POST-QUANTUM AUTHENTICATION: THE BEST TIME TO SWITCH WAS YESTERDAY

Mar 24, 2025 / Petr Dvořák

POST-QUANTUM AUTHENTICATION: THE BEST TIME TO SWITCH WAS YESTERDAY

MAR 23, 2025 PETR DVOŘÁK

Quantum computers are changing the field of cryptography and, with it, the foundation of user authentication. Relying heavily on cryptography, authentication systems will need to evolve and adapt quantum-resistant algorithms. While transitioning to post-quantum authentication (PQA) is necessary, it is not easy to get right and requires specific considerations.

The algorithms that we have relied upon for our logins and transactions for decades, such as RSA or Elliptic Curve Cryptography (ECC), will no longer work under the post-quantum paradigm. While various processes constituting the overall authentication task are impacted in different ways, they are all affected.

To make matters worse, the timing of transitioning to quantum-resistant solutions is also critical. According to the generally accepted timeline[1], transitions must be completed before the moment when large quantum computers can break encryption algorithms (a moment referred to as "Q-Day"). Most organizations have not historically invested in crypto-agility and cannot upgrade cryptographic systems without investing significant time and effort. After all, replacing classical algorithms with post-quantum cryptography is not a straightforward drop-in replacement. The failure to act on time can make the transition substantially more complicated and costly down the line.

While this white paper focuses on mobile-first authentication (authentication performed via a dedicated mobile app), other methods, such as authentication via passkeys, FIDO2 tokens, or certificates, are impacted similarly, and the principles can be adjusted to cover them as well.

Recommendation Summary

- To take all the necessary steps on time, organizations should initiate projects to migrate from legacy authentication to post-quantum authentication immediately, by 2026 at the latest.
- Organizations should assess the possible migration strategies while considering the size of their customer base, impacts on user experience, execution timelines, and related costs.
- Organizations should re-evaluate their current authentication providers to see if they are the right partner for the necessary transformation.

[1] *See the Chapter 4 of NIST IR 8547 (Initial Public Draft), "Transition to Post-Quantum Cryptography Standards", available at https://csrc.nist.gov/pubs/ir/8547/ipd.*

WHY IS AUTHENTICATION IMPACTED?

To illustrate why quantum computers impact the underlying authentication fabric, let’s break down the practical cryptographic approaches that enable user authentication. They generally fall under two categories:

- Message authentication codes
- Digital signatures

Both of these approaches to authentication are legitimate and come along with positives and negatives, which we can summarize as follows:

Process	Message Authentication Codes	Digital Signatures
Key Type	Symmetric Keys *(Shared Secret)*	Asymmetric Keys *(Private and Public Key)*
Data Integrity	⊕ Yes	⊕ Yes
Data Authenticity	⊕ Yes	⊕ Yes
Non-Repudiation[2]	⊖ No	⊕ Yes
Q-Day Impact	? Mild: Extending the key size	⊖ Catastrophic: Full algorithm replacement

The impact of quantum computing on message authentication codes significantly differs from the impact on digital signatures.

Impact on Message Authentication Codes

Message authentication codes (MAC), sometimes called “keyed hashes,” are based on symmetric primitives and algorithms like hash-based message authentication codes (HMAC), used in schemes like HOTP, TOTP, or OCRA. These schemes are practically implemented in applications like Google Authenticator (or its multi-factor variants with an individual symmetric key associated with each authentication factor) or in single-button hardware authenticators that produce one-time codes.

While authentication schemes based on message authentication codes do not provide non-repudiation (in other words, service providers can forge message authentication codes), they’re still a suitable option for specific use cases.

One example is Strong Customer Authentication (SCA) under PSD3, which explicitly requires computing an “authentication code” for user logins, payment approvals, and enrollment of new SCA elements. Affirming compliance with the regulatory requirements is easier because MACs better map multiple symmetric keys (each related to a different authentication factor) to a single proof represented by an authentication code for a given transaction. It is also easier to implicitly encode time into the resulting MAC, which helps prevent replay attacks by design and allows offline usage by generating a short decimal OTP code linked to a given transaction that’s easy to rewrite manually (although this approach is becoming less popular due to the rise of phishing attacks).

[2] *Non-repudiation is a principle in cryptography that ensures a party in a communication cannot deny the authenticity of their signature or the sending of a message.*

While the impact of quantum computing on the algorithm for computing authentication codes is generally low, there are still two primary considerations:

- **Secret Key Length**
  - Does the symmetric key used for the MAC have at least 256 bits of entropy?
  - Using a shorter symmetric key would result in insufficient strength of the proof.
- **Initial Secret Key Exchange**
  - Was the symmetric key established in a way that would allow its usage in the post-quantum authentication context?
  - For example, symmetric keys established with standard Diffie-Hellman key agreement (ECDH) or symmetric keys exchanged via legacy encrypted channels (ECIES) cannot be used alone. They must be augmented with or exchanged for new cryptographic keys established in a quantum-safe manner (such as via ML-KEM).

Impact on Digital Signatures

Digital signatures belong to asymmetric cryptography, with the private key signing the message and the public key verifying the signature. The asymmetric approach provides an additional valuable property compared to MACs: Non-repudiation.

Algorithms such as RSA or ECDSA, which are used in most modern authentication solutions that leverage digital signatures, such as FIDO2 (passkeys) or X.509 PKI, are broken under the quantum paradigm due to the impact of Shor's algorithm[3]. Merely extending the key length is not an option — instead, the algorithms must be either augmented with or replaced for the new quantum-safe algorithms (such as ML-DSA).

Impact on Supporting Scenarios

The need for quantum resistance also occurs in various supporting processes closely related to authentication.

End-to-end encryption may occur to protect data in transit, such as user credentials during authentication enrollment or payment data during transaction signing. Depending on the encryption type, different measures must be taken when migrating to quantum-resistant solutions:

- Symmetric encryption, typically realized via algorithms such as AES, must use a key of sufficient length of at least 256 bits of entropy. For example, AES with 128-bit encryption keys is not recommended due to the impact of Grover's algorithm[4]. Existing encrypted data should be re-encrypted using a longer key.
- Asymmetric encryption, typically realized via algorithms such as RSA or ECIES, is broken under the quantum paradigm due to the impact of Shor's algorithm and must be migrated to quantum-resistant algorithms.

Digital signatures and MACs are used in various supporting scenarios, such as assuring the authenticity of data retrieved from the server (for example, providing an authentic challenge value or ensuring the payment data were not modified before the authenticator receives them) or holding the issued identity proofs together (for example, claims in signed JWT or Verifiable Credentials). The impact of quantum computing on these scenarios is the same as in the case of digital signatures and MACs used in primary authentication scenarios.

While hash algorithms are not directly affected by quantum computers, it is a good idea to consider upgrading them to newer variants (i.e. move from SHA256 to SHA3, which uses more modern cryptographic primitives). All implementations should also review their source of randomness and migrate to strong randomness generators.

[3] *You can learn more about Shor's algorithm here: https://en.wikipedia.org/wiki/Shor%27s_algorithm*
[4] *You can learn more about Gover's algorithm here: https://en.wikipedia.org/wiki/Grover%27s_algorithm*

WHAT DOES IT MEAN FOR AUTHENTICATION TOKENS?

Authentication tokens are the most common way of implementing MFA support, leveraging common cryptographic algorithms outlined below. The following overview table provides insights into quantum computing's impact on different MFA modes.

Token Type	Examples	Cryptography Used	Impact of Quantum Computing
Passkeys	FaceID on Mac, Windows Hello	RSA, ECDSA	**High impact.** Full replacement required.
FIDO2 tokens	YubiKey 5	RSA, ECDSA	**High impact.** Full replacement required.
X.509	Smartcards, USB tokens	RSA, ECDSA	**High impact.** Full replacement required.
Mobile Push	Microsoft Authenticator	HMAC, KMAC, RSA, ECDSA	**Medium impact** depending on the algorithm used. RSA and ECC require a full replacement. MAC-based methods require key length extension and may require re-enrollment depending on how the symmetric key was established.
HOTP/TOTP	Google Authenticator, one-button hard tokens	HMAC	**Medium impact.** The algorithm requires key length extension and may require re-enrollment depending on how the symmetric key was established.
Random OTP	SMS OTP received on a feature phone, OTP code sent to WhatsApp	RNG	**Low impact.** Security depends on the quality of the random number generator used and the delivery mode of the OTP value (security in transfer).

PLANNING FOR THE CHANGE

Understanding the Timeline

While quantum computers' impact on authentication only occurs after Q-Day (unlike in the encryption case, where "harvest now, decrypt later" is a concern), it must still be upgraded in advance to remain functional in practice. The inability to act promptly can limit an organization's ability to perform specific paths to migration. Additionally, previously stored digital signatures or other authentication proofs computed before Q-Day must be quantum-stamped (re-signed with a quantum-resistant proof) in time to ensure that the audit trail remains trustworthy even after Q-Day.

Harvest now, decrypt later blindness

The "harvest now, decrypt later" attack is an urgent problem posed by quantum computers to data encryption. In these attacks, adversaries can record encrypted conversations but may not be able to decrypt them immediately. However, decryption will become possible once the attacker acquires a quantum computer. For many pieces of exchanged secret information, this presents a significant problem.

While the impact of "harvest now, decrypt later" is severe, it shouldn't overshadow other essential topics related to quantum computing's impact on applied cryptography, such as the need for quantum-resistant digital signatures and post-quantum authentication. Organizations should understand that "harvest now, decrypt later" is not their only problem in the post-quantum world paradigm. They must also migrate their current digital signature and authentication systems to post-quantum cryptography and retroactively quantum-stamp existing signed documents or transactions with quantum-resistant proofs at least a year before Q-Day occurs.

Retroactive quantum-stamping of legacy signatures and other authentication proofs will no longer be trustworthy after Q-Day (or shortly before). It could be argued that incorrect information was augmented with a quantum-resistant stamp, sparking debates about when the adversaries actually had a quantum computer capable of an attack before publicly announcing Q-Day.

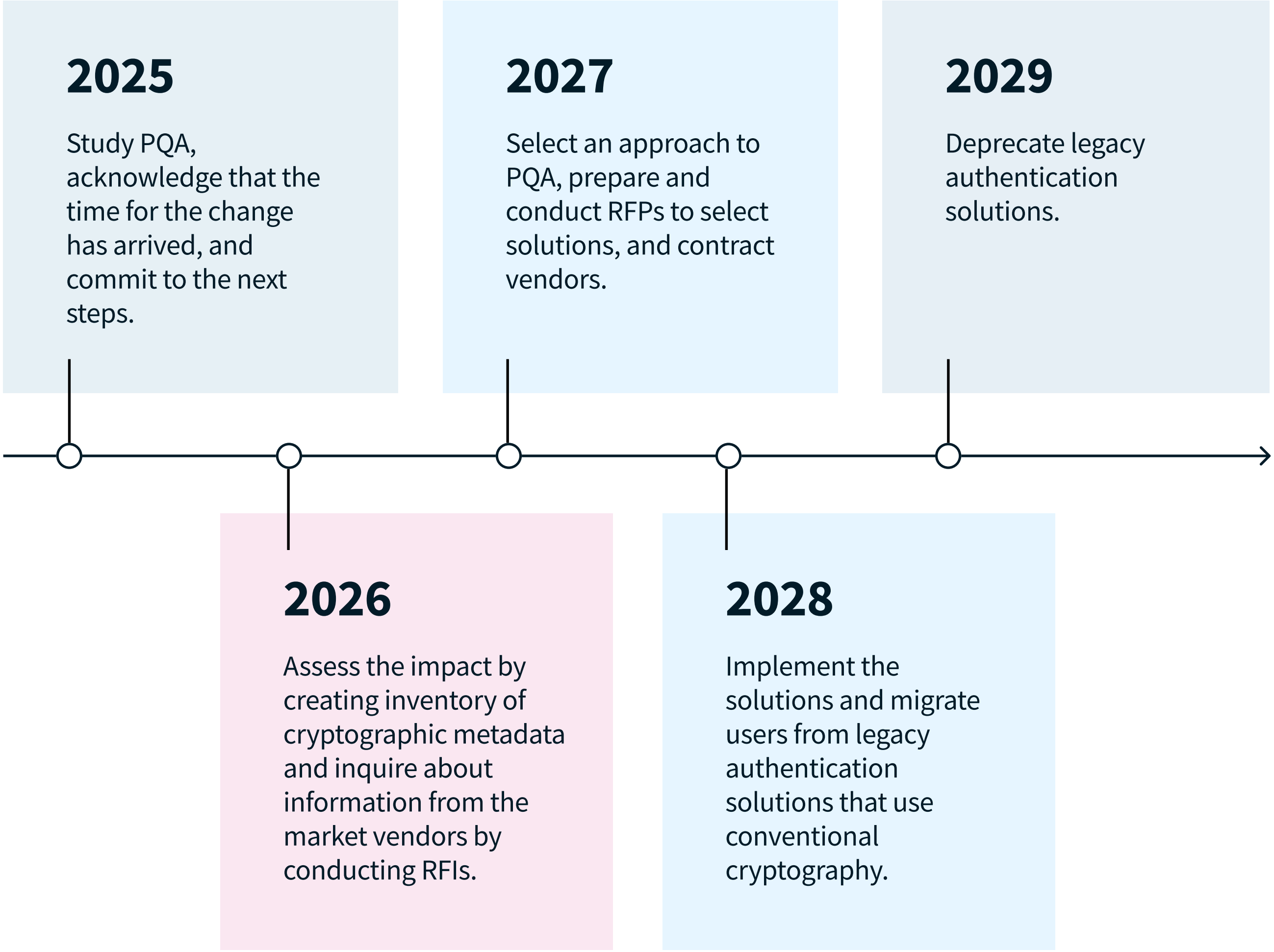
According to the timelines outlined by Gartner[5] and NIST[6], organizations should complete their transition to post-quantum cryptography by 2029 or 2030, respectively. Therefore, the change is more urgent than it may seem at first glance. Furthermore, there's the risk that a sudden, unexpected breakthrough in academic research related to quantum computing will suddenly accelerate the timeline. As many of today's tech giants are focusing their research resources on this topic, quantum computing is an industry well-placed to have its ChatGPT moment.

[5] *https://www.gartner.com/en/newsroom/press-releases/2024-10-21-gartner-identifies-the-top-10-strategic-technology-trends-for-2025*
[6] *https://csrc.nist.gov/pubs/ir/8547/ipd*

Facing Big Responsibility in the Snail-Like Pace of Changes

Let's look back at the organization's perspective. Banks and other large organizations hold valuable assets and resources for retail customers or companies and have high stakes in protecting them. Thus, the possibility of a quantum breach poses a significant high-cost risk. At the same time, these organizations typically need years to execute significant changes. It can often be a challenge for them to assess the impact of the changes, let alone manage the new vendor selection process, project and migration planning, and actual implementation. Performing these steps correctly is crucial, requires proper care, and shouldn't be rushed.

With this in mind, we advise banks and large organizations to start preparing for the transition immediately, moving the latest possible timeline for project kick-offs to 2026.



2025

Study PQA, acknowledge that the time for the change has arrived, and commit to the next steps.

2026

Assess the impact by creating inventory of cryptographic metadata and inquire about information from the market vendors by conducting RFIs.

2027

Select an approach to PQA, prepare and conduct RFPs to select solutions, and contract vendors.

2028

Implement the solutions and migrate users from legacy authentication solutions that use conventional cryptography.

2029

Deprecate legacy authentication solutions.

SWITCHING FROM LEGACY TO POST-QUANTUM AUTHENTICATION

End-user migration from legacy to post-quantum authentication is another task requiring special consideration. The key material associated with end users' authentication factors cannot be transparently migrated from legacy algorithms to new ones without the users' active involvement, which prompts the need for active (visible) user migration.

There are three possible approaches to enrolling users in PQA:

- Existing legacy authentication
- Full identity proofing
- A trusted, quantum-resistant third-party provider

Each of these approaches has both substantial benefits and drawbacks, which need to be evaluated in the organization's specific context.

Enrollment via Existing Legacy Authentication

Since many end users will already use a legacy authentication solution to be migrated, the migration can use legacy proof as a means of identity assertion during enrollment to post-quantum authentication. The migration process must be performed before Q-Day, as after it occurs, the proof provided by the legacy authentication cannot be considered trustworthy.

The main benefit of this approach is the user-friendliness. To enroll, users only need to authenticate themselves via legacy authentication (for example, by entering a PIN code). The process is also very cost-effective, as authentication is typically a low-cost transaction.

On the other hand, the process of activating a new authentication element using an old one may not be implemented at a given organization. In this case, it would need to be implemented in a one-time investment made solely to support the migration scenario from legacy to post-quantum authentication. The effort involved may not be worth it for organizations with few users to migrate. However, for organizations with larger user bases (tens of thousands of users), the one-time investment in a specific process could be balanced out by total savings on per-user, migration-related transactions.

PSD3 Note

From the banking regulation perspective (requirements on Strong Customer Authentication under PSD3), enrollment is performed via the existing SCA element based on cryptography that is still valid before Q-Day.

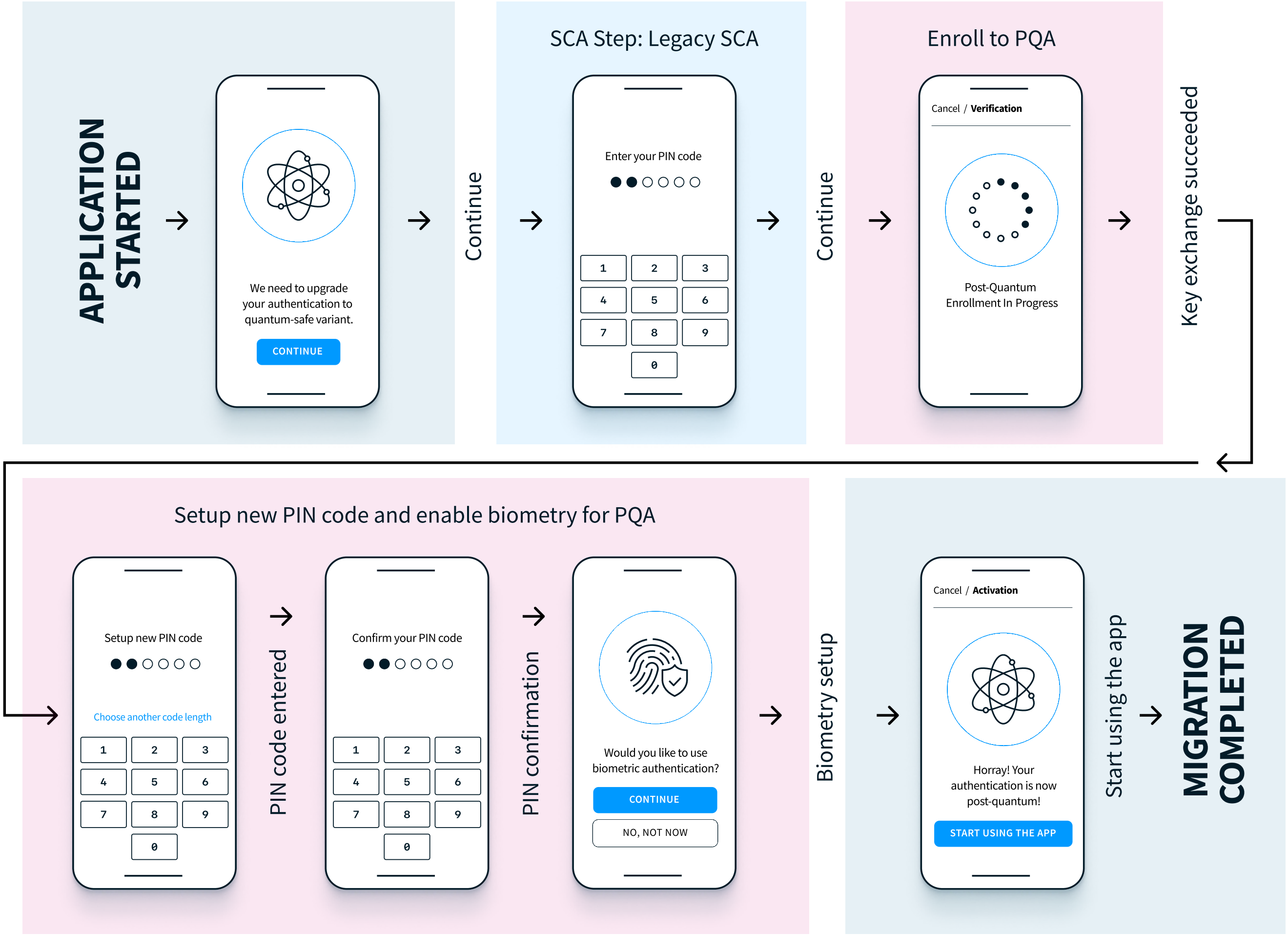
+ The process is user-friendly. Users only need to perform one additional authentication.

+ Using existing authentication is a cost-effective solution for large user base migrations.

? The process of activating a new authentication element using an old one may not be implemented — in this case, organizations would need to implement it only for migration.

− The process must be performed before Q-Day. Otherwise, it will be untrusted.

Example Process Flow



APPLICATION STARTED

We need to upgrade your authentication to quantum-safe variant.

CONTINUE

Continue

SCA Step: Legacy SCA

Enter your PIN code

●●○○○○

1 2 3 4 5 6 7 8 9 0

Continue

Enroll to PQA

Cancel / Verification

Post-Quantum Enrollment In Progress

Key exchange succeeded

Setup new PIN code and enable biometry for PQA

Setup new PIN code

●●○○○○

Choose another code length

1 2 3 4 5 6 7 8 9 0

PIN code entered

Confirm your PIN code

●●○○○○

1 2 3 4 5 6 7 8 9 0

PIN confirmation

Would you like to use biometric authentication?

CONTINUE

NO, NOT NOW

Biometry setup

Cancel / Activation

Horray! Your authentication is now post-quantum!

START USING THE APP

Start using the app

MIGRATION COMPLETED

Enrollment via Full Identity Proofing

Another approach to enrolling existing users in post-quantum authentication is to drop their existing cryptographic credentials enrolled in the legacy systems and re-enroll them in post-quantum authentication using one of two methods:

- **In-person physical proofing:**

  A personal visit to the organization's point of sale, where a user's identity can be verified in person by presenting identity documents.

- **Online identity proofing:**

  Using a digital process — for example, via SMS proofing (assuming that telco infrastructure provides post-quantum security), document ID capture (optical capture, as reading the NFC chip on a long-lived document may not provide quantum resistance), and advanced biometric proofing, such as facial recognition with a liveness check.

The main benefit of enrollment via full identity proofing is that it can also be used by customers who have yet to enroll in authentication for the first time (customers who do not migrate from the legacy methods). Hence, it does not result in any additional one-time implementation costs. Another benefit is that this enrollment can be performed even after Q-Day, which relieves organizations of time sensitivity.

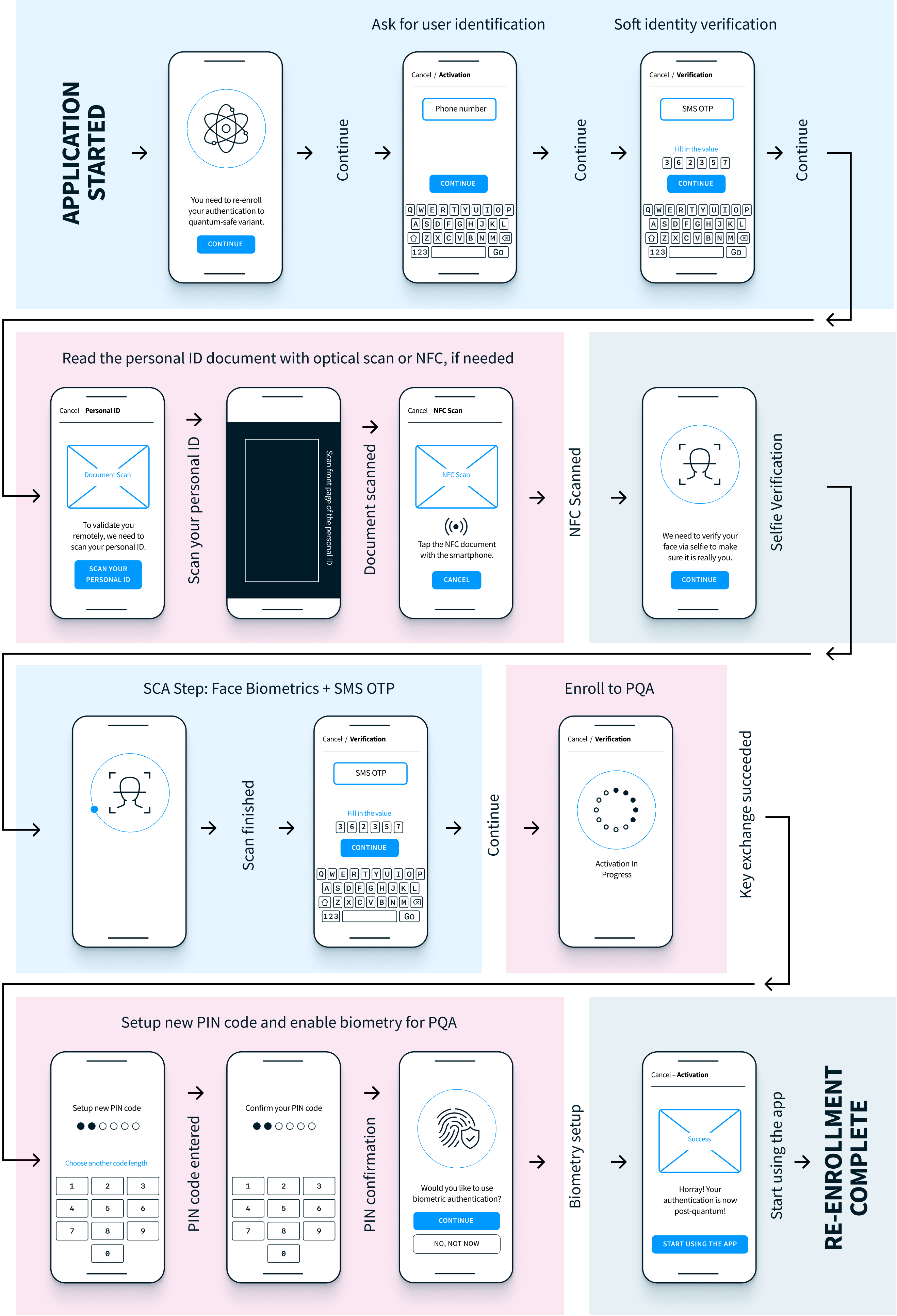
On the other hand, identity proofing that provides sufficient identity assurance is costly and unsuitable for bulk-migrating an organization's entire customer base that exceeds a certain size. The process is also inconvenient for users already enrolled in the legacy authentication, as they might not be in the proper context to perform identity proofing — and even if they are, the process is usually quite lengthy and cumbersome.

PSD3 Note

From the banking regulation perspective (requirements on Strong Customer Authentication under PSD3), enrollment is performed via a combination of the possession factor, as evidenced by SMS OTP, and the inherence factor, as evidenced by facial biometrics.

+ The process is usable beyond just migration from legacy to post-quantum authentication.	− Full identity proofing is costly and not suitable for high-volume user migration.
+ The process does not have to be performed before Q-Day.	− The process is not user-friendly. It takes time and may surprise users when it is least convenient.

Example Process Flow



APPLICATION STARTED

You need to re-enroll your authentication to quantum-safe variant.

Continue

Ask for user identification

Cancel / Activation

Phone number

Continue

Soft identity verification

Cancel / Verification

SMS OTP

Fill in the value

3 6 2 3 5 7

Continue

Read the personal ID document with optical scan or NFC, if needed

Cancel – Personal ID

To validate you remotely, we need to scan your personal ID.

Scan your personal ID

Scan front page of the personal ID

Document scanned

Cancel – NFC Scan

Tap the NFC document with the smartphone.

NFC Scanned

We need to verify your face via selfie to make sure it is really you.

Selfie Verification

SCA Step: Face Biometrics + SMS OTP

Scan finished

Cancel / Verification

SMS OTP

Fill in the value

3 6 2 3 5 7

Continue

Enroll to PQA

Cancel / Verification

Activation In Progress

Key exchange succeeded

Setup new PIN code and enable biometry for PQA

Setup new PIN code

Choose another code length

PIN code entered

Confirm your PIN code

PIN confirmation

Would you like to use biometric authentication?

Biometry setup

Cancel – Activation

Horray! Your authentication is now post-quantum!

Start using the app

RE-ENROLLMENT COMPLETE

Enrollment via Trusted, Quantum-Resistant Third-Party Provider

This alternative approach to enrolling customers in PQA is similar to enrollment via full identity proofing but with one significant difference: Instead of organizations directly performing identity proofing using their own identity proofing systems, identity is asserted by delegating proofing to a third-party solution using a federated authentication approach.

The benefit of this approach is that it can be an option for customers who have yet to enroll in authentication (customers who do not migrate from the legacy methods). Hence, it does not need to be implemented exclusively for the post-quantum cryptography migration process. Enrollment can also be performed after Q-Day, which relieves organizations of time sensitivity.

The primary disadvantage of this approach is that no third parties currently operate an identity service based on post-quantum cryptography, so for now, this option remains purely hypothetical. On the other hand, QTSPs can — and likely will — eventually adjust their offerings, and government initiatives, such as the EU Digital Identity Wallet (EUDI-W), may introduce quantum resistance as a requirement.

Considering the above, the cost of the approach is currently difficult to predict. It can be costly when provided by commercial subjects (like QTSPs), who generally only compete with identity proofing solutions providers. However, in the case of funding via government initiatives, such as EUDI-W, this approach's cost could be completely free of charge.

Finally, it is worth noting that this process assumes that the end user has the relevant third-party authentication enrolled. For example, the end user would need to install and activate a third-party mobile app. This assumption could limit the approach's applicability if such third-party solutions do not gain significant adoption, as users would be given the enrollment option via an app they do not have. For users already enrolled, however, the process would be very fast and convenient, as only authentication in the third-party solution is required.

PSD3 Note

From the banking regulation perspective (requirements on Strong Customer Authentication under PSD3), enrollment is performed via outsourcing SCA to a compliant provider. This can be done after assessing the provider's methods for verifying and authenticating users as well as confirming the process's compliance with the regulation.

+ The process is usable beyond just migration from legacy to post-quantum authentication.

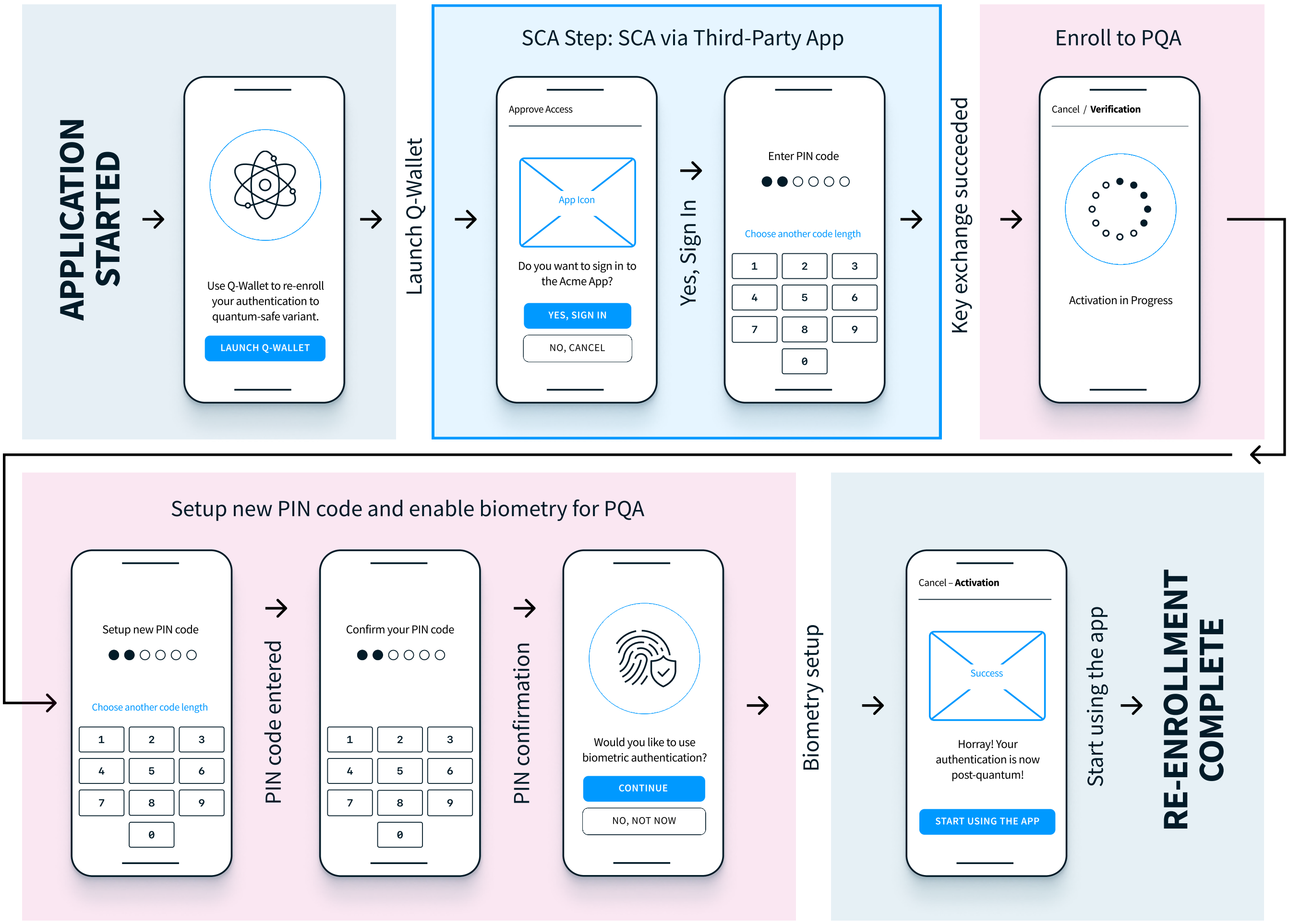
+ The process does not have to be performed before Q-Day.

? Using a third-party service may be costly or free of charge, depending on the provider.

− Users need to have third-party authentication enrolled, which may limit applicability.

− There is currently no suitable third-party provider (although QTSPs and government initiatives, such as EUDI-W, will likely adapt).

Example Process Flow



DILEMMA: EXISTING VENDOR OR A NEW ONE?

During their journey towards post-quantum authentication rollout, organizations will have to decide whether to retain their existing authentication vendors and wait for them to upgrade their current solution to be quantum-resistant or switch to new vendors already providing PQA as a quantum-resistant alternative.

Since the change will result in an active user base migration (as mentioned in the previous chapter, the change cannot be made invisibly to the user), both vendor strategies require significant planning effort from the organization. The positive angle of this fact is that migration to PQA also represents an opportunity to re-evaluate current authentication vendors.

To help with making a calculated decision, we advise organizations to consider the following points:

Capability of the Current Authentication Vendor

- Does the current vendor have sufficient knowledge and capabilities to properly modernize their authentication solution to be quantum-safe?
- Is the current solution well-packaged and regularly updated?

Flexibility of the Current Authentication Vendor

- Does the current vendor operate quickly enough to provide a quantum-safe solution so that full deployment and user migration can happen before Q-Day?
- Could switching to a vendor that offers PQA out of the box be faster and more convenient?

- **Complexity of Existing Integrations**
  - Is the current authentication solution integrated with multiple systems via complex custom integrations that would make switching the vendor exceedingly complicated and costly?

- **Current and Future Feature Requirements**
  - Does the solution provide a reliable and user-friendly authentication experience?
  - Does the current solution meet all the organization’s current requirements?
  - Does the current solution accommodate features needed for future development or does it limit the organization's ability to innovate its applications?

- **License and Support Costs**
  - By switching vendors, could the organization significantly save operating costs due to more cost-effective licensing and support?
  - Is the current vendor’s quality of support sufficient?
  - Can the current vendor guide the organization in a consultative manner through the necessary changes?

HOW WE SOLVE POST-QUANTUM CHALLENGES

We are pioneers of post-quantum authentication. To address the challenges arising from quantum computers' impact on authentication and accelerate our customers' migration before Q-Day, we committed to making our authentication solutions quantum-safe in 2025. Our mobile-first authentication solution, PowerAuth®, has now been adjusted to support post-quantum cryptographic algorithms. Other PQA solutions on our roadmap, such as post-quantum passkeys and quantum-safe FIDO2 hardware tokens, have prototype versions planned in late 2025.

What is PowerAuth®?

PowerAuth® is an advanced customer authentication and transaction signing solution with dynamic linking support built on an open authentication protocol designed to address customers' challenges, primarily in banking and financial services. It supports:

- Secure mobile device enrollment and linking with the customer account
- Multi-factor authentication codes based on symmetric keys
- Digital signatures based on asymmetric keys

The broad feature support makes our solution versatile and the best-in-class choice for various banking and financial services applications. Following the best practices in using cryptography and embracing crypto-agility has allowed us to remain consistently compliant with regulatory requirements, such as PSD2 or eIDAS, as well as roll out agile improvements in the cryptographic backbone of our solution, which has resulted in valuable features for our customers.

In the latest version of PowerAuth®, which we are currently piloting with several customers, we’ve added support for post-quantum cryptography (PQC) and are assessing proper functionality and performance impact.

What Makes PowerAuth® Quantum-Resistant?

We have upgraded our solution by designing a hybrid scheme for our mobile-first authentication that improves all impacted processes by combining conventional ECC with post-quantum cryptographic algorithms that were endorsed by NIST in August 2024.

The upgrade of the scheme consists of two main areas of improvement:

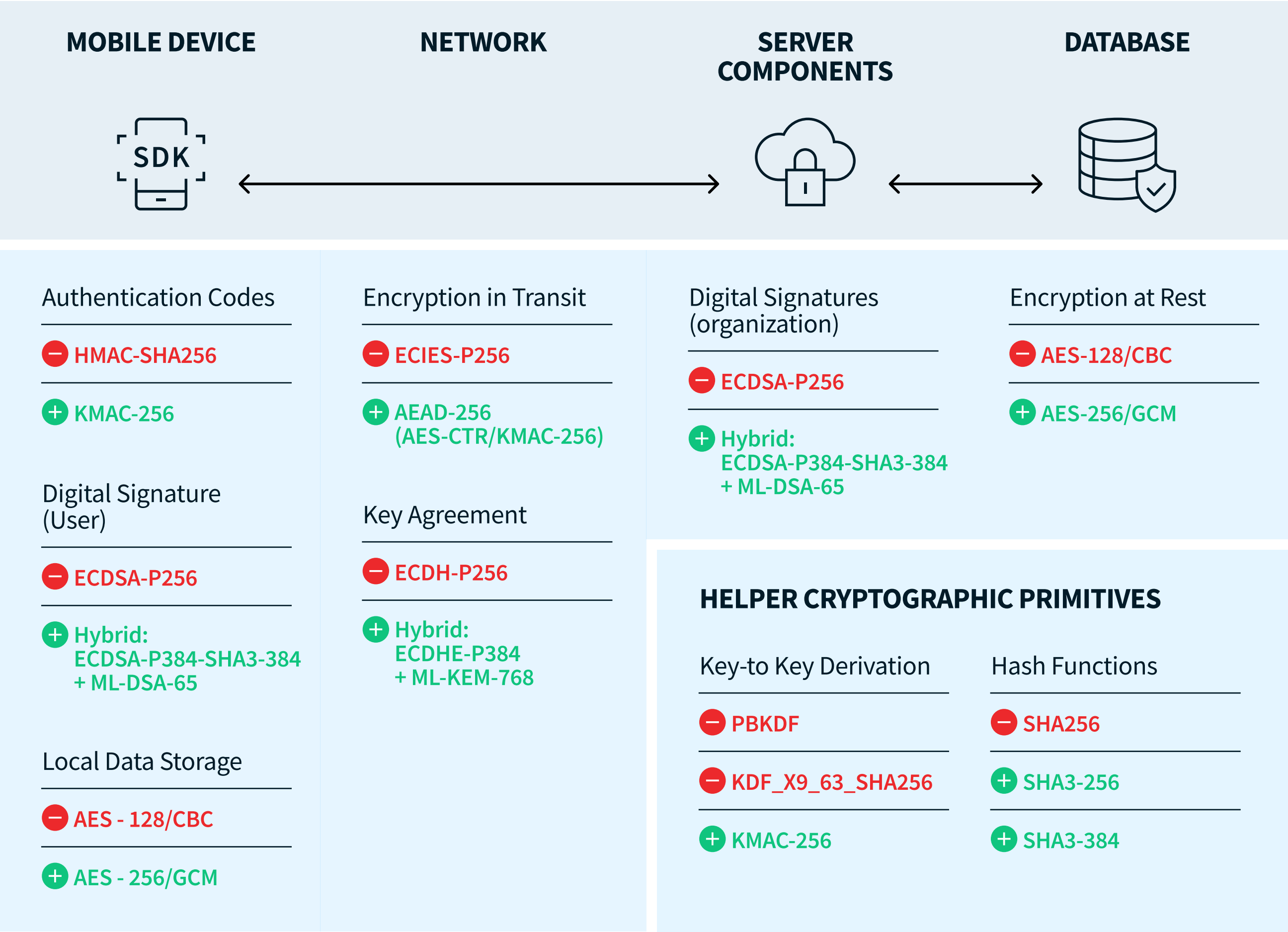
- Conventional cryptography has been updated to use stronger variants and longer keys
- Quantum-resistant algorithms ML-KEM and ML-DSA have been added

More specifically, our upgraded solution delivers the following changes in cryptographic primitives:

Process	Conventional (Legacy)	Post-Quantum (Updated)
Message Authentication Codes	HMAC-SHA256	KMAC-256
Digital Signatures	ECDSA-P256	Hybrid: ECDSA-P384-SHA3-384 + ML-DSA-65
Hash Functions	SHA256	SHA3-256 or SHA3-384
Symmetric Encryption	AES/CBC, 128-bit keys	AEAD (AES-CTR/KMAC-256), with 256-bit keys, or AES/GCM, 256-bit keys
Asymmetric Encryption	ECIES-P256	N/A: replaced by symmetric encryption that uses keys established by hybrid KEM with one-shot keys for certain use cases
Key Agreement	ECDH-P256	Hybrid: ECDHE-P384 + ML-KEM-768

Architecture Impact Overview

The following scheme shows the migration impact in various solution systems:



MOBILE DEVICE

Authentication Codes

- − HMAC-SHA256
- + KMAC-256

Digital Signature (User)

- − ECDSA-P256
- + Hybrid: ECDSA-P384-SHA3-384 + ML-DSA-65

Local Data Storage

- − AES - 128/CBC
- + AES - 256/GCM

NETWORK

Encryption in Transit

- − ECIES-P256
- + AEAD-256 (AES-CTR/KMAC-256)

Key Agreement

- − ECDH-P256
- + Hybrid: ECDHE-P384 + ML-KEM-768

SERVER COMPONENTS

Digital Signatures (organization)

- − ECDSA-P256
- + Hybrid: ECDSA-P384-SHA3-384 + ML-DSA-65

DATABASE

Encryption at Rest

- − AES-128/CBC
- + AES-256/GCM

HELPER CRYPTOGRAPHIC PRIMITIVES

Key-to Key Derivation

- − PBKDF
- − KDF_X9_63_SHA256
- + KMAC-256

Hash Functions

- − SHA256
- + SHA3-256
- + SHA3-384

How to Migrate to Our Solution

Our solutions' hallmark is their ease of deployment. We design all products so that our components' installation, configuration, and integration are straightforward and carried out via comprehensive SDKs and APIs. Deploying PowerAuth® in the context of post-quantum authentication is no exception.

For our existing customers who have already selected PowerAuth® and use the conventional cryptography variant, we support migration as a seamless process natively integrated into the product. To migrate customers from classical to post-quantum cryptography, our SDK contains methods to re-enroll the device based on the user's authentication via PIN code.

New customers can leverage our existing and proven migration scenarios to switch from their current legacy authentication solutions to our modern post-quantum PowerAuth® variant. Generally, migration can be performed in short time frames — weeks rather than months. We will also assist new customers in quantum-stamping legacy authentication proofs and digital signatures stored in systems with post-quantum signatures.

Enrolling new users in PowerAuth® is as easy as fetching the activation code for a previously verified user (with verification performed using any of the methods outlined in the "Switching from Legacy to Post-Quantum Authentication" chapter), setting up new PIN codes for post-quantum authentication, and enabling local biometric authentication on the mobile device.

Our consultants are available to you throughout your PQA migration journey to ensure smooth integration of our solution, recommend best practices in authentication and identity proofing, help design user journeys, troubleshoot any potential issues, and review the resulting solution to ensure that everything works properly.

Contact us at **sales@wultra.com** for more information.

Reviewers

- **Roman Štrobl**
  Senior Engineer at Wultra
- **Juraj Ďurech**
  Cryptography Engineer at Wultra
- **Tomáš Rosa**
  Principal Cryptologist with Raiffeisenbank and Raiffeisen Bank International Competence Centre for Cryptology and Biometrics

About Wultra

WE HELP BANKS AND FINTECHS SECURE THEIR DIGITAL CHANNELS WITH SEAMLESS, POST-QUANTUM AUTHENTICATION BUILT FOR TODAY’S USERS AND COMPLIANCE NEEDS, AND READY FOR TOMORROW’S THREATS.

Ready when you are

www.wultra.com

sales@wultra.com

wultra

AUTHENTICATION FOR TODAY AND THE QUANTUM ERA

www.wultra.com