FS-ISAC

Post Quantum Payment Card Industry Use Cases: Card Provisioning Setup and Cardholder Data Provisioning

A Technological Review

Written by the FS-ISAC Post Quantum Cryptography Working Group

Post Quantum PCI Use Cases:

Card Provisioning Setup and Cardholder Data Provisioning

Contents

Contributors

- Andrew Mulvenna
- Oscar Covers, Dutch Banking Association
- Erwin Carrow, U.S. Bank
- Dr. Kenneth Giuliani, CIBC
- 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:

Card Provisioning Setup and Cardholder Data Provisioning

Introduction

Quantum computing will enable threat actors to break forms of cryptography that the payment card industry (PCI) relies on for its cybersecurity. In this document, designed for PCI technologists, FS-ISAC's Post Quantum Cryptography Working Group examines the impact of quantum computing on two PCI use cases: Card provisioning setup and cardholder data provisioning.

In this document, we examine those use cases in granular detail to help practitioners make decisions regarding their institutions' cybersecurity in a changing tech landscape. Our findings are organized by:

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

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

- Transaction Routing and Authorization and Retail Transaction Detail and Routing
- ATM and POS Card Capture and ATM and POS Setup With Backend Acquiring Systems

We use the Banking Industry Architecture Network (BIAN)[i] 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
- Cyber hygiene best practices

Post Quantum PCI Use Cases:
Card Provisioning Setup and Cardholder Data Provisioning

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 1: Card Provisioning Setup

Card provisioning setup deals with the environment used to create actual plastic cards. It does not involve card data or the keys used to create data. Instead, card provisioning setup refers to the mechanisms that securely create and transport card-related data elements for plastic cards and PIN mailers.

The main types of keys used in card provisioning:

- Storage Keys
- Key Encryption Keys (KEKs)
- PIN Encryption Keys (PEKs)
- Secure Element (SE) keys for mobile devices
- Trusted Execution Environment (TEE) keys for mobile devices

Table 1 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 Europay, Visa, and Mastercard (EMV) cards and remote key loading
Asymmetric	Elliptic Curve Cryptography	Available with the latest EMV specifications
Triple-DES has been deprecated as an approved algorithm at the time of this writing.		

KEKs are transitioning to the TR-31 standard,[ii] while PEKs leverage the PIN block formats from the ISO.[iii] These keys can be any symmetric key algorithm but are typically two-key or three-key Triple-DES. The keys for mobile devices follow the Global Platform (GP) standard[iv] that has Triple-DES, although more recent implementations allow for AES. Mobile devices also have asymmetric keys for communication and verification.

This document proposes migration to AES at various points but leaves the selection of 128-, 192-, or 256-bit key size to the discretion of the organization in the context of the use case.

Storage Keys

Cryptography and Assumptions: Card-based and PIN-based keys exist in every entity involved in the card provisioning process and typically leverage a hardware security

module (HSM). The HSMs often have a hierarchy of storage keys to enforce segmentation. For our purposes, we classify storage keys as either an HSM master key or other storage key.

- HSM master key: The main key stored within the HSM under which all other keys are encrypted. Depending on the make and model, the HSM master key may be a suite of keys rather than a single key.
- Other storage keys: These are keys encrypted by the HSM master key or other storage keys and used to encrypt keys used for card provisioning. They may be inherent to the HSM or maintained by the application calling the HSM.

The main function of these keys is to store other cryptographic keys (e.g. KEKs, PEKs, or actual card provisioning keys) for storage and import into the HSM.

Effects of Quantum: Storage keys are typically internal to a given system and never leave its immediate environment. While quantum computing could potentially compromise Triple-DES keys, the user would have to have access to data on an internal system.

> Should Triple-DES keys become compromised, the malicious entity would have access to enough data to recreate cards and PINs en masse, depending on the encrypted data they were able to exfiltrate.

Mitigation Techniques: Storage keys can be migrated to AES. This can be done individually on each system and by each organization if the HSMs and proper coding changes are ready. A data migration will likely be needed to convert all existing stored information from the old storage key to the new one.

Current Industry Status: Storage keys are inherently local on the application or infrastructure on which they reside. Hence, each implementation is independent of each other and can be in any valid state.

Key Encryption Keys (KEKs)

Cryptography and Assumptions: KEK keys are used to wrap other keys for transport from one entity to another. There are different scenarios in which this could occur. For example:

- Card provisioning keys could be exchanged between the entity creating card provisioning data and the card embosser or PIN mailer creator to exchange card data, such as chip keys and PEKs.

- Card provisioning keys could be transported offline to authorization systems if created on the provisioning side. Note that if Stand-In Processing is performed, the appropriate keys would need to be transported offline to the card brand.

Individual card issuers will likely have their own internal setup and system architecture and may leverage third parties for some or all of the card provisioning process.

Effects of Quantum: KEKs are shared between systems. Some are shared in an offline channel that is not easily accessed. Others are shared over internal or external TLS connections between systems. If they are Triple-DES keys over an accessible TLS-protected channel, the malicious entity may be able to obtain either the card provisioning master keys or individual card keys, depending on which channel they have access to. They could then either reproduce cards en masse or individually, depending on the data they can access.

Mitigation Techniques: KEKs can also be migrated to AES where applicable. This would need to be coordinated between entities. However, as all systems belong to or are working for the card issuer, this can be done at the card issuer's discretion. Because connections are typically non-persistent, there is no need for a migration. It only requires a coordinated change to use the new key.

Current Industry Status: As of Version 3 of the PCI PIN Security Standards,[v] PCI is mandating the KEKs encrypt keys in keyblock format such as TR-31. This is a phased rollout with the final phase due to be completed by 1 January 2025.

The migration to keyblock format does not inherently mean that AES keys will be used. There is still a prevalence of Triple-DES keys even in keyblock format.

Phase 1:
Effective 1 June 2019

- Implement key blocks for internal connections and key storage within service provider environments

Phase 2:
Effective 1 June 2021

- Implement key blocks for external connections to associations and networks

Phase 3:
Effective 1 June 2025

- Implement key blocks to extend to all merchant hosts, POS devices, and ATMs

PIN Encryption Keys

Cryptography and Assumptions: PEK keys are used to convey PINs from the PIN creation system to the card embossing and PIN mailer creation systems. These keys encrypt PINs in ANSI PIN block format 0, 1, 3, or 4. Format 0, 1, and 3 are Triple-DES-based whereas format 4 is AES-based. Currently, most keys tend to be Triple-DES based.

Effects of Quantum: PEKs are shared between systems that are transmitting PINs, typically during the card provisioning process where the PINs are transmitted to the card embosser or PIN mailer creator over an internal or external TLS channel. If the keys are Triple-DES based, the PINs would be accessible, but only those PINs involved in the process at that time.

Mitigation Techniques: Migration to ANSI PIN block format 4 and AES keys is recommended.

Current Industry Status: While migration to ISO PIN block format 4 is available, there is currently no mandate to migrate to it at the time of this writing. Hence, these keys are still predominantly Triple-DES.

Secure Element Keys for Mobile Devices

Cryptography and Assumptions: Secure Elements are typically hardware-based. The main storage keys are the symmetric keys SCP02 (Triple-DES) and SCP03 (AES), which handle most of the protection and authentication of the Trusted Applications (TAs) that work within them. Note that these keys are shared with the backend system. There is

also a symmetric SCP80 key that handles Over-The-Air (OTA) protection of transmissions.

The main asymmetric keys used for messaging are the SCP10 (RSA) and SCP11 (ECC) keys. The SCP81 keys are used for asymmetric protection of OTA transmissions.

These keys are meant to register the device, conduct internal preparations, and accept card provisioning keys.

Effects of Quantum: Older implementations leveraging SCP02 keys and use of Triple-DES keys for SCP80 will be vulnerable to quantum and result in compromise of the Secure Element itself. This could lead to the disclosure of card-based keys for every provisioned card on the device and fraudulent transactions.

The asymmetric keys used for card provisioning would also be vulnerable to quantum and could disclose card-based keys, which could be used for fraudulent transactions.

Note that devices would be compromised individually unless the backend system is involved. In that case, the compromise could affect many devices.

Mitigation Techniques: Migration to AES for symmetric keys is already possible. This will likely occur naturally as devices are upgraded.

There is currently no standard or known mitigation technique for mitigating the use of asymmetric keys for this use case. The only option is to leverage symmetric-key-based communication as much as possible.

Current Industry Status: Global Platform currently allows the use of symmetric AES keys in its standard and new implementations of mobile devices are encouraged to adopt it. Global Platform has identified asymmetric keys as vulnerable but does not currently offer a replacement.

Trusted Execution Environment Keys for Mobile Devices

Cryptography and Assumptions: TEEs are not purely hardware-based nor completely isolated on a mobile device. Nevertheless, they offer a higher security level than

standard mobile device storage and operations. TEEs are not as rigidly defined as SEs, but there are some common characteristics.

There is a main storage key in the TEE used to encrypt keys and other sensitive information for storage on the device. This key is typically symmetric and either Triple-DES or AES. There is also a Root of Trust that dictates which Outside World Entities (OWEs) are to be trusted by the TEE. These are asymmetric keys and certificates that leverage mTLS.

mTLS secures the TLS connection in a two-way authentication process between clients and servers using X.509 digital certificates.

Effects of Quantum: Implementations using Triple-DES as its main storage keys could be compromised and lead to the disclosure of card-based keys. The Root of Trust is vulnerable to quantum and could lead to fraudulent transactions or malicious apps being enabled.

Mitigation Techniques: Migration to AES for symmetric keys is already possible. This will likely occur naturally as individuals upgrade their devices.

There is currently no standard or known mitigation technique for mitigating the Root of Trust. Eventually, a migration to quantum-safe asymmetric keys or a paradigm change will be needed.

Current Industry Status: Global Platform currently allows the use of symmetric AES keys in its standard. New implementations of mobile devices are encouraged to adopt it. Global Platform has identified asymmetric keys as vulnerable but does not currently offer a replacement.

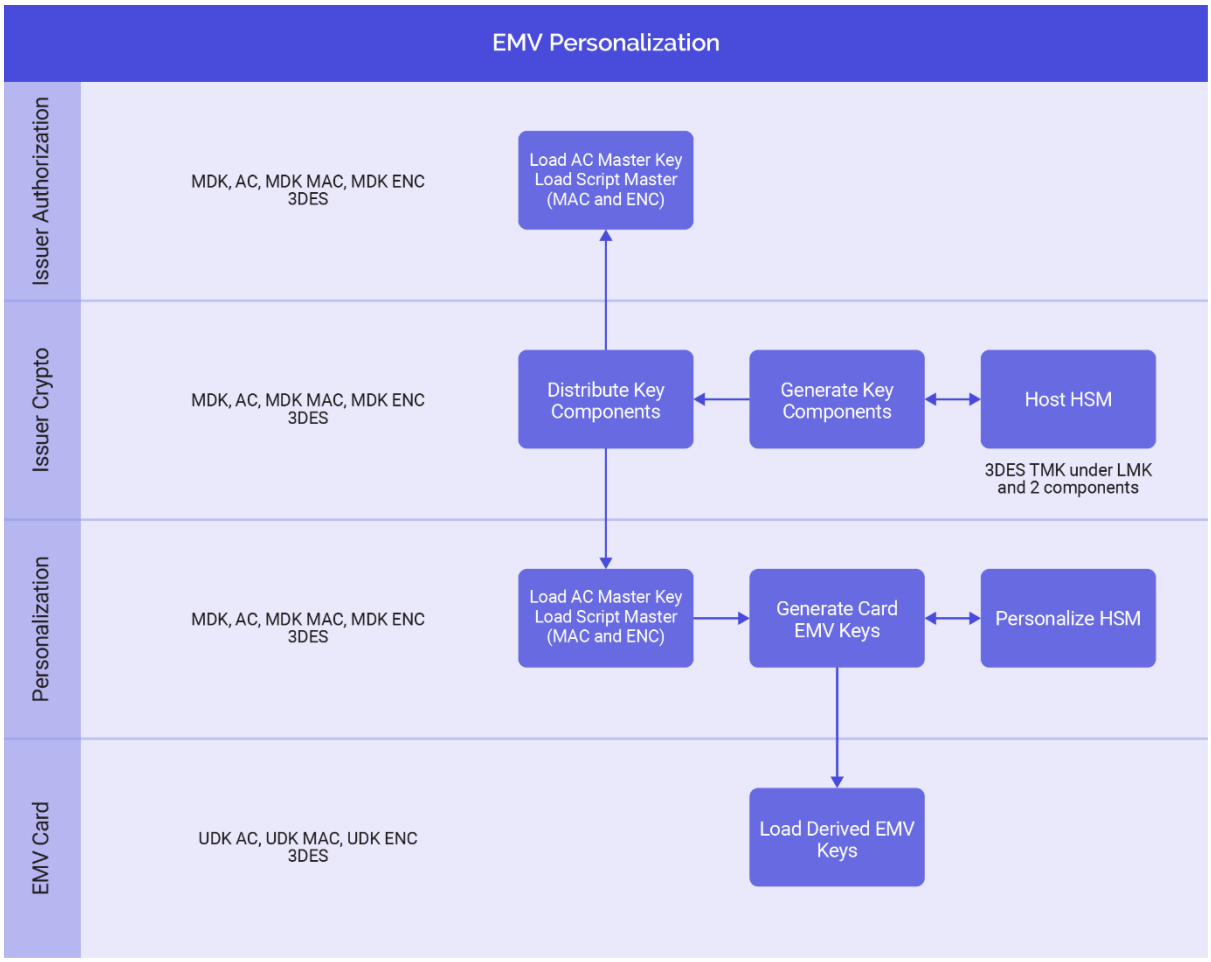
Use Case 2: Cardholder Data Provisioning

This use case covers the provisioning of cardholder data for credit and debit cards, including the following sub-use cases:

- Chip keys provisioning – symmetric
- Chip keys provisioning - asymmetric
- Magnetic stripe keys and Card-Not-Present (CNP) provisioning

Credit and debit cards are very similar from a technology point of view, so this use case makes no distinction between the two.

- PIN provisioning
- PAN protection
- Cardholder data encryption-at-rest



Chip Provisioning – Symmetric

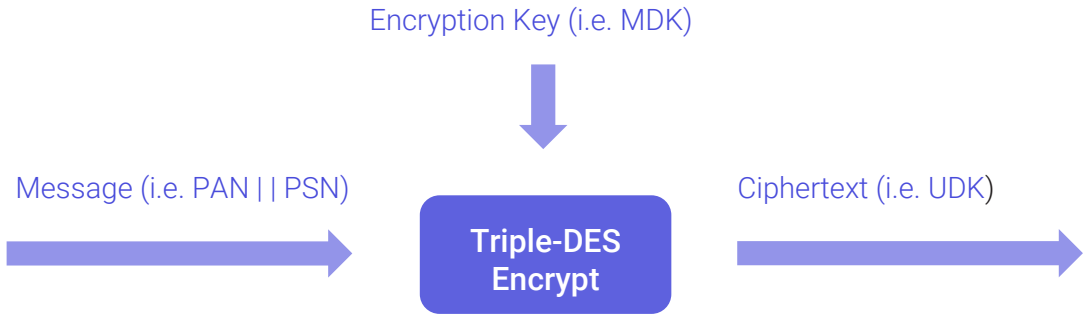
Cryptography and Assumptions: Chip keys are specified in the EMV standard.[vi] The symmetric chip data on an individual card consists of the following four keys corresponding to the EMV standard:

- Unique Derived Key – Authorization Cryptogram (UDK-AC)
  - Derived from a Master Derivation Key (MDK-AC)
  - Used for chip transaction authorization
- Unique Derived Key – Message Authentication Code (UDK-MAC/SMI)
  - Derived from a Master Derivation Key (MDK-MAC/SMI)

- Used for authenticating scripts to and from the card

- Unique Derived Key – Encryption (UDK-ENC/SMC)
  - Derived from a Master Derivation Key (MDK-ENC/SMC)
  - Used to encrypt the PIN to the card
- Unique Derived Key – Dynamic CVV (UDK-DCVV/CVC3)
  - Derived from a Master Derivation Key (MDK-DCVV/CVC3)
  - Used for transaction authorizations of contactless transactions at magstripe-only terminals

Currently in practice, the MDKs and UDKs tend to be Triple-DES keys, often two-key Triple-DES. The MDKs are typically generated at random using an HSM. The UDKs are derived from the MDKs by Triple-DES encrypting the PAN and PAN Sequence Number (PSN) using the appropriate MDK as the encryption key. The resulting ciphertext is the appropriate UDK, as shown in the bottom swimlane of the diagram below.



For mobile devices, only the UDK-AC (and possibly UDK-DCVV/CVC3) is sent to the mobile device to perform transactions. It is essentially identical to that of a contactless transaction, thus the following considerations apply in the same way. Mobile devices do not perform scripting.

In this case, the only entities involved are the card brand and mobile device manufacturer.

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.

MDKs are kept in hardware secure storage on networks that are not publicly accessible and hard to access, even in encrypted form. The one exception is during transport to third-party providers using a KEK.

Similarly, UDKs are also kept in hardware secure storage on networks that are not publicly accessible except during transport to the card embosser using a KEK (it may be possible to get a UDK by observing transaction information).

The main risk has to do with the UDKs that exist on the card itself, which are necessary to conduct transactions. An attacker with a legitimate card could theoretically scan the chip to get the UDK from it. With a small number of UDKs, the attacker could use a quantum computer to obtain the MDK used for the chip. This would allow the attacker to clone many fake cards, which would be accepted by authorization systems.

Note that card EMV verification is only one method of transaction verification. Other controls such as cardholder verification (i.e. PIN) and card validity checking could potentially mitigate the attack.

Mitigation Techniques: The natural method to avert these attacks is to use a quantum-safe algorithm for EMV card creation such as AES. It is not clear if the current EMV standard is compatible with AES as there is a different block size involved. Even if this is resolved, there will be challenges with implementation as chips must be made compatible while maintaining their tamper-resistance and provisioning systems and HSMs would need to be able to support the new algorithm. It should be noted that this is an industry issue and not confined to a specific issuer.

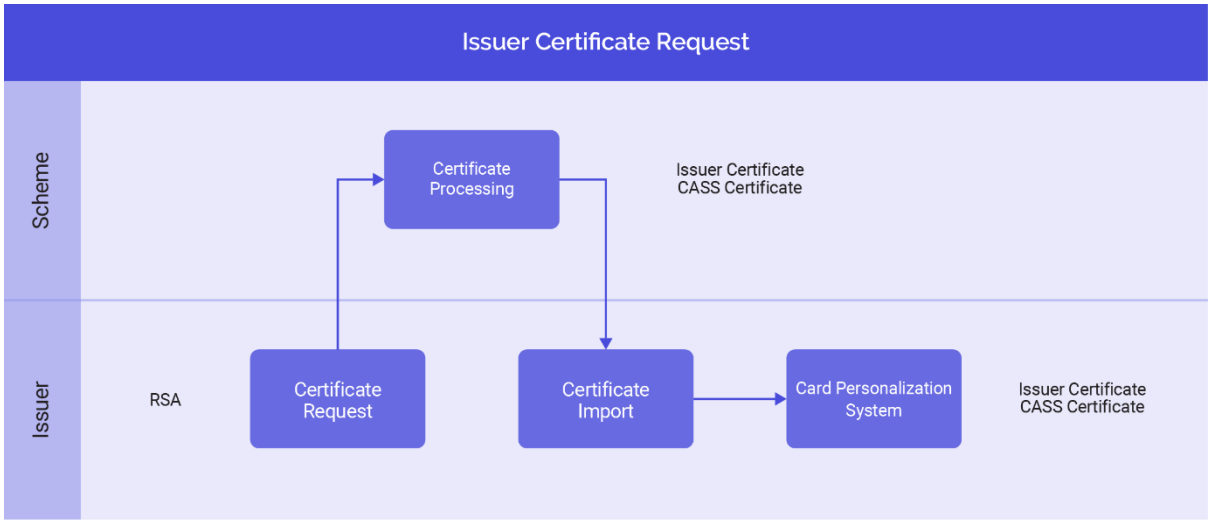
Chips are tamper-resistant, which would make it difficult but not impossible for an attacker to obtain UDKs. And because an attacker can be a valid customer, there is no way to prevent threat actors from obtaining a valid card.

From an individual issuer's perspective, the best mitigation technique would be to segment their cards into different MDKs to confuse the attacker and potentially reduce the attack surface. This could be done by employing different MDKs for different Bank Identification Numbers (BINs) or over different card expiry dates.

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

Chip Provisioning – Asymmetric

Cryptography and Assumptions: The chip has access to an issuer certificate unique for each BIN. The certificate is signed by the global certificate belonging to the card brand. This key is typically a 1984-bit RSA key.[vii]



The chip also has access to an ICC certificate signed by the issuer. It is an RSA key that can be a minimum of 1024 bits.

These certificates work in combination to perform two different tasks:

- Card verification at a POS device, either SDA, DDA, or CDA.
- Offline PIN encryption at a POS terminal, i.e., a client PIN input to a POS device is encrypted at the terminal using the ICC certificate and then decrypted by the chip.

Effects of Quantum: As the asymmetric keys are RSA-based, they would be vulnerable to quantum. Of particular concern are the global CA certificates that belong to the card brands. Compromise of these certificates would allow forgeries of any issuer certificate for that card brand. This could be used to create fake cards that would validate at POS terminals.

The issuer and ICC certificates can also be compromised. This would allow the issuance of fake cards for a particular issuer and BIN.

Note that compromising an ICC certificate could be used to compromise customer PINs if these PINs can be read on the wire of the POS during a transaction.

Mitigation Techniques: The obvious mitigation would be to use a quantum-safe certificate chain starting with the card brand and filtering down. It is not known if EMV is able to accommodate quantum-safe certificates. This would be an industry problem started by the card brands to the issuer. However, it would also involve chip manufacturers and even POS manufacturers as they would need to support the new algorithms. This problem would have to be tackled industry-wide.

One option would be to migrate to AES and authorize all card transactions near real-time. The security of the EMV transaction then relies on the symmetric algorithm of AES. The risk of fake cards is circumvented as the issuer cannot authorize the fake card and will therefore reject the required authorization. With this, EMV will lose the option to authorize transactions offline.

Another option would be to move away from issuer and ICC certificates to an entirely new paradigm. However, there is no indication as to what that paradigm would be.

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

Harvest Now, Decrypt Later Attacks

Harvest now, decrypt later is an exploit strategy in which nation-states or criminal organizations steal and store encrypted data until quantum computing can break the encryption.

For more information, see FS-ISAC's *PQC Working Group Risk Model Technical Paper*

Magnetic Stripe and Card-Not-Present Keys

Cryptography and Assumptions: Magnetic stripe and card-not-present authorization both revolve around a three-digit number: the CVV and the CVV2, respectively.

The calculation of these values is inherently dependent upon and actually modifies the Triple-DES algorithm, so the calculation can't be used with AES.[viii] In addition, the calculation does not allow three-key Triple-DES. (Magnetic stripe and CNP specifications have not been publicly disclosed, but this is known to be the case.)[ix] Hence, all implementations are two-key Triple-DES.

Effects of Quantum: As magnetic stripe and card-not-present authorization use two-key Triple-DES, they are 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 of the Triple-DES encryption. It is not immediately clear if the reduced ciphertext data would complicate the quantum decryption of the CVK1 or CVK2. However, it must be assumed that a quantum computer can crack these keys from enough CVV or CVV2 values.

A compromised CVK1 or CVK2 could yield a large swath of magnetic stripe authorization and card-not-present values.

While the three-digit value for a particular card can be obtained through other methods, the compromise of these keys could lead to the compromise of other cards and widespread fraud on many cards.

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.

However, because magnetic stripes are inherently insecure and can be easily copied using present-day technology, another 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.

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

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

PIN Provisioning

Cryptography and Assumptions: PINs are created by taking the card number and offset along with a PIN Verification Key (PVK) to output the PIN. PIN verification methods exist on the system that creates PINs and are Triple-DES, although AES may also be used. There are several algorithms for PIN offsets; IBM's is the most notable.[xi]

Effects of Quantum: Threat actors who collect many PINs protected by the same key could obtain many customer PINs from only one successful quantum decryption.

Mitigation Techniques: PIN creation could be migrated to AES keys. As PIN creation is handled by the card issuer, migration could happen at the issuer's convenience.

Current Industry Status: All algorithms are available to migrate. The card issuer can do so at any time, so long as the HSM and applications support it.

Note that mobile devices use a PAN different from an associated physical card. This alternate PAN may be a tokenized version of the original.

PAN Protection

Cryptography and Assumptions: Some systems leverage technologies and algorithms to protect the PAN. Some methods such as tokenization are not related to cryptography and so are not in the scope of quantum. Some use Format Preserving Encryption (FPE) to protect PANs.[xii] There is generally a facility that can be called to encrypt and decrypt PANs. As this is newer technology not typically dependent upon HSMs, AES tends to be used.

Effects of Quantum: As PANs are typically protected with AES, they would not be affected by quantum. There is no evidence to suggest the application of FPE would make PANs vulnerable.

Mitigation Techniques: No mitigation required.

Current Industry Status: PAN is largely already quantum safe.

Cardholder Data Encryption at Rest

Cryptography and Assumptions: Cardholder data is often encrypted at rest when it is stored in a database. Usually, a technology such as TDE is used. The keys generally exist only in proximity to the database and tend to be AES keys since this is newer technology. Note that TDE use tends to be proprietary, so it is not bound to a particular specification.

Effects of Quantum: Databases are typically encrypted with AES, so there is no direct threat from quantum.

Mitigation Techniques: No mitigation required.

Current Industry Status: Cardholder data encryption at rest is largely already quantum safe.

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,	Business agreement between merchant and acquirer

		and overall operations between the merchant bank and the merchant itself with the various networks	Resolution of fraudulent transactions

[i] Banking Industry Architecture Network (BIAN), 2025. *BIAN*. [online] Available at: https://bian.org/
[ii] ASC X9, 2018. *ASC X9 TR 31-2018*. [online] at: https://webstore.ansi.org/standards/ascx9/ascx9tr312018?srsltid=AfmBOorFKsLHd1IE7bj25_K9NmAjpPTTzJw27i9w_hFermWJ0XbFXjAg
[iii] ISO, 2025. *ISO 9564-1:2017*. [online] Available at: https://www.iso.org/obp/ui/#iso:std:iso:9564:-1:ed-4:v1:en
[iv] GlobalPlatform, 2025. *GlobalPlatform Technology: Cryptographic Algorithm Recommendations*. [online] Available at: https://globalplatform.org/specs-library/globalplatform-technology-cryptographic-algorithm-recommendations/
[v] 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
[vi] EMVCo, 2025. *Specifications*. [online] Available at: https://www.emvco.com/specifications/
[vii] Visa, 2025. *Visa Smart Debit/Credit*. [pdf] Available at: https://www.visa.com.pe/dam/VCOM/global/support-legal/documents/visa-smart-debit-credit-vbn-visa-public.pdf
[viii] [viii]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
[ix]IBM, 2025. *PIN Formats and Algorithms*. [online] Available at: https://www.ibm.com/docs/en/linux-on-systems?topic=information-pin-formats-algorithms
[x] Mastercard, 2021. *Magnetic Stripe*. [online] Available at: https://www.mastercard.com/news/perspectives/2021/magnetic-stripe/
[xi] IBM, 2025. *PIN Formats and Algorithms*. [online] Available at: https://www.ibm.com/docs/en/linux-on-systems?topic=information-pin-formats-algorithms
[xii] National Institute of Standards and Technology (NIST), 2025. *SP 800-38G Update 1: Final*. [online] Available at: https://csrc.nist.gov/pubs/sp/800/38/g/upd1/final
EMVCo, 2025. *4 Key Features of the New EMV® Contactless Kernel Specification*. [online] Available at: https://www.emvco.com/news/perspectives/2021/magnetic-stripe/
EMVCo, 2025. *EMV® Specifications & Associated Bulletins Archive*. [online] Available at: https://www.emvco.com/specifications/

