactless transactions using a plastic chip card, NFC-enabled mobile device or wearable device, or other NFC-enabled form factor.

[2] For a detailed discussion of security, see the Secure Technology Alliance publication, "Contactless Payment Security Questions & Answers," available at https://www.securetechalliance.org/wp-content/uploads/Contactless-Payments-Security-QA-FINAL-Dec-2016.pdf.

2. Adding a Contactless Environment to ATMs

Instead of physical contact, contactless payments rely on radio frequency (RF) technology to securely send payment information between two devices. Issuers must enable contactless (i.e., enable the appropriate BINs) through their processors/network in order for tap with card or tap with device holding a token to work.

Support for contactless functionality at the ATM provides the following benefits:

- Avoids traditional card skimming.
- Offers better convenience for consumers.
- Delivers a platform for advanced ATM features (e.g., mobile/ATM integration).
- Provides the same EMV level of security as contact transactions for online authorizations, including the cryptogram.

The contactless environment includes both contactless chip cards and Near Field Communication (NFC)-enabled mobile devices and wearables. NFC[3] is a short-range wireless communication technology that enables two devices to communicate with each other when they are placed in close proximity. NFC technology is being increasingly used in a variety of applications ranging from tap-and-go payment applications to access control systems, ticketing machines and more. An NFC reader is a device used to receive and transmit data between two compatible NFC-enabled devices, such as mobile phones, tablets, and other compatible NFC-enabled hardware. These readers use RF technology to enable secure, automatic, and contactless data transfers between the two devices.

2.1 Understanding the Differences Between EMV Contact and EMV Contactless Transactions at the ATM

EMV are global specifications for payment cards that use integrated circuit chips (also known as "chip cards" or "smart cards") to store and process payment information. EMV was originally developed to combat rising card fraud. The specifications use a microchip embedded in payment cards that generates a unique, one-time cryptogram for every transaction, making it much harder for fraudsters to copy or clone cards and re-use transaction data. The two main types of EMV transactions are contact and contactless.

EMV contact transactions involve inserting a payment card into a card reader, which then establishes a secure connection with the card's chip. The cardholder is prompted to proceed with the transaction by entering their personal identification number (PIN) to verify their identity. The transaction is completed once the transaction reply and authorization data obtained from the card issuer are passed to the card for verification. EMV contact transactions also provide card issuers with the opportunity to do post-issuance modifications to the cards, typically only at ATMs since the card is secured in the card reader. EMV contact transactions offer strong security features, as the chip generates a unique, one-time cryptogram for every transaction, making it very difficult for fraudsters to steal sensitive information or create fraudulent EMV cards.

[3] "Welcome to Near Field Communication," NearFieldCommunication.org, http://nearfieldcommunication.org/http://nearfieldcommunication.org/.

EMV contactless transactions, on the other hand, use a payment card or NFC-enabled mobile device to make a payment without needing physical contact with a card reader. The payment information is transmitted wirelessly using RF technology, which allows the card to communicate with a contactless-enabled device. EMV contactless transactions are based on the same security standards as EMV contact transactions; they also generate one-time cryptograms but usually do not provide the opportunity to send post-issuance commands since the card is not held in the card reader and would need to be presented again. In addition, when a contactless NFC-enabled mobile device wallet is used, tokenization adds another layer of security.

2.1.1 Implementation Differences

Overall, the implementation differences between EMV contact and EMV contactless transactions primarily involve the payment infrastructure and the payment cards themselves. EMV contact transactions require card readers with slots and payment cards with contact microchips. EMV contactless transactions require contactless-enabled payment terminals and payment cards with contactless microchips.

Implementation differences between the two include the following:

- **Card Design and Interface**
  - EMV contact cards have metallic contacts on the card surface, allowing for physical contact with the card reader.
  - EMV contactless cards have an embedded contactless chip and an antenna, typically indicated by a small symbol or logo on the card. The cardholder can make payments by tapping or waving the contactless card near a compatible EMV contactless reader.
- **Communication Protocol**
  - EMV contact transactions use a protocol called "contact card protocol" or "T=0/T=1 protocol." The protocol defines the communication flow and commands exchanged between the card and the terminal through the physical contact interface. This protocol ensures secure data transfer and authentication.
  - EMV contactless transactions use a specific communication protocol known as "contactless card protocol" or "ISO/IEC 14443." This protocol defines the rules and commands for communication between the contactless-enabled card/device and the terminal during the transaction. It ensures secure data transfer and authentication.
- **EMV Contactless Transaction Flow**
  - EMV contactless transactions follow a different process from contact transactions. When a contactless-enabled card/device is tapped or waved near a compatible payment terminal, the terminal initiates communication with the card/device using RF. The card and terminal exchange data wirelessly. The transaction flow includes card activation, data transfer, authentication, and completion. In addition, for contactless transactions using an NFC-enabled mobile device, the actual primary account number (PAN) is replaced with an EMV token (also called the tokenized PAN).
  - Figure 1 and Figure 2 illustrate the process for a "not-on-us" (or "interoperable") transaction. The acquirer icon represents various acquiring processors or gateways situated between the ATM and a payment network. Similarly, the issuer icon represents multiple issuing processors or gateways that facilitate the authorization process.

It is important to note that these flowcharts can be adapted to accommodate specific local regulations and unique scenarios. A detailed breakdown of the functions, with a particular focus on aspects relevant to ATM operations, are included with the two figures.

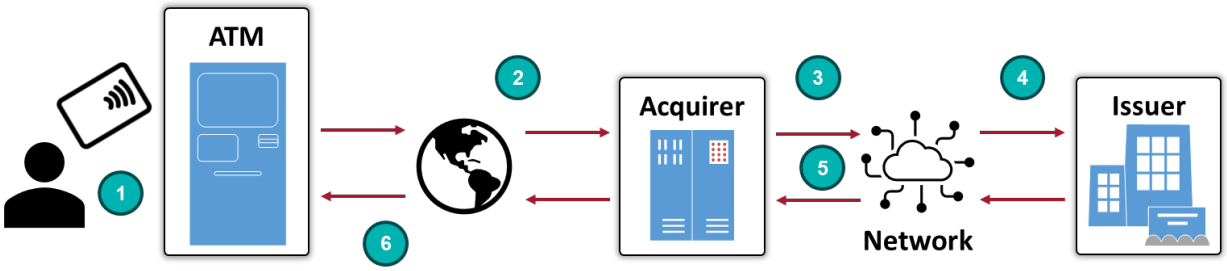

Figure 1. Contactless Card Form Factor (i.e., Non-tokenized) Transaction Flow

1	**Transaction Initiation** - The customer starts the transaction by tapping their contactless card. - The card generates a cryptogram, which is then transmitted to the ATM terminal.
2	**Transaction Request Generation** - The ATM creates a transaction request, which includes essential information such as the card's PAN, the cryptogram, EMV tags, and other pertinent transaction data. - This request is then sent to the acquirer.
3	**Transmission to the Network** - The transaction request proceeds from the acquirer to the payment network.
4	**Authorization from the Issuer** - The transaction is forwarded to the card issuer, where it undergoes authorization.
5	**Authorization Response from the Issuer** - The authorization response travels back through the payment network to the terminal.
6	**Transaction Completion** - With the authorization obtained, the transaction is finalized. - The cardholder is promptly notified of the transaction's outcome, and cash, if required, is dispensed.

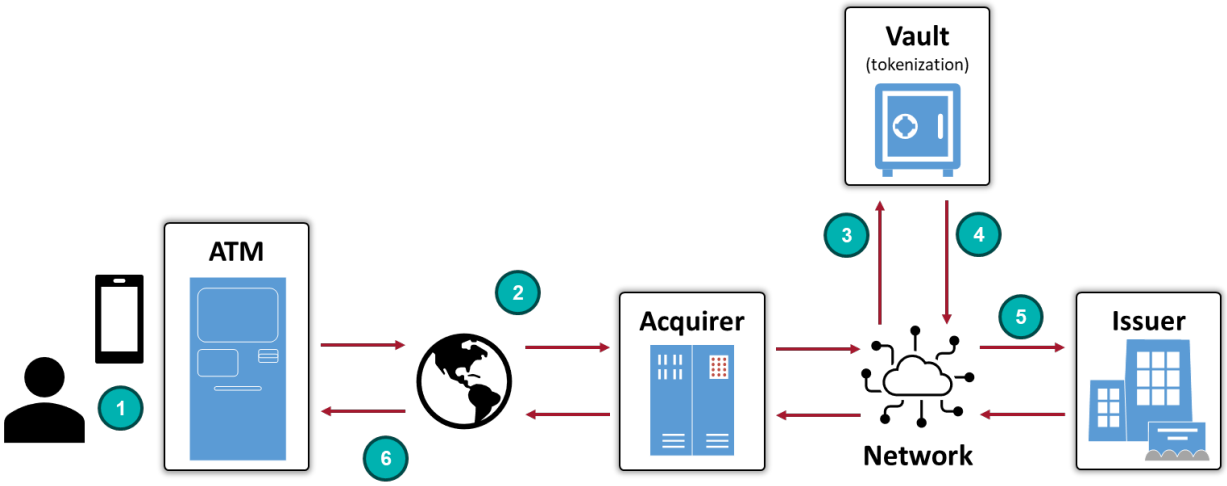

Figure 2. Mobile Device Form Factor (Tokenized) Transaction Flow

1	**Transaction Initiation** - The customer initiates the transaction by tapping their NFC-enabled mobile device or wearable. - A cryptogram is generated by the device and transmitted to the ATM terminal. Instead of the actual PAN, a token is included in the transaction message.
2	**Transaction Request Generation** - The ATM generates a transaction request, incorporating essential information such as the token, the cryptogram, EMV tags, and other pertinent transaction data. - This request is then forwarded to the acquirer.
3	**Transmission to the Network** - The transaction request moves from the acquirer to the payment network.
4	**Token Service Provider Vault De-tokenization** - The transaction is sent to the token service provider (TSP) vault for de-tokenization.
5	**Authorization Response from the Issuer** - The customer's PAN, token, and transaction details are conveyed to the issuer for authorization.
6	**Transaction Completion** - Following authorization, the transaction is completed. - The transaction is completed, the cardholder is notified of the result, and cash is dispensed.

2.2 Device Tap vs. Card Tap

Contactless transactions performed at an ATM are functionally similar in most respects regardless of whether the transaction is initiated with a card or a device-based mobile wallet (like Apple Pay® or Google Pay™). Transactions with both form factors:

- Use the same communication methods.
- Use the same payment-network-specific contactless kernel.
- Pass the same transactional data between the device/card and the ATM terminal.
- Use BINs for both actual PANs and token PANs that are present in network BIN files.

The primary difference between the two is the use of tokenization.

- Contactless cards use the actual PAN for transactions.
- Device-based mobile wallet transactions use EMV payment tokens for transactions.

For contactless transactions to operate correctly, the terminal needs to be able to load digital BIN prefixes. Contactless devices will hold tokens instead of the card PAN. Since tokens have their own BIN tables, these need to be configured on the ATM to be able to control the options that can be offered to the consumer and to allow the correct routing of the transaction, as per card BINs.

Tokenized transactions may include additional information that is not present in card-based transaction data and that is sent to both issuers and acquirers. Acquirer and issuer processors are responsible for ensuring their systems are capable of handling both EMV and token data from each network when a contactless transaction is performed, regardless of the form factor.

Tokenization has no direct impact on either acquirers or issuers for PIN encryption and validation. Payment networks handle PIN translation when tokenized PANs are presented at an ATM terminal, resulting in no impact to acquirers or issuers. When a PIN is entered at either an ATM or POS terminal, the PIN is encrypted under the PAN presented to the terminal which may be either an actual PAN or tokenized PAN. If the transaction routed to the chosen payment network is a tokenized transaction, the network “detokenizes” the token PAN and translates the encrypted PIN block (i.e., re-encrypts it to coincide with the actual PAN) so that both the actual PAN and PIN block now encrypted under the actual PAN can be authorized by the issuer using standard procedures. Card-based transactions do not require PIN translation by the network for successful processing by issuers.

2.3 Contactless Symbol

Consistent display of a standard contactless symbol improves the cardholder experience. The symbol promotes awareness that a terminal accepts contactless devices and avoids customer dissatisfaction if it is ambiguous that a contactless device may be used at a terminal. Displaying a contactless symbol also helps to guide the cardholder interaction at the terminal by properly placing the symbol in the area with the strongest signal. The industry has aligned on the use of the EMVCo Contactless Symbol to provide consistent guidelines for use at terminals and in marketing collateral.

Displaying the contactless symbol on a terminal indicates to a cardholder that a contactless device should be able to be used at the terminal.

Figure 3. EMVCo Contactless Symbol

The EMVCo guidelines include specific requirements for placement, size, and color options that may be appropriate for various environments. The contactless symbol is a trademark of EMVCo, LLC. Please visit the EMVCo Trademark Centre[4] for a royalty-free license and associated reproduction requirements.

ATM owners are advised to consult the financial institution or terminal provider to confirm if contactless is available at the participating ATM. ATM owners that do not accept contactless transactions should not display the EMVCo Contactless Symbol since this would lead to consumer confusion. The EMVCo Contactless Symbol should only be present at the ATM when both contactless cards and NFC-enabled mobile wallet transactions are accepted.

Note that some ATM devices are being implemented with the EMVCo Contactless Symbol on the body of the terminal; in these cases, an ATM owner ideally would cover the symbol if they do not accept contactless transactions to reduce consumer confusion.[5]

[4] EMVCo Trademark Centre, https://www.emvco.com/trademark-centre/

[5] "Guidelines for Contactless ATM Transactions – A Guide for ATM Owners and Operators," U.S. Payments Forum white paper, July 2019, https://www.uspaymentsforum.org/guidelines-for-contactless-atm-transactions-a-guide-for-atm-owners-and-operators/.

3. Considerations for Deploying Contactless Solutions

Deploying a contactless solution on ATMs presents several complexities and implementation considerations that ATM operators need to address. While contactless technology offers numerous benefits, including convenience and enhanced user experiences, ATM operators must address numerous considerations in order to ensure successful implementation. Examples include the following:

- **Infrastructure and Compatibility**. Significant updates to existing infrastructure are generally required to support contactless payments. These updates include ensuring that the ATMs have the proper device that is compatible with contactless EMV technology. ATM owners are strongly encouraged to check and confirm the device compatibility with the suppliers. Retrofitting or replacing hardware can be costly and time-consuming, particularly for larger financial institutions with widespread networks.
- **Security Concerns**. Security is a paramount concern when deploying contactless solutions in the banking sector. Operators generally must implement robust security measures to protect sensitive customer data, prevent fraud, and mitigate risks associated with unauthorized access or interception of transactions. Implementation requires employing encryption protocols, secure tokenization, and strict authentication processes to ensure the confidentiality and integrity of transactions.
- **Standardization and Interoperability**. Following proper EMVCo[6] and NFC[7] specifications and providing interoperability across different contactless payment platforms and devices are crucial. The specifications ensure seamless communication and interoperability between various contactless-enabled devices and payment terminals, promoting wider acceptance and adoption.
- **Regulatory and Compliance Considerations**. Operators must navigate regulatory and compliance frameworks when deploying contactless solutions. They need to adhere to industry standards, data protection regulations, and payment card network requirements. Compliance with these regulations helps ensure data privacy, consumer rights, and overall transaction security.
- **Legacy Systems Integration**. Integrating contactless solutions with existing banking systems and backend processes can be a complex task. Banks often have legacy systems in place, which may require modifications or upgrades to accommodate contactless functionalities. Seamless integration of contactless technology with core banking systems, transaction processing, and reporting systems is crucial for a smooth transition.
- **Testing Requirements**. Significant testing is also needed, including integration testing, hardware/device testing, software testing, device tap testing, and card testing.

By successfully addressing these other considerations, banks can help to successfully deploy contactless solutions that provide customers with convenient and secure payment options while enhancing operational efficiency. Overcoming infrastructure limitations, ensuring robust security measures, promoting standardization, educating customers, complying with regulations, and integrating with legacy systems are key focus areas for banks looking to embrace the global move to contactless.

---

[6] EMV Specifications and Associated Bulletins, EMVCo, https://www.emvco.com/specifications/.

[7] NFC Forum Specifications, https://nfc-forum.org/build/specifications.

3.1 Hardware and Software Vendor Differences in Implementation

When considering contactless transaction adoption, banks must recognize the variation in hardware and software implementations across different ATM vendors. To address these differences effectively, banks should engage with vendors that have a strong track record in EMV implementation and are well-versed in the intricacies of the EMV Level 1 (L1) and Level 2 (L2) certifications. (See Section 5 in the appendix for additional detail on the certification requirements and process.) This section describes key considerations and potential divergences in implementation arising from these choices.

3.1.1 Hardware Vendor Differences

ATM hardware forms the physical foundation of the contactless integration process. ATM manufacturers may employ distinct hardware components and configurations.

- **Contactless Reader Hardware Compatibility**. ATM manufacturers incorporate distinct contactless readers, antennas, and sensors, which can significantly influence the ATM's ability to efficiently process contactless transactions. One key factor to consider here is EMV L1 compliance. This compliance specification concentrates on the physical aspects of contactless transactions, ensuring seamless communication between cards, mobile devices, and terminals. L1 compliance governs fundamental hardware elements like card detection, power levels, and signal modulation, making it a critical prerequisite for the successful initiation and execution of contactless transactions. Therefore, when choosing a hardware vendor, banks should strive to ensure that the contactless hardware is not only compatible with existing contactless technologies but is also upgradable to support emerging standards, thus future-proofing the ATM infrastructure.
- **Form Factor and Aesthetics**. The physical design of the ATM, including how and where contactless components are integrated, varies between hardware vendors. Aesthetic choices, like the placement of contactless readers and branding, can influence customer engagement and the overall ATM experience.
- **Durability and Reliability**. Different hardware vendors may offer varying levels of durability and reliability in their contactless components. This is especially important as ATMs operate around the clock and need to withstand various environmental conditions. Decisions regarding hardware purchases should include consideration of whether the contactless hardware is robust enough to withstand these challenges and maintain consistent performance.

3.1.2 Software Vendor Differences

The ATM system software layer is equally critical, and it is here that the divergence among vendors becomes pronounced. Variations in software architectures, operating systems, and application programming interfaces (APIs) can present formidable challenges during integration. Differences in transaction protocols, data formatting, and security measures may make customized solutions necessary to ensure interoperability.

- **User Interface Customization**. One significant point of divergence is the user interface software that drives the ATM. Different software vendors may offer distinct user interface designs and functionality. These differences influence how customers interact with the ATM and shape their overall user experience. Consider whether a vendor allows for comprehensive customization of the user interface, enabling the bank to brand the ATM's contactless payment screens and prompts. A user-friendly interface can enhance customer satisfaction and trust, facilitating a smooth transition to contactless payments.

- **Integration with Backend Systems**. Another essential consideration is the level of integration that software vendors provide with a bank's backend systems, including core banking platforms and payment networks. The extent of integration can significantly affect transaction processing, including real-time authorization and settlement processes. Some software vendors offer seamless integration, ensuring that ATM transactions are synchronized with core banking systems in real-time. This can streamline account management, provide up-to-the-minute transaction data, and enhance the customer's financial experience. In contrast, less integrated solutions may require additional manual reconciliation steps, potentially delaying transaction posting and impacting the accuracy of account information.
- **Transaction Protocols and Data Formatting**. Software vendors may employ different transaction protocols and data formatting standards, requiring customized solutions to ensure seamless interoperability. Differences in these technical aspects can lead to complexities during integration and may require specialized development efforts. Evaluating the alignment of a vendor's transaction protocols with industry specifications, including L2 certification for secure transaction processing, is critical to achieving a smooth and efficient adoption of contactless transactions.
- **Security Measures**. The security features embedded in the software layer can differ significantly among vendors. These include encryption protocols, authentication mechanisms, and compliance with industry standards and regulations. Robust security measures are essential to protect sensitive customer data and ensure that transactions meet the stringent requirements of the financial industry. Banks must scrutinize the security offerings of software vendors to protect against potential vulnerabilities and data breaches.
- **Flexibility and Scalability**. Some software vendors provide solutions that are highly flexible and scalable, allowing banks to adapt their ATM networks to evolving customer needs and technology advances. Evaluating the extensibility and scalability of a vendor's software is crucial to accommodate future innovations and maintain a competitive edge in the market.
- **Operational Efficiency**. Operational efficiency can also vary among software vendors, affecting the management and maintenance of the ATM network. Consider features like remote management and updates, which can simplify software maintenance and minimize disruptions. A robust, operationally efficient solution can reduce downtime, ensure the timely implementation of software updates, and facilitate proactive issue resolution.

3.1.3 Vendor Collaboration

To navigate the hardware and software differences among ATM vendors, banks are strongly encouraged to establish collaborative relationships with trusted vendors who can provide guidance and support throughout implementation. This collaboration should encompass robust testing procedures to ensure L1 and L2 certification compliance, seamless integration of contactless transaction capabilities, and the ongoing maintenance and updates required for a secure and efficient transaction environment.

The choice of hardware and software vendors for contactless integration in ATMs is a decision that impacts the overall performance and customer experience. It is essential to carefully evaluate the options available, considering factors such as contactless hardware capabilities, form factor, durability, software adherence to standards, user interface design, and backend integration. A well-informed choice of vendors can lead to a more efficient and customer-friendly ATM experience, ensuring that ATMs are not only convenient but also secure and future-proofed for emerging payment technologies.

3.2 Hardware/Software Updates and Standard/Regulatory Compliance

For banks that are planning to adopt contactless ATM transactions, maintaining awareness of contactless hardware and software requirements is critical to ensure proper functionality and enablement. Staying at the forefront of technology not only affects operational efficiency but also helps to provide customers with secure and convenient transaction experiences.

- **Adherence to Industry Standards and Specifications**. Forward looking banks will want to maintain their ATMs to align and adapt to evolving changes in industry specifications and standards, to ensure that contactless transactions are both secure and interoperable through these changes.
- **Hardware Upgrades**. In many cases, existing ATMs may lack built-in contactless capabilities. Banks considering contactless implementation should conduct a thorough evaluation to determine if their current hardware can be upgraded to support contactless transactions. If this is not feasible, investing in new ATMs with the requisite hardware becomes a strategic step to embrace the future of banking technology.
- **Software Updates and Security**. Compliance with regular ATM software updates is essential to ensure that the latest contactless technologies and specifications are being followed.
- **Regulatory Compliance**. Banking operations are subject to a range of regulatory requirements, which may vary by state or locality. Staying informed about and adhering to these standards are vital for the seamless operation of contactless ATMs.

4. Conclusion

While there are differences between contact EMV and contactless EMV transactions, both technologies are in use globally and are supported by well-defined specifications and certification processes. Implementing contactless ATM transactions requires an assessment of the current infrastructure and careful planning to deploy hardware and software and integrate with legacy systems. As with contactless acceptance at retailers, the benefits for ATMs have been proven – improved convenience for consumers, strong security, advanced features, and the flexibility to accept transactions from both EMV chip cards and NFC-enabled mobile devices.

In conclusion, when implementing contactless technology at the ATM, all stakeholders should stay connected and work together to do their part to ensure enablement of contactless and to provide a better customer experience. The references in Section 6, Appendix II, provide additional information.

5. Appendix I: Contactless Certification

Contactless payment technology is still a relatively new and rapidly evolving field, with new and improved specifications being introduced regularly. EMVCo, the organization responsible for managing the EMV payment specifications, has been actively developing and refining its contactless payment specifications to improve security, interoperability, and ease of use.

Other organizations are also developing their own contactless payment specifications, each with their own unique features and capabilities. For example, some mobile payment systems use their own proprietary contactless payment technologies that are not based on the EMV specifications. As a result, payment terminal manufacturers and financial institutions must ensure that their payment systems support multiple contactless payment specifications to ensure that they can accept a wide range of payment methods. As the market for contactless payments continues to grow, it is likely that the specifications and standards used for contactless payments will continue to evolve to meet the changing needs of the market.

EMVCo provides certification programs for payment system components to ensure that they meet the organization's technical specifications and security requirements.

One of EMVCo's key certification programs is its contactless Level 1 (L1) certification program, which is designed to ensure that contactless payment terminals and mobile devices comply with the organization's technical specifications. The contactless L1 certification program covers a range of technical requirements, including those related to RF performance, signal modulation, and power levels, to ensure that contactless payments can be reliably and securely processed across different payment terminals and mobile devices.

EMVCo also provides a contactless Level 2 (L2) certification program. This certification program ensures that contactless payment terminals and mobile devices can properly interpret and process the data transmitted between the payment card or digital wallet and the terminal or mobile device.

EMV L1 and L2 testing assesses if payment cards, devices, and acceptance terminals comply with the EMV chip specifications. The specifications create a blueprint for chips and the machines that accept chip-based payments to work in the same way, no matter where they are used. The EMV chip specifications outline the “protocol” or necessary elements for the chip to communicate with a chip reader in an acceptance terminal and exchange information to execute a payment. The testing and certification are done by EMVCo-accredited external test laboratories and the process for product providers includes registration, selection of laboratory, testing, and approval. This process allows card, device, and terminal manufacturers to demonstrate that their products are certified as meeting EMV specifications and provides financial institutions and consumers with secure chip card-based payments anywhere in the world.

Together, the contactless L1 and L2 certification programs help to ensure the reliability, interoperability, and security of contactless payments, and provide a framework for financial institutions and payment providers to confidently deploy and accept contactless payments.

Contactless certifications are similar to the EMV contact certifications.

5.1.1 EMVCO Level 1 Certification

EMV L1 certification is an important process for device vendors whose devices process payment transactions from a contactless form factor (e.g., chip card, mobile device, wearable). The certification process ensures the security and reliability of payment terminals and POS systems so that customers can feel confident and safe when making purchases.

EMV L1 certification is done by an accredited third-party testing laboratory to ensure that all necessary security requirements are met. The testing agency will examine the hardware and software components of the terminal and make sure that the terminal meets all of the security requirements set by the payment networks and EMVCo. The evaluation includes making sure the terminal is tamper-proof, has a secure operating system, and is compliant with the payment industry's data security rules.

Once a terminal has passed all the certification processes including L1, it can be used to process payments using EMV-enabled cards and devices.

EMVCo L1 approval is granted to a contactless card reader called a proximity coupling device (PCD). The PCD needs to be approved as an intelligent card reader to be able to manage the kernels that reside in the reader.

Overall, the EMV L1 test is an important tool for protecting consumers and financial institutions from fraud and is an essential part of ensuring the security and reliability of chip card payments.

5.1.2 Level 2 Certification

Contactless EMV, unlike contact EMV, does not have one kernel that fits all payment systems. Due to the lack of a common specification being available when the major payment networks defined their contactless payment applications, the payment systems work on their own specifications. The lack of a common specification led to different specifications and different requirements. Initially the specifications were only available through the payment networks; subsequently the payment network specifications were also made available on the EMVCo website and have been renamed with a "Cn" convention.

The L2 contactless EMV approvals, as with EMV contact, are granted to the kernels, since each payment network has its own kernel. The two types of L2 approvals are the following:

- **EMVCo Pathway**. An EMVCo contactless product approval means that the PCD and the L2 kernels included have been approved by EMVCo through the EMVCo contactless process. The result of the approval is one unique letter that lists the kernels supported. The EMVCo contactless product also includes the entry point component that controls the kernel selection and kernel data exchange. The approved EMVCo contactless devices can be found on the EMVCo website.[8]
- **Payment Network Pathway**. Most solutions available in the U.S. have kernels that implement the payment network certification process. For this pathway, each payment network supported by the device is certified by that payment network and individual letters of approval (LoA) are granted. These L2 LoAs are normally not publicly available and need to be requested directly by the ATM vendor.

[8] "Approved Products and Solutions, EMVCo, https://www.emvco.com/approved-products/.

EMV L2 certification is important for contactless payments because it ensures that devices and kernels comply with the security requirements of the major payment networks. The two pathways – the EMVCo pathway and the payment network pathway – are both valid and accepted today for Level 3 submissions.

Table 1 summarizes the payment network and EMV specifications for contactless EMV.

Payment Network Specification	EMV Specification
EMV L1	EMV L1
N/A	EMVCo Entry Point
Mastercard Contactless	C2 for Mastercard AIDs
VISA qVSDC[9]	C3 for Visa AIDs
American Express ExpressPay	C4 for American Express AIDs
JCB Contactless	C5 for JCB AIDs
Discover D-PAS[10]	C6 for Discover AIDs
UnionPay QuickPass®	C7 for UnionPay AIDs
N/A	C8 – new specification from EMVCo

Table 1. Contactless EMV Specifications

The new EMVCo Contactless Kernel Book C-8 specification[11] is the result of the initiative to reduce the complexity of the current multi-kernel environment for contactless. Over time, this specification could lead to a single, global contactless kernel that is used by all major payment networks, making it easier and more affordable for merchants and ATM vendors to support contactless payments.

In summary, EMV L2 certification is an important part of ensuring the security and reliability of contactless payments. The new EMVCo Contactless Kernel Book C-8 specification is a promising development that could simplify the contactless landscape in the future.[12]

5.1.3 Level 3 Certification

EMV Level 3 (L3) certification must be done by an acquirer prior to a terminal being allowed in the field. The terminal is configured for field use and the parameters are configured according to the payment networks' requirements (e.g., contactless cardholder verification method (CVM) limits, action codes).

[9] quick Visa Smart Debit Credit (qVSDC).

[10] D-Payment Application Specification (D-PAS).

[11] "Coming Soon: First EMV® Contactless Kernel Specification," EMVCo, https://www.emvco.com/knowledge-hub/coming-soon-first-emv-contactless-kernel-specification/.

[12] "What are EMV® Level 1 and Level 2 Testing?," EMVCo, https://www.emvco.com/knowledge-hub/what-are-emv-level-1-and-level-2-testing/.

Each payment network will define its own tests to ensure requirements are met and that transactions are interoperable – i.e., all cards accepted by the acquirer are accepted by the terminal and processed accurately. The acquirers will check that L1 and L2 certification and Payment Card Industry Data Security Standards (PCI DSS) implementation have been performed appropriately and will require the appropriate certificates for supported kernels. All certificates will be checked by the acquirer's certification team to ensure that they have valid dates (and, in some cases, are within the extension date allowed by the payment networks). The financial institution should ensure that their certificates are within the expiration date or ask the acquirer what the extensions are for the L2 certification.

Some examples that require a new L3 certification for each new terminal the financial institution wants to deploy include: if the terminal has to have a new kernel or new payment application; or if the processing path changes (i.e., moves from one acquirer host to another).

L3 testing is an end-to-end test suite and host messages are checked from the acquirer.

The EMV L3 certification is the final step for ensuring the security of card transactions. By verifying that the terminal meets the specifications, financial institutions can be sure that their customers' data is secure and that the terminal is compliant with the payment networks' requirements. This helps to prevent fraud and protect the customer's information, while also ensuring that the terminal works properly.

EMVCo has developed a framework that each payment network follows to ensure that the format of the test plan and the file outputs are consistent. A number of EMVCo-qualified test tool vendors can provide the L3 test tools for each payment network. Due to this EMVCo initiative, the quality of the test plans and testing is higher, and the output is consistent across tool vendors. Each payment network publishes the qualified tool vendor list.[13]

5.2 U.S. Common Debit AID

Contactless card readers may support and be preconfigured to manage U.S. common debit AID selection, where applicable. ATM acquirers may need to work with networks to decide on the AID selection process for U.S. debit cards. When performing L3 testing, ATM acquirers have to indicate what their AID selection process is so that the relevant set of test cases can be performed.

5.3 Payment Network End-To-End Level 3 Approval Diagram

The diagram in Figure 4 presents a visual representation of a payment network's end-to-end L3 approval process, highlighting the key components involved in facilitating secure and efficient transactions. The process diagram and network illustrate the seamless interaction of critical players in a transaction: the ATM, acquirer, payment network, issuer, and the integral element of tokenization represented by the vault.

Each element plays a key role in ensuring the swift and secure approval of transactions, including vital steps such as authorization, encryption, and, when a mobile device or wearable form factor is used, the transformation of sensitive data into tokens. This illustration provides insight into the complex interplay of these components, ultimately resulting in a successful payment transaction that provides peace of mind to both cardholders and stakeholders alike.

[13] "What is Level 3 Terminal Integration Testing," EMVCo, https://www.emvco.com/knowledge-hub/what-is-level-3-terminal-integration-testing/.

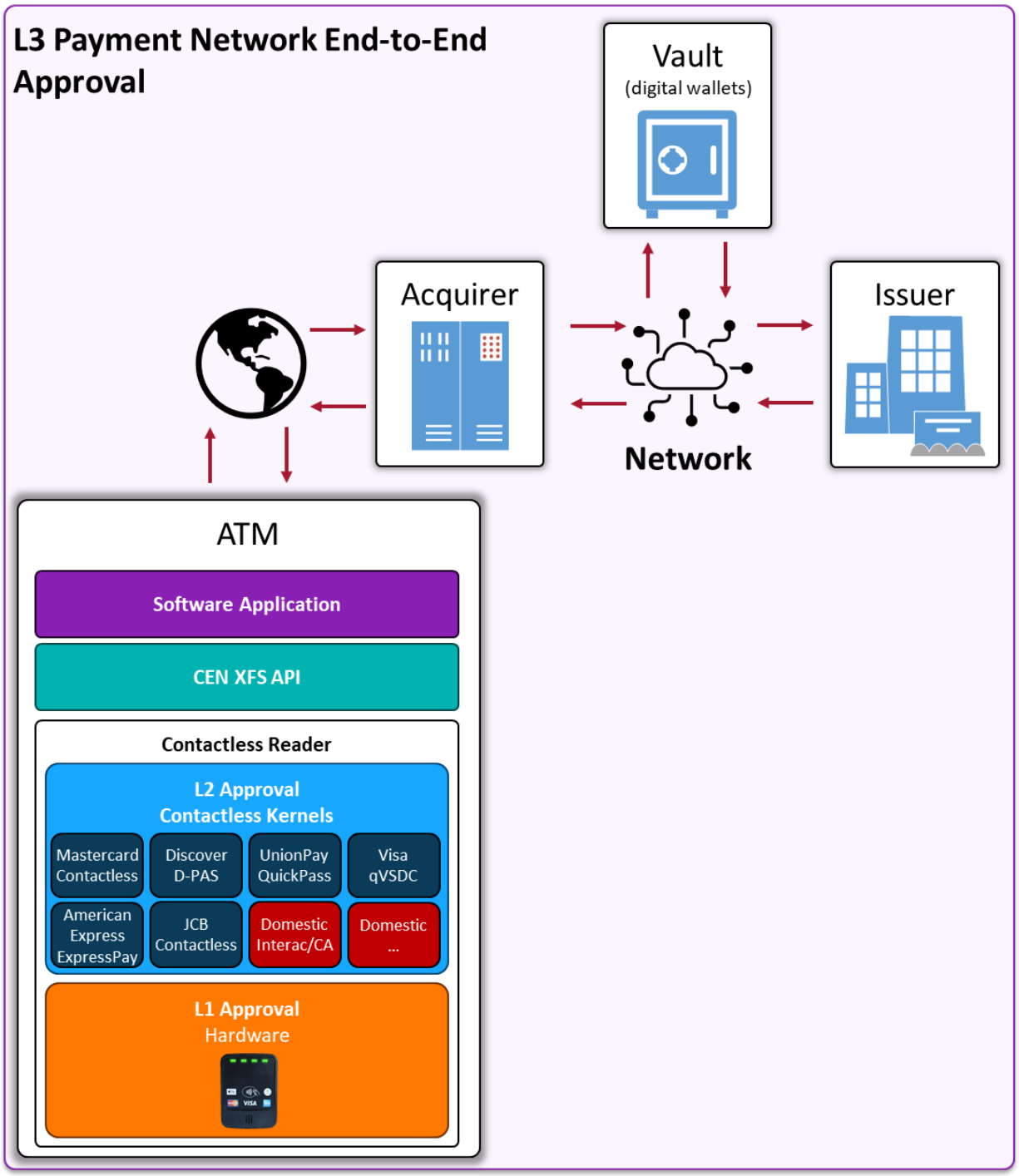

Figure 4. Payment Network End-to-End Level 3 Approval Process

6. Appendix II: References

6.1 EMVCo

EMVCo website: www.emvco.com

EMV Specifications - EMV® Specifications & Associated Bulletins Archive: https://www.emvco.com/specifications/

EMVCo Trademark Centre: https://www.emvco.com/about/trademark-centre/

6.2 Global Payment Networks

American Express

American Express technical specification website: https://network.americanexpress.com/globalnetwork/

Discover

Contact the PULSE relationship manager or visit https://www.pulsenetwork.com/

Mastercard

Mastercard Connect website: https://www.mastercardconnect.com/-/sign-in (login required)

Visa

Visa Online website for Visa clients: https://www.visaonline.com (login required)

Visa Technology Partner website for vendors: https://technologypartner.visa.com/ (login required)

Transaction Acceptance Device Guide: https://technologypartner.visa.com/Library/specifications.aspx (publicly available)

6.3 U.S. Payments Forum

U.S. Payments Forum website: www.uspaymentsforum.org

EMV Connection website: www.emv-connection.com

EMV Knowledge Center: http://www.emv-connection.com/emv-migration-forum/knowledge-center/

"EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community," U.S. Payments Forum Testing and Certification Working Committee, http://www.uspaymentsforum.org/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/

"EMV Troubleshooting Guide for ATM Owners and Operators," U.S. Payments Forum ATM Working Committee, http://www.uspaymentsforum.org/emv-troubleshooting-guide-for-atm-owners-and-operators/

"Glossary of Standardized Terminology," U.S. Payments Forum Communications and Education Working Committee, http://www.emv-connection.com/standardization-of-terminology/

"Implementing EMV at the ATM," U.S. Payments Forum ATM Working Committee, http://www.emv-connection.com/implementing-emv-at-the-atm-requirements-and-recommendations-for-the-u-s-atm-community/

"Implementing EMV at the ATM: PIN Change at the ATM," U.S. Payments Forum ATM Working Committee, http://www.emv-connection.com/implementing-emv-at-the-atm-pin-change-at-the-atm/

"Mobile and Contactless Payments Glossary," U.S. Payments Forum Mobile and Contactless Payments Working Committee, http://www.uspaymentsforum.org/mobile-and-contactless-payments-glossary/

"U.S. Debit EMV Technical Proposal, U.S. Payments Forum, http://www.uspaymentsforum.org/u-s-debit-emv-technical-proposal/

7. Appendix III: Glossary of Terms

ATM (Automated Teller Machine). An electronic telecommunications device that enables the clients of a financial institution to perform financial transactions without the need for a cashier, human clerk, or bank teller.

AID (Application Identifier). A representation of the application defined within ISO/IEC 7816, technically defined as binary though typically implemented as alphanumeric. A data label that differentiates payment systems and products. The card issuer uses the data label to identify an application on the card or terminal. Cards and terminals use AIDs to determine which applications are mutually supported, as both the card and the terminal must support the same AID to initiate a transaction. Both cards and terminals may support multiple AIDs. An AID consists of two components, a registered application identifier (RID) and a propriety application identifier extension (PIX).

ATM provider. An ATM owner, operator or deployer.

API (Application Programming Interface). A software interface that provides a way for two or more computer programs or components to communicate with each other.

BIN (Bank Identification Number). The first part of the card number/PAN that identifies the institution that issued a card. Also known as the IIN (Issuer Identification Number).

CVM (Cardholder Verification Method). In the context of a transaction, the method used to authenticate that the person presenting the card is the valid cardholder. EMV supports four CVMs: offline personal identification number (PIN) (offline enciphered and plain text), online encrypted PIN, signature verification, and no CVM required. The issuer decides which CVM methods are supported by the card; the merchant chooses which CVMs are supported by the terminal. ATMs currently only support online PIN. The issuer sets a prioritized list of methods on the chip for verification of the cardholder.

D-PAS (D-Payment Application Specification). Discover's chip specification.

EMV (Europay, MasterCard, Visa). Trademark referring to the three organizations that founded EMVCo. The EMV specifications have evolved from a single, chip-based contact specification to include EMV Contactless, EMV Common Payment Application, EMV Card Personalization, and EMV Tokenization.

EMVCo. An organization overseen by six member organizations (American Express, Discover, JCB, Mastercard, UnionPay, and Visa) and supported by many other payment industry stakeholders, whose goal is to facilitate worldwide interoperability and acceptance of secure payment transactions. EMVCo is responsible for managing and evolving the EMV specifications and related testing processes.

ICC (Integrated Circuit Card). See chip card.

IEC (International Electrotechnical Commission). A non-profit, non-governmental international standards organization that prepares and publishes international standards for all electrical, electronic, and related technologies.

IIN (Issuer Identification Number). A six-digit number that identifies the institution that issued a card. Also known as the BIN (Bank Identification Number). The IIN is the first part of the card number/PAN.

ISO (International Organization for Standardization). An international standard-setting body composed of representatives from various national standards organizations.

Kernel. The set of functions required to be present on every terminal (or card reader) implementing a specific interpreter. The kernel contains device drivers, interface routines, security and control functions, and the software for translating from the virtual machine language to the language used by the real machine. In other words, the kernel is the implementation of the virtual machine on a specific real machine.

LoA (Letter of Approval). Document issued to a vendor when the certifying agency approves the product being certified. The vendor may then advise their customers that the product has met the requirements of the certifying body.

Magnetic stripe. A band of magnetic material used to store data. Data is stored by modifying the magnetism of magnetic particles on the magnetic material on a card, which is then read by a magnetic stripe reader.

MSD (Magnetic Stripe Data) transaction. A contactless payment transaction that transfers data that is formatted as the magnetic stripe of a credit or debit card.

NFC (Near Field Communication). A standards-based wireless communication technology that allows data to be exchanged two ways between devices that are a few centimeters apart.

NFC reader. A device used to receive and transmit data between two compatible NFC-enabled devices, such as mobile phones, tablets, and other compatible NFC-enabled hardware. These readers use radio frequency (RF) technology to enable secure, automatic, and contactless data transfers between the two devices. This technology can be used to establish secure connections, share data, and make payments without requiring physical contact, making NFC readers an ideal solution for a range of tasks and applications.

PAN (Primary Account Number). The payment card number.

PCD (Proximity Coupling Device). An electromagnetic device that enables wireless communication between two devices. The device enables contactless communication using radio frequencies to transmit data, allowing for a more secure and efficient transfer of information. The PCD is a key component of EMV[14]-enabled devices, which are commonly used with payment cards and other financial applications. PCDs are designed to be small, lightweight, and low power, and they can be used in a variety of applications including point-of-sale (POS) and access control systems. PCDs provide a secure and reliable way to communicate data between two devices and are becoming increasingly popular in many industries.

PCI DSS (PCI Data Security Standards). A framework developed by the PCI Security Standards Council (SSC) for developing a robust payment card data security process – including prevention, detection, and appropriate reaction to security incidents.

PIN (Personal Identification Number). An alphanumeric code of 4 to 12 digits in length that is used to identify the cardholder upon entry at a customer-activated PIN pad.

PIX (Proprietary Application Identifier Extension). The last digits of the AID that enable the application provider to differentiate between the different products they offer.

POS (Point of Sale). The location where a retail transaction is completed, and at which a customer makes a payment to the merchant in exchange for goods or services.

[14] "PCD Level 1 Approval Process," EMVCo, https://www.emvco.com/processes/pcd-level-1-approval-process/.

RID (Registered Application Provider Identifier). First part of the AID. Used to identify a payment system or network (e.g., Mastercard, Visa, Interac).

Tag. Values involved in an EMV transaction (which result from the issuer's implementation choices) that are transported and identified by a tag which defines the meaning of the value, format, and length. The tag is simply a set of hexadecimal characters that identify the meaning of each piece of data transmitted between the ICC and the terminal.

TC (Transaction Certificate). A cryptogram generated by the card at the end of all offline and online approved transactions.

TSP (Token Service Provider). Entity within the payments ecosystem that provides registered token requestors with "surrogate" PAN values, otherwise known as payment tokens by managing the operation and maintenance of the token vault, deployment of security measures and controls, and registration process of allowed token requestors.

VSDC (Visa Smart Debit/Credit). Visa's chip specification.

8. Legal Notice

This document is provided solely as a convenience to its readers, as a high-level overview of considerations relevant to the adoption of contactless transaction processing for ATMs. While great effort has been made to ensure that the information provided in this document is accurate and current, this document does not constitute legal or technical advice and should not be relied upon for any legal or technical purpose; accordingly, all warranties of any kind, whether express or implied, relating to this document, the information herein, or the use thereof are expressly disclaimed, including but not limited to warranties as to the accuracy, completeness or adequacy of such information, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement. Any person that uses or otherwise relies on the information set forth herein does so at his or her sole risk. Readers interested in implementing contactless transaction processing in ATMs are strongly encouraged to consult with their respective security providers, subject matter experts and professional and legal advisors, as well as relevant payments industry stakeholders, such as payment networks, issuers, acquirers, and others, prior to any implementation decisions.