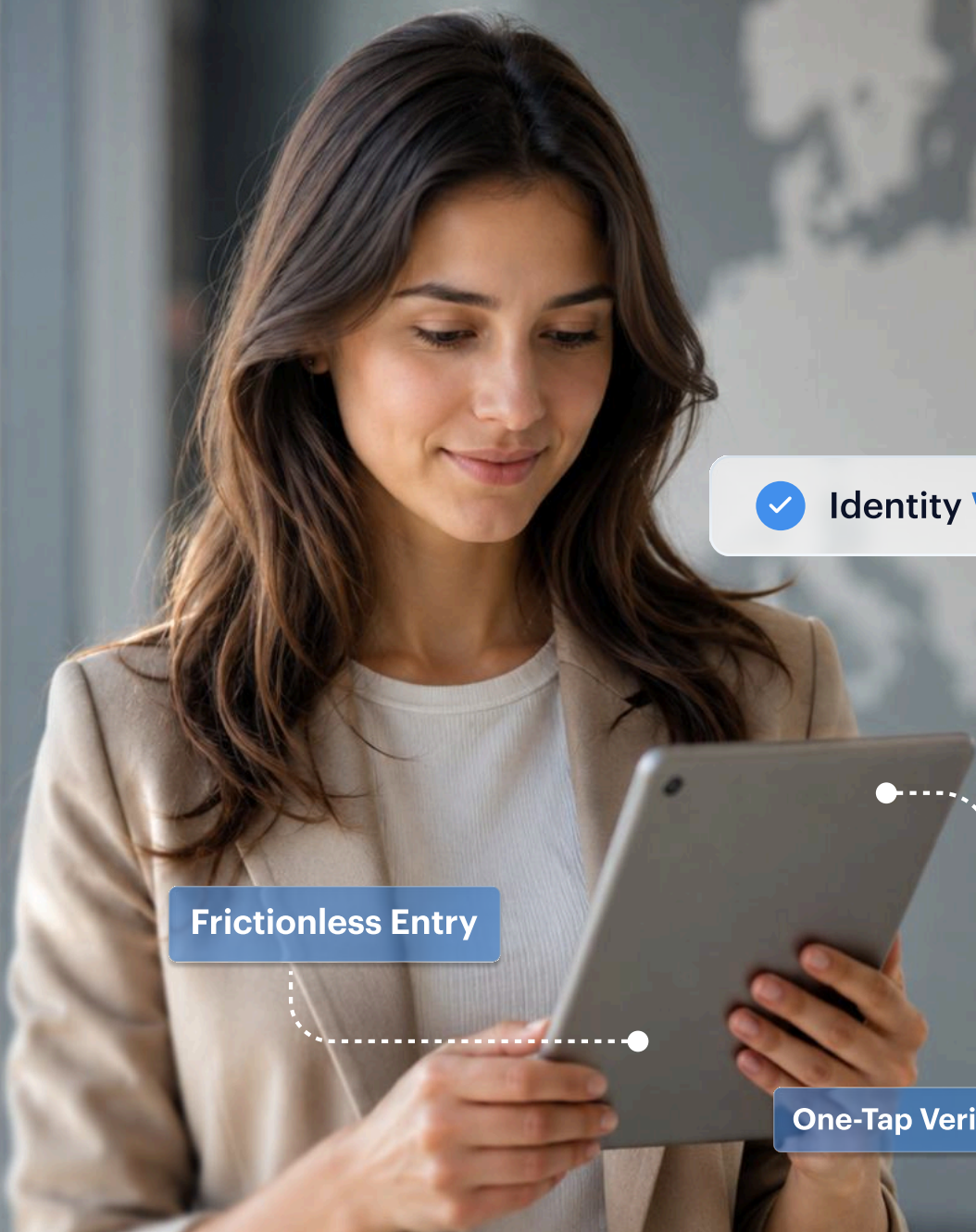


The Future of Docless Verification in Europe

How eIDs, Digital Identity Wallets, and Trusted Data Sources Are Helping
Businesses Onboard More Customers with Less Friction



✓ Identity Verified

Frictionless Entry

One-Tap Verification



VÉRIFICATION
D'ÂGE KJM



PCI DSS



iBeta Niveau 1



ISO 27001: 2013



CE+



QG GDPR



SOC2



GDPR



CCPA



Table of Contents

Navigating the Challenge of KYC Compliance and Business Conversion	01
The Next Phase of European Digital Identity	03
Risk-Based Orchestration: Using the Right Format of Docless Verification	06
How Shufti Empowers Docless Verification with Higher Level of Assurance in Authentication	08
The Infrastructure for the European Union's Doc-less Identity Verification Layer	10
Provider Evaluation: Choosing the Right eID Provider across the European Union	12
References and Citations	15

Executive Summary

European regulated businesses are navigating three converging pressures that are reshaping digital onboarding.

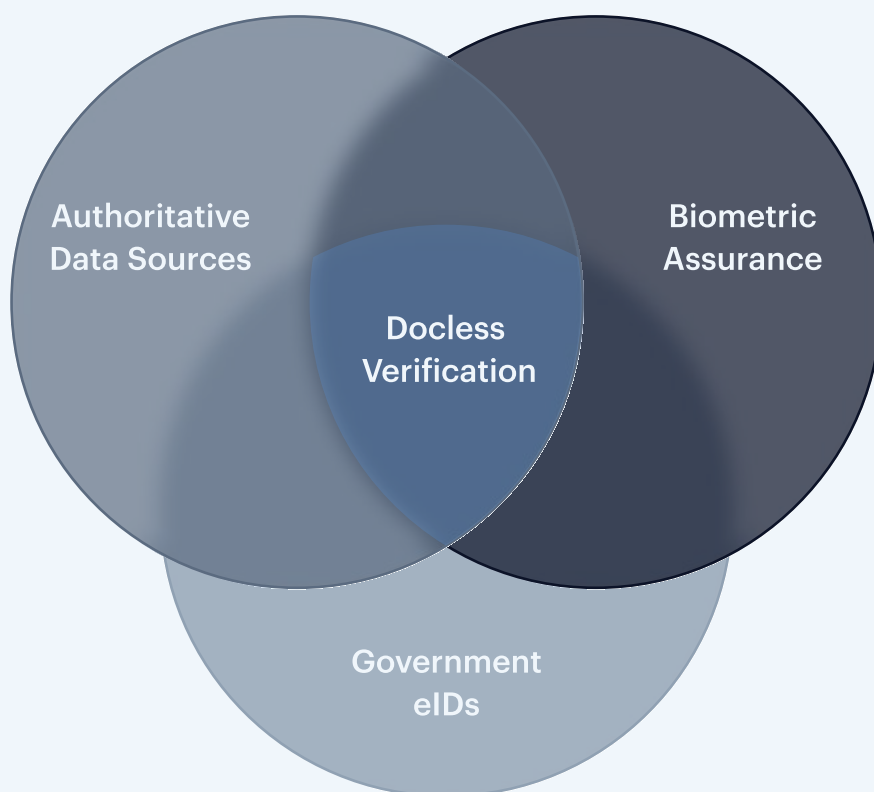
The first is commercial. The digital native users expect onboarding journeys to be completed in minutes, not forms, document uploads, and repeated verification steps. Research consistently shows that onboarding friction directly impacts conversion, with nearly half of prospective customers abandoning digital onboarding journeys when the process becomes too lengthy or cumbersome.

The second is regulatory. Across Europe, electronic identity verification is becoming foundational infrastructure. National eID schemes such as BankID, MitID, SPID, DigiD, and itsme etc. already enable millions of citizens to authenticate and verify their identities digitally, while eIDAS 2.0 mandated European Digital Identity Wallet which will become mandatory by end of 2027 are accelerating the shift towards reusable, government-backed digital credentials for coming years.

The third one is the assurance. Verifying that data retrieved from an authoritative database or even government backed digital identity is genuine is no longer sufficient. Businesses must also establish that the person presenting that credential is its legitimate owner. As synthetic identities, deepfakes, presentation attacks, and injection attacks become increasingly sophisticated, even trusted digital identity credentials require biometric identity binding capable of confirming real-time user presence and detecting advanced forms of impersonation.

These pressures compound rather than cancel each other. Businesses must reduce onboarding friction, support Europe's rapidly expanding digital identity ecosystem, and satisfy increasingly demanding assurance requirements at the same time. Docless verification can address all three challenges simultaneously by combining authoritative data-source verification and government-backed eIDs with independently audited biometric assurance, enabling faster onboarding, stronger identity confidence, and regulatory readiness through a single identity infrastructure layer.

DOCLESS VERIFICATION — WHERE THREE PILLARS CONVERGE



Docless verification sits at the intersection of authoritative data-source verification, government-backed eIDs, and biometric assurance.

Three Questions This Guide Answers

1. How does friction in customer onboarding create measurable revenue loss?
2. How does docless verification ensure the frictionless customer onboarding while ensuring compliance?
3. What does a complete docless verification capability look like, and what criteria should drive provider evaluation?

Navigating the Challenge of KYC Compliance and Business Conversion

European regulated businesses are navigating two converging pressures that directly affect compliance standing and commercial performance.

The first one is ensuring customer conversion.

Europe's digital economy has grown to a scale at which remote customer onboarding friction translates immediately into lost revenue. Eurostat's 2025 Digitalisation in Europe report confirms that 72% of EU internet users now use online banking services, up from 56% in 2014, and that 75% of EU individuals bought goods or services online in 2023. With 94% of EU individuals using the internet in 2025 and nearly 9 in 10 accessing it via mobile devices, regulated digital platforms are onboarding at volumes and velocities that demand an identity layer that does not create bottlenecks.

The second one is ensuring compliance with KYC regulations to make sure that the legitimate user is onboarded. The threat environment has shifted, with AI-generated deepfakes and synthetic identity attacks requiring a more sophisticated verification response than was necessary five years ago.

This guide walks European businesses through how docless verification in the form of eIDAS-compliant electronic identity verification, enables higher customer acquisition while simultaneously ensuring a higher level of assurance in the remote customer onboarding process.

Onboarding Friction Is a Measurable Revenue Problem

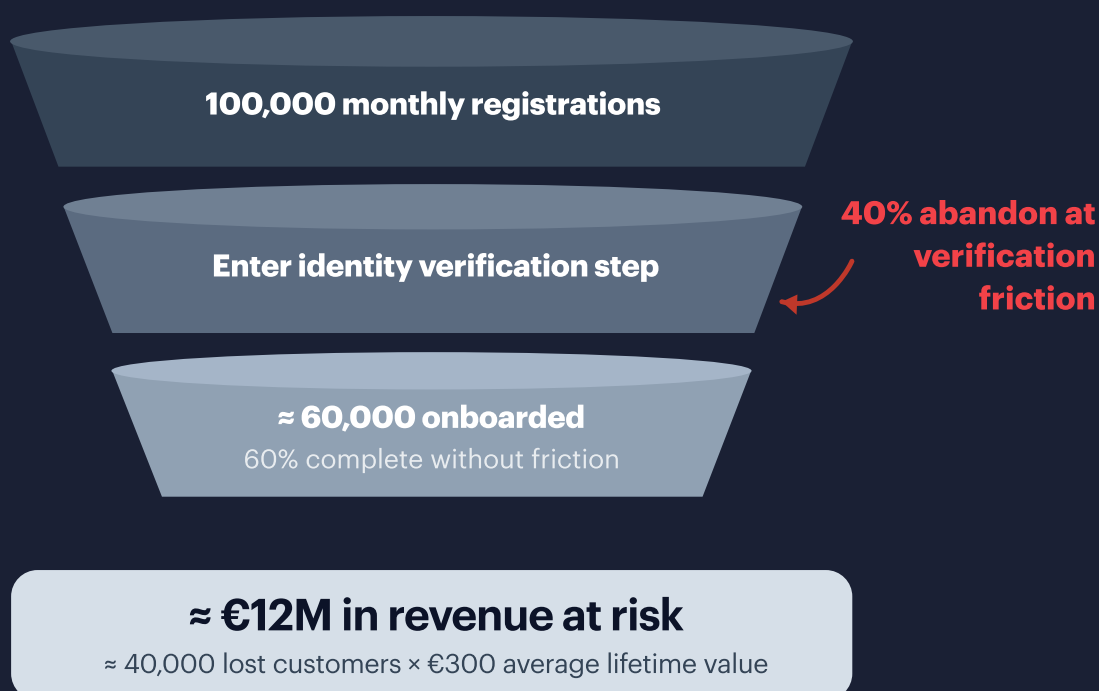
Capgemini's 2025 World Retail Banking Report found that 47% of prospective customers abandon digital onboarding mid-process, with the primary cause being manual friction that document-heavy flows introduce.

Deloitte research found that 38% of customers abandon the process due to the volume of information required, and a PwC survey found that nearly 60% would abandon a banking application if it was too lengthy or cumbersome.

TO ILLUSTRATE THE REVENUE SCALE

€12M in potential annual revenue

A regulated platform processing 100,000 monthly registrations with an average customer lifetime value of €300 and a 40% abandonment rate attributable to verification friction is forfeiting approximately €12 million in potential annual revenue.



Fraud Is Escalating Specifically at the Remote Onboarding Stage

Account creation has become the highest-risk stage across the entire consumer lifecycle.

According to Shufti's Internal verification data overall [deepfake powered identity fraud](#) is likely to surge upto 495% by the end of 2026 and this takes into account document deepfakes and synthetic IDs.

While these numbers represent the most recent state of Identity fraud due to democratization of deepfake tools, EU laws have been very clear on how the risk should be taken into account while doing the remote Verification.

European businesses subject to remote identity verification are governed by EBA/GL/2022/15, which has applied across all EU member states since 2 October 2023. The guidelines were issued because the 5th AML Directive left remote identification defined differently in each member state, creating compliance fragmentation and regulatory gaps that financial crime exploited.

Risk-sensitive customer due diligence. Verification depth must correspond to the actual risk level of each customer. Institutions are explicitly permitted to rely on notified eID schemes operating at substantial or high Levels of Assurance under the eIDAS Regulation, allowing them to leverage trusted national digital identity frameworks as part of their remote onboarding controls.

Confirmed presence and identity binding. A mandatory liveness check must confirm the user is present in the session in real time. The business must further satisfy itself that the individual presenting the identity is its genuine owner — ruling out replays, masks, or AI-generated substitutes. Where the risk profile warrants it, reliability must be increased through biometric data capture compared against independently sourced data.

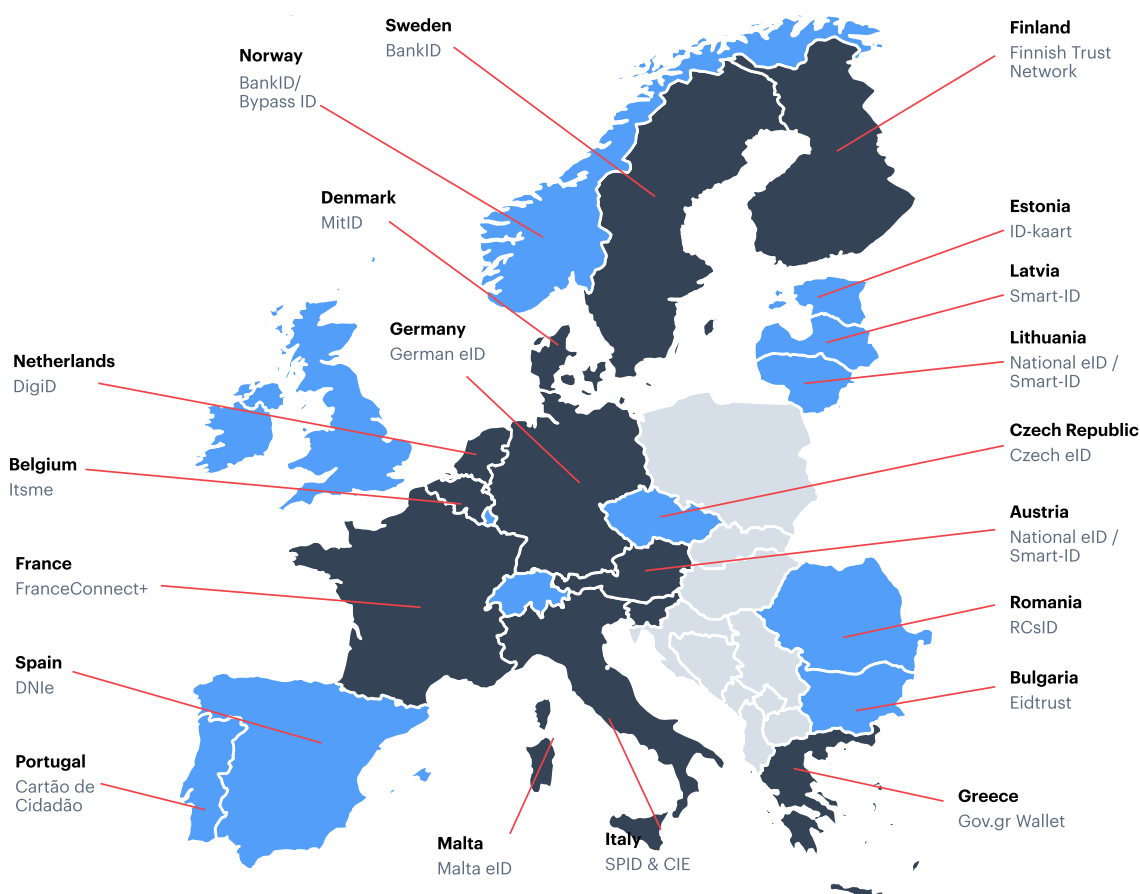
Your Users Are Already Verifying with eIDs. Your Infrastructure Needs to Support It.

Reusable Identity verification through eIDs is already very common across the EU. The businesses only need the infrastructure and the right solutions that support verification through these and hence enable smooth customer onboarding. The European Commission's 2030 Digital Decade target states that 80% of EU citizens should be using a digital ID solution by 2030, and adoption is already well ahead of that trajectory in several major markets.

The question is not whether to support eID verification. That decision has been made by your users and by regulation. The question is whether your Identity Verification Provider is capable of providing a verification through these eIDs using a single platform.

The European eID Ecosystem at a Glance

To understand why docless verification is becoming foundational infrastructure across Europe, it is useful to understand the identity ecosystem that has formed beneath it. Each EU member state has developed its own national digital identity scheme, and those schemes collectively cover hundreds of millions of verified citizens.



National eID schemes across Europe. Navy denotes labelled national schemes; lighter shading denotes additional eID coverage.

An overview of digital identity schemes in some of the European Economies.

Country	Scheme	Key Facts
Sweden	BankID	8.6 million active users, 99.9% of adults 18-67. 7.6 billion authentications in 2024, accepted by 7,500 services.
Denmark	MitID	97% penetration among residents 15+. Primary authentication for banking, tax, healthcare, and regulated services.
Italy	SPID & CIE	SPID has exceeded 36 million registered users. CIE is the government-backed electronic identity card.
Netherlands	DigiD	Near-universal penetration. Used for government, healthcare, and financial services access.
Belgium	itsme	6 million+ verified users across banking, insurance, government, and regulated onboarding.
Greece	Gov.gr Wallet	Government digital identity infrastructure providing citizens with access to government services and digital credentials.
France	FranceConnect+	Operates at substantial and high assurance levels under eIDAS. Used to access government and regulated services.
Austria	ID Austria	National digital identity system providing government-backed credentials for public services and regulated sector access.
Germany	German eID	Embedded in national identity card. Supported via AusweisApp infrastructure, operating at high assurance under eIDAS.
Baltics	Smart-ID	Leading digital identity solution across Estonia, Latvia, and Lithuania. Government-backed eID across the Baltic states.
Finland	Finnish Trust Network	Aggregates authentication from Finnish banks and telecommunications operators as national identity infrastructure.

What this ecosystem map reveals is that docless verification through national eID schemes is not a future capability. It is the current reality for the majority of Europe's digitally active population. A regulated business operating across multiple EU markets without eID acceptance capability is creating friction at exactly the point where users have already been verified by their national government.

eIDAS 2.0 and EUDI Wallet: How to Prepare Your Business for Acceptance

Regulation EU 2024/1183, entered into force 20 May 2024, establishes a mandatory acceptance obligation. Every EU member state is required to issue a European Digital Identity Wallet to citizens by December 2026. From late 2027, regulated relying parties — including banks, financial services providers, payment institutions, and regulated digital platforms, are required to accept those wallets as a valid method of identity verification.

Under eIDAS 2.0, the wallet is not simply another digital identity credential. It is a government-issued portable identity container that citizens can use to share verified attributes, name, date of birth, nationality, age confirmation, professional qualifications, and other government-held data, with regulated services, without sharing unnecessary personal information beyond what the transaction requires.

Identity Binding for EUDI Wallet

Commission Implementing Regulation (EU) 2026/798, published 8 April 2026, establishes the technical framework for remote onboarding of users onto EUDI Wallets.

The regulation defines remote user onboarding as a crucial step in binding a user's personal identification data to their wallet and to their device, and makes clear that a reasonably reliable identity input is not sufficient on its own. The overall process must be reinforced through additional remote onboarding procedures until the combined result satisfies the high assurance level.

This implies that a user onboarding through the EUDI Wallet in future should undergo rigorous liveness detection to ensure that the same person who was enrolled is also the one who is being onboarded.

What This Means for Businesses Accepting EUDI Wallets in Future

The organisations that will integrate EUDI Wallet acceptance most efficiently in 2027 are those that have already partnered with a provider who has built the required infrastructure: active eIDV for receiving government-backed identity attestations, biometric liveness detection for higher level of assurance in customer verification and a single API architecture that can accommodate new identity schemes as they are certified by the government. A programme built on document capture alone will require a more fundamental rebuild.

The Next Phase of European Digital Identity

The Convergence of Identity, Authentication, and Trust Services

For more than a decade, European organisations have treated identity verification, authentication, and electronic signatures as separate technology categories.

Identity verification was used to satisfy customer due diligence obligations. Authentication confirmed access to an account or service. Electronic signatures enabled legally binding transactions. Each capability was typically procured, integrated, and managed independently.

eIDAS 2.0 is beginning to dissolve those boundaries.

The emergence of national eID schemes, the European Digital Identity Wallet, high-assurance biometric identity binding requirements, and Qualified Electronic Signatures is creating a single trust ecosystem in which identity, authentication, attribute sharing, and transaction authorisation operate together rather than separately.

A typical customer journey in the coming years will increasingly follow a single trust flow:

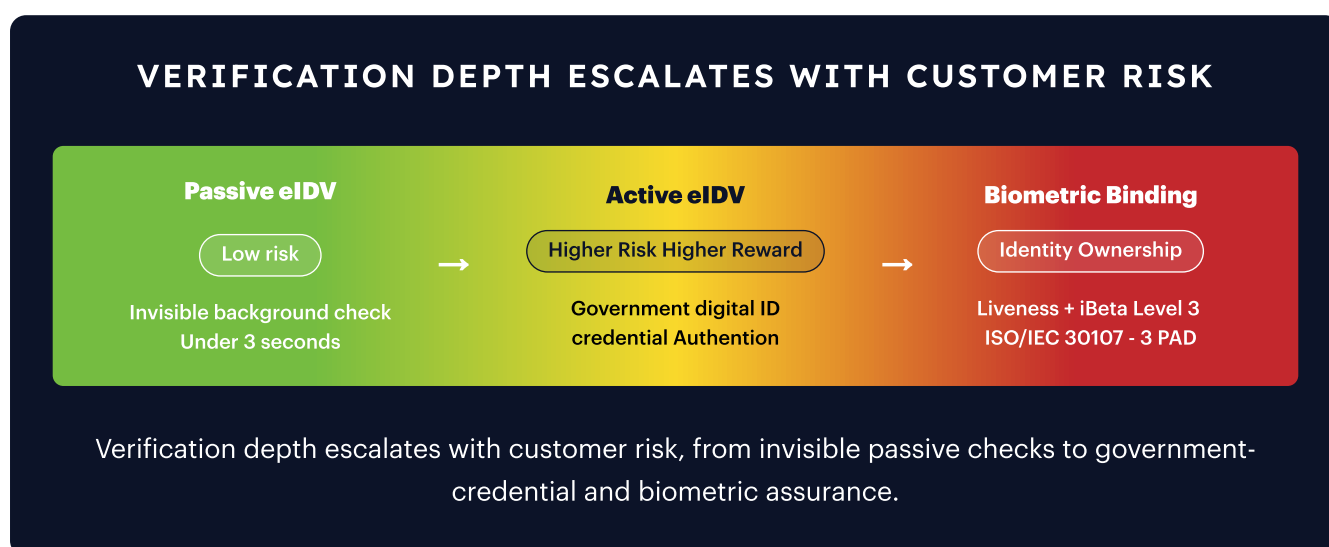
- 1. Identity Verification.** A customer's identity is verified against an authoritative data source of government-backed digital identity credential. The customer authenticates using a trusted national eID scheme such as BankID, MitID, SPID, DigiD, itsme, FranceConnect+, or a future EUDI Wallet credential.
- 2. Identity Binding.** Biometric verification confirms that the individual presenting the credential is its legitimate holder, satisfying high-assurance requirements for remote onboarding.
- 3. Legally Binding Consent and Signing.** Transactions are completed using electronic signatures, including Qualified Electronic Signatures where regulatory certainty or evidentiary strength is required.

Viewed individually, these capabilities appear to be separate products. Viewed through the lens of eIDAS 2.0, they form a single trust infrastructure.

This shift has important implications for identity verification provider selection. Organisations that continue integrating separate point solutions for identity verification, biometric assurance, wallet acceptance, and trust services may face increasing operational complexity as new regulatory requirements emerge. Organisations that adopt a unified trust architecture are better positioned to accommodate future identity schemes, EUDI Wallet deployment, and evolving assurance requirements without repeated integration projects.

Risk-Based Orchestration: Using the Right Format of Docless Verification

The most effective docless verification flows do not apply the same process to every customer. They match verification depth to customer risk, running a lighter check for low-risk users and escalating only when the risk profile warrants it. This is risk-based orchestration, and it is the architecture that makes docless verification both commercially viable and compliance-grade simultaneously.

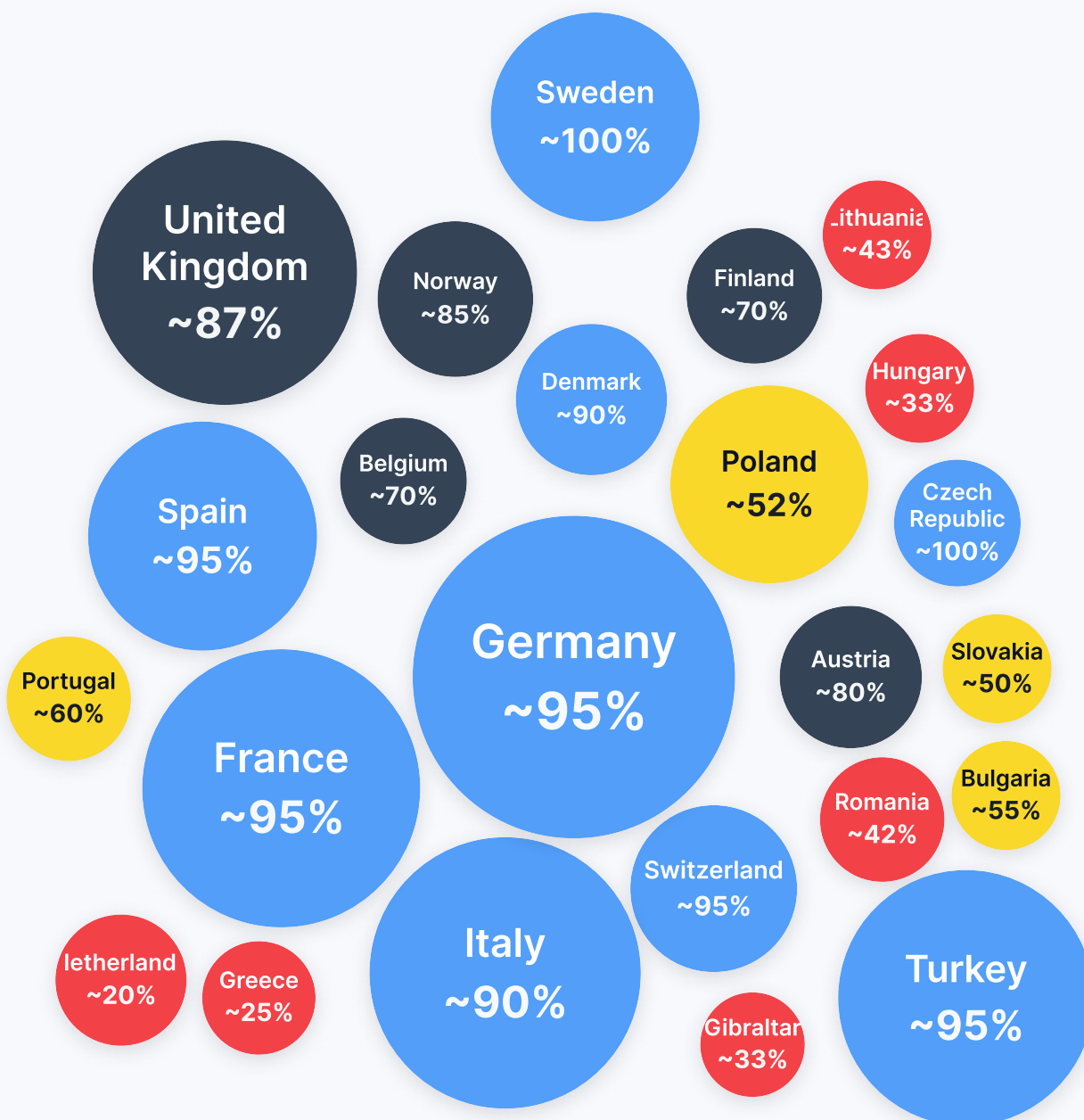
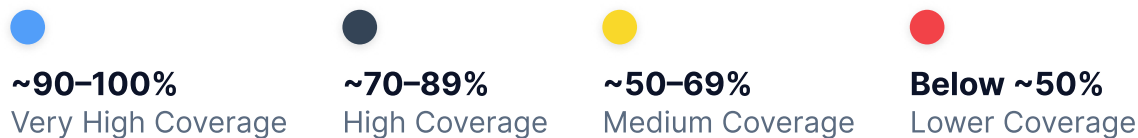


Passive Docless Verification- Frictionless Onboarding for Low Risk Sectors

While eIDs and digital identity wallets represent the future of customer verification in Europe, businesses need verification coverage today. The reality is that eID availability, adoption, and customer readiness vary significantly across markets. Passive docless verification helps bridge this gap by enabling identity verification through trusted government, telecom, credit, utility, and consumer data sources without requiring customers to present documents or authenticate through an eID. As a result, organisations can deliver broader verification coverage, reduce onboarding friction, and create a smoother path towards future digital identity frameworks without sacrificing customer experience or compliance.

European eID Population Coverage

Estimated adult population coverage by digital identity scheme across Europe



The above map shows the Shufti's Passive IDV coverage.

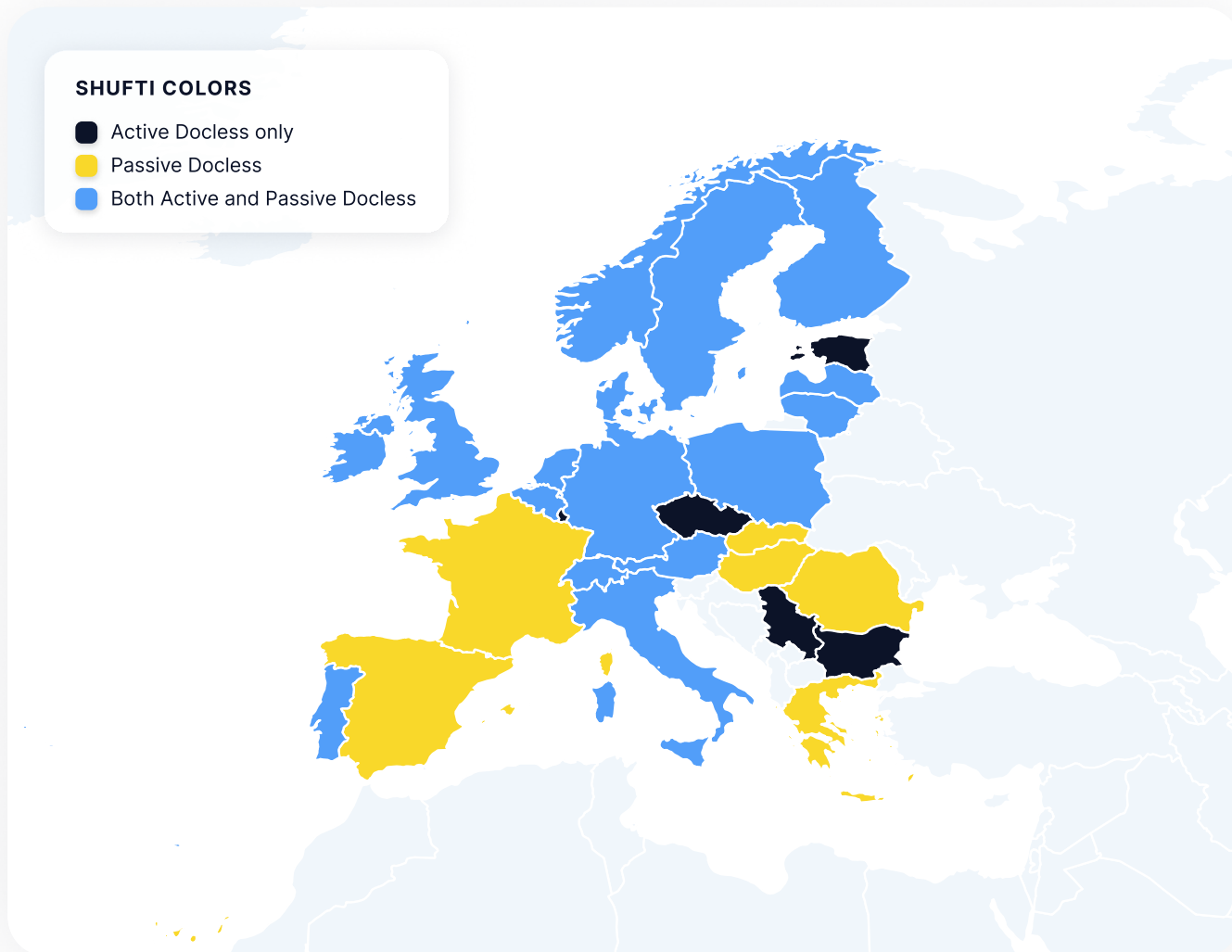
Active Docless Verification: Frictionless Onboarding for Higher Risk Sectors

For higher-risk scenarios, the flow escalates to active eIDV, where the user authenticates using a government-issued digital identity credential they already hold. The platform receives a government-backed confirmation at the highest available assurance level.



The correct approach is configurable escalation, matching the verification method to what each customer's risk profile actually requires:

Risk Level	Method	User Experience	Assurance Achieved
Low risk	Passive eIDV	Invisible, under 3 seconds	Identity confirmed against live authoritative data including non-government sources
High risk / high value	Active eIDV	One authentication step via government digital identity credential	Government-backed confirmation; age confirmed where applicable



Liveness Detection for Higher Level of Assurance in Remote Identity Verification

Even in a well-designed docless verification flow, one challenge remains: confirming that the identity attributes presented are being submitted by the person who genuinely owns them, rather than by someone who has obtained those details through a data breach, social engineering, or synthetic identity construction. This is the identity ownership problem, and it is where biometric assurance enters the flow.

Synthetic identity construction is the fastest-growing fraud category at the onboarding stage and one that document-based verification is not structurally equipped to catch.

When liveness detection is added to a docless flow, the user completes a brief facial capture. The benchmark that matters include, iBeta Level 3 conformance under ISO/IEC 30107-3 — which is independent laboratory testing using expert human attackers, extended breach attempt periods, and explicitly includes AI-generated face attacks. Very few providers globally hold Level 3 conformance.

WHAT IBETA LEVEL 3 CONFORMANCE MEANS

iBeta Level 3 conformance under ISO/IEC 30107-3 is conducted by an independent test laboratory using expert human attackers, no budget constraints, extended attempt periods, and AI-generated face attacks. It is the highest independently audited standard for liveness attack detection globally. The assurance delivered is not a self-claimed accuracy rate, it is an audited result against the most sophisticated attacks currently available.

How Shufti Empowers Docless Verification with Higher Level of Assurance in Authentication

Shufti's docless verification capability operates across two assurance pathways depending on the market. In major European economies, Shufti accepts credentials from national eID schemes and bank-backed identity providers where biometric authentication is completed on the user's own device by the issuing scheme — delivering a higher level of assurance without requiring a separate document upload or selfie capture. In select markets, Shufti goes further, integrating with government-issued eIDs where biometric verification is returned directly, delivering the highest level of identity assurance available in remote onboarding. In both cases, the business receives an identity input that satisfies the identity binding requirements.

Markets where docless verification with direct biometric verification is available: Belgium, Estonia, Lithuania, United Kingdom.

Markets where docless verification with on-device biometric authentication is available: Denmark, Sweden, Norway, Netherlands, Finland, Germany, Austria, Poland, Italy, Bulgaria, Czech Republic, Switzerland, Ukraine.

Countries where government eIDs are available: Austria, Poland, Italy, Bulgaria.

Countries where both government and commercial eIDs are available: Belgium, Estonia, Latvia, Lithuania, United Kingdom.

Countries where commercial eIDs (bank eIDs) are available: Denmark, Norway, Sweden, Finland, Netherlands, Germany, Czech Republic, Switzerland, Ukraine.

The Infrastructure for the European Union's Docless Identity Verification Layer

The requirements described across this guide describe a platform designed as a complete infrastructure layer rather than a collection of point solutions. The distinction matters because the European identity landscape is not static, national eID schemes are expanding, the EUDI Wallet is moving from specification to deployment, and EU 2026/798 has raised the assurance bar for remote onboarding. A provider built on third-party components updates when its suppliers do. A provider that owns its stack updates when the threat or the regulation requires it.

Shufti was built as that infrastructure. Its OCR, liveness detection, deepfake detection, and document intelligence are built and owned by Shufti rather than licensed from subprocessors.

ONE PLATFORM, BUILT END TO END

Active eIDV, passive eIDV, iBeta Level 3 liveness detection, deepfake defence, age verification, and Qualified Electronic Signatures, through a single API, configurable to each customer's actual risk level. No third-party dependencies on the critical verification path.

European eID coverage. Shufti's Docless solution covers more than 30 countries through passive verification. Active eIDV supports BankID, MitID, SPID and CIE, DigiD, itsme, Gov.gr, FranceConnect Plus, and the German eID. A single API returns a consistent result schema regardless of which source resolved the verification.

Verification depth configured to each customer. The operator defines the confidence threshold at which the system escalates from passive eIDV to active eIDV, and from active eIDV to biometric assurance, delivering only the verification depth each customer's risk profile warrants.

iBeta Level 3 liveness and deepfake defence. Shufti's liveness engine holds [iBeta Level 3](#) conformance under ISO/IEC 30107-3, built and owned by Shufti, not licensed from a third-party provider. Deepfake detection is trained against current-generation AI attack methods and updated on Shufti's own development schedule, satisfying identity binding requirements under EU 2026/798.

Age verification and trust services. Hard age confirmation via live government and data-source date-of-birth matching is available within the same API call, covering GlüStV 2021, MGA, ANJ, and DSA Article 28 without a separate verification event. Shufti supports Qualified Electronic Signatures under eIDAS 2.0 and is positioned as an acceptance-layer partner for EUDI Wallets ahead of the late 2027 obligation.

Deployment for data residency requirements. Cloud, Local Cloud in EU region for GDPR data localisation, and on-premises for full data sovereignty obligations.

Access

450+ Million

Pre-Verified Digital Identities Across the European Union with Shufti's Docless Verification

Infrastructure for Frictionless Onboarding Exists. You Need the Right Identity Verification Service Provider to Support It.

European regulated businesses do not need to build docless verification infrastructure from scratch. The eID schemes are live, the regulatory framework is set, and the verification capability already exists. What matters is choosing a provider who has already built it end to end.

The right provider gives your business passive docless that verifies identity using government and commercial databases invisibly, active docless that accepts the government credentials your customers already carry, liveness detection at the highest independently audited standard for cases that require it, and a single API that handles all of it without redirects or separate integrations.

For European businesses that need to onboard customers quickly and compliantly, the question is not whether to adopt docless verification. It is whether your current provider is already capable of delivering it across the markets you operate in and it is equipped with eID coverage, Qualified Electronic Signatures capability and also future ready for EUDI Wallet so that your business can adopt without rebuilding from scratch.

Provider Evaluation: Choosing the Right eID Provider across the European Union

Selecting a docless verification provider is an infrastructure decision whose consequences extend well beyond the initial integration. Use this checklist to evaluate whether a provider meets the full requirements of European regulated businesses.

COVERAGE

- ☐ The provider supports active eIDV via national government-issued digital identity credentials across all major EU markets, not only BankID and MitID but also the growing ecosystems in Italy, the Netherlands, Belgium, Greece, France, Germany, Austria, Finland, Baltics and the rest of EU eIDs for Active docless verification?
- ☐ The provider offers passive data-source verification across European countries, drawing on both government and non-government authoritative sources.
- ☐ The resolution rate per market, the proportion of users successfully verified without document escalation, can be demonstrated specifically, not just headline country coverage.
- ☐ A single API returns a consistent result schema across all markets and verification methods.
- ☐ Age verification via live government or data-source date-of-birth confirmation is available within the same API call.
- ☐ Does solution offer 1X1 and 2X2 for speed and dual source to cross reference data?

ASSURANCE LEVEL

- ☐ The provider holds iBeta Level 3 conformance under ISO/IEC 30107-3 for liveness detection, the only independently audited standard that explicitly tests against AI-generated face attacks at the level of sophistication now in operational use.
- ☐ Deepfake detection is built and updated by the provider on its own development timeline, not licensed from a third-party model that the provider cannot update independently.
- ☐ Liveness detection runs within the same user session without redirecting the customer.

RISK CALIBRATION

- ☐ Verification depth is configurable by customer segment, with operator-defined confidence thresholds at each escalation point.
- ☐ The system escalates automatically within the session when a risk signal appears mid-flow.

REGULATORY ALIGNMENT

- ☐ The provider can demonstrate that docless output satisfies AMLA CDD requirements and national age verification obligations in a single result.
- ☐ The provider is positioned for EUDI Wallet acceptance ahead of late 2027 and can demonstrate readiness for identity binding requirements under EU 2026/798.
- ☐ The provider supports or has a clear roadmap toward Qualified Electronic Signatures under eIDAS 2.0.

DATA RESIDENCY AND DEPLOYMENT

- ☐ In-region deployment is available for EU clients with GDPR data localisation requirements.
- ☐ On-premises deployment is available for organisations with full data sovereignty obligations.

References and Citations

1. Eurostat (2025). Digitalisation in Europe 2025. European Commission.
 2. Capgemini (2025). World Retail Banking Report 2025. Capgemini Research Institute.
 3. Deloitte. Digital Banking Maturity Study. Deloitte Insights.
 4. PwC. Financial Services Technology Survey. PricewaterhouseCoopers.
 5. McKinsey & Company. The value of getting personalization right or wrong is multiplying. McKinsey Global Institute.
 6. TransUnion (2026). H1 2026 Fraud Trends Report. TransUnion LLC.
 7. European Banking Authority (EBA). Guidelines on the use of remote customer onboarding solutions (EBA/GL/2022/15). EBA.
 8. European Commission (2024). Regulation (EU) 2024/1183 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union.
 9. European Commission (2026). Commission Implementing Regulation (EU) 2026/798 of 8 April 2026. Official Journal of the European Union.
 10. European Commission (2023). 2030 Digital Decade Policy Programme. European Commission.
 11. BankID (2024). BankID Annual Statistics 2024. Finansiell ID-Teknik BID AB.
 12. iBeta Quality Assurance. Presentation Attack Detection (PAD) Testing under ISO/IEC 30107-3. iBeta.
-



The Right Provider Has Already Built It

The eID schemes are live, the regulatory framework is set, and the verification capability already exists. The right provider gives your business passive docless that verifies identity invisibly, active docless that accepts the government credentials your customers already carry, liveness detection at the highest independently audited standard, and a single API that handles all of it.

[Request a Docless Verification Demo](#)

shuftipro.com
sales@shuftipro.com

