LOOQR

Unlocking Digital Trust

Digital Trust & Identity in Banking

Regulatory Playbook 2026

What European banks must prepare for in digital identity, authentication, and trusted digital transactions.

Executive Summary

The European banking sector is entering a new phase of regulatory and technological transformation.

Over the next few years, several regulatory developments will reshape how banks verify customer identities, authenticate users, and execute digital agreements.

Among the most significant developments are:

- eIDAS 2.0 and the European Digital Identity Wallet.
- New authentication expectations resulting from wallet-based identity.
- PSD3 and the evolution of Strong Customer Authentication (SCA).
- Increasing adoption of instant payments.
- Stronger AML supervision under the new EU Anti-Money Laundering Authority (AMLA).
- Higher expectations around audit evidence and digital trust infrastructure.

These developments accelerate the transition toward fully digital banking journeys, where customers can onboard, authenticate, and sign contracts remotely with strong legal assurance.

To support this transformation, banks must implement infrastructures capable of providing:

- Strong identity verification.
- Secure authentication mechanisms.
- Legally valid electronic signatures.
- Structured audit evidence.

Digital trust Platforms such as LOQR|core provide the orchestration layer required to implement these capabilities across digital banking journeys.

The New European Digital Identity Landscape

Digital identity is becoming a central component of financial services across Europe.

The revised eIDAS 2.0 regulation introduces the European Digital Identity Wallet (EUDI Wallet), a digital identity solution that will allow citizens to:

- Store government-issued identity credentials.
- Share verified attributes with service providers.
- Authenticate themselves in digital services.
- Sign documents electronically.

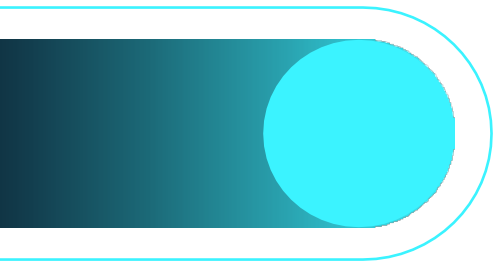
Banks will play a key role in this ecosystem as relying parties, meaning they must be able to accept wallet-based identity and authentication mechanisms.

This shift will transform how banks handle:

- Identity verification.
- User authentication.
- Digital contract execution.

Financial institutions will need platforms capable of integrating wallet-based identity, strong authentication, and digital signatures into their digital channels.

Solutions such as LOQR|core provide the orchestration layer required to integrate these identity services into banking systems.



Evolution of Strong Customer Authentication (SCA)

European banking authentication is entering a new phase shaped by three regulatory forces: PSD3, eIDAS 2.0, and the expansion of instant payments, which increases the security criticality of transaction authentication.

Strong Customer Authentication (SCA) became a core regulatory requirement for European banks with the introduction of PSD2.

Under PSD2, financial institutions must authenticate users using at least two independent factors from the following categories:

- Something the user knows (password or PIN).
- Something the user has (device or token).
- Something the user is (biometrics).

The proposed PSD3 framework aims to further strengthen authentication requirements across the European financial ecosystem.

PSD3 is expected to:

- Reinforce strong authentication requirements for payment initiation.
- Strengthen fraud prevention mechanisms.
- Reduce reliance on weaker authentication mechanisms.
- Increase supervisory expectations regarding authentication security.

At the same time, eIDAS 2.0 introduces a new paradigm for digital identity and authentication through the European Digital Identity Wallet.

Authentication may increasingly rely on:

- Wallet-based authentication.
- High-assurance digital identity credentials.
- Cryptographic authentication mechanisms.
- Verified identity attributes.

These developments are expected to accelerate the transition away from weaker authentication mechanisms such as SMS-based OTP toward stronger, identity-based authentication.

Solutions such as LOQR|sca enable banks to implement next-generation Strong Customer Authentication aligned with PSD3 and eIDAS 2.0.

When integrated with LOQR|core, banks can design authentication journeys capable of adapting to future regulatory requirements.

Instant Payments and the growing importance of strong authentication

Another important driver of stronger authentication is the rapid adoption of instant payments across Europe.

Under the SEPA Instant Credit Transfer scheme and the EU Instant Payments Regulation, payment transfers can be executed within seconds.

While this improves customer experience, it significantly increases fraud risk.

When a payment is executed instantly:

- Funds leave the originating account immediately.
- Recovery of fraudulent transactions becomes extremely difficult.
- Banks have little opportunity to intervene after the transaction.

As a result, the moment when a customer authenticates and authorises a payment becomes the most critical security control.

Banks must therefore ensure that the person initiating the payment is strongly authenticated and reliably identified.

Solutions such as LOQR|sca allow banks to implement authentication mechanisms capable of protecting digital transactions in an environment increasingly dominated by real-time payments.

Impact on Digital Onboarding

Remote onboarding has become a standard capability in modern banking.

However, regulators continue to scrutinise remote onboarding processes to ensure that identity verification is reliable and fraud-resistant.

Banks must ensure that onboarding processes provide guarantees that:

- Identity documents are authentic.
- The person interacting with the system is the Legitimate holder of the document.
- The onboarding process generates traceable audit evidence.

Common mechanisms include:

- Document verification.
- Biometric verification.
- Video identification.
- Verification against trusted databases.

Modular identity verification components such as LOQR|brick can support this layer, while LOQR|core orchestrates the onboarding journey and compliance controls.

Electronic Signatures in Banking

Digital contracts are increasingly executed entirely online.
Under the eIDAS Regulation, three levels of electronic signatures exist.

Simple Electronic Signature (SES)

Examples include clicking an acceptance button.
SES signatures are legally valid but have limited evidential value.

Advanced Electronic Signature (AES)

AES signatures uniquely identify the signer and detect document modification.

Qualified Electronic Signature (QES)

QES signatures provide the highest level of legal assurance.

They:

- Use qualified certificates issued by qualified trust service providers.
- Rely on secure signature creation mechanisms.
- Have the same legal effect as handwritten signatures in the EU.

Solutions such as LOQR|sign enable banks to integrate qualified signatures within digital journeys orchestrated by LOQR|core.

Evolution of AML Supervision

The creation of the European Anti-Money Laundering Authority (AMLA) marks a new phase in AML supervision across Europe.

This will increase scrutiny on:

- Remote onboarding.
- Identity verification.
- Customer due diligence.
- Audit documentation.

Banks must therefore ensure their digital processes remain auditable, documented, and fraud-resistant.

Reference Architecture for Digital Trust in Banking

A modern digital banking infrastructure typically includes several layers.

Journey Orchestration Layer

Responsible for orchestrating onboarding, authentication, and contract execution.
LOQR|core provides this orchestration layer.

Identity Verification Layer

Responsible for identity proofing.
Supported by modular components such as LOQR|brick.

Authentication Layer

Responsible for Strong Customer Authentication.
Supported by LOQR|sca.

Digital Signature Layer

Responsible for executing legally valid digital contracts.
Supported by LOQR|sign.

Evidence Layer

Responsible for storing audit evidence, including:

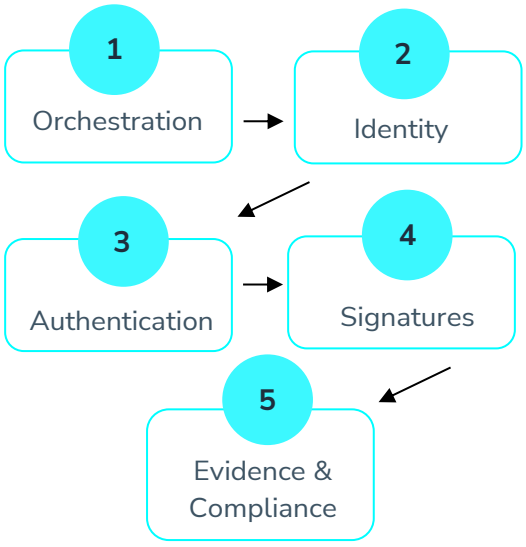
- Identity verification logs.
- Authentication events.
- Signature certificates.
- Document hashes.
- Timestamps.

LOQR Digital Trust Stack for Banking

A modern digital banking infrastructure requires multiple trust capabilities working together.

The LOQR platform provides a modular architecture for implementing these capabilities.

LOQR|core



This architecture enables banks to integrate identity verification, authentication, and digital signing into a single, orchestrated digital journey.

Authentication Methods vs Regulatory Assurance

Different authentication methods provide different levels of regulatory assurance.

Authentication Method	Security Level	Regulatory Confidence	Future Readiness
Password only	Low	Weak	Not acceptable
SMS OTP	Medium	Increasingly questioned	Declining
App-based authentication	Medium–High	Acceptable	Transitional
Biometric authentication	High	Strong	Future-ready
Identity-based authentication (wallet / cryptographic identity)	Very High	Strongest	Strategic

The evolution of European regulation suggests a progressive shift toward identity-based authentication models supported by secure digital identity frameworks.

Preparing for the Future of Digital Banking

The regulatory landscape for digital identity and authentication is evolving rapidly.

With the emergence of the European Digital Identity Wallet, the strengthening of AML supervision, and the expansion of instant payments, banks must modernise their digital trust infrastructure.

Future-ready banking platforms must support:

- Strong identity verification.
- Flexible authentication mechanisms.
- Legally valid electronic signatures.
- Traceable digital evidence.

Digital trust platforms such as LOQR|core enable banks to orchestrate these capabilities while integrating specialised modules such as LOQR|brick, LOQR|sca, and LOQR|sign.

About

LOQR is a trusted digital identity and e-signature provider, empowering financial institutions to comply, scale, and simplify user journeys under eIDAS 2.0.

With deep expertise in identity verification, compliance automation, and qualified e-signature solutions, our Identity Orchestration Platform helps banks and financial institutions deliver exceptional financial services while future-proofing their digital operations.

To find out more about how to get the most out of our technological solutions to solve your daily challenges, please contact us at sales@loqr.com.

LOQR

For more information, visit LOQR.COM

Or contact us at SALES@LOQR.COM

Unlocking Digital Trust