Cryptographic Agility Strategies for Card and Mobile Payments

Position Paper of the ECPC Security Working Group

Version 1.0

December 2025

1 Introduction

We are presently in an age where the major evolution of cryptographic recommendations and standard updates is to be quickly taken into account. Indeed, there is an important need to consider classical attacks making current cryptographic mechanisms or key lengths obsolete, e.g. the use of the RSA asymmetric algorithm is urgently in need of reform given that it has reached its maximum key size under the EMV[1] card specifications constraints. But also, the quantum threat must be considered, as detailed in Section3.

There are already cryptographic mechanisms that provide protection against attacks using quantum computers, but the situation is very dynamic and gives rise to the need for crypto agility in payment systems. Crypto agility is the capability of an IT system to change its cryptographic algorithms and protocols swiftly and efficiently. Crypto agility is crucial in the payment context, especially to address the risks posed by quantum computing and the ongoing race for mature post-quantum cryptography (PQC) algorithms.

It is strongly recommended to consider integrating PQC in future products in a hybrid fashion following European recommendations[2] and to implement cryptographic agility, especially to counterbalance the lack of maturity of the PQC algorithms. It should be possible to update the cryptographic algorithms without recalling a product already deployed in the field.

In card-based payment systems, there are three possible cryptographic migration strategies:

- *Card-based migration*: One migration strategy is achieved by migrating all the cards to support both legacy and new algorithms, and only when the last legacy card has been retired, can the first terminals with new algorithms start to be deployed. This will be a time-consuming and risk-prone strategy.
- *Terminal-based migration*: The inverse strategy; starting with the complete terminal migration before issuing the first new card, is equally Herculean.
- *Card <u>and</u> terminal-based migration*: Preparing both cards and terminals to support simultaneously legacy and new algorithms in order to guarantee a quicker transition.

In principle, there is a good reason to encourage the migration of cards: Firstly, cards are completely under the control of the issuer. Secondly, the terminal market tends to be driven by developments on the card market. However, only the third option is viable to provide for a quick transition of cryptographic algorithms and, therefore, cryptographic agility.

This position paper provides a common understanding among ECPC of the challenges in achieving crypto agility for these card-based payments systems as well as the path forward.

In Section 2**Fehler! Verweisquelle konnte nicht gefunden werden.**, we describe cryptographic agility principles.

In Section 3, we describe the concept of PQC readiness.

[1] EMVCo, EMV Specification Bulletin (No. 208): Clarification of Maximum Public Key Lengths, First Edition, July 2018

[2] ENISA, Agreed Cryptographic Mechanisms, Version 2.0, April 2025

In Section 4, we analyse cryptographic challenges on the interface between card and terminal, namely:

- The card authentication, both offline and online
- The encrypted PIN validation, both offline and online

In Section 5, we look into terminal design issues so as to protect the communications between the terminal and the various servers for remote key loading, terminal parameter configuration, transaction authorisation and transaction capture for clearing and settlement.

We conclude with final "Summary and Recommendations" in Section 6.

2 Crypto-Agility Principles

Crypto agility is the capability of an IT system to change its cryptographic algorithms and protocols swiftly and efficiently. For example, the migration of algorithms implemented on cards is to be achieved by issuing new cards. While this takes at most as long as the validity period of the card, the migration process including the timeline is fully controlled by the issuer. Today, a special aspect of crypto agility is quantum readiness, i.e. systems being ready to move to quantum-resistant cryptographic algorithms. Thus, migration to quantum-resistant cryptography can be considered the current challenge of crypto agility and should be facilitated in a way that improves future migrations.

To ensure the swift exchangeability of the used algorithms several aspects of crypto agility have to be addressed:

- Discovery aspect: The used cryptographic algorithms and the possible challenges in replacing them have to be known. This position paper is a contribution to this aspect of cryptographic agility.
- Specification aspect: Specifications have to be written in a way that they do not rely on a specific choice of algorithms, e.g. that the different lengths of data elements are supported.
- Implementation aspect: The implementation of the components has to take into account that cryptographic algorithms might have to be updated:
    - In regard to payment instruments:
        - Cards will be gradually replaced by issuing new cards in accordance with the regular lifecycle. Therefore, it is not necessary to implement a dedicated update mechanism for cards.
        - Mobile applications are more versatile and can be updated with processes common to the mobile environment. New versions of a mobile application can be distributed via the app stores, which provide a security anchor by app signing. As of Android 11, the Merkle Signature scheme is supported, which is secure against attacks with quantum computers[3].
    - To achieve crypto agility for terminals, an update mechanism is required. This is discussed in section 5 in detail.

[3] APK signature scheme v4, https://source.android.com/docs/security/features/apksigning/v4

    - Backend systems, and especially hardware security modules, must also have the ability to be updated securely. This problem is not specific to card payment schemes.
- Migration aspect: A defining feature of card payment schemes is the decentralized organization, i.e. the payment schemes consists of many cards and terminals, which have to be interoperable. Therefore, any migration strategy must include a mechanism for terminal and card to negotiate the cryptographic algorithms.

It is recommended to implement all four aspects of crypto agility. In particular, it is recommended to avoid a hard-coded choice of algorithms for all specifications.

3 Quantum Readiness

3.1 The Quantum Threat and Post-Quantum Cryptography (PQC)

The possibility of quantum computers developed in the near future poses a serious threat to the cryptography used today. Grover's algorithm, which is a very fast quantum search method, theoretically reduces the security level of block ciphers to a half, while there is some discussion on the practical applicability. Based on current knowledge, the use of a key size of 256 bits is considered to provide sufficient protection against attacks using quantum computers in the long term and the use of key sizes of 128 bits will also provide a sufficient security level in many use cases. The impact for asymmetric cryptography is even greater: Shor's algorithm completely breaks asymmetric cryptography primitives like RSA used in the EMV specifications[4] as well as Elliptic Curve Cryptography like for instance the EC-SDSA signature primitive which is used in the EMV contactless specification[5].

To address this, NIST initiated a process in which the scientific community analysed several proposed post-quantum cryptography (PQC) algorithms, resulting in the first standardised mechanisms. These mechanisms fall into two categories:

- *Key Encapsulation Mechanisms (KEMs):* They allow one party to securely provide an encapsulated, i.e., asymmetrically encrypted, secret key to another party.
- *Digital Signature Mechanisms:* They enable a signer to prove the authenticity and integrity of messages to any verifier that processes and trusts the signer's public keys.

[4] EMVCo, EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Version 4.4, October 2022

[5] EMVCo, EMV Contactless Specifications for Payment System, Book E, Version 1.1, February 2025

ENISA is recommending PQC algorithms, some of which, but not all, are standardised by NIST. The following table provides an overview of these algorithms:

ENISA currently recommends the following PQC algorithms[6]	***Key Encapsulation***	***Signature***
Based on the Ring Learning With Errors (R-LWE) Problem	*ML-KEM (FIPS203)*	*ML-DSA (FIPS204)*
Based on the Learning With Errors (LWE) Problem	*FrodoKEM*	-
Hash-based, state-based	-	*XMSS (NIST SP800-208)* *LMS (NIST SP800-208)*
Hash-based, state-less	-	*SLH-DSA (FIPS205)*

Thus, a variety of mechanisms based on different mathematical problems has already been standardised. Nevertheless, choosing the right protocol and finding secure and efficient implementations may still remain a challenge for the next years.

In a joint statement[7] the European security agencies identify two main risks in the context of the quantum threat: "store-now, decrypt-later" -attacks and long transition periods for complex systems. The statement suggests that threat analysis, the creation of a cryptographic inventory and migration planning as well as the promotion of research and standardisation should be top priorities from now on. Until the end of 2030, for the "most sensitive use cases"[7] long-term secrets should be protected against "store-now, decrypt-later"-attacks. Payment transactions require the authentication of the payer as well as the protection of authenticity and integrity of payment data for as long as the payment can be contested. Also, secrets such as the Personal Identification Number (PIN) of the payer are used to secure payment transactions, but these secrets can be in principle re-issued, although issuing many new PINs at a time might be challenging and costly. Furthermore, it might be necessary to disallow PINs chosen by the customer. Still, the PIN is dynamic and the issuer is able to replace it. Therefore, long-term secrets are not used for securing payments and this use case is not vulnerable to "store-now, decrypt-later"-attacks. However, where payment service providers process personal data, "store-now, decrypt-later"-attacks might still pose a risk.

Furthermore, the joint statement recommends transition plans for complex systems like PKI to be developed until the end of 2030. The payment landscape consists of decentralised systems with a lot of participants. Thus, the transition will be indeed complex.

3.2 Hybridisation

In our context, hybridisation means to combine two cryptographic algorithms, e.g. one classical algorithm and one PQC algorithm, in a way that both of them have to be broken to compromise the

[6] ENISA, Agreed Cryptographic Mechanisms, Version 2.0, April 2025

[7] Securing Tommorow, Today; Transitioning to Post-Quantum Cryptography," 27.11.2024

confidentiality or integrity of the protected assets. This principle can further improve resilience against two types of events:

- A breakthrough in quantum computing, that may render classical algorithms unsuitable, and,
- the discovery of a vulnerability in one of the chosen post-quantum algorithms (due to their still embryonic maturity), may cause the algorithm to be considered impaired or broken.

If both events occur, long-term secrets may be compromised, even if hybridisation is employed.

Thus, there is a transitional phase during which any impaired or broken post-quantum algorithm can safely be replaced thanks to classical cryptography algorithms as long as the Y2Q[8] has not arrived.

At some point during this transitional phase in cryptography, we are likely to observe a trend, where classical cryptographic algorithms are increasingly viewed as insecure due to the advancements in quantum computing.

At the same time, post-quantum cryptographic (PQC) algorithms are expected to advance and mature. As these PQC algorithms develop, their robustness will improve, leading to a decreased likelihood of vulnerabilities being discovered.

Essentially, as classical algorithms become more susceptible to being broken due to quantum advancements, PQC algorithms will become more reliable and secure, offering a stronger defence against potential cryptographic threats.

> It is recommended to consider hybridisation for all sensitive applications, especially when long-term security is to be considered, as long as PQC algorithms are not mature enough to be fully trusted.

4 Crypto Agility for Card and User Authentication

Card-based payment systems face three major challenges with regard to crypto agility:

- Firstly, a card payment scheme is by design decentralized, i.e. to migrate to new cryptographic algorithms or protocols, many different system components (cards, terminals, backend systems) have to be changed using one of the migration strategies outlined above.
- Secondly, the communication between terminal and card is limited both in terms of transmission time[9] and in terms of data sizes that can be transmitted, such that not every cryptographic algorithm and protocol can be used between card and terminal.

[8] Y2Q stands for Year to Quantum, that is, the moment in time when a quantum computer is sufficiently at scale to threaten classical algorithm of cryptography. At the time of writing, the estimates for Y2Q range from 2030 BSI/NIST) to 2040 (EMVCo).

[9] The bit rate transmission influences the performance significantly, but higher transmission rates are already accommodated in relevant standards (e.g. ISO 7816) allowing to reach good performances

- Thirdly, cards have limited memory resources[10], which also reduces the number of algorithms that can be implemented.

For the communication between card and terminal, the concept of crypto agility has to be applied to several cryptographic tasks:

- Authentication of the card against the acceptance (terminal) system using asymmetric cryptography and/or against the issuer system using symmetric cryptography.
- PIN encryption by the terminal and PIN decryption by the card to ensure the confidentiality of the PIN

4.1 Issuer Authentication

4.1.1 Online Authentication of the Card

Today, the online authentication of the card is fully based on the verification of the ARQC by the issuer's authorisation system. Thus, terminals do not have to be updated to achieve crypto agility in this regard. As far as cryptogram computation is based on AES[11], it can be considered quantum-resistant for now.

Thus, the transition to a quantum-resistant solution can be facilitated by issuing cards supporting the AES algorithm and by updating the authorisation systems. CPACE specifications support AES as an option and almost all products certified by ECPC already support AES.

It is recommended that issuers expedite the adoption of AES for application cryptograms and for secure message integrity and confidentiality.

4.1.2 Offline Authentication of the Card

Offline authentication of the card seems to be the hardest challenge for crypto agility. For offline authentication to be realised such that it is protected against attacks using quantum computers, either a signature scheme or a key encapsulation mechanism must be used. In principle, PQC algorithms can be implemented on chip payment cards, but they are not considered yet by EMV card and kernel specifications.

Given this situation, one way to protect card payments against the quantum threat is to rely on online authentication as much as possible. However, there are use cases for which this is not an option.

Mass transit: The use of payment cards in mass transit environments consists usually of an offline authentication as a condition to give the user access to the means of transportation (as long as the card is not blacklisted). Subsequently, a deferred authorisation is sent to the issuer to complete the payment. If this authorisation request fails, the card will typically be blacklisted for future use. Thus, breaking the offline authentication will result in the one-time opportunity for a fraudster to transit without paying, which is in itself not a plausible fraud scenario for an attacker having access to a

[10] Card technology already exists to support PQC algorithms together with classical ones.

[11] EMV Integrated Circuit Card Specifications for Payment Systems, Book 2 Security and Key Management, Version 4.4, October 2022

quantum computer. However, a fraudster breaking the issuer certificate or the certificate of the payment scheme may be able to forge cards that can be used as one-time ticket. Depending on the costs of such an attack (using a quantum computer to break RSA or ECC), this might not be the most probable fraud scenario that would be pursued by the fraudster. However, note that attacks on payment and mass transit might also occur from malicious actors without financial motivation to harm the scheme image or the public infrastructure..

To enhance resilience, payment systems are currently using asymmetric cryptography, RSA and Elliptic Curves[12], which is weak to quantum computing because of Shor's algorithm. Thus, to maintain such a resilience in the perspective of the Y2Q, it is required to move to post-quantum cryptography in a hybrid fashion following European recommendations[13].

However, security is not a patch and must be considered at the design stage. Some academic papers[14] already proposed some modifications of available payment protocols between a card and a payment terminal to integrate post-quantum algorithms. Although in recent years it was considered that post-quantum algorithms would not fit the constraints of payment cards, mostly because the data exchange between a card and a payment terminal would take too long, chip manufacturers recently reported encouraging news showing that, provided higher bitrates are negotiated between the card and the terminal, post-quantum algorithms can be carried out in an acceptable timeframe. They reported figures only for the contactless interface as this was the only interface for which a bitrate negotiation (Protocol and Parameter Selection) was allowed at that time. Indeed, the situation has changed when EMVCo released a specification bulletin[15], which specifies such a negotiation protocol also for the contact interface, allowing to negotiate higher bitrates. The size of cryptography data objects is really inflated by the transition to PQC. Therefore, the question of whether or not new available bitrates will be sufficient to exchange post-quantum cryptography data objects is still at stake.

It is recommended to pursue higher bitrates for the communication between card and terminal, such that the user experience will not be impacted by long transaction times.

[12] See for instance EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Version 4.4, October as well as EMV Contactless Specifications for Payment System, Book E, Version 1.1, February 2025

[13] See for instance European Cybersecurity Certification Group (ECCG), Sub-group on Cryptography, Agreed Cryptographic Mechanisms, Version 2.0, April 2025

[14] IDEMIA, Post-Quantum Protocols for Banking Applications, CARDIS 2022

[15] EMV Specification Bulletin (No. 246): Contact – Introduction of Protocol and Parameters Selection, First Edition, July 2025

4.2 PIN Encryption

4.2.1 PIN Encryption for Online PIN Verification

The ISO 4 format[16] has a length of 128 bits and therefore enables PIN encryption using a 128-bit block cipher such as AES. Still, this format has to be supported by terminals as well as backend systems. Overall, migration remains a manageable challenge.

4.2.2 PIN Encryption for Offline PIN Verification

For offline PIN verification, which is used in contact mode only, an asymmetric encryption algorithm is required. As a result, offline PIN encryption is currently not secure against attacks with quantum computers. For offline PIN verification, so far, no solution is specified, while offline PIN verification remains crucial for payment scheme resilience, e.g. with regard to communication outages. It is important to note that offline PIN verification is not used in transaction with deferred authorisation as in the mass transit use case.

5 Crypto Agility for Terminal-to-Host-Communication

Regarding the terminal-to-host communication link, potentially several assets conveyed by well-defined protocols need to be protected. Without pretending to exhaustivity, it can be cited:

- Key injection and remote key loading which typically consists in provisioning the terminal with PIN encryption key(s) either locally in a personalisation facility or remotely when the terminal is already on the field
- Terminal parameter downloading which consists of configuring a terminal remotely with integrity from an authorised host
- Authentication between the terminal and the acceptance/acquirer system to ensure authenticity and integrity of transaction data
- Encryption of card data (if required by the rules of the payment scheme or the acquirer)
- PIN Encryption for online PIN verification

Payment terminals are thus connected to several remote servers either for transactional or administration purposes or even for key management. Different so-called ‘application’ protocols are indeed carried out between a terminal and remote servers. All these protocols are secured either by using cryptography mechanisms directly at the Application level or by relying on the layer below, for instance using the TLS protocol (Transport layer) or IPSec (Routing layer). In the sequel we focus on the case when the application protocols’ security relies on TLS for the sake of clarity and due to the large deployment and availability of TLS. Notice that the security principles exposed hereafter can be applied at the Application and Routing levels as well.

Indeed, on the Application Layer, symmetric cryptography may be used to protect the integrity of the messages by MACing and – if demanded by the payment scheme or the Acquirer – encrypt card data. Thus, with AES there is an obvious quantum-resistant solution for this use-case. Furthermore, when

[16] ISO 9564-1:2017, Financial services — Personal Identification Number (PIN) management and security, Part 1: Basic principles and requirements for PINs in card-based system

the key loading and replacement can be secured by symmetric cryptography, there is no need for a PKI.

Payment transactions are handled by at least two payment applications which are represented by the blue boxes (top row) in Figure 1, one for contact payments and one for contactless payments. As already mentioned, the terminal is also supported by Application protocols (prefixed with the acronym 'A2AP' which stands for 'Acceptor to Acquirer Protocol') which are illustrated in green boxes (middle row):

- Box 'A2AP – RKL' is the Remote Key Loading protocol which allows to load application keys remotely, e.g. PIN and data encryption key(s).
- Box 'Parameter Download Protocol' is the protocol which allows the Acceptor or Acquirer to configure the terminal remotely (AC certificates of accepted schemes cards, floor limit, TAC, IAC, terminal CVM limit, etc.).
- Box 'A2AP – Author' is the protocol which allows the terminal to connect to the Acceptor or to the Acquirer to request an online authorisation.
- Box 'A2AP – Data Capture' is the protocol which allows the terminal to connect to the Acceptor or Acquirer to send transactions that have been performed offline at the Point of Sale and must be cleared and settled.

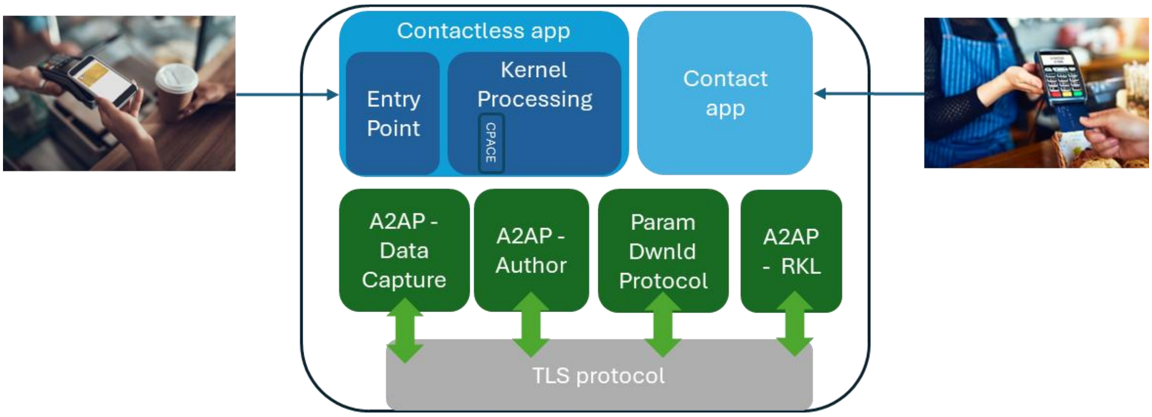


FIGURE 1: TERMINAL ARCHITECTURE OVERVIEW

When TLS is used to secure those Application protocols, TLS cipher suite with a 3072-bit RSA key for authentication, and an ephemeral key exchange based on Elliptic Curve Diffie-Hellman is commonly used. The exchanged ephemeral key is usually a 128-bit AES key. Terminals in the field may support multiple TLS cipher suites, allowing them to switch to an alternative suite if a particular suite is no longer supported by the remote server. This versatility feature, which is at the heart of the well-known TLS handshake protocol, may be viewed as way of providing crypto agility in a very straightforward way.

Building upon this inherent agility supported by TLS and progressing to a PQC-ready solution, ECPC strongly recommends the adoption of

1. hybridisation of each currently TLS cryptographic suite with a PQC algorithm
2. several hybridisation configurations (e.g. using different PQC algorithms to make a classical TLS cipher suite hybrid) to anticipate possibly impaired or broken post-quantum algorithms.

This is illustrated by Figure 2 which shows a terminal where TLS protocol can negotiate three cipher suites, each with different hybrid configurations, with the servers.

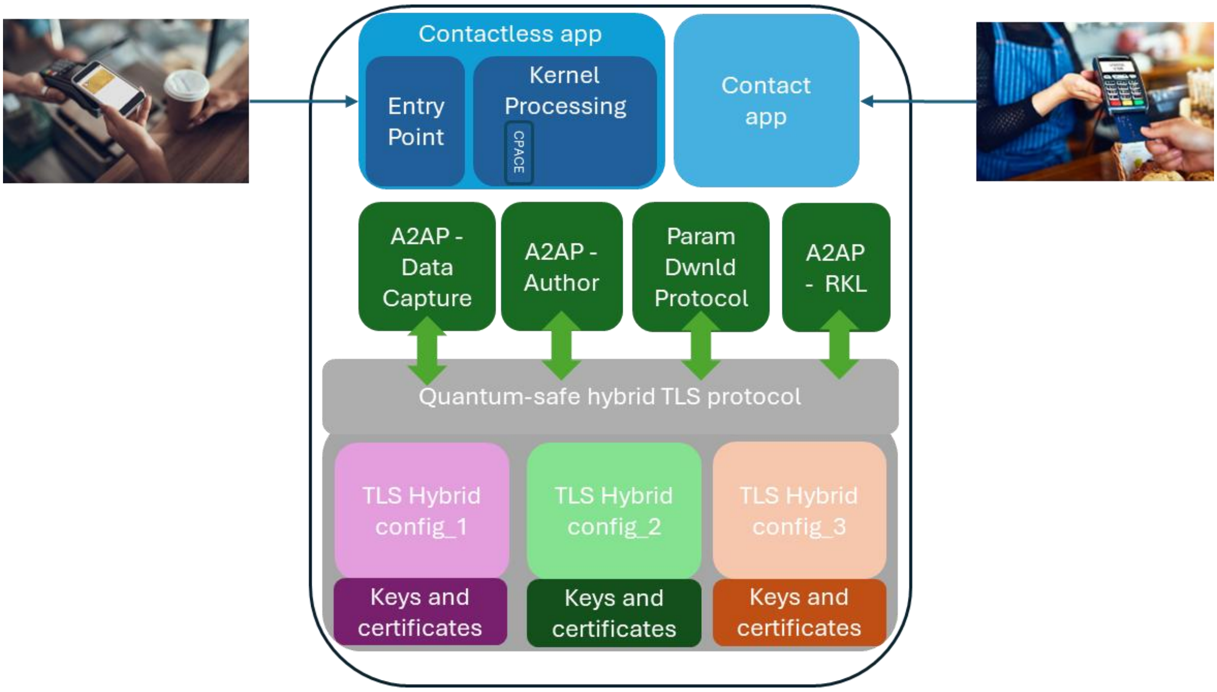


FIGURE 2: TERMINAL SECURITY ARCHITECTURE WITH CRYPTO AGILITY

As soon as a TLS hybrid configuration is no longer secure (i.e. impaired or broken), the servers can be updated to no longer accept such an impaired configuration while terminals remain at risk. Indeed, as soon as a malicious server can interact with terminals, it can negotiate for that weak TLS hybrid configuration.

Thus, the versatility feature of the negotiation phase of TLS (handshake protocol) provides crypto agility as long as the servers are honest but is no longer sufficient in case of malicious servers. One security improvement regarding this issue would be to remotely turn off impaired hybrid configurations at terminals. This could be possible if a cryptographic mechanism was available to (de)activate some TLS hybrid configurations explicitly, for instance from an administration server which would monitor a fleet of terminals. The cryptographic mechanism(s) allowing such a (de)activation of some hybrid configurations shall not rely on the same primitives which are intended to be monitored and shall rely on primitives for which we are sufficiently confident that they will pass this Y2Q.

Figure 3 illustrates such an architecture where the lowest cryptographic layer can receive signed (de)activation orders to disable impaired hybrid configurations. These orders do not require to be encrypted but only signed. The lowest cryptographic layer at terminals is only required to be able to verify signed orders received from the remote administration server.

Candidates for implementing such a cryptographic mechanism are for instance hash-based signature schemes (XMSS, LMS, SPHINCS+, etc) or Message Authentication Codes (HMAC, CMAC, etc). Such high resilient primitives can also be mixed together if required.

The benefit of using such kind of cryptographic mechanisms is the lack of strong assumptions; usually only collision resistance is required which is really standard for hash-based signatures and HMAC for instance.

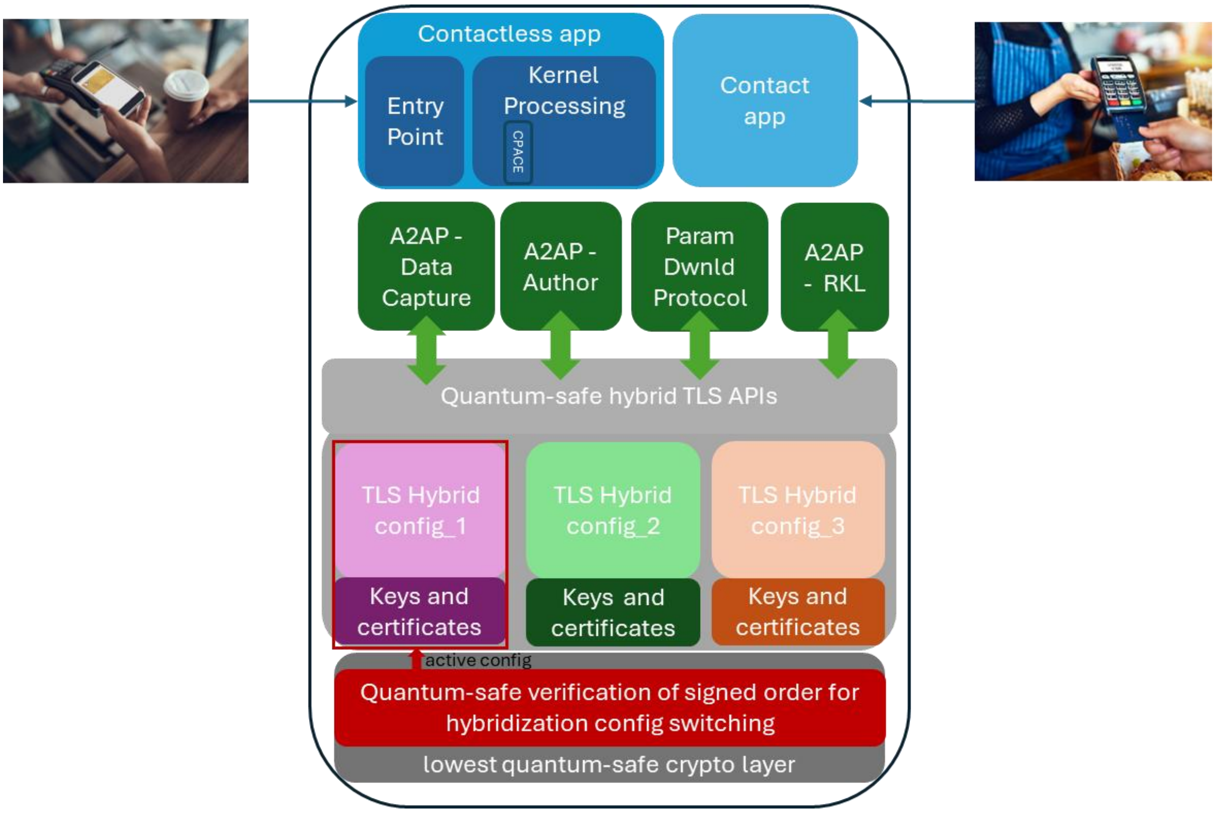


FIGURE 3: TERMINAL SECURITY ARCHITECTURE WITH HYBRID CONFIGURATION (DE)ACTIVATION FUNCTIONALITY

To conclude this section, it should be again emphasized that crypto agility principles described here for the purpose of TLS protocol can largely be applied to any other cryptographic protocol would it be at the Application or Routing layers.

Terminal vendors should implement crypto agility to enable long-term security for firmware and key updates.

6 Summary and Recommendations

The evolution of cryptographic threats, namely those posed by quantum computing—demands a coordinated action to achieve crypto agility in card and mobile payment systems. The risk landscape includes both established vulnerabilities (such as those now affecting RSA and ECC) and emerging “store-now, decrypt-later” quantum threats. The adoption of not yet mature algorithms, however, is a risk that must be considered during this unprecedented period of cryptographic changes in the payment world.

This paper presents the following key recommendations:

- **Adopt crypto agility by design**: All systems (cards, terminals, and backends) should be architected to support the transition and rapid replacement of cryptographic algorithms, avoiding hardcoded primitives and supporting negotiation or update mechanisms across all layers and platforms.

- **Enable POS terminal updates**: Given the limited possibilities to update a card, terminals should implement a quantum-resistant mechanism enabling firmware and key updates.

- **Prepare for cryptography hybridisation**: Both card and terminal systems should implement hybridisation techniques combining legacy and post-quantum algorithms. This combined approach enables mitigating risks during the transitional phase towards Y2Q.

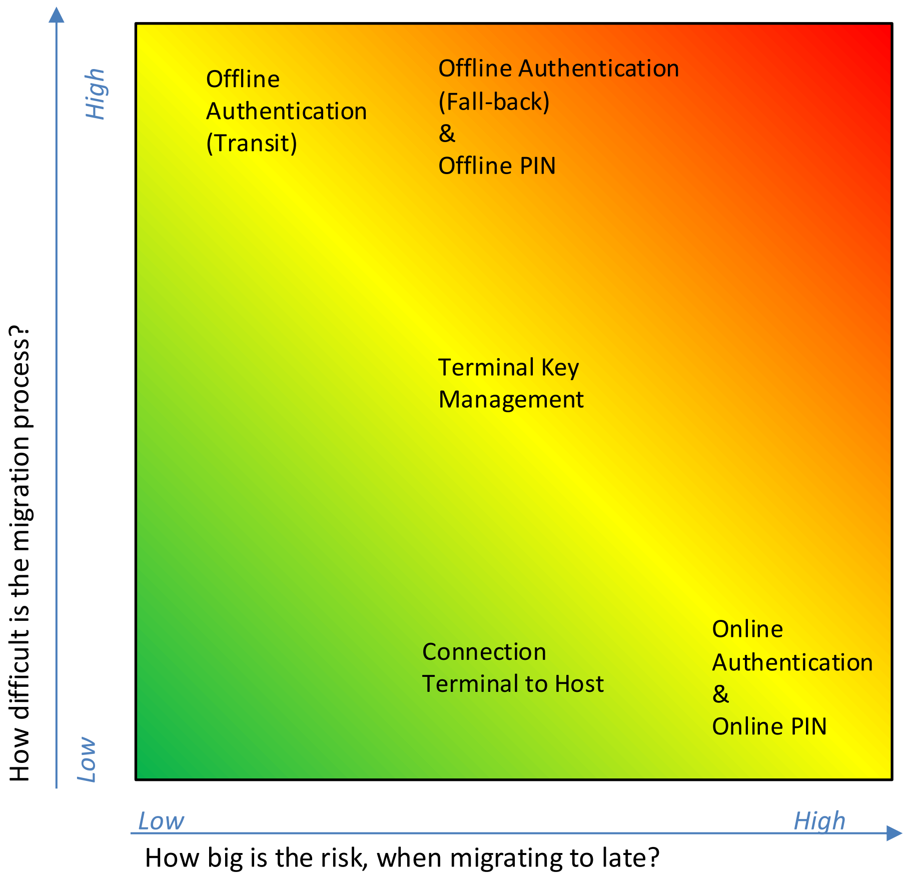
- **Accelerate symmetric cryptography upgrades**: Issuers should swiftly migrate to AES for card application cryptograms and online PIN encryption given the consensus on the quantum resistance benefits, and the relatively low complexity tied to this migration

- **Enable higher data rates for PQC**: Standards and products must accommodate increased communication bitrates, especially for contact interfaces, to support the larger key and signature sizes required by post-quantum cryptography without impacting transaction speed and, hence, user experience.

- **Focus on online authentication**: Given the current complexity of securely transitioning offline authentication, it is advisable to prioritize online authentication using quantum-resistant algorithms. This approach ensures that a reliable payment fall-back context is in place.

- **Terminal and server agility**: Payment terminals and remote servers must be equipped to negotiate, (de)activate, and update cryptographic suites dynamically, ideally with administration channels based on robust cryptography not susceptible to the same vulnerabilities as mainline mechanisms.

- **Continuous inventory and migration planning**: Organizations must maintain an up-to-date cryptographic inventory, regularly assess risk, and develop detailed migration paths for each system component, as recommended by European cybersecurity authorities.


High
Low
How difficult is the migration process?
Offline Authentication (Transit)
Offline Authentication (Fall-back) & Offline PIN
Terminal Key Management
Connection Terminal to Host
Online Authentication & Online PIN
Low
High
How big is the risk, when migrating to late?

In summary, the roadmap should include a prompt migration of online authorisation and PIN cryptography to AES, followed by enhancement of terminal and backend systems for full crypto agility and hybrid post-quantum support. The future direction and viability of offline authentication must be developed in close cooperation with all stakeholders. These proactive steps can prepare card payment ecosystems to remain resilient in the face of accelerating cryptographic change.