Post Quantum PCI Use Cases: ATM and POS Card Capture and ATM and POS Setup With Backend Acquiring Systems

A Technological Review

Written by the FS-ISAC Post Quantum Cryptography Working Group

Post Quantum PCI Use Cases:
ATM and POS Card Capture and ATM and POS Setup With Backend Acquiring Systems

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:
ATM and POS Card Capture and ATM and POS Setup With Backend Acquiring Systems

Introduction

Though it's expected that quantum computing will exponentially expand and speed certain payment card industry (PCI) processes, the technology will also enable threat actors to vastly increase the scope of their crimes.

In this document, designed for PCI technologists, FS-ISAC's Post Quantum Cryptography Working Group examines the vulnerabilities that quantum computing will create in Automated Teller Machine (ATM) and Point of Sale (POS) card capture and ATM and POS setup with backend acquiring systems.

The focus of this document is on:

- 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

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

- Card Provisioning Setup and Cardholder Data Provisioning
- Transaction Routing and Authorization and Retail Transaction Detail and Routing

- Considerations for standard-setting bodies
- Considerations for implementations in the payment card ecosystem
- 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 5: ATM and POS Card Capture

For this use case, we assume that the ATM and POS devices have been set up and are ready to process transactions. The ATM and POS generally act as a pass-through for Europay, Mastercard, and Visa (EMV) and magnetic stripe data. Their main cryptographic functions are:

1. Online PIN verification, which sends the PIN encrypted with the acquirer key to the acquirer
2. Offline PIN verification using the public key from the chip's integrated circuit card (ICC) – or smart card – certificate
3. Offline card verification using the public key from the issuer and ICC certificates

ATM and POS technology tends to be proprietary, and so do not reference in the public domain. However, they must comply with the PCI PIN Transaction Security (PTS) Point-of-Interaction (POI) Modular Security Requirements.[i] In addition, the PCI issues requirements regarding handling key material used to secure and process PIN transactions and the PCI PIN security standards.[ii]

Online PIN Verification

Cryptography and Assumptions: The main function here involves encryption of the PIN for conveyance to the acquiring system. The PIN is typically encrypted with a Terminal PIN Key (TPK) – which is similar to a PIN Encryption Key (PEK) – using ISO PIN block format 0, 1, 3, or 4. ISO PIN block formats 0, 1, and 3 are 64-bit block size, which essentially mandates the use of Triple-DES. ISO PIN block 4 allows a larger 128-bit block size to permit 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.

The TPKs themselves are re-established between the device and acquiring systems at various intervals, such as every 2,000 transactions or every day. If the TMK is used to exchange the TPKs, then PCI PIN mandates that they be exchanged in keyblock format such as TR-31.

The other alternative is to establish a new TPK to use the Derived Unique Key Per Transaction (DUKPT), which the device and acquiring system can use to automatically generate a new TPK for every transaction.

The TPKs would generally have the same algorithm type as the TMKs and would thus mostly be Triple-DES.

Effects of Quantum: If both the TMK and TPK are Triple-DES, then they would be vulnerable to quantum. An attacker with access to the channel would be able to retrieve and harvest customer PINs. It should be noted that there will likely be an additional layer of channel protection such as TLS present.

Harvest Now, Decrypt Later Attacks

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

To learn more, see PQC Working Group Risk Model Technical Paper.

Mitigation Techniques: The obvious solution is to migrate the TMK and TPK from Triple-DES to AES. This would entail the use of ISO PIN block 4 in EPPs and POS devices as well as acquiring systems. This would be dependent upon the acquiring system. However, once the technology became available, individual acquirers would be able to migrate at their convenience.

Current Industry Status: ISO PIN block 4 is available for use. At the time of this writing, there is no information available as to its availability in EPP and POS devices.

Offline PIN Verification

Cryptography and Assumptions: Offline PIN verification would happen only at a POS device. The keys used for this verification would be the card brand, issuer, and ICC certificate. Verification would be 1984-bit RSA certificates except for the ICC certificate, which is a minimum of 1024-bit. Note that the card brand certificate would be placed in the device either at the factory or during POS setup.

The POS would import the issuer and ICC certificate from the chip and encrypt the input PIN using the ICC certificate to send it back to the chip.

Effects of Quantum: The certificates are inherently vulnerable to quantum. This means that PINs could be deciphered at the POS terminal when the communication channel is tapped.

Mitigation Techniques: One option would be to change the public key encryption algorithm of EMV to a quantum-safe algorithm. This would then require changes to POS devices, chip manufacturers, card brands, and issuers. The alternative would be to move to a new paradigm for offline PIN. This would be an industry problem to solve.

Payment terminals/POS also have the option to use the online PIN validation option and use AES and ISO PIN block 4. Payment infrastructures, however, may not be up to the task and the EMV chips would have to use AES. If all EMV card transactions are processed near real time, then the security of the EMV transaction relies on the symmetric algorithm of AES.

In this case, the risk of fake cards is circumvented as the issuer cannot authorize a fake card and will therefore reject the requested autorization. By processing all EMV card transactions online, EMV will lose the option to authorize transactions offline.

Current Industry Status: Indicators are that EMV is exploring the use of AES.[iii]

Online Card Verification

Cryptography and Assumptions: Online card verification only happens on a POS device. The same card brand, issuer certificate, and ICC certificate would be used to perform either Static Data Authentication (SDA) – which is outdated and deprecated – Dynamic Data Authentication (DDA), or Combined Dynamic Data Authentication with Application Cryptogram (CDA) as specified in EMV standard to verify the card offline.

Effects of Quantum: The certificates are vulnerable to quantum. Fake certificates can be created to allow arbitrary cards to pass the authentication. This applies to each of the three certificates: Card Brand Certificate, ICC Certificate, and Issuer Certificate.

Mitigation Techniques: As with offline PIN verification, mitigation options include changing EMV to use quantum-safe certificates (which would require changes to POS devices, chip manufacturers, card brands, and issuers), moving to a new paradigm for offline PIN, or moving to near real-time processing of the card transaction. If the EMV transaction is processed near real time, the use of CDA is recommended because the EMV chip itself reports to the issuer of the card of the checks performed. These 'Card Verification Results' are part of the online authorization request and the card can use AES to protect the authorization request.

Current Industry Status: Indications are that the use of AES is being explored by EMV.[iv]

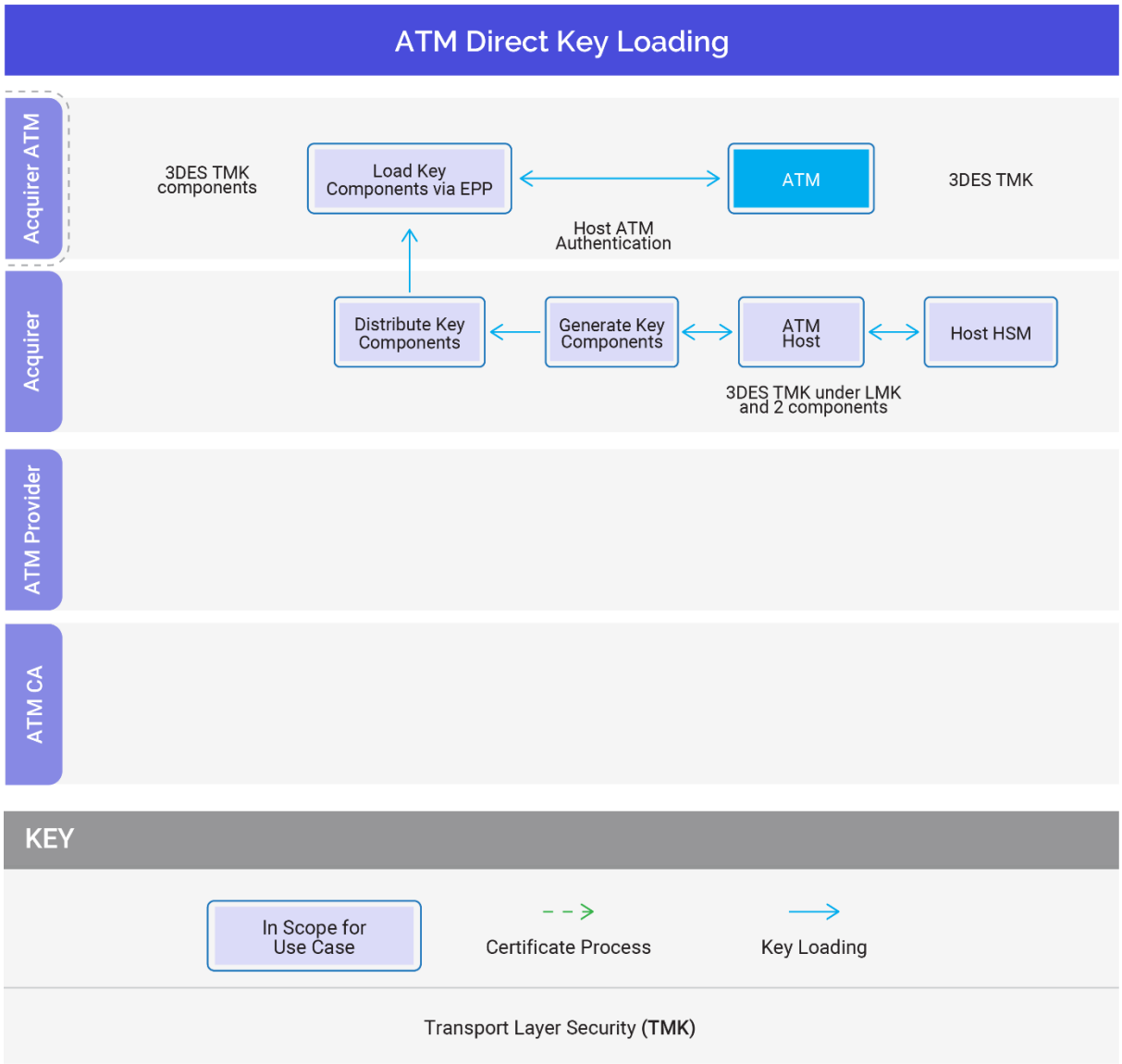
Use Case 6: ATM and POS Setup With Backend Acquiring Systems

Generally speaking, there are two ways that an ATM or POS can be set up for function:

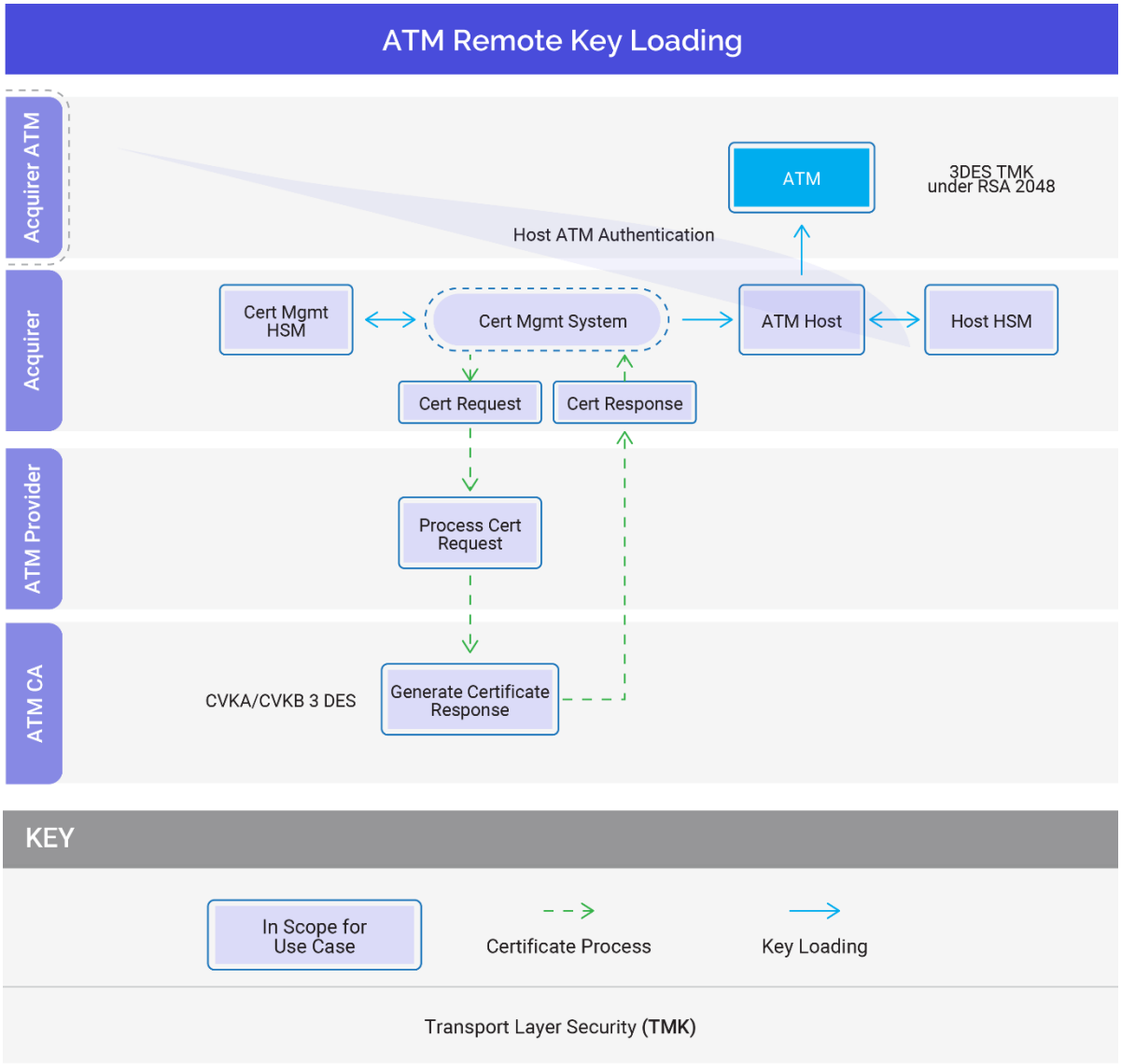
1) Manual Key Injection
2) Remote Key Loading

For our purposes, we will consider injection into ATM and POS as a similar function. The end goal is to have a Terminal Master Key (TMK) that can be used for PIN functions. This case will cover the process up until the TMK is established.

Manual key injection is described in the following diagram.



Remote key loading is described in the following diagram.



Key injection systems tend to be proprietary, so their details are not available publicly. However, the requirements are subject to PCI PIN version 3.1.[v]

Manual Key Injection

Cryptography and Assumptions: Manual key injection involves injecting a key into an ATM or POS using a direct air-gapped offline channel. The TMK is created on an HSM and then injected into the ATM/POS over a physical wire. It is also possible that the TMK is transferred onto some sort of removable media to be taken to the location where the ATM or POS exists.

The TMK itself is typically a two- or three-key Triple-DES key although it is possible to use an AES key.

Effects of Quantum: Many of the keys for manual key injection are now Triple-DES. Because the channel is offline, quantum computers will have little impact. However, the root key will always have to be stronger than the underlying keys. It is therefore recommended that root keys migrate to AES.

Mitigation Techniques: Manual key injection tends to be secure and does not require much mitigation from quantum. Migrating HSM and other facilitating keys to AES is recommended.

Current Industry Status: Manual Key Injection is becoming less prominent due to its cost and the effort involved in physical access.

Remote Key Loading

Cryptography and Assumptions: The basic idea behind RKL is that the Encryption PIN Pad (EPP) for an ATM or a POS comes with its own certificate in its factory state, injected by the manufacturer. This certificate has been signed by the manufacturer's own certificate authority (CA).

The acquiring system is then given its own certificate from the ATM/POS manufacturer. The two certificates are exchanged in a TLS-like protocol and used to establish a KEK to exchange the TMK. TMKs can be updated at any point using the same protocol at the request of the acquiring system.

These certificates vary among manufacturers, but certificates tend to be 2048-bit RSA. The manufacturer may employ additional cryptography to exchange the acquirer certificates for signing.

Effects of Quantum: If an attacker is able to listen to the initial RKL exchange upon setup or TMK re-establishment, they would be able to determine the TMK and eventually compromise client PINs, which would traverse the network. A threat actor could also substitute their own certificate or TMK and compromise the device.

Mitigation Techniques: The EPP or POS manufacturer would need to change the certificates to be quantum-safe or otherwise change the protocol to use a quantum-safe protocol. This would involve a change to the acquiring system as well. Note ATM and POS devices are in the scope of PCI PTS (applies to remote key loading and remote software download) and PCI PIN (applies to key loading and key management), so changes would need to be compliant.

Note that for remote key loading, the bootloader of the EPP or POS must also use quantum secure cryptography and the implemented quantum secure encryption algorithms must be resistant to side-channel attacks in accordance with PCI PTS. Manufacturers know how to securely implement AES in firmware, but may need to acquire knowledge of PQC-safe algorithms.

Alternatively, it is possible to move toward manual key injection as a fallback.

Current Industry Status: At this point, there is no publicly available reference regarding changes to RKL.

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

[i] PCI Security Standards Council. (n.d.). The PCI PIN Transaction Security (PTS) Point-of-Interaction (POI) Modular Security Requirements. Retrieved from https://www.pcisecuritystandards.org/about_us/press_releases/pci-security-standards-council-updates-standard-for-device-security/

[ii] PCI Security Standards Council. (2023). PCI PIN security standards. Retrieved from https://blog.pcisecuritystandards.org/just-released-version-3-1-of-the-pci-pin-security-standard

[iii] EMVCo. (n.d.). AES exploration for offline PIN verification in POS. Retrieved from https://www.emvco.com/knowledge-hub/how-emvco-is-supporting-card-data-encryption-advancements-for-card-personalisation/ and https://www.emvco.com/knowledge-hub/4-key-features-of-the-new-emv-contactless-kernel-specification/#:~:text=It%20introduces%20Advanced%20Encryption%20Standard,In%2DThe%2DMiddle%20attack

[iv] EMVCo. (n.d.). AES Exploration for online PIN verification in POS. Retrieved from https://www.emvco.com/knowledge-hub/how-emvco-is-supporting-card-data-encryption-advancements-for-card-personalisation/ and https://www.emvco.com/knowledge-hub/4-key-features-of-the-new-emv-contactless-kernel-specification/#:~:text=It%20introduces%20Advanced%20Encryption%20Standard,In%2DThe%2DMiddle%20attack

[v] PCI Security Standards Council. (2023). Version 3.1 of PCI PIN Security Standard. Retrieved from https://blog.pcisecuritystandards.org/just-released-version-3-1-of-the-pci-pin-security-standard