FS-ISAC

Post Quantum PCI Use Cases: Transaction Routing and Authorization and Retail Transaction Detail and Routing

A Technological Review

Written by the FS-ISAC Post Quantum Cryptography Working Group

FS-ISAC

Post Quantum PCI Use Cases:

Transaction Routing and Authorization and Retail Transaction Detail and Routing

Contents

Contributors

- Andrew Mulvenna
- Erwin Carrow, U.S. Bank
- Dr. Kenneth Giuliani, CIBC
- Oscar Covers, Dutch Banking Association
- Dr. Carrie Gates, FS-ISAC
- Mike Silverman, FS-ISAC

The opinions are those of the writers, are made as of the date of this document, and are subject to change without notice. Contributors' employers may have opinions that are different from and/or inconsistent with the views expressed in this document.

Post Quantum PCI Use Cases:

Transaction Routing and Authorization and Retail Transaction Detail and Routing

Introduction

The payment card industry (PCI) relies on certain forms of cryptography that will be vulnerable to attack when quantum computing becomes accessible to threat actors. Much of this cryptography is woven into the architecture of transaction routing and authorization and retail transaction detail and routing.

In this document, designed for technologists in the payment card industry, FS-ISAC's Post Quantum Cryptography Working Group examines the impact of quantum computing on those use cases, paying particular attention to:

- Cryptography and assumptions
- Effects of quantum
- Mitigation techniques
- Current industry status

We use the Banking Industry Architecture Network (BIAN) to provide structure and frame these use cases. BIAN lists use cases down to four distinct levels of specification. As our purposes are in-depth and PCI-specific, we apply a fifth level to the BIAN model to better describe the implications of quantum. The References and Resources section includes a chart of all five levels.

A business perspective on quantum computing is available in The Impact of Quantum Computing on the Payment Card Industry. That document provides a comprehensive overview of:

- Components of quantum computing threats and standards
- Quantum-specific cryptographic implementations related to payment cards
- Quantum computing risks to common infrastructure areas
- Considerations for standard-setting bodies
- Considerations for implementations in the payment card ecosystem

Two other documents for PCI technologists cover four other use cases, including:

- Card Provisioning Setup and Cardholder Data Provisioning
- ATM and POS Card Capture and ATM and POS Setup With Backend Acquiring Systems

- Cyber hygiene best practices

Payment Card Terminology

Card brands and third parties often use slightly different naming conventions for the same cryptographic inventory item. For convenience, we use these terms in this document.

Card Verification Value (CVV)

Card brands may call it CVC, CSC, CID, etc., but they all mean the 3- or 4-digit security code printed on the card and encoded on the magnetic stripe and the Europay, MasterCard, and Visa (EMV) chip, depending on the type of CVV.

Local Master Key (LMK)

Sometimes called the Master File Key, LMKs are the top key in the cryptographic hierarchy and are generally stored securely within a hardware security module. They may also be stored securely in component form.

Use Case 3: Card-Present Transaction Routing and Authorization

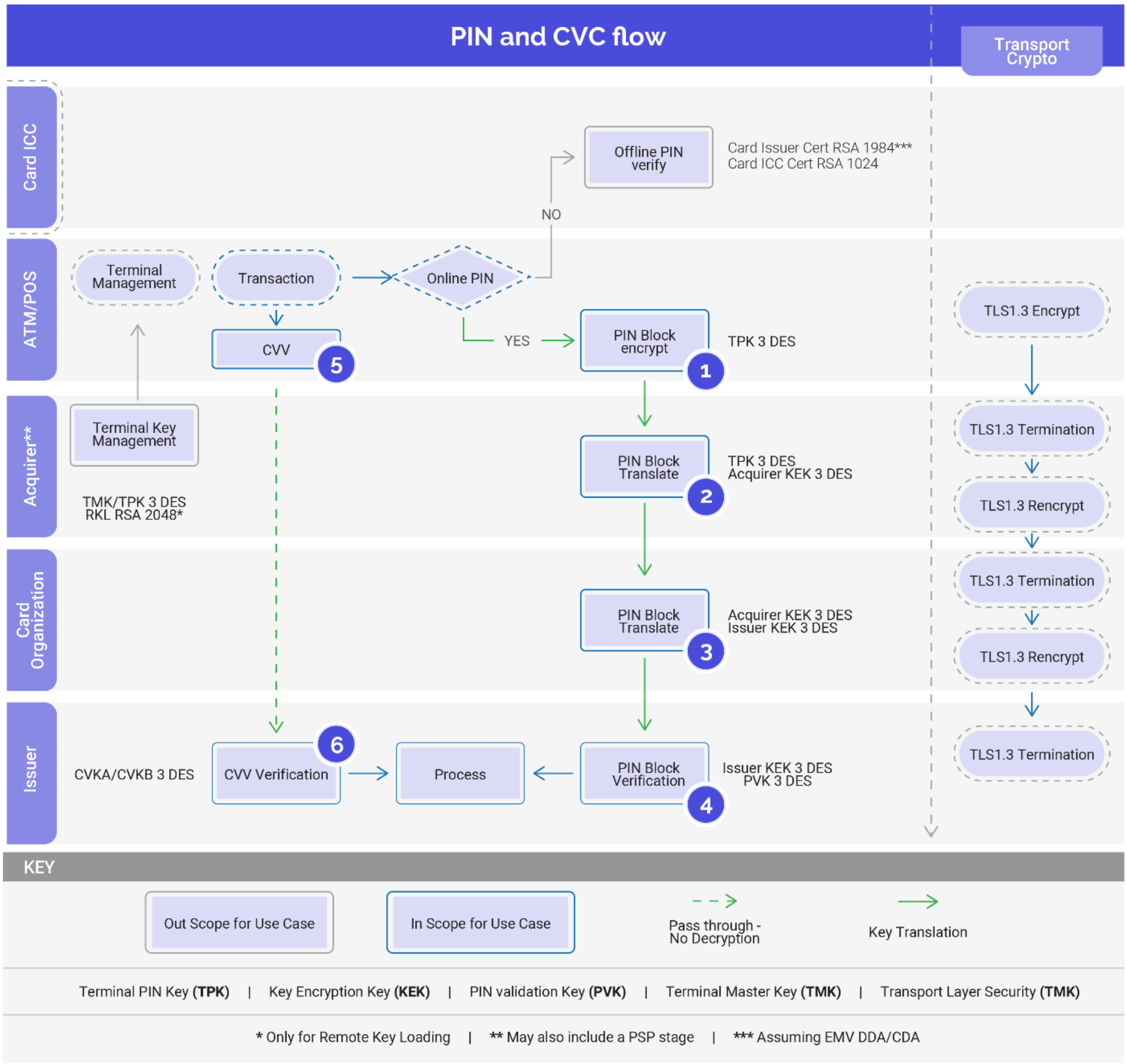
This use case focuses on transactions at an Automated Teller Machine (ATM) or a Point-of-Sale (POS) device.

There are three major elements to ATM and POS transactions:

- PIN processing
- Magnetic stripe authorization
- Chip authorization

Note that transactions involving Interactive Voice Response (IVR) acquisition of PIN and card information follow the same flow as those of ATM and POS transactions, hence no distinction is made for the purposes of this use case.

The following diagram shows the flow and cryptography of PIN processing and magnetic stripe authorization. The steps are numbered, which is reflected in the guidance below.



The channels between ATM/POS, acquirer, card brand, and issuer are likely all protected, sometimes by end-to-end encryption or channel encryption such as TLS 1.3. This is out of scope but stated here for completeness.

As the flow involves acquired PINs, the specifications and controls are subject to the PCI PIN standard.[i]

Pin Processing

Cryptography and Assumptions: When a PIN is entered into an ATM and POS, it must be properly verified for the transaction to complete. There are two types of PIN verification:

- Offline PIN verification
- Online PIN verification

Offline PIN verification is handled by the EMV chip as seen in the top swimlane of the diagram. Note that offline PIN verification occurs only at a POS device. All ATM transactions perform online PIN.

The PCI PIN standard mandates that only dynamic key exchanges be in place by 1 January 2025. This would apply to the keys shared between the ATM/POS and acquirer (1) and the acquirer and card scheme (2). The Terminal PIN Key (TPK) between the card scheme and the issuer (3) is not in scope for PCI PIN, but card scheme mandates and good practice often hold this key to the same requirement.

For online PIN, the PIN is encrypted by the ATM and POS and routed to the issuer or their delegate for verification. This involves several different steps:

- The PIN is formed into a PIN block and encrypted with a Terminal PIN Key (TPK) by the ATM/POS using a key that it shares with the acquirer (1) and is routed to the acquirer.
- The PIN block is translated by the acquirer to encryption with a PIN Encryption Key (PEK) it shares with the card brand (2).
- The PIN block is then translated by the card brand to a PEK it shares with the issuer or its delegate (3). Note that the issuer may elect to have the card brand perform Stand-In Processing (STIP) and have the PIN verified by the card brand at this point during the transaction.

- The issuer decrypts the PIN and verifies it against the record in its cardholder database.

The TPKs established between the acquirer, brand, and issuer can be either static or dynamic.

- Static: The TPK is exchanged between entities using standard key management techniques such as key components. This key directly encrypts the PIN.
- Dynamic: A Key Exchange Key (KEK) is established between entities using standard key management techniques such as key components. This key is used to dynamically exchange TPKs that will be used to encrypt the PIN. The TPKs are rotated after a certain number of transactions or a certain length of time.

Current Cryptographic Algorithms Commonly Used for PCI Card Manufacturing

Encryption Type	Algorithm	Description
Symmetric	Triple-DES (3DES)	Most implementations are two-key Triple-DES
Symmetric	Advanced Encryption Standard (AES)	Though available, not in use in many cases
Asymmetric	RSA 2048	In use for multiple use cases such as EMV cards and remote key loading
Asymmetric	Elliptic Curve Cryptography (ECC)	Available with the latest EMV specifications

Triple-DES has been deprecated as an approved algorithm at the time of this writing.

The PIN block itself is mandated to be one of ISO PIN block formats 0, 1, 3, or 4. ISO PIN block formats 0, 1, and 3 are set to be 64-bit block size, which essentially mandates the use of Triple-DES. ISO PIN block 4 allows a larger 128-bit block size to allow for the use of AES. Most current implementations use ISO PIN block formats 0, 1, or 3, which means that the TPKs are typically either two-key or three-key Triple-DES.

When the issuer receives the PIN (or the card brand if STIP is selected), it must verify the PIN against the record in its cardholder database. It does so using a PIN verification algorithm using a PIN Verification Key (PVK). (One of the most common type of these PIN verification methods is the IBM 3624 PIN verification method).[ii] These methods can be used with both Triple-DES and AES. However, most current implementations tend to gravitate toward two-key or three-key Triple-DES.

Effects of Quantum: All cryptography used in this case is symmetric. Implementations typically use Triple-DES, mainly two-key but with some three-key as well. Although Triple-DES has been deprecated as an approved algorithm at the time of this writing, it is still safe to use if only a limited amount of data is encrypted with the same key (as is common for card transactions) though the use of PINs is inherently vulnerable to quantum computing using Grover's algorithm. The smaller key size of two-key Triple-DES makes PIN particularly vulnerable. This applies to all instances of PIN protection, i.e., (1), (2), (3), and (4).

Grover's Algorithm

Formulated by Lov Grover in 1996, this quantum algorithm provides a quadratic speedup for database searching problems and can be adapted to attack symmetric cryptographic algorithms. While not as devastating as Shor's algorithm to current cryptography, it implies that symmetric key lengths might need to be doubled to maintain current security levels against future quantum computers.

Threat actors who collect many PINs protected with the same key could yield a large harvest of customer PINs from only one successful quantum decryption. So, migrating to AES is highly recommended.

Mitigation Techniques: The main mitigation technique for PIN processing would be to migrate to ISO PIN block 4 with AES keys when encrypting PINs with TPKs. This would negate the threat of quantum computing on PINs. This would require a change to the hardware security modules (HSM) that support PIN processing as well as potential coding changes to the requisite software to accommodate increased PIN block sizes.

Such a change would be a massive undertaking and would require the coordination of many different parties across the financial industry, including:

- All acquirers, issuers, and card brands
- HSM manufacturers and transaction software developers
- Regulatory bodies like PCI PIN.

The other mitigation would be to leverage AES keys for PIN verification. It is believed that much of this infrastructure is in place as most PIN verification algorithms already support AES. As this is typically done within an organization, PIN verification can be performed by each organization individually.

Current Industry Status: The move to ISO PIN block 4 is already underway.[iii]

The use of AES in PIN verification is individual to an organization. It is believed that the majority of organizations still use Triple-DES. There has been no concerted effort to encourage moving to AES.

Magnetic Stripe Authorization

Cryptography and Assumptions: Magnetic stripe authorization revolves around a three-digit CVV. The transaction verification works as follows:

- The three-digit CVV is read directly from the magnetic stripe (5).
- After being forwarded through the acquirer and card brand to the issuer as a pass-through (unless Stand-In Processing is in play), the issuer will verify the CVV using cardholder information and its Card Verification Key (CVK1).

The verification takes as input the PAN, expiry date, and country code and – combining with the CVK1 – outputs a three-digit number. If the CVV from the transaction is verified, the authorization is successful.

The calculation of the CVV value itself is inherently dependent upon and actually modifies the Triple-DES algorithm.[iv] It therefore cannot be used with AES. In addition, the calculation does not allow three-key Triple-DES. Hence, all implementations are two-key Triple-DES.

See Cardholder Data Provisioning in Table 1 for more information about the production of the CVV value on the magnetic stripe.

Effects of Quantum: As magnetic stripe authorization uses two-key Triple-DES, it is theoretically very vulnerable to quantum computing. It should be noted that, unlike PIN or chip processing, the three-digit CVV is only a small portion of the ciphertext from the Triple-DES encryption. It is not immediately clear if the reduced ciphertext data would complicate the quantum decryption of the CVK1. However, it must be assumed that a quantum computer can crack a CVK1 if it has enough CVV values.

Mitigation Techniques: The obvious mitigation technique would be to change the CVV algorithms to support AES. This would require a new standard and change to all implementations on the issuer side. Because only the issuer performs this calculation, it would not require coordination from other entities.

Current Industry Status: Mastercard will be sunsetting magnetic stripe cards.[v] The rest of the industry may follow suit at some point.

Chip Authorization

Cryptography and Assumptions: Chip keys are specified in the EMV standard.[vi] The symmetric chip data on an individual card consists of the following four keys corresponding to the EMV standard: Authorization Cryptogram (AC), Message Authentication Code (MAC), encryption (ENC), and Dynamic CVV (DCVV). However, during a transaction, Session Keys (SKs) are derived from the respective Unique Derived Keys (UDKs) using the Application Transaction Counter (ATC), which is just an incremental value on the chip.

The SK-AC key will be used to generate the Authorization Request Cryptogram (ARQC) to compute an authentication tag on the transaction data (e.g. amount, currency, etc.) to send to the issuer's authorization system. The authorization system will compute the same UDK, SK, and ARQC to verify the transaction, then compute the Authorization Response Cryptogram (ARPC) to send back to the chip.

The SC-ENC key will be used by the authorization system to encrypt a new PIN to send to the chip if there is a need to do so. The SC-MAC key will compute an authentication tag on the script containing the encrypted PIN and other card status information to send to the chip.

The SK-DCVV will be used to compute a three-digit DCVV value to be sent to the authorization system if the transaction is a contactless transaction at a magnetic-stripe-only terminal.

Generally, the SK keys are Triple-DES of the same length as the UDKs.

Note that transaction routing and authorization are identical for mobile device authorizations, with the limitation that it is chip-only without scripting and the authorization is done by the card brand, not the issuer.

Effects of Quantum: As the typical algorithm is Triple-DES (and mostly two-key Triple-DES), these keys are inherently vulnerable to quantum. A collection of a small number of known UDKs as well as their corresponding PANs and PSNs, the MDK can be determined on a quantum computer. However, compromising enough ARQCs, ARPCs, or scripts could lead to compromising SKs. Obtaining SKs could lead to a compromise of the UDK. Obtaining enough SKs could lead to compromise of UDKs and obtaining enough UDKs could compromise Master Derivation Keys. (Note that each card has a unique Master Derivation Key, so breaking the Master Derivation Key has limited value.)

> Magnetic stripes are inherently insecure and can be easily copied. Another mitigation option may be to simply retire this technology completely. Magnetic stripes account for fewer and fewer transactions every year as chip adoption is nearly universal.

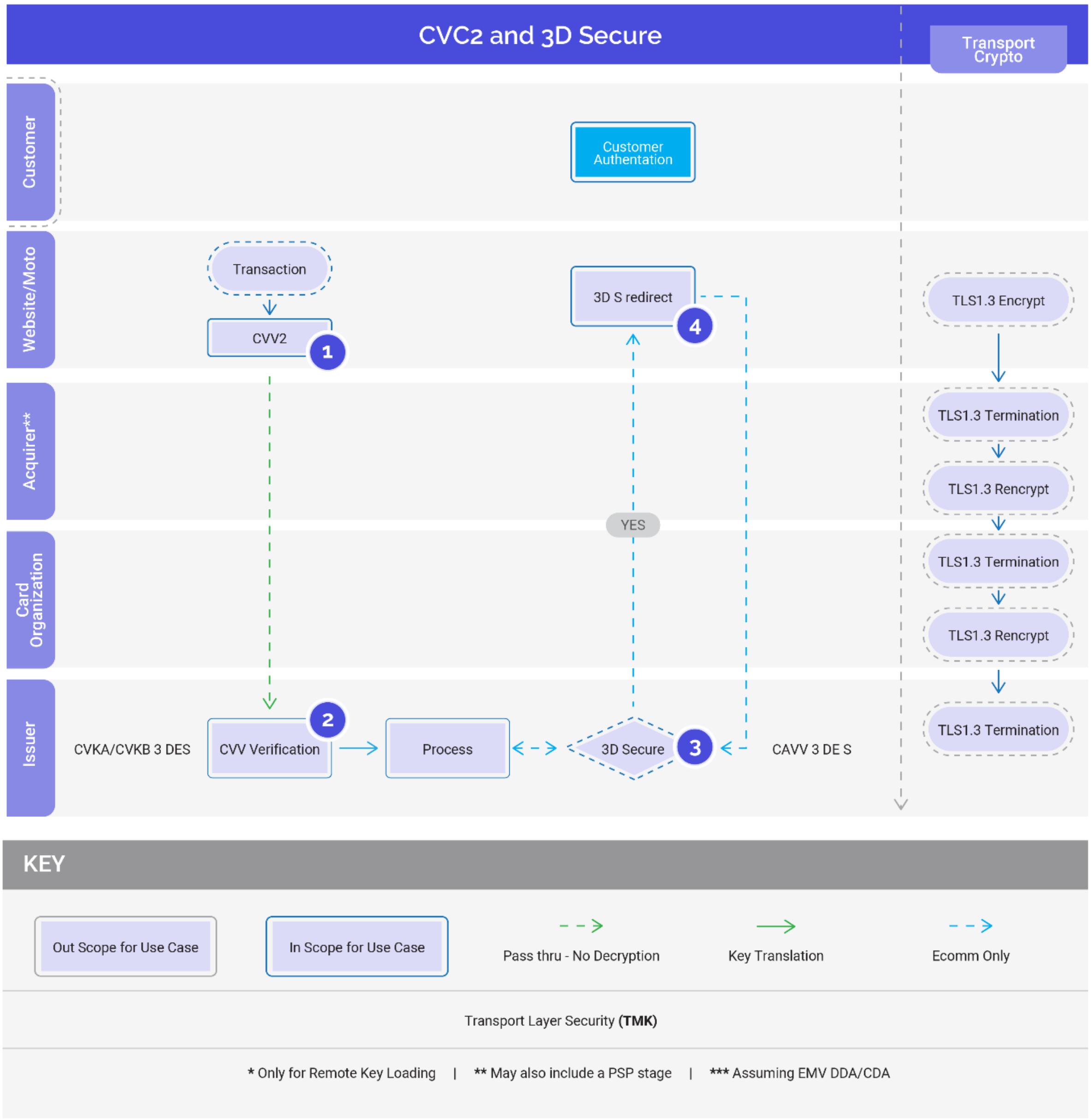
Mitigation Techniques: The natural method to avert these attacks is to use a quantum-safe algorithm for EMV card creation, such as AES. Though AES is supported in the EMV specifications 'EMV Book 3 Application Specification,' cards that have not released derivative EMV chip specifications that support AES could not deploy AES. The mitigation strategy would follow that as described in Use Case 2.

Current Industry Status: There is no publicly available information regarding changing EMV at the time of this writing.

Use Case 4: Card-Not-Present Transaction Detail and Routing

This use case focuses on card-not-present transactions, described in the following diagram. The steps are numbered, which is reflected in the guidance below.

Note: Telephone and postal transactions follow the same flow as online transactions, hence no distinction is made for the purposes of this use case.



There are two main elements of a transaction:

- Card verification: This involves the use of the Card Verification Value 2 (CVV2), the three-digit number on the back of the card.
- Additional cardholder verification: This is the additional step that an issuer can place on its cardholder to give the merchant extra assurance as to the validity of the transaction.

Cryptography and Assumptions: The CVV2 functions in essentially the same way as the Magnetic Stripe Authorization reference from use case 3. It is calculated in the same way but with a different key, the Card Verification Key 2 (CVK2). The CVV2 is entered onto the website (1) and sent to the issuer for verification (2). The algorithm is again dependent upon Triple-DES.

On 14 September 2019, Strong Customer Authentication (SCA) became a requirement for businesses processing online payments in Europe. These requirements were part of the Revised Payment Services Directive (PSD2). This means that for a card-not-present transaction, the PAN combined with the expiry date and CVV is insufficient to authorize the transaction in many cases.

The additional cardholder verification is performed by the 3D Secure service.[vii] Prior to transaction completion, the merchant will redirect the customer to the 3D Secure website where an additional verification step will occur based on the instructions of the issuer. This verification step typically does not involve cryptography. However, upon completion, the issuer's 3D Secure provider will issue a token calculated from a CAVV key (3), which the merchant will retain. The merchant will then submit this token back to the issuer as proof of the transaction (4).

The CAVV value is calculated from the CAVV key using standard cryptography. The key may be AES, but is often two- or three-key Triple-DES.

Effects of Quantum: Quantum will affect the CVV2 in much the same way it affects the CVV: because it is two-key Triple-DES-based, it will be vulnerable. While the three-digit value for a particular card can be obtained through other methods, the compromise of a CVK2 could lead to the compromise of other cards, leading to widespread fraud on many cards.

Quantum would affect those issuers who have implemented CAVV values based on Triple-DES. It could be used to circumvent controls for transaction authorization.

Mitigation Techniques: Unlike CVV, there is currently no plan to sunset CVV2. It is still the main authentication used for transactions. The natural method to mitigate quantum threats would be to upgrade to AES-based CVV2. This would be an extensive effort as it would require a new standard and a large change to implementation followed by a card migration. Another option is to adopt the European method for card-not-present transactions, i.e., Strong Customer Authentication (SCA).

The better technique may be to either change the CVV2 paradigm or apply additional quantum-safe controls on transactions.

For the CAVV, achieving quantum safety would simply be a matter of changing to an AES key. As the CAVV value is only ever calculated by the issuer and is ephemeral (it's only used for a particular transaction), this could be done individually and with relatively little effort.

Current Industry Status: There is no publicly available information regarding changing CVV2 at the time of this writing.

As for CAVV, most implementations are likely Triple-DES and there has been no conversation regarding mandatory migration to AES.

References and Resources

This chart includes BIAN's lower two levels along with our fifth, PCI-specific level.

Table 1. PCI Use Cases by BIAN Model

BIAN L3	BIAN L4	Description	FS-ISAC PQC Working Group L5
Cards	Debit/Credit/Charge Card Fulfillment	The lifecycle of fulfilling a card, from creating numbers, setting interest rates and limits, etc.	Product definition (e.g., type of card, terms and conditions, interest rates)
			Card provisioning setup (e.g. physical systems, HSMs, DBs, etc.)
			Client request mechanism (i.e. tech channel through which requests are made)
			Initial account creation (backend, includes account number)
			Cardholder data provisioning and manufacturing (PAN creation, creation of data for chip, magstripe, CNP, PIN, cardholder record storage)
			Card activation (client activates card)
Cards	Card Authorizations	The authorization, settlement, and funding between merchants, their bank, the issuing	Card-present transaction routing and authorization (includes PIN routing and verification, chip transaction authorization, magstripe authorization, IVR, etc.)

		bank, and the cardholder's account	Card status authorization (e.g. account in good standing, sufficient funds, account not deemed as fraudulent or lost/stolen)
			Transaction status authorization (e.g. transaction deemed anomalous or outside of usual client behavior, AI ML, AML, etc.)
			Settlement of accounts between merchant, acquirer, issuer
Cards	Card Capture	Capturing the payment at the point of sale or transaction, as well as card-not-present cases	ATM and POS setup with backend acquiring systems (e.g. key injection)
			ATM and POS card capture (i.e. actions taken when ATM and POS process transactions)
			Card-not-present transaction detail and routing
Cards	Card Billing and Payments	Bank to consumer issuing of bills and collecting payments	Transaction aggregation and sorting
			Bill creation
			Client payment through different channels
			Account updates based on client activity
			Delinquent account management

Cards	Merchant Relations	Establishing relationships, terms, and overall operations between the merchant bank and the merchant itself with the various networks	Business agreement between merchant and acquirer
			Resolution of fraudulent transactions

References and Resources

[i] PCI Security Standards Council, 2025. *Just Released: Version 3.1 of the PCI PIN Security Standard*. [online] Available at: https://blog.pcisecuritystandards.org/just-released-version-3-1-of-the-pci-pin-security-standard
[ii] IBM, 2025. *PIN Verification Method*. [online] Available at: https://www.ibm.com/docs/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.csfb400/csfb4za2597.htm#:~:text=3624%20PIN%20Verification%20Algorithm,of%20the%20customer%2Dentered%20PIN
[iii] PCI Security Standards Council, 2025. *Implementing ISO Format 4 PIN Blocks Information Supplement*. [pdf] Available at: https://listings.pcisecuritystandards.org/documents/Implementing_ISO_Format_4_PIN_Blocks_Information_Supplement.pdf
[iv] IBM, 2025. *How Visa Card Verification Values Are Used*. [online] Available at: https://www.ibm.com/docs/en/linux-on-systems?topic=services-how-visa-card-verification-values-are-used#:~:text=Because%20most%20online%20transactions%20use%20track-2%2C%20the%20CCA,using%20two%20data-encrypting%20keys%20or%20two%20MAC%20keys
[v] Mastercard, 2021. *Sunsetting Magnetic Stripe Cards*. [online] Available at: https://www.mastercard.com/news/perspectives/2021/magnetic-stripe/
[vi] EMVCo, 2025. *Chip Keys EMV Standard*. [online] Available at: https://www.emvco.com/specifications/
[vii] EMVCo, 2025. *3D Secure Service*. [online] Available at: https://www.emvco.com/emv-technologies/3-d-secure/