entersekt

The Financial Authentication Company.

From PSD2 to PSD3:
Turning a compliance challenge into business success

Can you transform a set of mandatory security standards into a competitive advantage? With the right partner, you can.

entersekt.com
info@entersekt.com

From PSD2 compliance to PSD3 readiness

The European Union's revised Directive on Payment Services (PSD2) has been reshaping the payments landscape since it came into force in 2018. What began as a compliance exercise became a catalyst for innovation, new competition, and fundamental change across financial services.

Entersekt's patented security solutions have long provided a clear and reliable path to PSD2-compliant strong customer authentication (SCA) — but our solutions go far beyond compliance. From the outset, we've focused on helping our customers meet regulatory obligations while also strengthening fraud prevention, protecting revenue, and creating seamless customer experiences.

Now, the industry is preparing for the next evolution — PSD3, expected to be formally implemented gradually between 2026 and 2028. The new directive refines requirements around open finance, consumer protections, digital identity, and fraud management, raising both challenges and opportunities.

Traditional players must defend their market share while contending with agile challengers: fintechs, retailers, telcos, and digital giants all competing to own the customer relationship.

Entersekt's mission remains the same: to position our customers not just to pass regulatory audits, but to thrive in this increasingly fluid and competitive market.

Audit proof, yes — but future proof too.

In the pages that follow, we explore what PSD3 means in practice — highlighting the key differences from PSD2, the timeline for implementation, and the implications for financial institutions. From there, we'll walk through three practical steps to success:

And, finally, we'll show how Entersekt's solutions not only ensure compliance but create lasting competitive advantage.

PSD2 vs PSD3: What's changing and why it matters

PSD3 is not just "PSD2 2.0" — it's a wider-reaching regulation that strengthens consumer rights and expands digital finance. For financial institutions, this means higher compliance stakes but also greater opportunity to innovate.

Focus area	PSD2	PSD3	Impact for FIs
Scope	Payments only	Expands to open finance (loans, savings, insurance, investments)	Broader compliance footprint and new business models
Authentication	SCA for payments	Stricter rules, wider use cases, cross-channel identity	Need for flexible, future-ready authentication
Liability	Shared, sometimes unclear	Clearer allocation, stronger consumer protections	Higher risk exposure if fraud controls are weak
Fraud monitoring	Required but limited scope	Stronger mandates on risk-based, real-time fraud detection	Investment in advanced fraud analytics becomes essential
Open Banking	Access to payment accounts (AISPs, PISPs)	Expanded to open finance with broader data sharing	New opportunities for data-driven services
Digital Identity	Not explicitly defined	Integration with EU Digital Identity Wallet	Banks can position as trusted identity providers

PSD3 implementation timeline

While the final text of PSD3 is expected in 2025, the rollout will be phased:

2025:
Formal adoption of PSD3 and the accompanying Payment Services Regulation (PSR).

2026:
Initial transposition into national laws begins; early compliance preparations start.

2027:
Financial institutions must demonstrate compliance with most key provisions (SCA, liability, fraud monitoring, open banking refinements).

2028:
Formal full enforcement of PSD3 across the EU.

This staged approach gives institutions time to adapt — but leaders are already investing in future-ready authentication platforms that minimize redevelopment and ensure continuity across PSD2 and PSD3.

Your path to success under PSD2 and PSD3

Success under PSD2 — and soon PSD3 — requires more than ticking regulatory boxes. It's about building a foundation that not only satisfies compliance but also unlocks growth.

By focusing on three key steps, financial institutions can move confidently from compliance to customer delight, and from defensive posture to growth:

STEP ONE

Meet immediate compliance objectives

STEP TWO

Provide a winning user experience

STEP THREE

Capitalize on the opportunity

Step 1: Meet immediate compliance objectives

Invest in a proven, scalable, interoperable, and well-documented strong authentication solution that eases auditing and reporting to regulatory authorities.

The regulatory technical standards (RTS) defined under PSD2 set the foundation for strong authentication and secure communication. These requirements remain core under PSD3.

Let's recap the basics, and Entersekt's approach to meeting them:

Strong customer authentication (SCA)

Except in defined circumstances, SCA is obligatory under PSD2 when a payer or proxy accesses payment accounts online, initiates an electronic payment transaction, or carries out any action through a remote channel that may imply a risk of fraud or other abuse. An SCA procedure must use at least two of the following factors:

- **Knowledge:** Something only the user knows (e.g. password, PIN, or identification number)
- **Possession:** Something the user possesses (e.g. token, smart card, mobile phone)
- **Inherence:** Something the user is (e.g. a computer-readable biometric characteristic)

Entersekt's solution uses digital certificates to uniquely identify each registered mobile phone or tablet, transforming it into a trusted factor of possession. These certificates are also used to generate authentication codes for every individual operation and to digitally sign them. In this way, the solution guarantees the authenticity of any digital transaction — that it was initiated and authenticated by the customer — and its integrity — that it has not been intercepted and modified by a third party in a man-in-the-middle or similar attack.

Independence of SCA elements

The transmission and use of authentication factors must ensure that they are independent of one other, so that a breach of one will not compromise the other. The channel, device or mobile app through which the authentication code is generated and received must be independent from the channel, device, or mobile app used for initiating the transaction.

Entersekt's solution is a self-contained, NIST-assured cryptographic stack and communications layer that enables an isolated, end-to-end encrypted communications channel between the service provider and its customer's secured mobile app or browser. No third party, including Entersekt, can access these communications. All cryptographic material is securely stored, ensuring that neither the user nor the application developer can access it. Knowledge or inherence factors like PINs or biometrics are similarly protected.

Dynamic linking

SCA must be uniquely tied to the specific payment transaction. Authentication prompts must be generated in a way that links them to the transaction amount and payee, ensuring any change invalidates the authentication, protecting against tampering and man-in-the-middle attacks.

Entersekt's solution delivers authentication prompts to the user over the out-of-band channel. Only the service provider and user know the nature of the encrypted request, which includes all the details required in the RTS, further allowing for informed decision making too.

Associate the user with their credentials, devices, and software

Authentication solutions must have the ability to securely associate the customer with their personalized security credentials, their authentication device(s), and any software that they use in the authentication process.

Entersekt's solution generates pseudonymous digital certificates, uniquely identifying a customer's mobile device or browser. This certificate is only linked to the customer by the service provider at registration, so only they are party to the relationship between device and customer. If the device is stolen, lost, or replaced, the provider simply unlinks the certificate from the user, rendering the app unusable.

Monitor access to user accounts

Authentication solutions must include monitoring and real-time risk assessment in order to protect users from unauthorized operations resulting from lost or stolen security credentials. The system should flag suspicious activity, including abnormal spending, atypical device or software usage, device- or software-based vulnerabilities, and malware infection.

Entersekt's solution leverages layered detection, advanced and dynamic risk signals, and prevention procedures, rendering it invulnerable to malware, SIM-swap fraud, and brute force attacks. It serves backend risk engines with device and application data, including device type, operating system version, and geographic location. It also provides app tamper awareness and advanced detection of rooting, jailbreaking, or similar mobile operating system security bypass hacks.

How will compliance objectives expand under PSD3?

Broader scope:

PSD3 extends beyond payments to cover a wider set of financial services under the open finance framework.

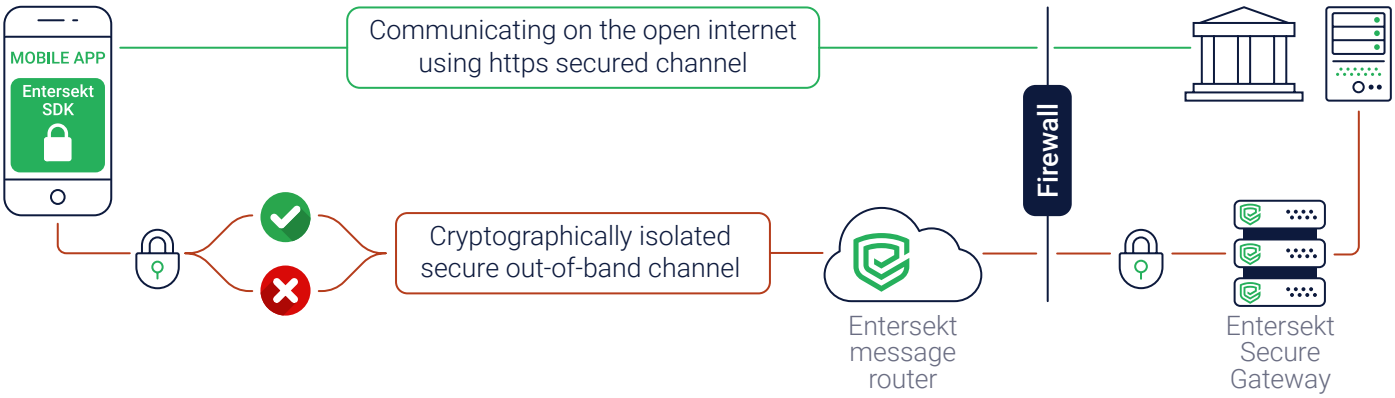
Enhanced liability rules:

Clearer allocation of responsibility between payment service providers and intermediaries.

Advanced fraud detection:

Institutions must demonstrate advanced real-time monitoring, risk-based authentication, and cross-border fraud prevention.

The bottom line: Entersekt's multi-factor, out-of-band authentication and app security solutions were built to meet and exceed these standards. Our solutions remain globally aligned, interoperable, and scalable, easing both auditing and reporting.



In the diagram above, we show the distinct channels Entersekt enables between the mobile phone and service provider:

- The green channel at the top is used to initiate a transaction.
- The amber channel below it authenticates the transaction.

These channels and the means by which Entersekt securely stores related cryptographic key material together enable transactions to be initiated and authenticated completely out of band using the same mobile app.

Financial institutions that invest in proven, standards-based solutions like Entersekt's today will be better prepared for tomorrow's more complex regulatory environment.

Step 2: Provide a winning user experience

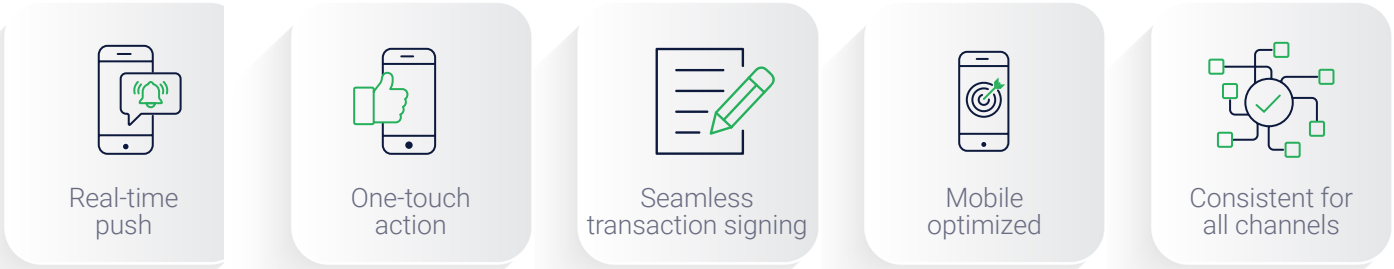
Empower your customers to transact anywhere, anytime, enhancing your relationship with each new interaction.

The introduction of SCA under PSD2 was initially seen as disruptive. Many feared customer abandonment and friction at checkout. However, as solutions matured, secure, seamless authentication became a differentiator.

That lesson is even more important under PSD3. With the directive set to expand protections across more use cases — from account-to-account payments to digital identity — the ability to deliver one-touch, mobile-first experiences will define market leaders.

Entersekt's solutions allow customers to approve transactions in real time via a secured mobile app. Each authentication request includes contextual details, empowering users with control and confidence.

The Entersekt user experience

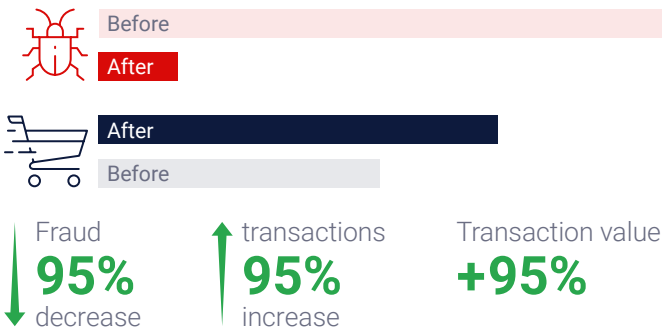


Case studies show that our mobile-based authentication has:

- Almost eliminated card-not-present fraud
- Increased digital payments processed by nearly 30%
- Improved customer satisfaction and loyalty

Under PSD3, consumer trust will be as much about usability as about compliance. Financial institutions that simplify authentication will win.

CASE STUDY: SCA usability driving channel growth



One European card issuer began rolling out Entersekt's mobile-based payments enablement solution in 2016. Its primary goal was to improve the 3-D Secure user experience. Within five months, it almost eliminated card-not-present fraud, but it is arguably the solution's beneficial effect on channel adoption that made the biggest impact: The number of digital payments processed climbed 29% and the total transaction value increased by over 15%.

Step 3: Capitalize on the opportunity

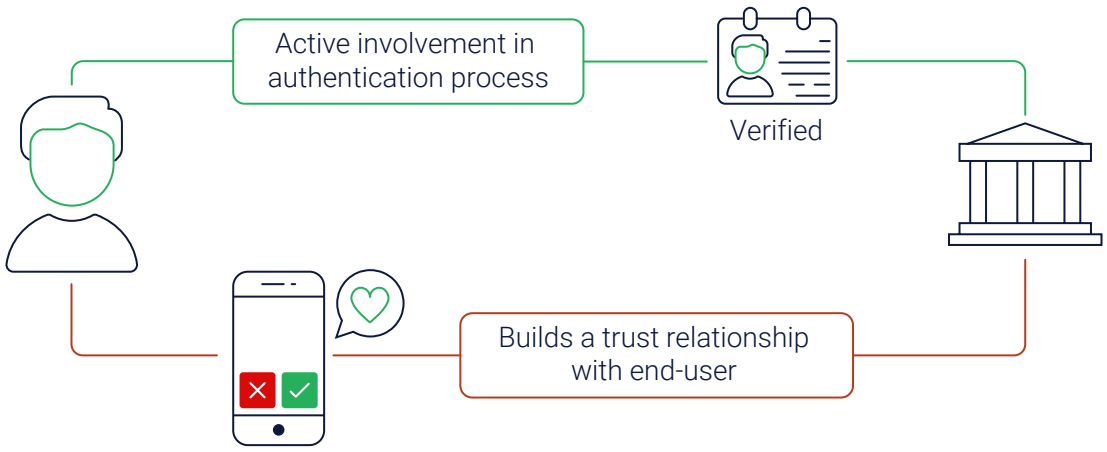
Become the trusted keeper of consumers' digital assets and change your strategic position relative to third-party payment service providers.

PSD2 reshaped the market by opening customer accounts to third parties, driving competition, and encouraging innovation. PSD3 goes further:

- Expanding to open finance (beyond payments into mortgages, savings, insurance, and more)
- Strengthening digital identity frameworks
- Introducing stricter rules on liability and consumer redress

For banks, this is a chance to reassert their position as trusted custodians of digital identities. By offering authentication as a value-added service across multiple channels — banking apps, e-commerce, call centers, and more — institutions can turn compliance investments into engines of growth.

Entersekt's flexible solutions are built to evolve with regulation, supporting convergence across channels and preparing institutions for both PSD2 and PSD3 compliance — and beyond.



Learn more about our approach to **meeting regulatory compliance with ease.**

The future is built on trust

"People need banking, not banks," say many fintech companies. The truth is, **people need trust**. In a payments ecosystem where new platforms, digital wallets, and non-traditional providers continue to multiply, the question consumers ask is simple: Who can I rely on to protect my identity, my data, and my money?

For decades, banks have held that position of trust — but the gap is narrowing. Since PSD2 came into force in 2018, challenger banks, big tech, and fintech players have steadily gained ground, reshaping consumer expectations for both security and experience. PSD3 will accelerate this shift.

Financial institutions face a choice: risk being reduced to utilities in the background, or seize the opportunity to become the trusted custodians of their customers' digital lives. By leveraging their inherent trust advantage and investing in flexible, future-ready authentication, banks can unlock new value-added services, deepen daily engagement, and reassert their place at the center of digital finance.

Entersekt helps make that future possible. More than a compliance solution, our platform gives financial institutions the foundation to innovate with confidence — delivering fraud-free security that builds trust today and prepares them for the opportunities of tomorrow.

Audit proof, yes — but future proof too.

About Entersekt

Entersekt, The Financial Authentication Company, provides financial institutions with digital banking fraud prevention and payment security solutions through its cross-channel, Context Aware™ Authentication platform that secures digital transactions and optimizes user experiences. Founded in 2008, Entersekt serves financial institutions around the world, and holds 120+ patents for its security innovations.

In 2023, Entersekt acquired the Modirum 3-D Secure software business from Modirum, a security technology firm based in Helsinki, Finland, positioning Entersekt as a global industry leader in authentication solutions for financial services. Entersekt processes 7.5bn+ transactions for 250m+ cardholders and 450,000+ merchants from nearly 900 banks in 70+ countries. Backed by companies like Silicon Valley-based Accel-KKR, one of the world's top private equity firms, Entersekt continues to expand its footprint across key regions.

For more information about Entersekt, or to speak to an expert, please visit **www.entersekt.com** or email **info@entersekt.com**.


/Entersekt


@Entersekt


/Entersekt

V01_202510_MKT7593