LOQR

Unlocking Digital Trust

LOQR SCA Solution:
From OTP-Based Security to Identity-Centric Trust in the eIDAS 2.0 Era

Strong Customer Authentication Solution

Strong Customer Authentication (SCA) is undergoing a fundamental transformation. What started as a regulatory requirement under PSD2 - largely implemented through passwords and SMS one-time passwords (OTP) - is rapidly evolving into an identity-centric security model driven by eIDAS 2.0, digital identity wallets, and cryptographically linked authentication factors.

This whitepaper presents LOQR’s vision for next-generation SCA: moving beyond fragile OTP-based mechanisms toward biometric, device-bound, and wallet-enabled authentication that meets the expectations of regulators, financial institutions and end users.

LOQR’s SCA solution is designed to address these challenges, enabling regulated entities to comply with PSD2, PSD3 and eIDAS 2.0 standards while future-proofing their authentication infrastructure in line with the European Digital Identity framework.

The Evolution of SCA

SCA under PSD2

PSD2 introduced SCA as a mandatory control to reduce fraud in electronic payments and remote account access. In practice, many institutions have implemented SCA using:

- Knowledge factors – Something the user knows (passwords, PINs).
- Possession factors – Something the user has (based on SMS OTP).

While compliant, these approaches revealed significant weaknesses:

- SMS OTP is vulnerable to SIM swapping, phishing, and interception.
- Limited cryptographic binding between user, device, and transaction.
- Unsatisfactory user experience and increasing abandonment rates.

PSD3 and the Need for Stronger Authentication

PSD3 reinforces SCA requirements while acknowledging emerging fraud patterns and digital behaviors. Regulators now expect:

- Stronger possession factors.
- Better fraud prevention.
- Improved customer experience.

This change sets the stage for eIDAS 2.0 to redefine how SCA should be implemented.

eIDAS 2.0: Redefining Digital Trust and Authentication

From Authentication Factors to Digital Identity

eIDAS 2.0 introduces a new paradigm based on:

- European Digital Identity Wallets (EUDI Wallets).
- High-assurance digital identities issued or recognised by Member States.
- Cryptographic binding of identity, device, and user consent.

Authentication is no longer just about proving control over a factor; it is about proving identity with a regulated level of assurance.

The Decline of SMS OTP

According to eIDAS 2.0 principles, SMS OTP is increasingly becoming obsolete:

- Weak possession factor.
- No inherent cryptographic protection.
- Inconsistent with wallet-based and identity-centric models.

While SMS OTP may persist temporarily, its role as a standard SCA mechanism for regulated entities is expected to decline rapidly.

Wallet-Based Authentication as the New Standard

Digital identity wallets enable:

- Strong possession (device-bound keys).
- Inherence through on-device biometrics.
- Explicit user consent.
- Secure transaction binding.

These capabilities naturally align with SCA requirements and regulatory expectations.

Biometrics as a Core Pillar of Modern SCA

Why Biometrics Matter

Biometric authentication, particularly facial recognition, provides:

- High usability and speed.
- Strong inherent security.
- Reduced cognitive load for users.

Facial recognition, when properly implemented, is particularly well suited for digital-first financial journeys, allowing users to authenticate themselves without remembering passwords or carrying additional devices.

In addition, facial biometrics can help mitigate a range of fraud scenarios where traditional credentials are transferable or vulnerable to manipulation. These include money mule accounts (where the individual operating the account is not the originally verified customer) and account takeover attempts enabled by phishing or SIM swapping attacks. By linking high-risk actions to a non-transferable biometric identity factor, institutions can strengthen identity assurance and introduce an additional layer of protection to reduce fraud's scalability.

The Role of Liveness Detection

Liveness detection is a critical enhancement to biometric authentication. Without liveness detection, biometric systems are vulnerable to spoofing attacks using photos, videos, or synthetic media.

LOQR’s biometric stack includes advanced liveness detection that:

- Detects presentation attacks in real time.
- Analyses dynamic facial and environmental signals.
- Operates seamlessly across different channels.

This ensures that biometric authentication remains robust even in high-risk scenarios.

LOQR’s Identity-Centric SCA Platform

LOQR provides a comprehensive authentication Platform designed to support secure, compliant, and user-centric digital operations.

SCA as Orchestration

LOQR approaches SCA as an orchestration layer capable of combining:

- Biometric authentication (Facial Recognition + Liveness Detection).
- Device-based possession factors.
- Knowledge factors when required.
- Digital identity wallets and verified attributes.

This flexibility ensures strong protection and allows institutions to dynamically adapt authentication strength to different journeys and channels.

Risk-Based and Context-Aware Authentication

Not all operations carry the same level of risk. LOQR enables risk-based SCA by considering:

- Transaction value.
- User behavior patterns.
- Device and environmental signals.

Low-risk actions can remain frictionless, while higher-risk operations trigger stronger authentication flows.

Alignment with eIDAS 2.0 and PSD3

LOQR’s Platform is designed to:

- Integrate with European Digital Identity Wallets.
- Support identity-based authentication flows.
- Ensure auditability and regulatory compliance.

This positions LOQR as a long-term trust infrastructure partner for regulated entities.

Benefits for Regulated Institutions

By adopting LOQR's SCA solution, institutions gain:

- **Future-Proof Compliance:** Built-in compliance with PSD2, PSD3 and eIDAS 2.0 requirements.
- **Reduced Fraud:** Through strong biometrics and device binding, reducing the risk of account takeover and payment fraud.
- **Improved Customer Experience:** Fast, intuitive authentication by eliminating OTP friction.
- **Operactional Efficency:** Through automated and scalable authentication, reducing manual reviews and operational costs.
- **Strategic Alignment:** With Europe's digital identity roadmap.

As banking operations continue to grow in scale and complexity, Strong Customer Authentication is a cornerstone of digital trust.
As Europe transitions toward identity-centric authentication under eIDAS 2.0, financial institutions must move beyond SMS OTP and fragmented security controls.

LOQR provides a modern SCA Platform that combines biometrics, liveness detection, device binding, and digital identity integration enabling regulated entities to meet today's requirements while preparing for tomorrow's trust ecosystem.

LOQR

Get Started with LOQR’s Identity-Centric SCA Platform Today!

Transform Your Digital Ecosystem with Trust!

For more information, visit LOQR.COM

Or contact us at SALES@LOQR.COM

BOOK A DEMO