Shufti

BUYER'S GUIDE

Strategic ID Verification Vendor for Crypto Industry

PCI DSS | SOC2 | GDPR | QG GDPR | ISO 27001: 2013 | CE+ | iBeta 2 | VÉRIFICATION D'ÂGE KJM | CCPA

Executive Summary

Effective identity verification for KYC Compliance requires maintaining a delicate balance between the False Acceptance Rate (FAR) and False Rejection Rate (FRR). **Striking this balance ensures that genuine users are verified seamlessly while fraudulent actors are accurately identified and blocked.** Yet, achieving this equilibrium across diverse markets, risk profiles, and regulatory frameworks remains a significant challenge. This makes it essential for organizations, particularly those operating in high-risk sectors such as crypto exchanges, to adopt a risk-based approach that dynamically adjusts verification logic according to jurisdiction-specific risks

A risk-based compliance model empowers businesses to assess and manage varying levels of exposure based on applicant profiles, transaction behavior, and regional regulatory expectations. Crypto exchanges can reduce the costs incurred due to onboarding friction by adopting a risk-based approach in the identity verification workflow. This adaptive framework enables firms to align with FATF guidelines, strengthen AML/CFT programs, and maintain a defensible audit trail for regulatory scrutiny.

For crypto exchanges, a risk-based approach by jurisdiction makes sense. Stringent checks for every user are unnecessary; most flows can start light and step up only when risk increases, for example, in higher-risk countries or for large trades or withdrawals. This meets local rules, reduces friction, and keeps genuine users moving. This flexibility is achievable only with a Crypto IDV solution that allows for quick in-house customization and avoids reliance on third-party technology. And this is the key to keeping compliance and revenue teams on the same page.

Balancing Compliance and User Experience Through Risk-Based Verification

Robert Frost once wrote, "Two roads diverged in a yellow wood, and I took the one less travelled by."

Crypto exchanges often find themselves at a crossroads, balancing strict regulatory compliance with the need for a seamless customer experience. Regulators such as the FCA (UK), FinCEN (US), and ESMA (EU) mandate rigorous AML and CFT standards that require advanced, reliable identity verification processes. At the same time, users expect quick, frictionless onboarding experiences.

Traditional systems often force businesses to choose between compliance and convenience, resulting in operational inefficiencies, frustrated users, and potential regulatory risk. The answer lies not in choosing one over the other, but in building a bridge between them through a risk-based identity verification (IDV) framework that intelligently adapts verification depth based on user risk, jurisdiction, and transaction behaviour.

Three Key Principles

False Acceptance Rate shows how often fake or fraudulent users are wrongly approved. In crypto verification, a low FAR means stronger protection against scams and account breaches. Keeping this rate minimal ensures that only genuine investors can pass the checks and access digital assets securely.

False Rejection Rate measures how often real users are mistakenly declined. A high FRR can frustrate legitimate crypto buyers and slow down onboarding. Balancing FRR with security controls ensures a smooth experience for verified users while maintaining robust safeguards against identity manipulation or fraud attempts.

True Acceptance Rate, or Pass Rate, reflects how efficiently genuine users are verified. A strong TAR means faster approvals, better trust, and fewer verification delays. In crypto platforms, maintaining high TAR builds user confidence and ensures compliance without compromising transaction safety or regulatory integrity.

Core Elements of a Balanced Framework

A balanced framework begins with dynamic risk scoring, which evaluates each user and transaction according to factors such as jurisdiction, behavioural patterns, and transaction value.

It then applies tiered verification, allowing low-risk users to pass through instant automated checks while directing higher-risk profiles toward enhanced due diligence, video KYC, or layered identity verification that includes human oversight when necessary.

Finally, adaptive thresholding ensures that verification parameters evolve with changing market risks, maintaining both security and a seamless user experience.

What is the right Identity Verification workflow for Crypto Exchanges to balance compliance with convenience?

Implementing Risk-Based AML Controls and Jurisdictional IDV Strategies

As regulatory expectations evolve globally, crypto exchanges must move from static compliance to adaptive frameworks that reflect jurisdictional nuances. Building on the regulatory overview above, this section focuses on how exchanges can operationalise compliance by integrating risk-based AML controls and region-specific identity verification (IDV) logic into their onboarding workflows.

Operating across multiple markets requires balancing AML rigour with local adaptability. A truly compliant Identity Verification Service must account for regional risk tiers, sanction lists, and evolving regulatory dynamics. For crypto platforms, long-term resilience depends on adopting IDV systems capable of interpreting and applying region-specific regulations in real time.

To remain compliant and competitive, exchanges should prioritise:

- Comprehensive AML/CFT compliance coverage across all operating jurisdictions
- Real-time regulatory mapping updates within 24 hours of legal change
- High cross-border ID verification success rates to support global growth

Escalation framework for high-risk scenarios

Risk-based verification flows usually begin with how often risk exposure is identified in the Compliance Programme.

For instance, when applicants originate from jurisdictions under the FATF's Increased Monitoring (Grey List), such as Syria, Shufti, on demand of crypto exchanges, applies enhanced due diligence (EDD) and customized verification workflows that align with international compliance standards while maintaining a seamless user experience.

For countries classified as High-Risk Jurisdictions (Black List), including Iran and North Korea, onboarding and verification follow strict legal and regulatory restrictions. Verification is conducted only when legally permissible and in full compliance with sanctions and regional frameworks.

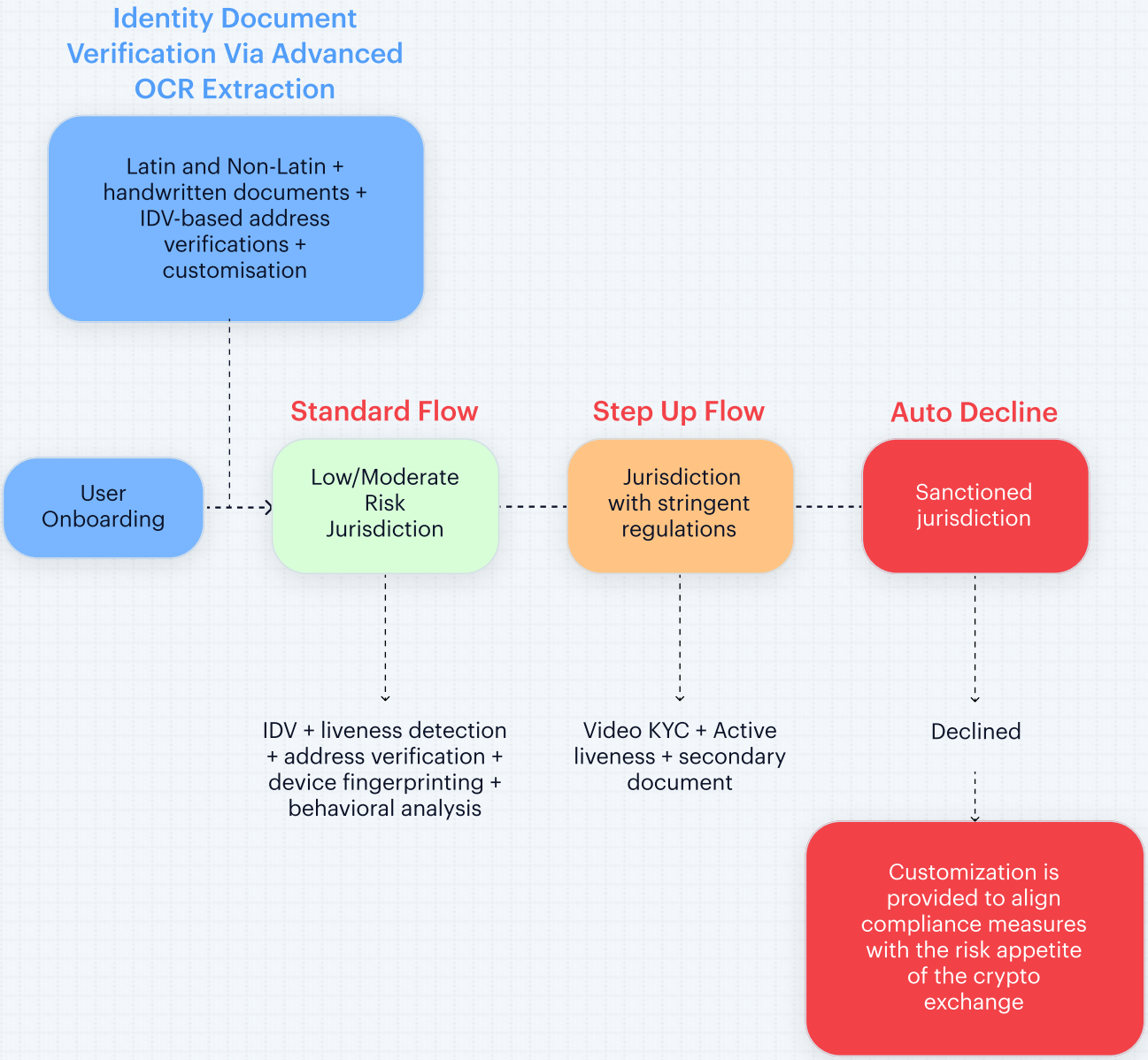
This process ensures that friction for low-risk customers is prevented.

2 . https://www.fatf-gafi.org/en/countries/detail/Syria.html

3 . https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-june-2025.html

4 . https://www.fatf-gafi.org/en/countries/detail/DPRK.html

Adaptive IDV Framework Aligned with Jurisdictional Risk



Evolving Global Regulatory Landscape for Crypto Exchanges

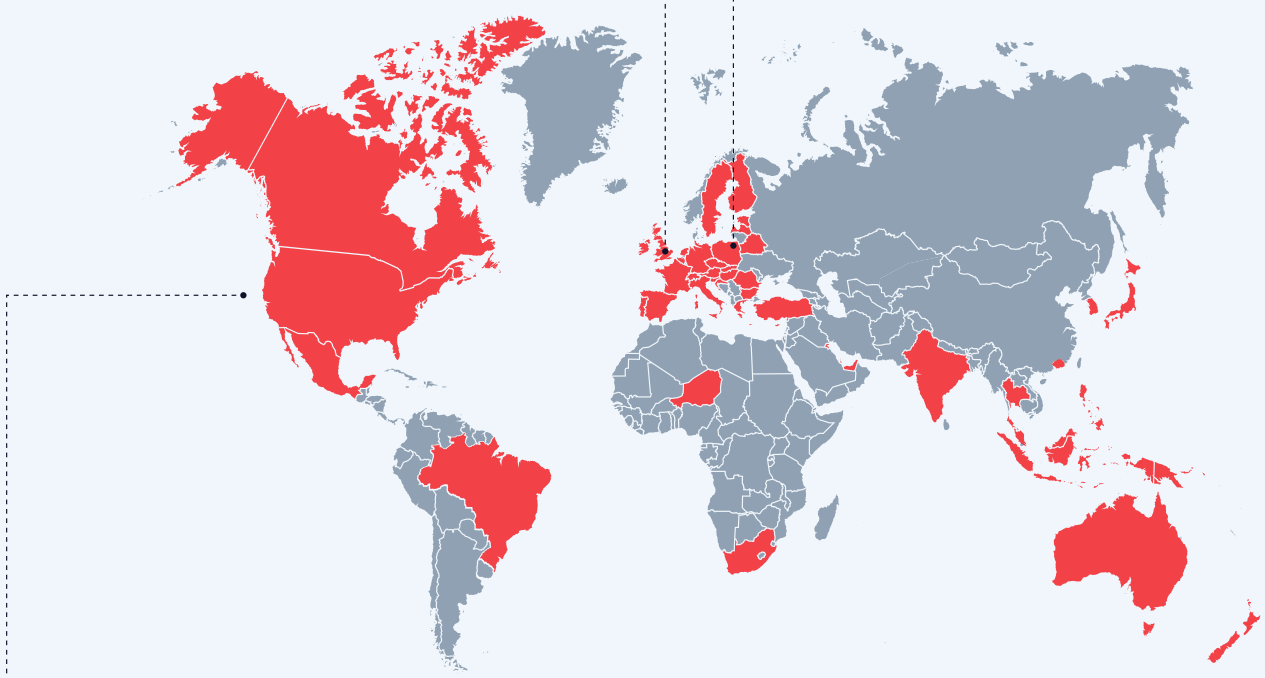
As crypto adoption expands, regulatory oversight is evolving rapidly across jurisdictions, shaping how exchanges operate and verify identities. Building on the need for risk-based verification highlighted earlier, understanding this global regulatory context is essential to designing compliance strategies that remain adaptable and defensible. While the objective of transparency and consumer protection is universal, enforcement and technical standards differ widely across regions.

United Kingdom:

In the United Kingdom, the Financial Conduct Authority (FCA) continues to integrate crypto oversight into traditional financial systems. By 2025, exchanges will be subject to capital adequacy, conduct, and risk management rules similar to those applied to established financial institutions.

European Union:

Within the European Union, the Markets in Crypto-Assets Regulation (MiCA), effective from December 2024, mandates licensing, capital requirements, and AML compliance. Complementary frameworks such as DORA (Digital Operational Resilience Act) and DAC8 (Tax Transparency Directive) further strengthen cybersecurity and reporting obligations.



United States:

In the United States, regulators are moving toward a unified compliance framework for digital assets through initiatives such as the GENIUS Act, the CLARITY Act, and the 2025 Digital Financial Technology Leadership Order. Exchanges are expected to demonstrate verifiable AML controls, robust KYC programs, and adherence to financial transparency requirements.

Country	Crypto-Specific Law / Regulation
European Union	MiCA
United Kingdom	Money Laundering Regulations & FCA Financial Promotions Regime
United States	FinCEN Convertible Virtual Currency (CVC) Guidance (2019)
Canada	CSA Oversight of Crypto-Asset Trading Platforms
Brazil	Law 14,478/2022 (Marco Legal dos Criptoativos)
Mexico	FinTech Law (Ley Fintech) & Banxico Rules
Australia	AUSTRAC Digital Currency Exchange (DCE) Regime
Japan	Payment Services Act / Financial Instruments and Exchange Act (FIEA)
South Korea	Virtual Asset User Protection Act (2024)
Singapore	Payment Services Act & MAS Notices (e.g., PSN02)
Hong Kong	AMLO (VASP Licensing) under SFC
India	PMLA (2023 VDA Notification)
Indonesia	Bappebti Regime & P2SK Law (2023)
Philippines	BSP Circular No. 1108 (2021)
Thailand	SEC/BOT Measures on Digital Assets
New Zealand	FMA Guidance (FMC Act & AML/CFT Act)
UAE (Dubai)	VARA Regulations & Rulebooks (2023)
Bahrain	CBB Crypto-Assets Module
Qatar	QFCRA Circular (2020)
Kuwait	2023 Supervisory Circulars (crypto prohibitions)
Turkey	2021 Payments Regulation & MASAK AML Rules
South Africa	FSCA (FAIS) Classification (2022/23)
Nigeria	CBN 2023 Circular on VASPs
Switzerland	DLT Act (2021) & FINMA Guidance
Liechtenstein	TVTG “Blockchain Act” (2019)

Key Red Flags That Signal an Ineffective IDV Partner

As crypto exchanges refine their compliance frameworks, selecting the right identity verification partner becomes a critical step. The strength of any AML or KYC program depends not only on policy design but also on the reliability, adaptability, and security standards of the technology provider.

The following red flags highlight common weaknesses that can undermine compliance effectiveness and operational efficiency:

- Inability to support jurisdiction-specific compliance and risk logic
- Limited global document verification coverage
- Weak security and compliance track record
- Lack of dedicated R&D teams and escalation pathways
- Inflexible or non-customisable workflows
- Slow, inconsistent, or insufficient verification processes
- Lack of interoperability with the government's eIDs
- Over-reliance on third-party providers for edge cases
- Lack of adaptability to fight evolving fraud typologies
- Reliance on third parties for non-latin identity documents verification

IDV as a Strategic Growth Driver Beyond Standard KYC Checks

After identifying common weaknesses in the identity verification landscape, it's equally important to understand what distinguishes a strong, future-ready solution. The right IDV framework does more than meet compliance requirements; it serves as a strategic enabler for global growth, empowering crypto exchanges to expand confidently while maintaining regulatory integrity.

For crypto, where customers transact across borders without physical barriers, global coverage is critical, and IDV stands at the core of ensuring secure, compliant, and seamless expansion.

Challenges within the IDV landscape:

Many identity verification providers continue to struggle with non-Latin documents, often requiring manual translation by end users. Despite claims of global reach, their OCR capabilities remain incomplete, lacking built-in technology for diverse scripts.

For Example:

Most solutions are designed primarily for Latin-based languages such as English, French, Spanish, or Italian but fail to accurately process widely used scripts like Arabic, Amharic, Farsi, Hindi, Khmer, and Georgian.

These gaps not only increase verification friction but also pose significant challenges for crypto exchanges seeking to expand into emerging markets where non-Latin scripts dominate user documentation.

What Makes an ID Verification Solution a Strategic Advantage for Crypto Exchanges?

- Offers comprehensive global coverage, with support for all document types, including handwritten and non-standard ones, across multiple jurisdictions and languages.
- Eliminates hidden costs by providing a single, streamlined Crypto IDV solution without additional configurations.
- Strengthens security with advanced crypto fraud prevention solutions, detecting deepfakes, tampered IDs, and synthetic identities through AI-powered technology.
- Enhances flexibility by allowing businesses to tailor verification flows in line with local compliance requirements and unique operational needs.
- Optimises user experience with features like auto-capture, glare and blur detection, and frictionless onboarding to minimise drop-offs.
- Ensures reliability by intelligently recognising worn, damaged, or less common documents that other providers often reject.
- Promotes transparency with visual cues and clear decline reasons, building trust and enabling auditability.
- Maintains a compliance-first approach with built-in alignment to global KYC/AML and data protection standards.

Key Questions For IDV Vendor Evaluation

What To Ask Your IDV Partner	Why It's Critical for Crypto	How Shufti Helps
Can the vendor customise workflows for risk-based compliance?	Jurisdictional risk varies because Same user could be low-risk under one jurisdiction and high-risk in another. You need adaptive flows aligned with AML/CFT thresholds.	Shufti enables dynamic verification flows tailored to the risk exposure and risk appetite of the businesses. Explore More
Can the vendor provide reusable identity verification for faster onboarding?	Reusable verification allows returning users to bypass redundant KYC checks, improving user experience and platform retention without compromising compliance.	Shufti's patent-protected Fast ID enables instant verification using biometric selfies and verified digital credentials for frictionless onboarding across exchanges. Explore Fast ID
Does the vendor offer extensive global eIDV coverage?	Crypto platforms operate globally and must verify users across multiple jurisdictions. Broad eIDV coverage ensures compliance and prevents onboarding delays in cross-border transactions.	Shufti's eIDV spans over sixty countries and billions of verified identities, offering unmatched global reach and real-time accuracy. Learn more about eIDV coverage
Can the solution verify NFC chips for tamper-proof validation?	Chip-based document verification adds an extra layer of trust, reducing fraud from forged or manipulated IDs common in high-risk regions.	Shufti's NFC Verification reads encrypted biometric and cryptographic data to deliver instant, tamper-proof verification. Discover NFC Verification

What to ask your IDV Partner	Why It's Critical for Crypto	How Shufti Helps
Does the vendor build technology in-house?	IDV vendor's full control over tech guarantees faster updates, fewer integration risks, and no data leakage via third parties.	Shufti's core tech stack, including Latin and Non-Latin OCR engines, liveness, and fraud detection, is entirely proprietary. [Learn about our tech ecosystem]
Can the vendor handle non-Latin scripts?	Global users in non-latin markets often submit documents in local scripts; failing to process these accurately leads to friction.	Shufti's AI-powered OCR supports 97 languages, including Arabic, Amharic, and Farsi [See OCR details]
Is seamless CRM integration supported?	Manual data transfer increases error rates and compliance gaps.	Shufti integrates directly with CRM and ERP systems via RESTful APIs. [View API documentation]
Can the vendor provide frictionless onboarding?	Speed is critical; drop-offs cost conversions and credibility.	Shufti delivers automated verifications in under 60 seconds [Book a demo]
Can the vendor meet country-specific KYC requirements?	Users from high-risk jurisdictions often require enhanced due diligence; vendors must apply targeted verification logic (e.g., stricter ID or proof-of-address validation).	Shufti allows geo-based rule customization, letting compliance teams tailor onboarding flows to country-specific risk logic [Learn more how we scale globally.]

What to ask your IDV Partner	Why It's Critical for Crypto	How Shufti Helps
Can the solution counter advanced fraud like deepfakes and spoofing while meeting SLA response times?	Fast response times defined in SLAs are vital for fraud prevention and user experience in high-risk industries.	Shufti delivers real-time fraud detection using liveness, device fingerprinting, and behavioural biometrics, while ensuring compliance with strict SLA response benchmarks. [Discover fraud prevention suite]

Strategic IDV Evaluation Matrix for Crypto Exchanges

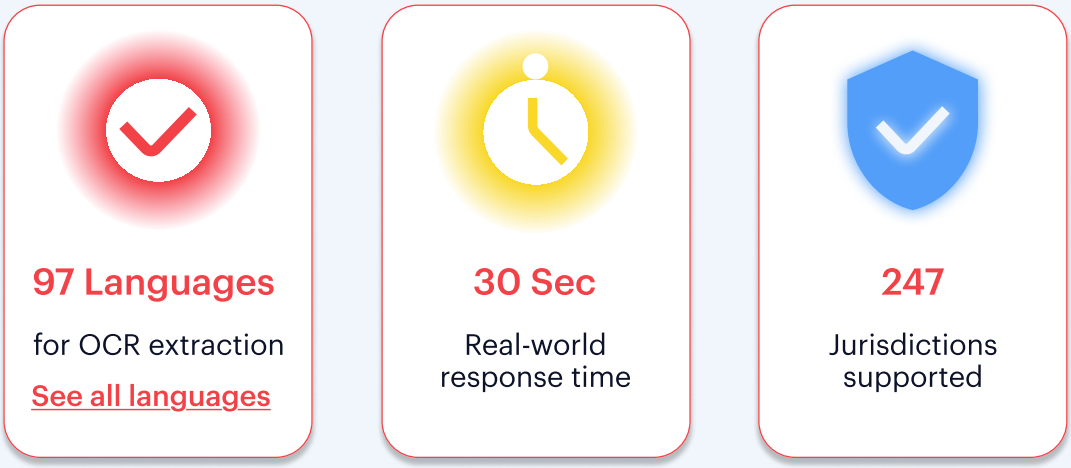
Assessment Dimension	Primary Consideration
Global Reach & Compliance	Non-standard ID support, multilingual OCR, jurisdictional regulatory mapping and anomaly monitoring.
Biometric Verification	Liveness detection, deepfake resistance, anomaly monitoring.
Fraud Defense	Device fingerprinting, behavioral biometrics, deepfake detection, and anti-spoofing capabilities.
Video KYC	Real-time face-to-face verification to meet requirements of regulators like BaFin in Germany.
Analyst Escalation	Dedicated R&D and human-in-the-loop teams review false alerts and high-risk cases to ensure accuracy
Onboarding Experience	Fast verification with minimal drop-offs.
Customization	Configurable workflows and white-label options.
Risk Logic	Dynamic verification flows tailored by user, and jurisdiction-specific risk logics.
Data Security	Encryption, data residency controls, GDPR/CCPA compliance.
Operational Efficiency	Reduced manual reviews with transparent pricing.
Verification Response Time	Average turnaround for automated and analyst-assisted verifications.
False Acceptance Rate (FAR)	Low false acceptance rate to prevent fraud.
False Rejection Rate (FRR)	Low false rejection rate to prevent fraud.
True Acceptance Rate (TAR)	High true acceptance rate to maximize legitimate user approvals.

End-to-End ID Verification Workflow

Buyer/ Exchange Step	What Shufti Does	What You Get	Decision/Next
User starts signup	SDK opens capture flow on web/mobile	Friction-light UX, device checks	Proceed to capture
Document Verification	Authenticates documents by analyzing security features with 61+ adaptive forgery checks.	Verified document authenticity score and fraud detection insights.	If verified → proceed to integrity validation; if suspicious → escalate for analyst review.
Selfie / Live video	Advanced active liveness + Face match (1:1), presentation-attack detection	Face match score + liveness verdict	For high-risk scenario Video KYC → retry/ escalated for R&D analysis
(Optional) Proof of Address	Extracts address from utility bill/bank/ statement; recency & tamper checks	Parsed address + freshness result	If mismatch → request new doc

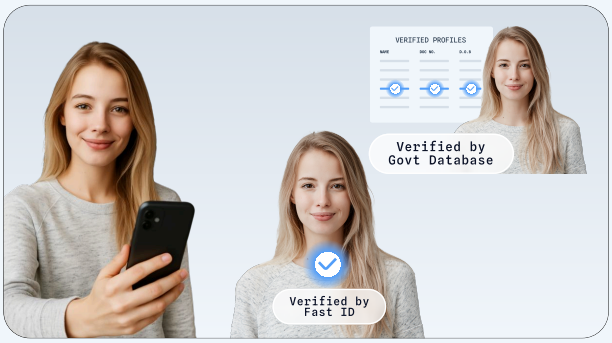
Buyer/ Exchange Step	What Shufti Does	What You Get	Decision/Next
Instant AML checks	Screen against sanctions, PEP, watchlists, adverse media	Risk labels (e.g., Sanctioned/PEP/ None), hit details	High-risk → case escalation
Fraud & integrity checks	Template/format validation, forgery/ tamper signals, duplicate detection (1:N optional)	Document authenticity score, duplicate flags	Auto-reject or escalate rules
Audit & compliance	Secure evidence, timestamped logs, webhook/API response	Audit trail for regulators & internal QA	Store per policy
Ongoing monitoring	Daily/weekly AML rescreening, trigger-based re-KYC	Alerts on status change	Continuous compliance

The workflow above outlines how Shufti enables crypto exchanges to streamline verification from signup to ongoing monitoring. Yet, behind this seamless user journey lies a sophisticated set of technologies purpose-built to address the unique challenges of the crypto ecosystem, such as anonymity, speed, and cross-border complexity. To ensure every wallet is linked to a verified, traceable identity, Shufti combines advanced document authentication, biometric verification, and multilingual data extraction into one cohesive framework.



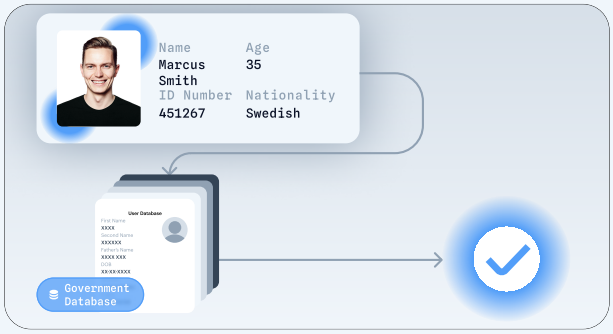
How Shufti Strengthens Crypto KYC Through Advanced Identity Document Verification

In the crypto ecosystem, where speed and security are paramount, identity verification begins with fast, reliable checks. Technologies such as reusable ID, eIDV, and NFC Verification enable instant validation before document review. Using NFC, the chip embedded in smart identity documents is scanned within seconds, confirming authenticity and accelerating onboarding for genuine crypto users.



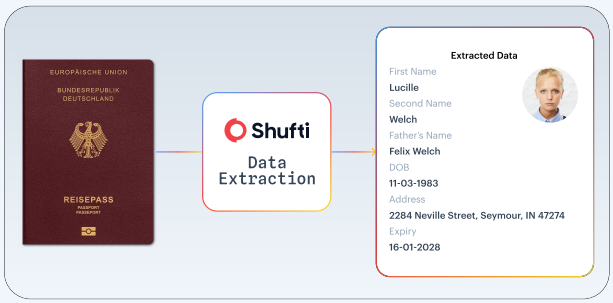
Reusable Identity Verification

Shufti's patent-protected proprietary solution enables instant and reliable identity verification by matching biometric selfies with verified identities. Built for speed and security, it allows crypto exchanges and wallet providers to onboard users within seconds while ensuring strict KYC and AML compliance. By leveraging reusable identity credentials, it prevents duplicate or fraudulent accounts and enables fast verification across the ecosystem.



Electronic Identity Verification (eIDV)

eIDV authenticates users by cross-verifying their information, such as name, date of birth, and address, against digital identities, credit, and telecom databases. With industry-leading coverage spanning over sixty countries and billions of verified identities, Shufti offers broader and deeper global reach than typical verification vendors. This ensures accuracy, speed, and compliance for crypto platforms operating across multiple jurisdictions.



NFC Verification

NFC Verification validates identity at the chip level by reading encrypted biometric and cryptographic data embedded in e-ID documents through Near Field Communication. This contactless and tamper-resistant method verifies document authenticity instantly, minimizing false acceptances, friction and fraud risks. Optimized for high-velocity crypto environments, NFC Verification ensures fast, compliant, and secure access to digital asset platforms.

Advanced Document Verification for Higher-Level of Assurance in Identity Verification

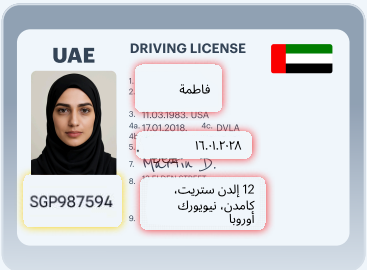
In the crypto ecosystem, where onboarding occurs globally, remotely, and instantly, and in real time, identity verification must do more than confirm a document's authenticity. It must establish whether each wallet is associated with a legitimate and traceable individual.

Document Authentication

Verifies the authenticity of identity documents by assessing native security features such as holograms, watermarks, and microtext. With 61+ types of subtle forgery checks, the highest in the industry, triggered dynamically based on adaptive risk scoring, it detects forged or manipulated credentials early to mitigate fraud risk and reinforce institutional trust across digital ecosystems.

Integrity Validation

Validates signatures, issuance and expiry dates, MRZ and layout formats while detecting subtle forgeries. Through NFC-chip verification, Shufti reads encrypted biometric and cryptographic data directly from e-ID chips, ensuring the highest level of document accuracy and transparency.



Multilingual Data Extraction

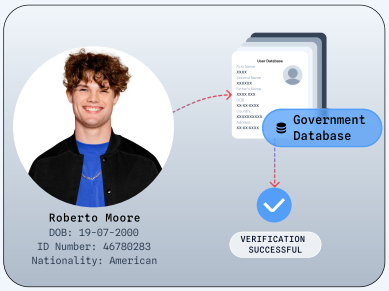
Powered by AI-based optical character recognition (OCR), Shufti extracts structured data from identity documents in multiple languages, including non-Latin scripts, without additional configuration or cost. Recursive parsing resolves field mismatches and standardises complex address data according to the requirements of crypto exchanges' CRMs, streamlining Enhanced Due Diligence (EDD) processes.

Proof Of Address Verification As A Key Element In Customer Due Diligence For High-Risk Cases

Enhanced due diligence requires more than verifying a customer's identity. For crypto exchanges operating in jurisdictions with stringent AML and CFT obligations, proof of address verification is an essential component of customer due diligence, ensuring that every verified identity is tied to a legitimate and traceable physical location.

Document-Based Address Verification

Addresses are verified using documents such as utility bills or bank statements issued within valid timeframes. Each document is checked for authenticity, clarity, and formatting accuracy. OCR technology extracts details like street, city, and postal code, ensuring reliable and consistent verification across diverse document types and jurisdictions.



Non-Doc Address Verification

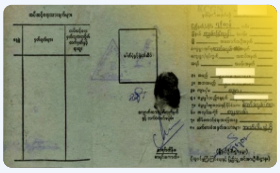
Verification can also be performed through real-time data from trusted sources such as government databases, telecom providers, and credit bureaus. This method enhances accuracy, reduces manual review, and speeds up onboarding while maintaining compliance integrity across global markets.

Geo-Based Address Verification

Geolocation tools compare a user's declared address with IP or GPS coordinates. Any mismatches are flagged for review, helping exchanges detect high-risk activity early and ensure each verified user is linked to a legitimate, traceable location.

No One-Size-Fits-All Approach To Identity Verification

Shufti designs adaptive identity verification frameworks that reflect the unique regulatory and operational needs of each client. Unlike standardized tools that often overlook regional nuances, our tailored solutions minimize vulnerabilities and ensure seamless compliance.



Custom OCR Extraction

Traditional OCR systems often struggle with non-Latin scripts, leading to data inaccuracies that can hinder onboarding and compliance. Shufti's advanced OCR technology is purpose-built for complex languages, delivering exceptional accuracy in data extraction and minimizing verification failures.

Enhanced Name Processing

Cultural variations in naming conventions often complicate screening accuracy. Shufti's enhanced name processing intelligently distinguishes between first, middle, and last names, applying differentiated weightages to reduce false positives during KYC checks. This ensures global consistency, compliance, and precision in identity verification.

Document Number Validation

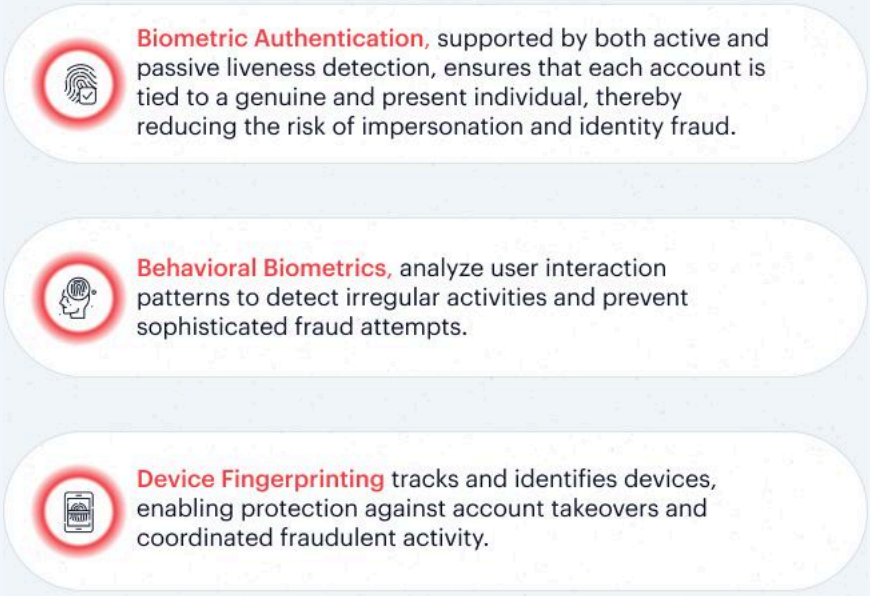
Processes paper-based cards and diverse document formats with high precision, addressing OCR challenges such as stamped CPF numbers, inconsistent field labels, and data validation anomalies to ensure integrity. In Brazil, the system effectively manages CPF-specific complexities, including stamped-over identifiers and edge-case validations, maintaining up to 99.8% accuracy in document verification.

ID Thickness Analysis for High-Risk Fraud Detection

In high-risk scenarios, Shufti employs ID card thickness analysis to detect tampering and presentation attacks. This additional layer of scrutiny helps prevent sophisticated fraud attempts such as deepfakes or PVC-printed fake IDs. For instance, in countries like Japan, this technique has proven effective against physical forgeries, reinforcing identity assurance at a material level.

Beyond Government ID Verification For Higher Assurance In Remote Onboarding

In sectors like crypto, where emerging threats such as deepfakes, synthetic identities, and stolen credentials are on the rise, standard ID verification alone is no longer sufficient. Shufti extends verification beyond government-issued documents by employing a multi-layered defense framework designed to safeguard platforms while ensuring regulatory compliance and operational efficiency.



Higher Level of Assurance in Remote Identity Verification

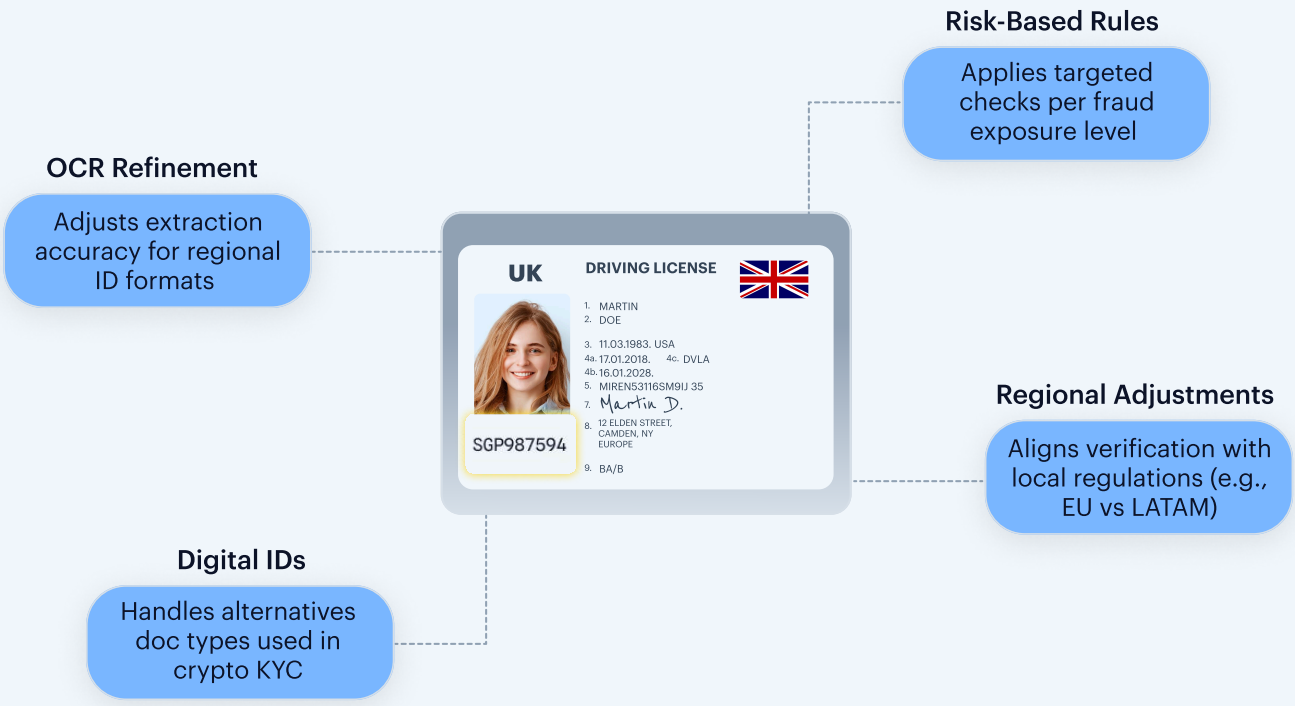
Achieving a higher level of assurance in remote identity verification requires multiple layers of intelligence working together to validate user authenticity. Beyond document checks, advanced techniques such as biometric authentication, behavioral biometrics, and device fingerprinting help verify identities in real time. These mechanisms collectively enhance security, reduce impersonation risks, and build trust across digital transactions.

Shufti IDV Customisations Based On The Risk Exposure

Shufti customises its identity verification (IDV) flows to address the unique operational, regulatory, and risk profiles of clients across different regions. Adjustments are implemented upon request, ensuring each verification process aligns with the client's specific compliance framework and onboarding strategy.

These customisations may include refining OCR logic, enabling e-document processing, or introducing additional document validation layers to enhance accuracy and efficiency.

In the crypto sector, Shufti further adapts verification flows to reflect each exchange's risk logic and jurisdictional requirements. Instead of applying rigid, one-size-fits-all policies, the platform enforces targeted verification rules where necessary. For instance, document types linked to higher fraud risks in certain regions may trigger enhanced checks or conditional declines.



Region	Country	Customisation / Challenge Addressed
Asia	 India	Enhanced address extraction to capture detailed address data; Aadhaar e-doc acceptance enabled for smoother onboarding.
	 Pakistan	Color copy documents restricted due to high risk of tampering and forgery in the region.
	 Afghanistan	Handwritten documents are restricted due to poor readability; passports are handled by analysts for certain risk scenarios.
Middle East	 Saudi Arabia	Duplicate side submission prevented to ensure document authenticity.
Africa	 Nigeria	E-documents processed only when merchants allow, due to risk of manipulation.
	 Ethiopia	Fyda ID not supported due to inconsistencies and unreliable verification sources.
Americas	 Mexico	Resident permits expiry date standardised to 2099-01-01 to meet merchant onboarding needs.
	 Brazil	Driving licence checks enhanced with layered verification instead of relying solely on ML to improve decision accuracy.
Europe	 Russia	Resident permits are declined based on the risk logic of the respective crypto exchange.

Disclaimer: Shufti offers these customizations based on each business's specific risk logic and compliance requirements.

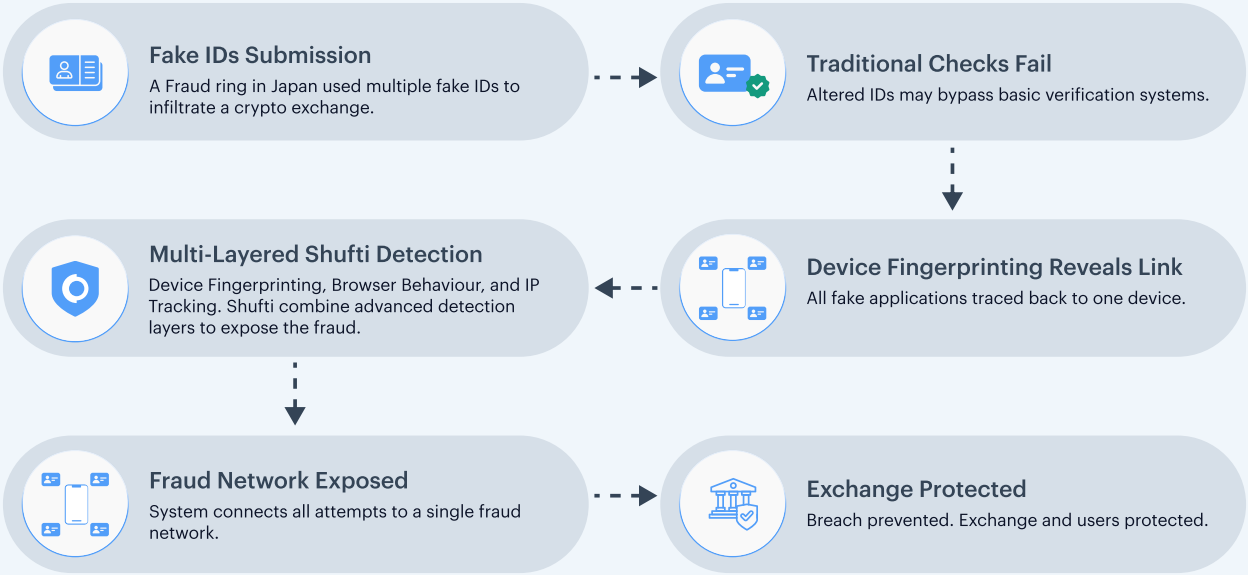
CASE STUDY 1

Proactively Detecting Advanced Identity Frauds by Criminal Networks

Fraud in the crypto industry has grown more sophisticated, blending technology and psychology to exploit system gaps. Crypto exchanges are prime targets for organized rings using fake IDs and deepfakes to bypass KYC, making layered defenses like device fingerprinting essential. A recent case in Japan showed how synthetic identities can evade traditional KYC checks not built to counter advanced fraud tactics.

Shufti's multi-layered fraud prevention framework provided the resilience needed. Through advanced device fingerprinting, the system identified that all applications originated from a single orchestrated source. Key capabilities, including IP intelligence, emulator and virtual machine detection, and browser behaviour analysis, uncovered hidden links between the synthetic identities, exposing the coordinated nature of the attack.

Inside the Fraud Detection

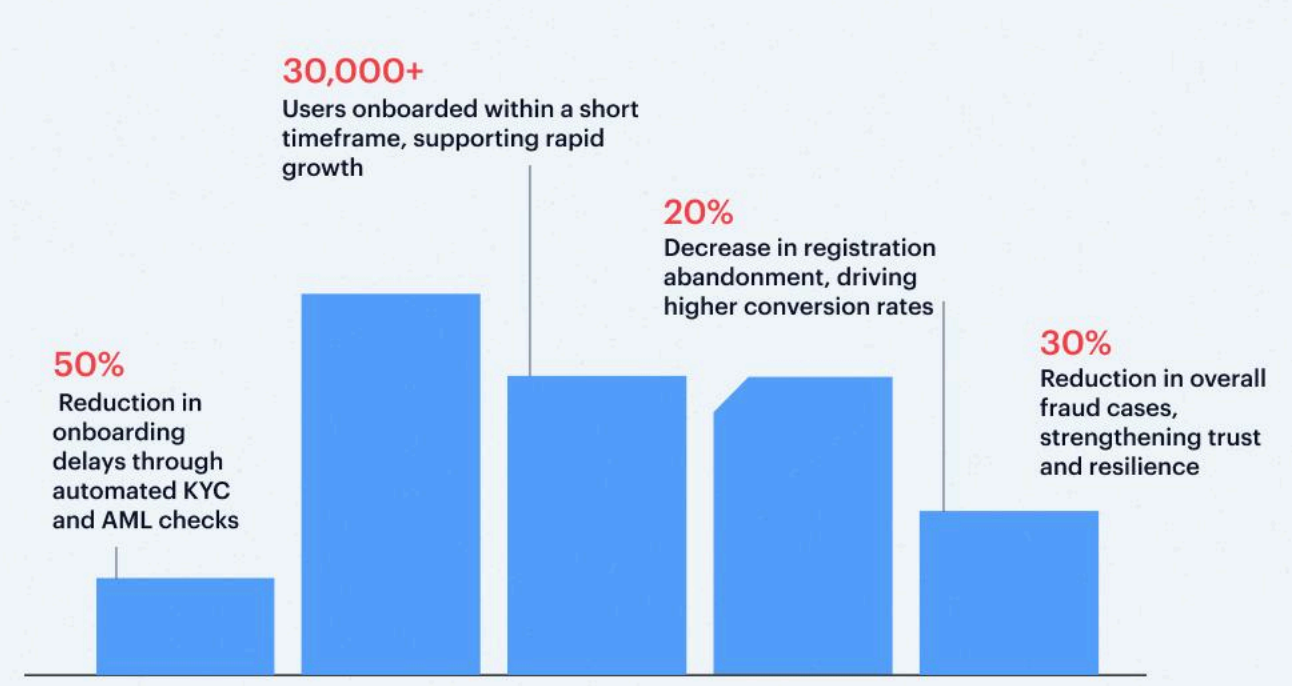


CASE STUDY 2

How a Crypto Exchange Reduced Onboarding Friction

A leading Crypto platform, operating in a highly competitive and tightly regulated market, was grappling with mounting onboarding inefficiencies. Manual KYC processes not only created significant delays but also contributed to higher customer abandonment rates. Simultaneously, escalating fraud attempts threatened compliance with global AML standards, placing both growth and reputation at risk.

To address these challenges, the platform adopted Shufti's identity verification framework, integrating automated KYC solutions, fraud risk assessment, and real-time onboarding capabilities directly into its existing systems. This strategic implementation delivered quantifiable improvements across compliance, fraud prevention, and customer experience.



Shufti

Ready to transform your crypto compliance with intelligent verification?

Build a resilient identity verification infrastructure that empowers your crypto business to grow securely while staying ahead of regulatory and AML obligations.

Discover how Shufti's AI-driven IDV platform combines biometric authentication, multilingual OCR, and continuous AML/KYC screening to detect fraud, meet global compliance, and ensure seamless onboarding, all in one unified framework.

Learn More