Reusable Identity in Finance: Faster KYC, Stronger Compliance

A practical guide for financial institutions to cut verification costs, reduce drop-offs, and deliver instant, compliant access across products and markets.

eVrotrust

Table of Contents

Introduction 1
Why reusable identity is becoming essential for financial institutions.

The Limits of Traditional Identity Systems 2
How fragmented verification processes slow onboarding and increase compliance costs.

Traditional Identity vs Reusable Identity 3
Comparing one-time verification models to reusable, continuous identity frameworks.

How Reusable Identity Works 6
Step-by-step overview of the reusable identity process and its impact on banking.

Types of Reusable Identities 8
Government-issued, bank-based, self-sovereign, and platform-based identity models explained.

The Reusable Identity Lifecycle 10
How verification, credential creation, reuse, and audit form one connected process.

The Challenges of Reusable Identity 12
Key barriers to implementation and how banks can overcome them.

How Banks Benefit from Reusable Identity 14
The strategic and operational advantages for retail, corporate, and digital banking.

Conclusion 19
The future of digital trust in banking and why reusable identity is becoming a competitive necessity.

About Evrotrust 19
Evrotrust's role as a Qualified Trust Service Provider enabling compliant reusable identity solutions across Europe.

Introduction

Digital identity sits at the heart of how modern financial institutions operate. From onboarding to authentication, every customer interaction depends on verifying who the user is and whether they can be trusted.

However, as digital channels expand and regulations tighten, the current model of identity management is becoming increasingly inefficient. Most financial institutions rely on fragmented systems that **repeat the same checks across multiple products**, creating high costs, inconsistent experiences, and compliance complexity.

At the same time, banks are under pressure to onboard customers, approve payments, and deliver new digital products with both speed and certainty.

Yet, **even verified users are often asked to complete the same verification steps** each time they open a new account, request a card, or access another service. This repetition slows processes, raises operational costs, and creates unnecessary friction for both customers and internal teams.

Reusable identity addresses this by **turning identity verification from a one-time event into a verified state** that can be trusted across products, channels, and time. Instead of performing multiple KYC checks for the same customer, the bank relies on a verified credential that can be reused securely whenever needed.

70%

lower onboarding costs with automated KYC

(Harvard Business Review, FNZ)

42%

of customers abandon account applications due to onboarding friction

(Liminal)

30s

onboarding for returning customers using reusable identity

(Evrotrust)

The Limits of Traditional Identity Systems

In most banks, **identity infrastructure has grown around individual business lines** rather than the customer journey. Retail banking, cards, and corporate services often operate separate onboarding systems and verification vendors. Each platform collects similar data but stores it in isolation, creating multiple versions of the same customer.

The outcome is **a fragmented identity environment** where information verified once cannot be reused elsewhere. Compliance teams must repeat checks, reconcile mismatched data, and maintain overlapping systems that serve the same purpose. This complexity drives up costs and slows every interaction that depends on verified customer data.

Traditional setups create several recurring challenges:

- Separate onboarding flows across products and regions
- Repeated KYC checks for existing customers
- Inconsistent assurance levels and audit requirements
- Disconnected data that prevents a single customer view

Over time, these issues compound into **measurable business strain.** Onboarding slows, compliance costs rise, and customers lose patience with repetitive processes.

The wider impact is clear:

- Higher drop-off rates and slower approvals for legitimate clients
- Growing vendor and maintenance costs
- Manual effort across compliance and audit teams
- Missed opportunities to reuse verified data for new services

Reusable identity removes these barriers by replacing isolated KYC events with a shared, trusted credential that works across the entire ecosystem. It provides a foundation for faster onboarding, lower costs, and consistent assurance across every channel.

From One-Time Verification to Continuous Trust

Traditional identity systems are built around one-time verification events. Each time a customer interacts with a new product, region, or service, they undergo the same process of document submission, validation, and approval. The result is **a linear, isolated model where verification begins and ends with onboarding.** Once complete, the data sits unused, disconnected from authentication or future interactions.

Reusable identity changes this foundation. It transforms verification from a single checkpoint into a continuous, verifiable state that can be applied across the entire organisation.

Once a user's identity is verified, the resulting credential becomes **a reusable trust asset** that allows the customer to authenticate instantly and securely, without repeating the process.

In the traditional model, **identity verification acts as a cost driver.** Each verification adds vendor fees, manual review time, and audit complexity. In contrast, reusable identity creates long-term value by consolidating verification into one process that can be applied repeatedly. The operational savings grow with every new interaction that uses the same verified credential rather than triggering another full KYC cycle.

From One-Time Verification to Continuous Trust

Feature	Traditional Identity	Reusable Identity
Account Opening Process	Separate flows for each country, product, or business unit. Customers repeat the same verification steps across services.	One-time, unified onboarding that establishes a trusted credential for use across all channels and markets.
Identity Confirmation	Fragmented methods such as passwords and SMS, leading to friction and inconsistent experiences.	Seamless biometric and/or PIN-based authentication that is fast, secure, and consistent everywhere.
Customer Data	Collected all at once, often including unnecessary data and higher processing costs.	Verified attributes are shared only when needed, reducing cost and ensuring privacy compliance.
System Architecture	Multiple vendors, legacy stacks, and manual integrations across departments.	A single, integrated identity layer managed through APIs or SDKs that connects all systems.
Regulatory Assurance	Separate audit trails and inconsistent assurance levels that complicate regulatory reporting.	Centralised, timestamped audit trail aligned with eIDAS, GDPR, AML, and PSD2 requirements.
Customer Experience	Repetitive onboarding steps, broken journeys, and inconsistent login experiences.	Unified customer experience across products and channels with instant, reusable authentication.
Data Governance and Access	Disconnected systems make it difficult to maintain data accuracy or personalise services.	Full attribute-level control with transparent consent management and real-time visibility through APIs.
Scalability	Each market or business line operates its own identity framework, increasing cost and complexity.	One reusable identity layer that scales across products, geographies, and the entire organisation.
Adaptability Across Markets	€10–25* per KYC for retail clients, higher for corporate accounts. Each new product triggers a new verification.	One-time verification cost; subsequent authentications are near zero and fully compliant.

** Based on PwC data*

From One-Time Verification to Continuous Trust

For the customer, the difference is immediate. Traditional systems lead to repeated form filling, document uploads, and long wait times that **disrupt the digital experience.** With reusable identity, verification happens once, and authentication is instant. The experience is faster, more consistent, and fully compliant across products and regions.

For the institution, the benefits extend beyond efficiency. A unified identity layer improves compliance reporting, strengthens fraud prevention, and creates a reliable foundation for innovation. When all services operate from a shared verification framework, data consistency improves, regulatory audits become simpler, and customer trust deepens.

Reusable identity is not an incremental improvement over traditional systems. It represents **a structural redesign of how identity is managed in financial services,** one that replaces repetition with continuity and converts compliance from a recurring task into a sustained state of verified trust.

How Reusable Identity Works

Reusable identity turns verification from a one-time event into a continuous, trusted process that balances compliance, security, and user experience. Once verified, an individual's digital identity becomes **a reusable credential** that can be instantly authenticated across products, channels, and jurisdictions.

The process begins with identity verification and credential creation. Customers complete verification through a trusted method such as eID, biometric scan, or NFC-based document check. The verified data is then converted into a secure digital credential containing key attributes like name, date of birth, and level of assurance. Each credential is cryptographically signed, encrypted, and stored under strict data protection standards to ensure it remains tamper-proof and private.

The verified credential can then be reused across the entire banking ecosystem. When a customer applies for another product or interacts through a different channel, **the organisation validates the existing credential within seconds.** No additional document uploads or manual checks are needed. Authentication occurs through secure token exchange or cryptographic proof, allowing banks to confirm identity instantly while maintaining compliance.

How Reusable Identity Works

For high-risk transactions or sensitive operations, **additional verification steps can be triggered automatically.** This may include biometric re-verification, a one-time password, or multi-factor authentication. The system adapts to the level of risk, ensuring that everyday interactions stay seamless while higher-value actions remain fully protected.

Behind the scenes, reusable identity operates through interoperable frameworks that connect identity providers, financial institutions, and service platforms. Standardised protocols ensure verified credentials can move securely between systems without loss of assurance or privacy. This interoperability allows verified **identities to be recognised and trusted across multiple services and jurisdictions.**

Modern implementations integrate onboarding and authentication within a single process. Banks can collect new attributes only when required for specific regulatory checks, reducing unnecessary costs and improving data accuracy. The result is **a unified, secure identity framework** that supports instant onboarding, consistent authentication, and full compliance across every product, region, and transaction type.

Continuous Compliance for Every Customer Interaction

eIDAS 2.0 and GDPR compliant

Qualified Trust Service Provider status ensures legal validity and data protection across Europe.

Audit-ready records

Every verification and authentication event is logged, timestamped, and instantly accessible for audits.

Attribute-level flexibility

Add or request KYC, AML, or DAC7 attributes on demand without re-verifying customers.

Unified identity across channels

Support every banking product and channel with one compliant, reusable identity framework.

Types of Reusable Identities

Reusable identity can take different forms depending on the trust framework, verification method, and regulatory environment in which it operates. Each model offers varying levels of assurance, interoperability, and user control.

Government-issued digital identities

These are digital versions of official government documents, such as eID cards or mobile IDs. They are issued by national authorities and used to access both public and private sector services. Government-backed systems, like those under the European eIDAS framework, provide the highest legal assurance.

They are typically used for identity verification, electronic signing, and secure access to regulated services. As the European Digital Identity Wallet (EUDI) becomes a standard, **this form of reusable identity will play a key role in cross-border trust** and interoperability.

Bank-based identities

Banks already maintain verified identity data through robust KYC processes. Bank-based reusable identities build on this foundation, allowing customers to use their verified banking identity to access other financial services securely.

This model has gained **strong traction** in countries such as Sweden, Norway, and Finland, where national BankID systems have become trusted digital credentials used across everyday services. It combines strong assurance levels with convenience, positioning banks as central players in the future digital identity ecosystem.

Types of Reusable Identities

Self-sovereign identities (SSI)

Self-sovereign identity frameworks offer a decentralised model where users fully control their verified credentials. Personal data is **stored securely on the individual's device and shared only with explicit consent.** Built on blockchain and cryptographic verification standards, SSI enables tamper-proof, privacy-preserving identity exchange.

Within the EU, the European Blockchain Services Infrastructure (EBSI) supports the adoption of SSI principles, paving the way for transparent and privacy-respecting digital identity systems.

Private sector and platform-based identities

Some reusable identity systems are developed and operated by trusted service providers or industry platforms. These solutions typically **combine onboarding, authentication, and signing capabilities under one framework,** ensuring compliance with eIDAS 2.0, GDPR, and AML regulations.

They are widely adopted in regulated industries such as banking, healthcare, and telecoms, where high assurance and interoperability are essential. Platform-based reusable identity models often serve as bridges between government, banking, and private-sector ecosystems, creating a unified, secure foundation for user verification and authentication across services.

The Reusable Identity Lifecycle

Reusable identity replaces fragmented KYC processes with a connected, secure lifecycle that covers every stage of customer interaction. Each verified credential becomes **a reusable trust asset,** enabling instant authentication and continuous compliance across products, regions, and channels.

The Reusable Identity Flow

1. Create an identity

Customers complete a one-time verification using a trusted method such as eID, biometric scan, or NFC-based ID check.

2. Customise identity attributes

Banks choose which verified attributes to collect, such as address, income, or ownership details, based on regulatory requirements. Additional attributes can be added or updated later without restarting the entire KYC process.

3. Cross-service reuse

Once created, the verified profile works across all products, regions, and channels without re-verification. The customer can authenticate instantly, improving experience and reducing onboarding time.

4. Risk-based verification

For higher-risk actions such as large transactions or cross-border transfers, additional verification is triggered automatically.

5. Own, visualise, and monitor

Banks maintain full control and visibility over identity use across their ecosystem. All verification and authentication events are logged and available for audit, reporting, and compliance reviews.

1. Verification

A customer completes a one-time verification using a trusted method such as eID, biometric scan, or NFC-based ID check. The level of assurance meets eIDAS, AML, and PSD2 requirements, ensuring both legal validity and regulatory compliance.

The Reusable Identity Lifecycle

2. Credential creation

Verified identity data is converted into a secure digital credential containing key attributes such as name, date of birth, and level of assurance. Each credential is encrypted, cryptographically signed, and stored under strict data protection controls to guarantee integrity and privacy.

3. Cross-service reuse

The verified credential can be reused across multiple banking products and channels. When a customer applies for a loan, investment, or new account, the institution validates the existing credential in seconds, no additional document uploads or manual checks are required.

4. Risk-based verification

When transactions require higher assurance, such as large payments or cross-border transfers, the system triggers step-up verification. This may include biometric re-authentication or one-time confirmation, ensuring security without interrupting the user experience.

5. Continuous monitoring and audit

Every verification and authentication event is logged in real time within a unified audit trail. Compliance teams can access timestamped records, export data for regulatory reporting, and maintain full traceability without additional manual work.

The outcome

Reusable identity delivers **a faster, privacy-first verification process** that meets both customer expectations and regulatory obligations. Banks gain a single, compliant identity framework that reduces operational cost, enhances transparency, and strengthens digital trust across their entire ecosystem.

The Challenge of Reusable Identity

Reusable identity promises simplicity, security, and interoperability, but delivering a solution that satisfies both regulators and end users is far from simple. The real challenge lies in aligning compliance, security, and usability across different industries, regulatory environments, and assurance levels.

1. Diverse risk and compliance requirements

Every institution operates under its own risk and compliance framework. Banks, fintechs, and payment providers must meet **stringent AML and KYC regulations,** while other industries face additional frameworks such as DAC7, PSD2, or local tax reporting obligations.

Even within one organisation, assurance requirements vary between onboarding, daily operations, and high-value transactions. A reusable identity system must adapt to each use case while maintaining consistency and integrity.

Key challenge:

Building a flexible identity framework that supports sector-specific compliance without losing standardisation.

2. Securing the verified identity

Each verified credential must be protected against impersonation, tampering, and synthetic identity fraud. Traditional methods such as passwords and SMS codes are vulnerable to interception and spoofing.

Even advanced biometric systems can be manipulated through deepfakes or synthetic media. The strongest **reusable identity models combine biometric verification, liveness detection, and cryptographic proof** to ensure that each credential can only be used by its rightful owner.

Key challenge:

Maintaining continuous assurance of identity authenticity, not only at onboarding.

The Challenge of Reusable Identity

3. Meeting user expectations for privacy and ease

Users expect fast, intuitive verification experiences while retaining full control over their data. They want to reuse their identity across platforms and devices, but they also need transparency on how information is stored and shared.

With increasing concern about data misuse and breaches, confidence in consent management and privacy protection is essential. A successful reusable identity feels seamless to use yet visibly secure and compliant.

Key challenge:

Delivering a frictionless experience while ensuring privacy, consent, and transparency.

4. Achieving true interoperability

Reusable identity depends on collaboration across public and private ecosystems, but today's landscape remains fragmented. Each country and sector uses different protocols, assurance levels, and verification methods.

The European Digital Identity Wallet (EUDI) will help create a shared foundation, yet private-sector systems still need to connect smoothly to national and cross-border infrastructures.

Key challenge:

Enabling interoperability between identity providers, markets, and technologies while maintaining assurance and trust.

5. Building institutional and consumer trust

Reusable identity cannot succeed without mutual trust. Institutions must be confident in credentials issued by others, and users must trust that their data remains secure, private, and under their control.

Transparent governance, clear consent mechanisms, and independent oversight are essential to achieving this trust at scale.

Key challenge:

Establishing confidence among both institutions and users through openness, accountability, and strong governance.

How Reusable Identity Strengthens Banking Operations

Reusable identity solves long-standing challenges in financial services, including **repeated KYC checks, inconsistent compliance, and fragmented customer experiences.** It creates measurable value across the entire organisation by improving efficiency, reducing cost, and reinforcing trust at every stage of the banking lifecycle.

Retail Banking

Retail banks manage large customer volumes and must balance speed, convenience, and compliance. Each product, such as a savings account, credit card, or loan, often relies on **separate onboarding systems and verification flows.** This duplication results in repeated KYC checks, inconsistent experiences, and higher abandonment rates.

Reusable identity allows retail banks to verify customers once and reuse that trusted credential across all products and channels. Onboarding becomes faster and more consistent, while verification costs decrease. Banks report up to 50 percent faster onboarding and higher customer satisfaction driven by simpler digital access.

Corporate and SME Banking

Corporate client onboarding involves multiple verification steps, including ownership validation, signatory checks, and enhanced due diligence. These processes can take weeks and require repeated document submissions. With reusable identity, **verified company data and ownership details can be securely reused** across accounts, lending, and compliance reviews.

Manual work is reduced, document collection becomes simpler, and approval times improve. Relationship managers spend more time on client engagement rather than

Payments and Fintech Partnerships

In payments and embedded finance, each new integration or partnership typically requires a separate KYC or AML process. This slows deployment and adds unnecessary complexity to the customer journey.

Reusable identity introduces **a shared verification layer** that both banks and fintech partners can trust. Once verified, users can access connected services instantly without additional checks. This shared infrastructure shortens integration timelines, maintains compliance, and ensures a consistent experience across partner ecosystems.

How Reusable Identity Strengthens Banking Operations

Private Banking and Wealth Management

High-net-worth clients often use multiple products and advisors across a single institution. Traditional verification processes require **repeated checks for identity, income, or source of funds** for each new service.

With reusable identity, verified client profiles are continuously updated and reused across all services. Advisors can access a single, compliant view of each client, while new verifications are triggered only when required. This approach enhances operational efficiency and delivers a premium, frictionless client experience.

Compliance, Risk, and Audit

Compliance and risk teams frequently deal with fragmented records and duplicated verification data. Manual reviews and audit preparation consume time and resources that could be spent on higher-value oversight.

Reusable identity **consolidates all verification and authentication events into a single, timestamped audit trail.** It aligns directly with eIDAS 2.0, GDPR, and AMLD6 standards, streamlining reporting and improving transparency. Compliance teams gain visibility, regulators receive consistent evidence, and audit cycles become significantly shorter.

Technology and Operations

Many banks still operate separate identity tools across regions and departments, increasing maintenance costs and creating inconsistent assurance levels.

Reusable identity introduces **a unified identity layer that integrates through APIs or SDKs.** It simplifies vendor management, standardises verification, and ensures consistent compliance across the organisation. IT and operations teams benefit from a scalable infrastructure that supports faster product launches and reduces technical debt.

Conclusion

The financial sector is moving toward **a new standard for digital trust.** Reusable identity is no longer a theoretical improvement. It is becoming an operational necessity for banks that need to meet regulatory expectations, reduce costs, and deliver a faster customer experience.

By replacing repeated verification cycles with a single reusable credential, financial institutions can achieve both compliance and speed at scale. This model simplifies audit readiness, strengthens fraud prevention, and gives customers the seamless access they expect from modern digital services.

Banks that adopt reusable identity now will gain a competitive advantage in readiness for eIDAS 2.0 and the European Digital Identity Wallet. Beyond compliance, they will establish a unified identity foundation that supports cross-border growth, faster onboarding, and more efficient internal operations.

Reusable identity represents **a structural shift in how trust is managed in banking.** It turns compliance into continuity and identity verification into a long-term asset that enables institutions to operate with confidence, consistency, and speed in an increasingly interconnected financial ecosystem.

Reusable identity redefines how banks verify and trust customers.

A single, compliant identity layer that brings speed, security, and consistency to every product, market, and customer journey.

Evrotrust provides the trusted digital foundation for regulated industries across Europe.

Aligned with eIDAS 2.0, GDPR, and AMLD6, our qualified trust services enable financial institutions to move faster, reduce compliance complexity, and deliver secure, seamless digital experiences.

One identity. One process. Infinite reuse. Build trust that works across every market.

Global leader in digital identity and trust services

1 800 000 +
Registered end users within the Evrotrust ecosystem

21 000 000 +
e-Signatures consumed through our ecosystem

95 %
Average pass rate

300 %
Average yearly digital revenue growth for our clients

12x
Faster than legacy process

2 mins
For a customer to have reusable verified identity

Trusted By Some of EU's Biggest Banks:

"Evrotrust helped us achieve a **15x cost reduction** in new customer acquisition with a fully remote process."

Join a community of **150+** clients around the globe serving **1 800 000+** users from **63** nationalities!

Sign Up for a Free Consultation or Live Demo