wultra

Paving the Way to More Secure, Usable, Diverse, and Accessible Authentication in Banking

AUGUST 2026

Paving the Way to More Secure, Usable, Diverse, and Accessible Authentication in Banking

Banking and financial services are among the most prominent adopters of modern digital identity solutions, especially in developed markets. By introducing modern passwordless authentication for access to banking services and payments, banks successfully balanced an excellent user experience with superior security. However, they also cultivated a strong mobile-first monoculture - a problematic trend in the long run.

Today, authentication in electronic daily banking mostly relies on smartphone apps, whether a dedicated mobile authenticator app or a mobile banking app. Such an approach is accepted, or even preferred, by the majority of end customers. Still, this reliance also creates several issues that affect specific customer segments and users with special needs.

In this article, you will learn how banks cultivated the mobile-first monoculture in authentication, why it is a problem, how regulation is shifting to break it up and introduce more secure, usable, diverse, and accessible authentication methods, and how banks should think about authentication in their digital banking in 2026 onwards.

Executive Briefing

Authentication in banking is gradually evolving from a single mechanism into a diversified and adaptive layer tailored to different customer situations, devices, risk profiles, and accessibility needs. PSD2 successfully accelerated the adoption of strong authentication and mobile-first banking, but PSD3/PSR now pushes the market toward a more inclusive and flexible model that no longer assumes one authentication method is suitable for everyone.

For banks, this transition is not only a compliance exercise. It is an opportunity to rethink how authentication supports customer experience, accessibility, fraud reduction, and digital trust across different customer segments.

As a result, banks can achieve better user satisfaction and higher customer retention.

Mobile apps will remain the dominant authentication method for most users, but they will increasingly coexist with passkeys, hardware authenticators, federated identity systems, biometrics, and accessible alternatives designed for specific use cases. Over time, the institutions that succeed will likely not be those offering the single “best” authentication method, but those capable of orchestrating multiple authentication approaches within a single, consistent, and secure identity platform.

The Catalyst for Strong Authentication

The most significant catalyst for stronger authentication in banking (and ultimately the inception point for the mobile-first monoculture in authentication) was undoubtedly the **PSD2 regulation**, which has been in effect since late 2018. Strong customer authentication was not the primary goal of the regulation, but it crystallized alongside the primary goal: access via open banking APIs.

The PSD2 regulation aimed to open banking services in Europe by requiring payment service providers (PSPs) to publish standardized APIs for core banking services, such as account information (AIS) and payment initiation (PIS). These APIs were intended to provide third-party fintechs with a secure alternative to screen scraping and foster greater competition and innovation in financial services.

However, access to bank accounts through third-party applications required a common security framework. Established banks were concerned about security risks, while fintech providers sought to avoid excessive friction that could create inconsistent user experiences and place them at a competitive disadvantage.

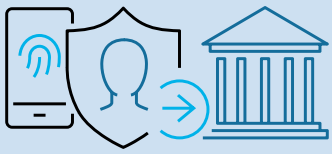
These conflicting views were why a unified set of requirements for access - strong customer authentication (SCA) - was established, governed by the regulatory technical standards (RTS) initially designed by the European Banking Authority (EBA), that set the minimal baseline for how people must authenticate to obtain access or make payments. These standards applied to all market participants, meaning that banks had to treat access to their own digital channels the same as access to third-party channels.

The requirements of SCA could be summarized as follows:

1

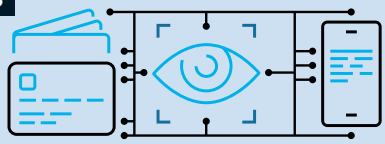
Multi-factor authentication (MFA) with at least two independent factors

2



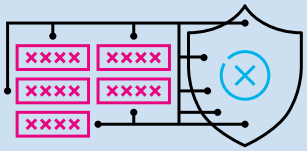
Secure enrollment remotely based on SCA, or at the bank's premises (including ATMs)

3



Dynamic linking for payments ("what you see is what you sign" principle)

4

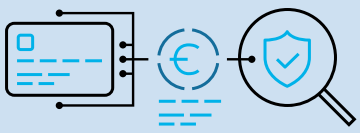


Permanent or temporary blocking after a maximum of 5 failed authentication attempts

5

Secure execution environment on multi-purpose devices (smartphones and tablets)

6



Transaction monitoring with risk evaluation

Strong customer authentication was mandatory for access to accounts, payments, new SCA element enrollment, and any operation that could be potentially risky and lead to account compromise, each with exceptions explicitly listed in the RTS

The introduction of SCA changed how people were supposed to log in to electronic channels, whether provided by the bank or a third party. It was no longer possible to log in with just a username and password, or to submit payments without explicit authorization. Commonly used SMS OTPs entered a gray zone and became discouraged by advisors and regulators.

At the time, these new requirements posed a significant design challenge.

Mobile Apps: The Evolutionary Winner

Banks evaluated multiple options for complying with SCA requirements. During these evaluations, mobile apps typically emerged as the most flexible, user-friendly, and cost-effective approach.

They provided:

Rich user interface that guided users through the enrollment process (self-service), presented authentication challenges and payment approvals comprehensively, showed adequate warnings when necessary, and allowed easy data input from the user where needed

Flexible programming model that allowed designing and iterating solutions that meet the SCA requirements, including:

- **biometric sensors** (Touch ID, Face ID)
- **secure data storage** (iOS Keychain, Android KeyStore, backed by hardware security capabilities where available)
- **data connectivity** (operations in online mode)
- **camera** (QR or other optical code capture)
- **location services** (GPS)

Easy rollout and update distribution to end users via application marketplaces (App Store, Google Play).

Modern cryptography support, enabling a proper underlying design and formal process validation.

These were the most significant winning factors that prompted the banks to introduce mobile-based SCA.

The approach caught on quickly. After all, mobile banking was already overtaking the traditional internet banking channel in terms of usage frequency and penetration among end users. The transition to mobile apps seemed very natural and inevitable.

Cracks in Mobile-First Monoculture

However, after introducing the mobile-based SCA, the SCA's conceptual design often stopped. The banks decided to prioritize mobile-based SCA or even make it the only option, pushing their customers toward it despite their dissatisfaction with the process, distrust of the mobile apps and their security, or reduced ability to use mobile apps for authentication.

The issues come from several directions.

1

Exposure to Specific Cybersecurity Risks

One of the issues is increased exposure to cybersecurity risks associated with multi-purpose devices, including phishing, authorized push payment (APP) fraud, remote desktop attacks, and mobile malware. While banks can mitigate these risks through measures such as in-app protection and anti-fraud systems, many consumers remain reluctant to trust smartphones with their finances, often due to media coverage of fraud incidents and resulting financial losses.

In addition, mobile-first authentication provides a fixed security baseline with limited opportunity for users to choose stronger authentication methods. As a result, more risk-averse individuals may be unable to apply additional protections, even when willing to accept greater friction in exchange for improved security.

2

Inclusivity and User Experience

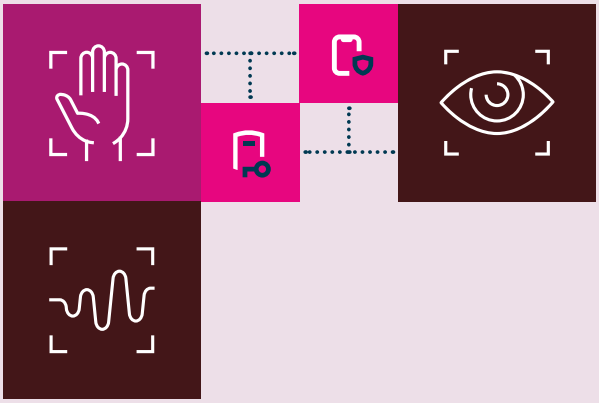
Having a smartphone app as the only authentication option also raises concerns about inclusivity. Such an approach restricts access to banking services for the underprivileged who cannot afford a smartphone, the elderly, or less digitally savvy users.

But even a digitally literate user might be negatively affected in certain situations, for example, should they be non-primary bank customers (i.e., only those with a mortgage). In these situations, banks would still force people to install and use mobile applications they rarely use, resulting in added risk, suboptimal user experiences, and more complicated lives.

3

Accessibility

Accessibility is another area where relying on a single authentication approach may fall short. While mobile apps can offer the highest level of comfort to people with visual impairment who are accustomed to using voice control and touchscreens, not all apps have been adequately tested and optimized for accessibility, resulting in a poor experience. For other groups of disabled people, such as those with reduced hand or arm mobility, smartphone apps may not be suitable at all because they cannot use touch controls or lift the smartphone to scan a QR code.



A Return to Human-Centric Authentication

While the problems above affect only a minority of users or specific customer segments, the issue was significant enough to merit regulatory action. The PSD3/PSR shifts from a technological view set by PSD2, where APIs and integrations were the primary motivators, back to a human-centric view: how to make lives easier for the bank customers.

PSD3/PSR mandates that banks ensure all customers, including persons with disabilities, older persons, persons with low digital skills, and those without access to digital channels or a smartphone, have at least one means to perform strong customer authentication.

Article 88

Accessibility requirements regarding strong customer authentication

1. Without prejudice to the accessibility requirements under Directive (EU) 2019/882, payment service providers shall ensure that all their customers, including persons with disabilities, older persons, with low digital skills and those who do not have access to digital channels or payment instruments, have at their disposal at least a means, adapted to their specific situation, which enables them to perform strong customer authentication.
2. Payment services providers shall not make the performance of strong customer authentication dependent on the exclusive use of a single means of authentication and shall not make the performance of strong customer authentication depend, explicitly or implicitly, on the possession of a smartphone. Payment services providers shall develop a diversity of means for the application of strong customer authentication to cater to the specific situation of all their customers.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Regulation (EU) No 1093/2010

An Expert View

"PSD3/PSR revisits a human-centric view of banking and requires banks to think about their customer segments and evaluate the needs of specific customers while designing and introducing methods for strong customer authentication."

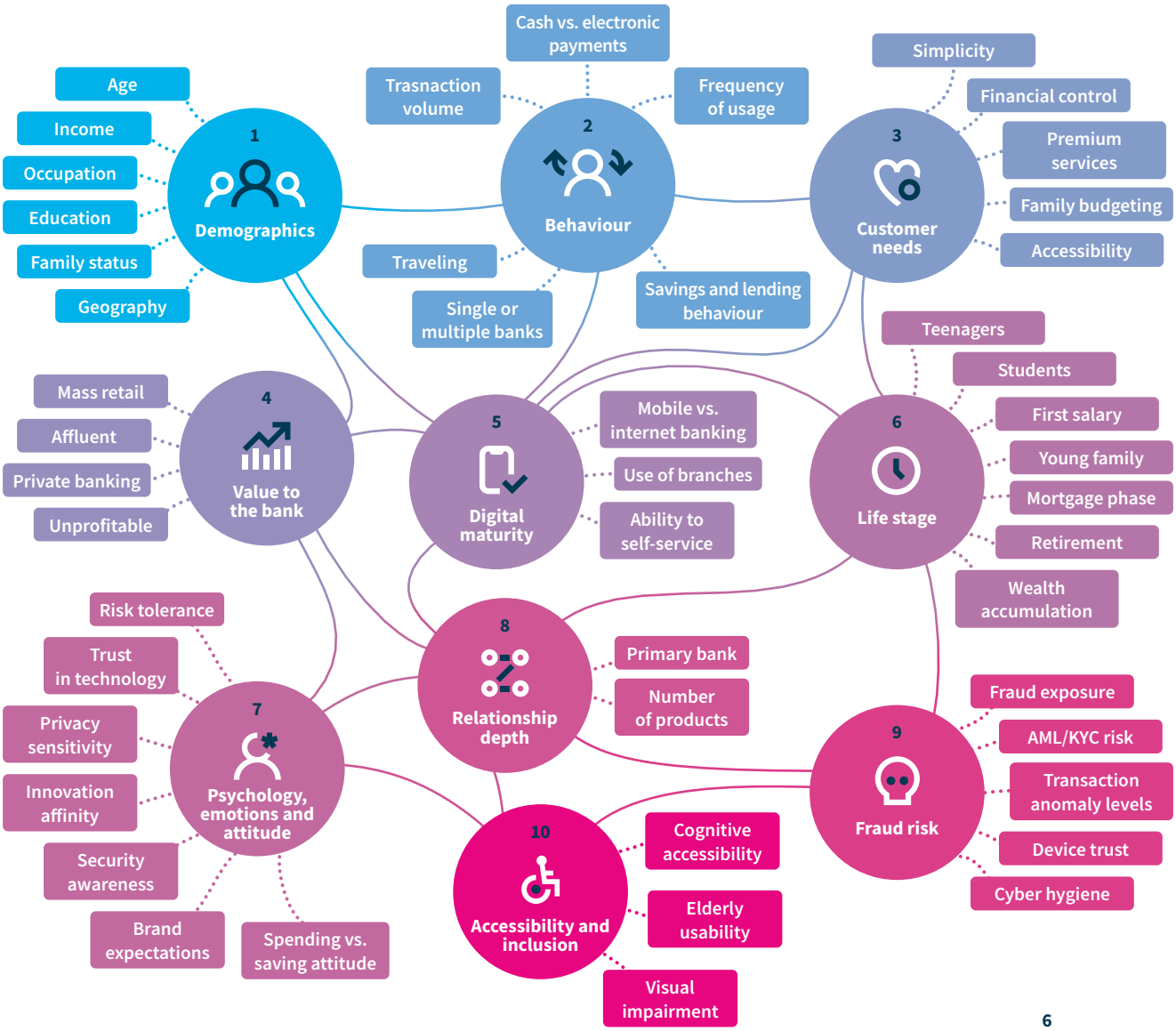
Petr Dvorak, CEO and Founder at Wultra

The Many Dimensions of Banking Customer Segmentation

Customer segmentation is not new to banks. Serving a broad customer base across current and savings accounts, loans, mortgages, investments, and specialized services has always required tailoring products and communication to different customer needs and situations.

After all, the banking experience differs significantly between a primary banking customer, an occasional user of a secondary product such as a mortgage, and a customer managing finances for a business.

Banks actually need to use many dimensions to segment their customers properly. For example, they can segment customers based on the following dimensions:



6

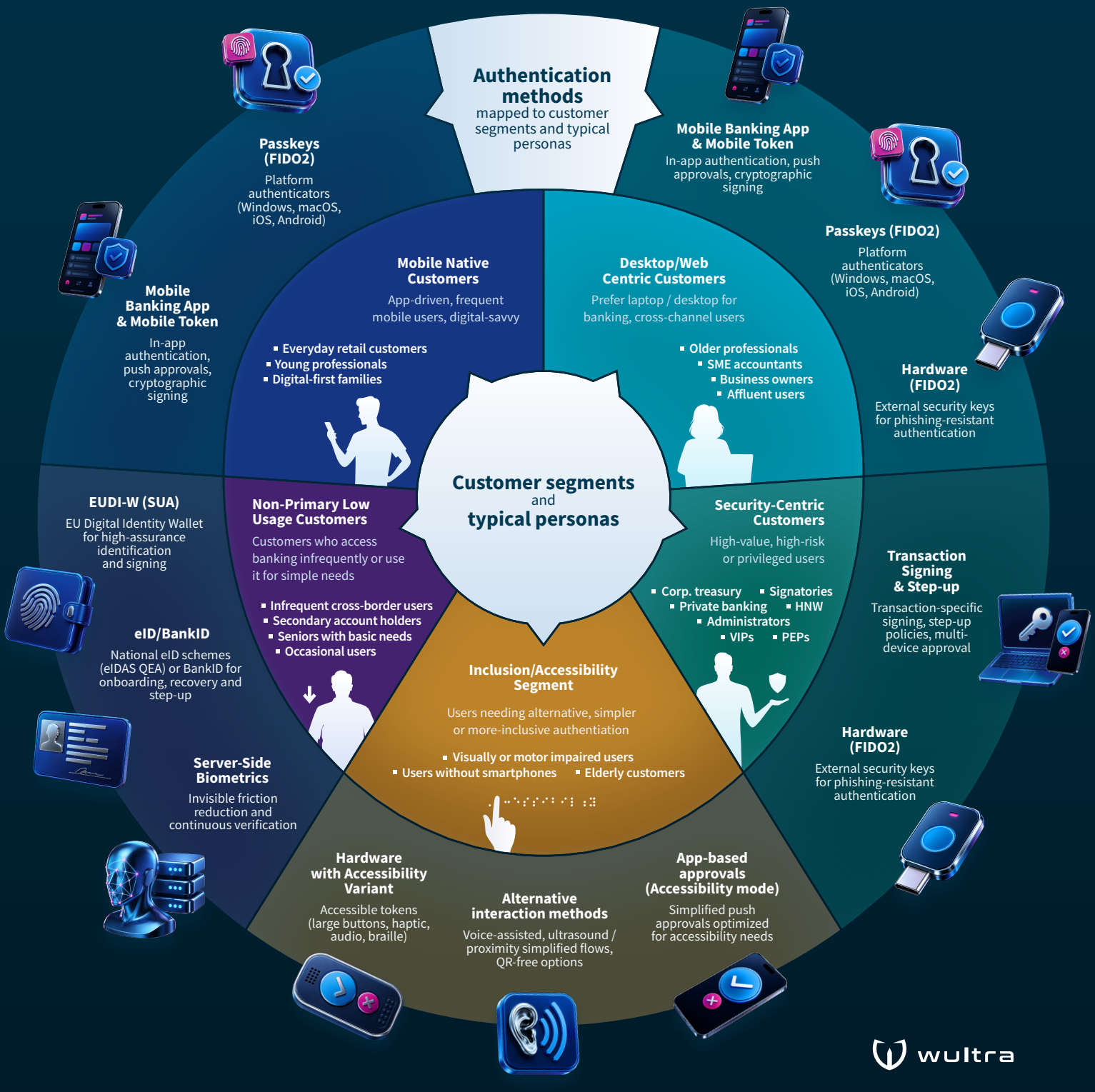
However, these dimensions and associated customer segments cannot be directly applied to authentication methods and must be combined into new, authentication-specific models.

The Example Model for Daily Banking

One way the bank can approach the task is by selecting 2-3 specific segmentation dimensions they already use, selecting the largest customer segments, and finding overlaps.

A Reference Authentication Segmentation Framework

For most daily banking apps, the following segmentation would work as a baseline. The model examines the following segments and asks, “What is the most natural way for the users to authenticate?”



wultra

Future Authentication Methods for Banking

Given the various customer segments, we can distill a suite of authentication methods suitable for most banks that provide daily banking services.

Mobile-First Authentication

While relying on mobile-first authentication monoculture completely can be harmful, smartphones are not going anywhere. In fact, most users will prefer mobile-first authentication. Any bank with a retail customer segment must adopt authentication based on the smartphone app for major mobile platforms - iOS and Android, at least.

Banks can provide mobile-first authentication in two distinct incarnations:

- **Embedded mobile authentication**
  Authentication provided as a plugin in mobile banking, the most suitable option for the majority of retail customers who increasingly access banking services via a mobile device.

- **Standalone mobile token app**
  An alternative best suited for customers who commonly use internet banking on a classic desktop, desktop-only users, or as an authentication means for small businesses.

Hardware Tokens (FIDO2)

While hardware tokens were once considered outdated, they still have their place in modern digital banking, especially for specific customer segments and corporate usage. Given current technology, the FIDO2 standard is the preferred approach for supporting hardware tokens over other possible candidates. Chip card readers are cumbersome to set up and difficult to use, just like conventional transaction-signing OTP generators, which are also prone to phishing.

We recommend that organizations evaluate the following incarnations of FIDO2 hardware tokens:

- **USB sticks**
  While not fully compliant on their own (missing dynamic linking, varying quality of authentication factors, different runtime environments, …), classic USB sticks (i.e., YubiKey) can provide an additional, phishing-resistant security element for security-sensitive customers or business owners.

- **USB-connected transaction signing device**
  To provide a fully compliant alternative for business users and retail customers who are unwilling to use a smartphone, banking-specific authenticator devices should be considered, offering decent comfort and excellent security.

- **Accessibility-focused alternative**
  For people with accessibility needs or elderly customers who opted out of smartphone authentication, a specialized hardware alternative with stronger accessibility features (larger buttons, haptics, audio output) should be evaluated as an additional option.

Biometric Authentication

Using biometrics for authentication provides one significant benefit: no additional device is typically required, so users can authenticate only with “something they are”.

PSD3/PSR regulation opened discussion around the use of two authentication factors from the same category, for example, two factors from the “inherence” category, which would essentially allow the use of two distinct biometric modalities.

These can be, for example, the following active biometric authentication methods:

- **Facial biometrics**
  Matching an authenticating person with the trusted reference photo, either extracted from a personal identity document or provided by the local government database.

- **Palm biometrics**
  Matching the palm shape and palmar creases of an authenticating person against a previously recorded palm template.

Note that each biometric modality has different benefits, limitations, and a risk profile. For example, while it is quite easy to log in with one's face, public facial imagery (e.g., profile pictures on social media or online profiles, screen captures during video calls, etc.) underscores the importance of robust presentation attack detection and certified liveness mechanisms during the authentication ceremony. It is much more difficult to obtain trusted data for palm biometrics, but palm-based authentication is less common, and users won't be familiar with it. On the other hand, it can provide an excellent alternative for users who are unwilling or unable to show their faces (e.g., for religious reasons).

With the rise of deepfakes, AI-supported presentation attacks, and camera-injection attacks, the use of a properly certified biometric solution is also a must.

Organizations can address some weaknesses in biometric authentication and improve the overall security of login and payment approval by adding a second authentication factor (even a weaker one, like SMS OTP or a password).

An additional measure could be provided using **continuous behavioral verification** - matching the usage patterns of an authenticating person against previously captured data, assessing aspects such as screen flow, unusual navigation paths in the user interface, mouse movement, or keystroke dynamics.

Federated Authentication and Decentralized Identity

For customers who only access banking services occasionally, any new authentication method is just an additional burden. For non-primary customers, the authentication methods they already have would provide significantly greater comfort.

Of course, from a bank's perspective, federated and decentralized methods are provided by a third party, and they must still provide sufficient credence to the user's identity and comply with applicable regulations, especially PSD3/PSR requirements on SCA.

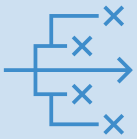
The following mechanisms are suitable candidates:

- **European Digital ID Wallet (EUDI-W)**
  A recent initiative by the European Commission, expected to be available to European citizens at the beginning of 2027 (with obligatory delays in implementation in specific markets), was explicitly designed with SCA requirements in mind, and banks will likely need to support wallet-based authentication flows in many regulated scenarios.

- **eID**
  In markets with strong eID (a predecessor of EUDI-W) adoption, an eID can provide a viable option for strong customer authentication, especially if its use is explicitly contracted by the bank with the provider and covered under the banking service outsourcing contract and independently assessed for compliance with banking regulations (especially requirements on SCA).

- **Bank ID**
  In markets where Bank ID is available, people can use it as a convenient strong customer authentication mechanism. Bank ID authentication methods are typically backed by other banks (or built as a central system by the banks). As a result, the regulatory risk is minimal, and users can rely on the authentication method they have from another bank, know it, and trust it.

The Transition Plan for Banks



Unfortunately, we anticipate that only a handful of banks are ready to diversify authentication methods without significant effort. Because banks did not need to consider diversity and inclusivity when designing their authentication approaches during the PSD2 transition, authentication methods are often hard-coded in legacy, proprietary systems.

So, what steps do we recommend taking?

Think About Your Customers

Before jumping into assessing technology and products on the market, organizations should start with people - their customers who need to authenticate. This includes conducting user research, analyzing customer needs, and quantifying the sizes of various customer segments.

Starting with customers will help determine which customer segments need access to online applications and allow for tailoring customer authentication methods specifically for the identified segments.

The goal of this activity is to understand where your organization wants to go, define an optimal user experience, and prioritize which authentication methods are worth exploring and which are just a waste of your resources.

Assess Where You Are Now

Once you know the desired business result and the optimal authentication methods for your customers, evaluate your existing user authentication technology stack to determine whether it naturally supports multiple authentication methods or relies heavily on a specific few.

This is where organizations will differ greatly.

For banks that invested in their customer identity program, making the change could be as easy as installing, configuring, and communicating new authentication methods in their existing systems.

For the rest, new integrations will be needed, which may require substantial time and resources to implement. As a result, the full replacement of the authentication platform (SSO and transaction authorization) might be a simpler option.

Implement the Change

Once you are clear about where you want to go and know your technological starting point, the final step is to implement the projects and open the necessary RFIs and RFPs for the new systems.

Don't forget that there are several steps beyond a technical migration that lead to the successful transition. The changes you make must be:

- Audited and pen-tested before go-live
- Reflected and published in the updated terms of service for end-customers
- Notified to the regulatory bodies if the transition results in a substantial change
- Communicated internally to enable branches and call centers to respond to inquiries
- Promoted to the right customer segments to maximize customer satisfaction and value

Because of the required workload, we recommend allocating sufficient time and resources needed to transition from a mobile-first authentication monoculture to a diversified set of authentication methods. Organizations should allocate sufficient time (at least 12 months) and human and financial resources to facilitate the required projects.

Recommendations summary

We recommend that banks:

- Assess which customer segments need access to their online applications and tailor authentication approaches to those segments to reduce friction.
- Evaluate whether their current authentication stack can naturally support multiple authentication methods or relies heavily on specific authentication mechanisms.
- Allocate sufficient time and resources to transition from a mobile-first authentication monoculture to a diversified set of authentication methods, as the transition requires more than technical migration alone.

If you would like to discuss how these changes may affect your organization, **feel free to reach out**.

Petr Dvorak
Founder & CEO

petr@wultra.com

wultra

ABOUT WULTRA

We help banks and fintechs secure their digital channels with seamless, post-quantum authentication built for today's users and compliance needs, ready for tomorrow's threats.

wultra.com linkedin.com/company/wultra sales@wultra.com

20+
COUNTRIES

70+
CLIENTS

4.8*
GARTNER PEER INSIGHTS RATING

Wultra Named in Gartner® Hype Cycle™ for Digital Identity, 2026 as a Sample Vendor for the Second Consecutive Year

READ MORE

Gartner