

Docless Identity Verification in the Middle East

A Practitioner's Guide to the GCC and Beyond

How national digital identity, fragmented regulation, and data-residency rules reshape identity verification across the GCC and beyond.

REGION

Middle East & N. Africa

PUBLISHED

2026

LENGTH

12-minute read

SOURCE

shuftipro.com

• CONTENTS

What's in this guide

01	Why the Region Is Nine Markets, Not One	03
	Different regulators, documents, and identity systems in every market, with little that transfers across borders.	
02	Digital Identity Adoption, Market by Market	05
	How widely each national digital identity is actually used, and what the spread means for onboarding.	
03	UAE and Saudi Arabia: The Anchor Markets	07
	The region's two most developed markets, and its strictest data regime.	
04	Who Regulates What, and Where Data Lives	09
	The regulator, AML law, and data rule in each market, and why transfer limits push processing in-country.	
05	Qatar, Kuwait, Bahrain, and Beyond	11
	Active remote onboarding past the two anchors, from the Gulf to North Africa.	
06	The Sectors Under Most Onboarding Pressure	14
	Where regulated onboarding volume and fraud risk concentrate, and why.	
07	Why Most IDV Vendors Fall Short Here	15
	Two reasons most vendors struggle, and the checklist that exposes them.	
08	Docless Onboarding via National eID Rails	17
	Verifying users against authoritative government identity sources, no document upload required.	
09	What the Right IDV Foundation Looks Like	19
	An architectural answer: owned, end-to-end, deployable where the data must live.	
10	Certifications That Matter to Compliance	20
	The external validations regional compliance, product, and risk teams check for.	

01 WHY THE REGION IS NINE MARKETS, NOT ONE

Teams expand into the Middle East and discover it is closer to a dozen markets than one.

A verification flow tuned for the United Arab Emirates will not satisfy a Saudi regulator, accept a Qatari credential, or meet Bahrain's transfer rules without rework. Each country has its own identity document, its own digital identity system, its own financial regulator, and its own data-protection law, and several of those laws have changed inside the last two years.

This matters to two kinds of reader. The first is a local team, a bank in Riyadh or a fintech in Manama, that must onboard customers under a named domestic regulator. The second is a global team, a payments company in London or an exchange in Singapore, onboarding customers from the region or expanding into it. For both, the failure mode is the same: a control that looks compliant in one Gulf state quietly breaks the audit trail in the next, and the gap usually shows up at the worst moment, during a regulatory review or a spike in onboarding volume. The region rewards teams that treat it as a set of distinct markets rather than a single block.

All 6

GCC states now run a national digital identity system, from UAE Pass to Saudi Arabia's Nafath. A verification setup that ignores them is already a step behind the markets it serves.

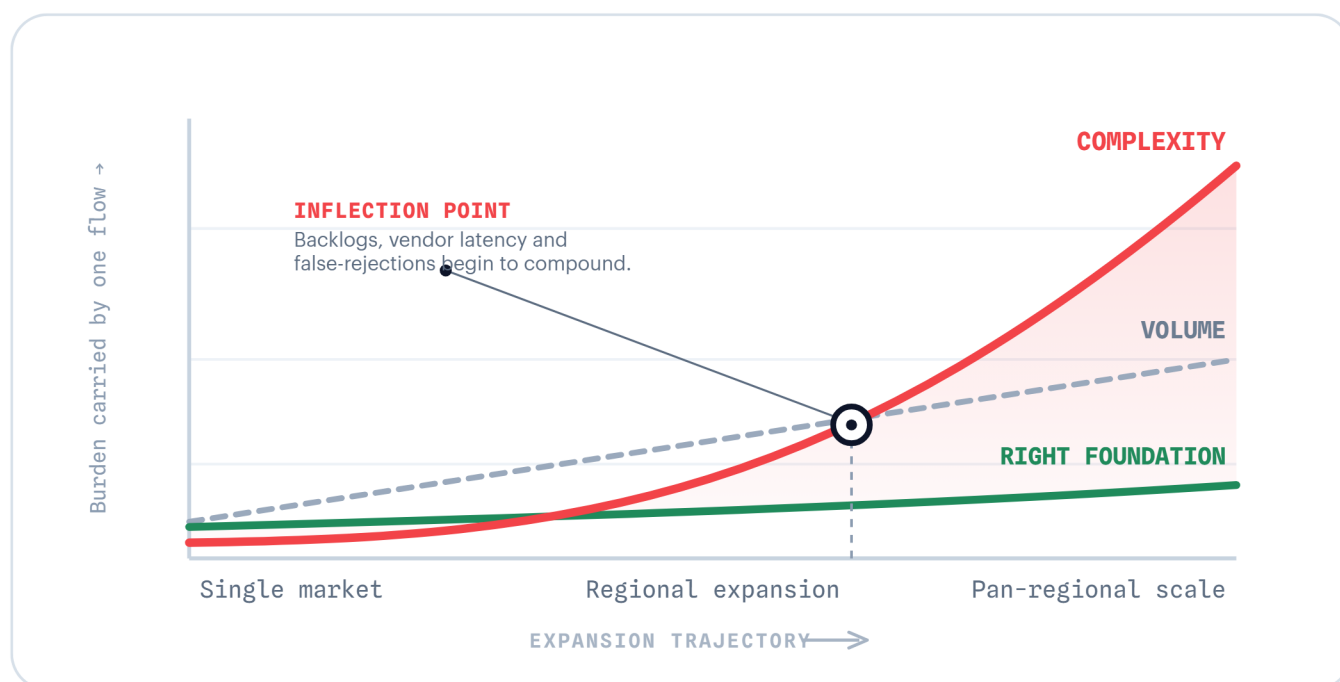
Three things vary market by market, and each can break an onboarding flow on its own.

- **The credential.** The national ID and the digital identity behind it are not the same in Riyadh, Doha, and Cairo.
- **The rule.** Some regulators have published explicit electronic KYC requirements; others have not.
- **The data rule.** Where the resulting personal data may sit is decided locally, and the answers are not the same.

FIGURE 01 WHY ONE FLOW DOES NOT TRANSFER

Why complexity multiplies the moment a business crosses a regional border

As a business adds markets across the region, verification volume grows in a straight line, but verification complexity grows faster. Every new market adds its own credential, its own regulator and eKYC rule, and its own data-residency posture. The three stack, and they rarely line up with the market next door.



Conceptual visualisation. The red curve traces complexity, distinct credentials, regulators, eKYC rules, and data-residency regimes, as a business expands across the region. The grey line traces transaction volume. The green line shows how an owned, jurisdiction-aware foundation keeps complexity flat as markets are added. The gap between the red and green lines is the advantage.

What it looks like in practice

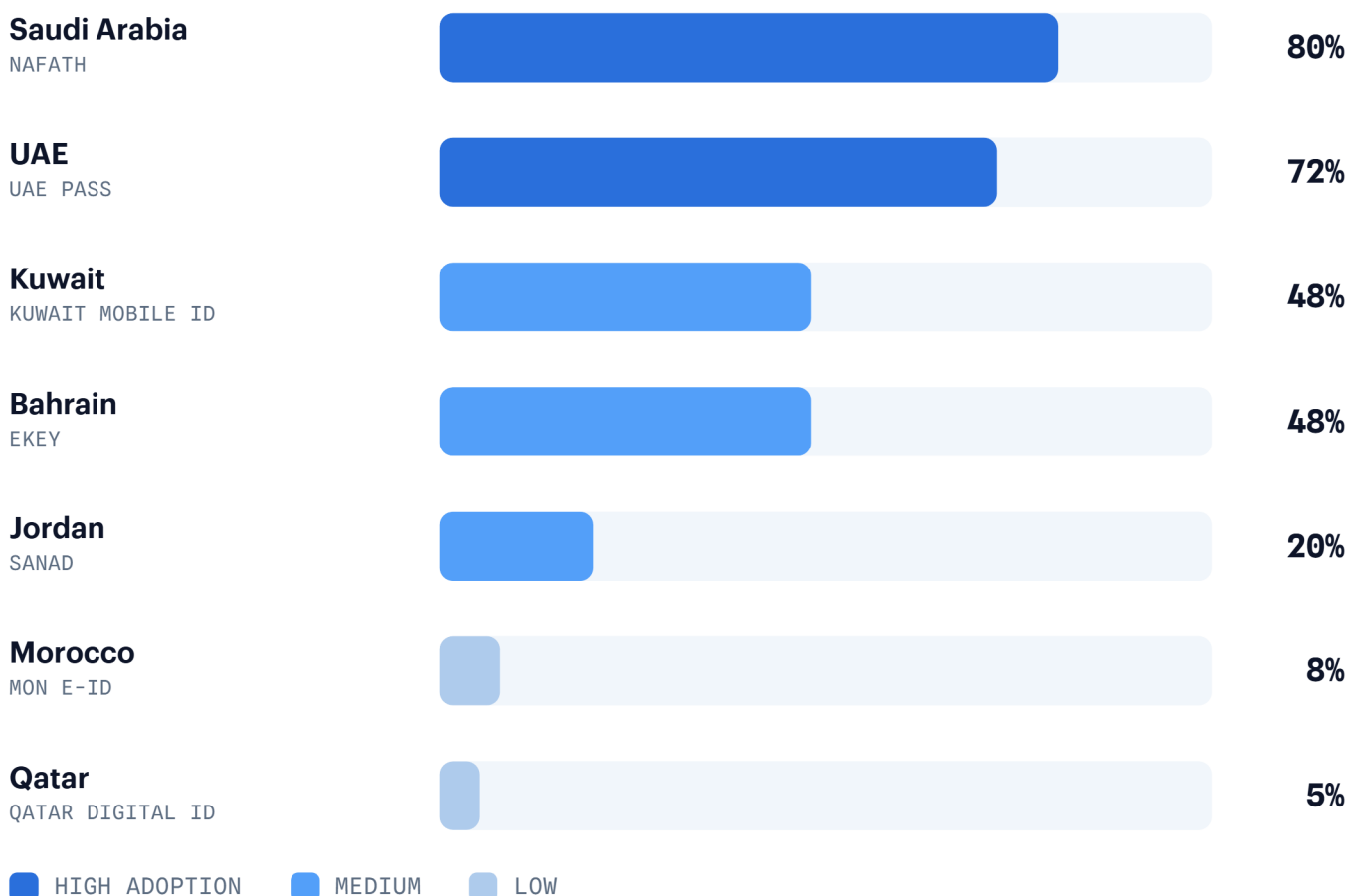
A flow built around UAE Pass and Emirates ID stalls when it meets Saudi Arabia's Nafath and Iqama. A cloud region that satisfies the UAE federal regime cannot clear Saudi Arabia's stricter transfer rules. A document reader tuned for Latin-script IDs drops accuracy on an Arabic-script national ID. None of these is an edge case. They are the operational reality of onboarding across the region. The rest of this guide maps that complexity market by market, then shows the verification foundation that keeps it flat as you add markets.

02 DIGITAL IDENTITY ADOPTION, MARKET BY MARKET

National digital-identity adoption across the region

The Gulf is moving fastest on national digital identity, and the spread is wide. In Shufti's coverage data, adoption of the national digital identity, measured as the share of the 18-65 population, **ranges from the low single digits to around 80%**. The markets with the highest adoption are the ones where a digital-identity route into onboarding is already the default rather than the exception. Adoption decides which route leads, not whether a market can be served: where it is high a docless route can run first, and where it is still building, document verification carries more of the volume, with a document and biometric fallback either way.

Digital-identity adoption by market (share of 18-65 population)



Adoption is the share of the 18-65 population using the national digital identity, from Shufti's coverage data. Bahrain is registered eKey users (iGA, H1 2024) as a share of the mid-2025 population (1,603,260), a slightly different basis.

• HOW TO READ THE REGION

Three things that vary by market

Onboarding in this region turns on three questions, and the answer to each changes as you cross a border. A verification setup that handles all three, market by market, is the one that holds up under audit.

THE CREDENTIAL

Which national ID and digital identity?

UAE Pass, Nafath, Qatar Digital ID, Kuwait Mobile ID, and others are distinct systems with distinct enrolment and verification paths. A flow built around one does not automatically accept another.

THE RULE

Has the regulator published eKYC rules?

Some regulators have explicit electronic KYC rules or platforms, the UAE, Saudi Arabia, Qatar, Bahrain, and Jordan among them. Others have none on the public record, so onboarding rests on the general AML framework.

THE RESIDENCY

Where must the data sit?

Most regimes allow cross-border transfer under conditions. Saudi Arabia is stricter and often points towards in-country processing. It can differ between Riyadh and Dubai for the same company.

Reading the pattern

The Gulf states lead on national digital identity and on explicit eKYC rules, while the Levant and North Africa are catching up fast, with Jordan and Egypt scaling national platforms. Adoption and regulatory clarity tend to move together.

“

A control that looks compliant in one Gulf state can quietly break the audit trail in the next. ”

Regional coverage is not a single integration decision but a sequence of market-by-market calls on credential, rule, and residency, and the vendor that absorbs all three without a separate build per border is the one that scales.

03 THE ANCHOR MARKETS • UAE



United Arab Emirates



The UAE is the region's most developed digital identity market. The mandatory national credential is the Emirates ID, issued by the Federal Authority for Identity, Citizenship, Customs and Port Security to every citizen and resident. On top of it sits UAE Pass, the unified national digital identity and signature platform, with adoption around 72% of the 18-65 population on Shufti's coverage data.

REGULATOR

Central Bank of the UAE

AML LAW

Federal Decree-Law 10 / 2025

DATA LAW

Federal Decree-Law 45 / 2021 (PDPL)

EID ADOPTION

~72% of 18-65 population

REGULATOR & AML RULES

Federal Decree-Law No. 10 of 2025 came into force on 14 October 2025, replacing the long-cited Federal Decree-Law No. 20 of 2018, so any policy still citing the 2018 law is now out of date. Electronic KYC is expressly permitted, with Central Bank guidance on using digital identification for customer due diligence.

DATA & FREE-ZONE REGIMES

The federal Personal Data Protection Law (Decree-Law No. 45 of 2021) imposes no blanket localisation. The complication is parallel regimes: the DIFC (Law No. 5 of 2020) and the ADGM (Regulations 2021) each have their own commissioner, so a deployment that satisfies the federal law may still answer to a free-zone regulator.

The practical gotcha: the majority case is the resident, not the citizen.

A large share of the population are expatriate residents whose Emirates ID and supporting documents differ from a citizen's. A flow built only around the national-citizen path will stall on the resident case, which is the majority case. For Dubai virtual-asset businesses there is a further layer, the Virtual Assets Regulatory Authority, established under Dubai Law No. 4 of 2022.

03 THE ANCHOR MARKETS • SAUDI ARABIA



Saudi Arabia



Saudi Arabia pairs the region's highest eID adoption with its strictest data regime. Its identity infrastructure is anchored on Nafath, the national single sign-on operated under SDAIA, alongside Absher, the Ministry of Interior's e-services platform. Adoption is the highest of any Gulf eID, around 80% of the 18-65 population. The underlying credentials are the National ID for citizens and the Iqama for residents.

REGULATOR

Saudi Central Bank (SAMA)

AML LAW

Royal Decree M/20 / 2017

DATA LAW

Royal Decree M/19 / 2021, enforced 2024

EID ADOPTION

~80% of 18-65 population

The Saudi Central Bank supervises banks, payments, and finance companies, under the Anti-Money Laundering Law issued by Royal Decree No. M/20 of 2017. Remote KYC is permitted: the rulebook sets the KYC requirements and recognises approved electronic services, with Nafath as the principal verification rail.

Where Saudi Arabia diverges: a transfer regime that points toward in-Kingdom data.

The Personal Data Protection Law, Royal Decree No. M/19 of 2021, came into force in 2023 and was enforced from September 2024. Its cross-border transfer regime is stricter than the UAE federal regime: outbound transfers must fit a permitted basis and may need safeguards and a risk assessment. The law states no blanket localisation rule, but in practice that can make in-Kingdom processing the lower-friction architecture. Saudi Arabia has also not published a broad dedicated crypto-asset regime, so virtual currencies remain outside the recognised local framework.

“

A global team cannot assume its existing cloud region will satisfy the Saudi regulator. ”

04 WHO REGULATES WHAT

Who regulates what, market by market

The primary financial regulator and the named AML statute differ by market, and so does whether the regulator has published explicit electronic KYC rules. Read it as the orientation map.

MARKET	PRIMARY REGULATOR	AML STATUTE & EKYC STATUS	EKYC PERMITTED
 UAE	Central Bank of the UAE	Decree-Law 10/2025 (in force 14 Oct 2025). Permitted via CBUAE digital-ID guidance.	Yes
 Saudi Arabia	Saudi Central Bank (SAMA)	Royal Decree M/20 of 2017. Remote KYC permitted, Nafath the principal rail.	Yes
 Qatar	Qatar Central Bank	Law 20 of 2019. QCB E-KYC Regulation effective 9 Oct 2023, prior approval to deploy.	Yes
 Bahrain	Central Bank of Bahrain	Decree-Law 4 of 2001. National eKYC platform live, confirmed January 2021.	Yes
 Kuwait	Central Bank of Kuwait	Law 106 of 2013. CBK digital-onboarding instructions; electronic KYC approved.	Yes
 Oman	Central Bank of Oman	Royal Decree 30 of 2016. CBO e-KYC instructions (2023) plus Mala'a registry.	Yes
 Jordan	Central Bank of Jordan	Law 20 of 2021. Binding CBJ E-KYC Instructions No. 7 of 2021.	Yes
 Morocco	Bank Al-Maghrib	Law 43-05 (amended 2021). Remote accounts under BAM Circular 1/W/2020.	Yes
 Egypt	Central Bank of Egypt	Law 80 of 2002. Remote eKYC live via CBE-backed Haweya; PDPL reg. Nov 2025.	Yes

Law numbers and dates are exact. Egypt's non-bank financial sector is supervised by the Financial Regulatory Authority (FRA).

The markets with published eKYC rules are, with few exceptions, the markets with the highest digital-identity adoption. The detail for each sits in the anchor and core sections.

04 WHERE DATA LIVES

Why transfer rules push businesses toward in-country data

With one main exception, the region's data rules are not blanket localisation mandates. The legal position is a conditional cross-border-transfer model: personal data may leave the country if the destination offers adequate protection, or under approved safeguards, or with the data subject's consent. The exception is **Saudi Arabia**, whose regime is stricter: outbound transfers must fit a permitted basis and may need safeguards, which can make in-country processing the lower-friction choice.

MORE PERMISSIVE

MORE RESTRICTIVE • IN-COUNTRY

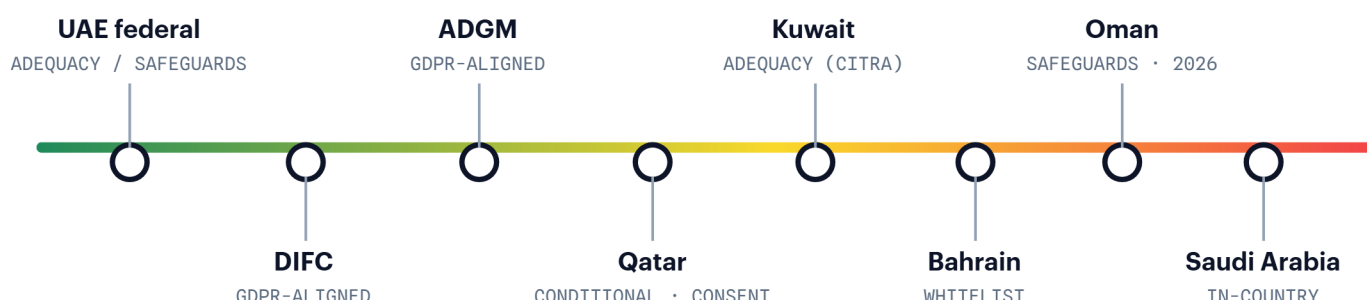


Figure 2 • Positions are relative, derived from the country data-protection sections. Confirm exact statutory wording before it drives an architecture decision.

The vendor consequence: on-premises deployment becomes a selection criterion.

Where a regime permits transfer only under conditions, those conditions still have to be demonstrated to a regulator if the deployment is audited, and the burden sits with the business. This is why many businesses decide to keep the data in country. One of the first filters teams apply when choosing a vendor is whether a verification solution can deploy on-premises or in-country and keep personal data inside the border. A SaaS-only solution with no in-region option often cannot clear that bar.

05 QATAR, KUWAIT, BAHRAIN, AND BEYOND

Qatar, Kuwait, and Bahrain

Beyond the two anchors, three more Gulf markets carry real onboarding activity, each with its own digital identity and its own regulatory posture.

THE NUMBERS AT A GLANCE



Qatar's two-system split is the common trap: Tawtheeq, the National Authentication System, is the federated login layer, while the Qatar Digital ID app is the credential wallet, enabled for airport e-gate use by early 2025. **Kuwait** has moved on too: the Central Bank has issued digital-onboarding instructions and approved electronic KYC, so remote onboarding is live. **Bahrain** has the cleanest documented story in the Gulf, with the platform operated by BENEFIT alongside the Information and eGovernment Authority.

05 BEYOND THE GULF

Oman, the Levant, and North Africa

Oman is often assumed to lack a national digital identity, and that is no longer accurate. The Royal Oman Police operates a digital identity service, and from September 2025 certified mobile versions of the national ID carry the same legal validity as the physical card for many official uses. The Central Bank issued digital-onboarding and e-KYC instructions in 2023, with a national eKYC registry (Mala'a), so remote onboarding is supported by national infrastructure as well as that digital identity.

EKYC IS PERMITTED AND SCALING

Beyond the Gulf, three markets are worth covering for teams whose footprint reaches the Levant and North Africa, and electronic KYC is permitted and actively scaling in each. **Jordan** has the strongest documented position: the Central Bank's binding E-KYC Instructions of 2021 authorise remote onboarding and set the minimum controls, and the national Sanad app added instant in-app activation in January 2026.

Morocco provides for remote account opening under Bank Al-Maghrib Circular Letter No. 1/W/2020, alongside the CNIE card and the Mon e-ID app. **Egypt** runs the Central-Bank-backed Haweya platform, which delivers remote eKYC and account opening across dozens of banks. The common thread is that national digital identity and remote eKYC are now the direction of travel across the whole region, not only the Gulf.

05 BEYOND THE GULF • AT A GLANCE

Where each market stands today

The national digital identity, the electronic-KYC basis, and the data-protection law for Oman and the Levant and North Africa trio.



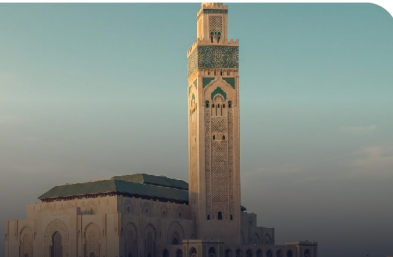

Oman

- **ROP digital identity**, legally recognised from Sept 2025
- CBO digital-onboarding and e-KYC instructions (2023), Mala'a registry
- AML Royal Decree 30/2016 · PDPL enforceable Feb 2026



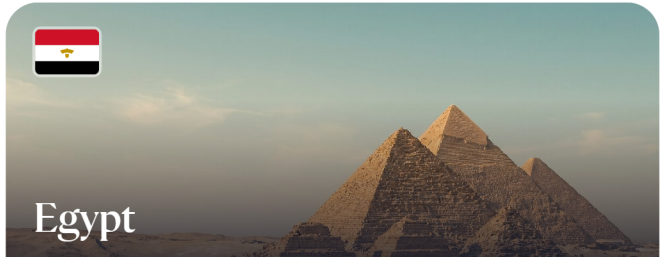

Jordan

- **Sanad** national app, ~20% adoption; instant activation Jan 2026
- Binding CBJ E-KYC Instructions (2021)
- PDPL Law No. 24 of 2023

Morocco

- **CNIE card + Mon e-ID**, ~8% adoption
- Remote accounts under BAM Circular 1/W/2020
- AML under Law 43-05 (amended 2021)

Egypt

- **Digital Egypt + CBE-backed Haweya**, remote eKYC across banks
- AML under Law No. 80 of 2002
- PDPL executive regulations, Nov 2025

Because national-eID adoption is still building in these markets, document verification is the primary onboarding lane here and the docless route the accelerator: Shufti reads Arabic-script IDs with proprietary **OCR at 94% accuracy, against 64%** for Google's general-purpose engine, so the document lane stays reliable where the eID has not yet scaled.

06 WHERE THE COMPLIANCE PRESSURE LANDS

Which industries feel the onboarding pressure most

The pressure this guide has mapped, explicit eKYC mandates, data-residency rules, and fast-changing regulation, does not fall evenly. Three industries absorb it most directly, and it takes a different shape in each.



Banking and fintech: the eKYC mandate

Central banks have made remote KYC explicit and prescriptive. Qatar's QCB requires prior approval to deploy an eKYC solution, and Jordan's CBJ Instructions specify biometrics, liveness, and tamper checks. National eID rails like UAE Pass and Nafath are becoming the expected route, and with expatriate-majority populations a flow must handle both citizen and resident credentials.



Crypto and virtual assets: a regulatory patchwork

Rules differ within countries, not just between them. In the UAE alone a provider may answer to VARA in Dubai, the FSRA in ADGM, or the DFSA in the DIFC, each with its own due-diligence bar, with the FATF Travel Rule on top. Orchestration resolves this: one flow reads the VASP's licensing zone and applies the matching Travel Rule data set from one integration instead of three builds. Saudi Arabia has no dedicated regime yet, so no single crypto-onboarding standard holds across the region.



Government and large enterprise: data residency first

For public bodies and large regulated enterprises, the national eID is both the verification method and the residency constraint, and procurement often calls for in-country or on-premises deployment a SaaS-only model cannot meet. A cross-border enterprise meets the full fragmentation at once: nine markets, nine regulators, nine credential sets.

07 WHY MOST IDV VENDORS FALL SHORT HERE

Two reasons most IDV vendors struggle in the region

Against this combination of distinct credentials, divergent data rules, and Arabic-script documents, most identity verification vendors are structurally disadvantaged in two compounding ways.

01

Cannot meet in-country data residency

A SaaS-only solution with no in-region or on-premises option cannot keep personal data inside the border. In a region where transfer rules are hard to demonstrate under audit and Saudi Arabia points towards in-Kingdom processing, that is a hard ceiling. The vendor either cannot serve the market or forces the customer into a transfer arrangement that may not survive a regulator's review.

02

Retrofitted for Western documents

Many verification systems were built around Western documents and retrofitted for everything else. That shows up as a failed read on an Arabic-script national ID or a rejected residence permit at the worst moment, when a genuine customer is mid-onboarding. A vendor that stitches together third-party engines is also always a step behind, waiting on someone else's roadmap when a regional requirement changes.

“

The two compound: a vendor that cannot keep data in-country and cannot read the region's documents is not one fix away from fit, it is the wrong architecture for the region. ”

• THE MENA IDV VENDOR CHECKLIST

Seven questions for your verification vendor

Seven questions every regional compliance and product team should put to their identity verification vendor, current or prospective.

- 01  Can the vendor deploy on-premises or in-country and keep personal data inside the border?

- 02  Does the vendor read Arabic-script national IDs and regional residence permits accurately?

- 03  Does the vendor cover the region's national digital identities, live or available for integration?

- 04  Can the vendor meet each market's electronic KYC rules without a separate build per country?

- 05  Does the vendor own its liveness and deepfake detection, with independent validation?

- 06  Does the vendor handle both citizen and expatriate-resident onboarding paths?

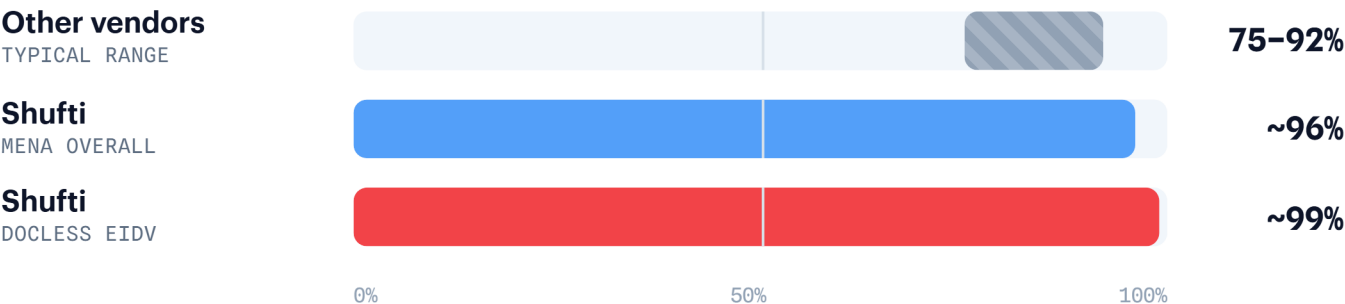
- 07  Does the vendor adapt quickly when a regional regulator changes the requirement?

08 DOCLESS ONBOARDING VIA NATIONAL EID RAILS

Why move to docless identity verification?

Electronic identity verification checks a person against an authoritative national identity source rather than a submitted document, and that switch changes both the economics and the risk of onboarding. Querying a source of truth is structurally harder to beat than inspecting an uploaded image, so the attack surface for template forgery and for deepfaked or AI-generated documents largely collapses. It also removes the document-capture step where much onboarding drop-off happens, so a user with a national digital identity finishes in seconds, and Shufti's eIDV deployments achieve **a pass rate of nearly 99%**. It pairs with document and biometric verification rather than replacing them, so coverage is never capped by how many people hold the eID.

MENA pass rate: how docless compares



Other-vendor figures are typical industry ranges, not a named-vendor comparison. Shufti overall is the blended document-and-docless pass rate across the nine markets; docless is the eIDV deployment figure. Shufti data, 2025.

National identity coverage in the region

 UAE	UAE Pass	Live national coverage
 Saudi Arabia	Nafath	Available for integration on request
 Kuwait	Kuwait Mobile ID	Available for integration on request
 Qatar	Qatar Digital ID	Available for integration on request
 Bahrain	OneID	Available for integration on request

FIGURE 02 HOW ROUTING WORKS

One platform decides the route per user

Docless leads wherever it can. The platform checks whether each user holds a usable national digital identity, then routes accordingly, so a high-assurance result is reached either way and coverage never depends on how many people in a market hold the eID.

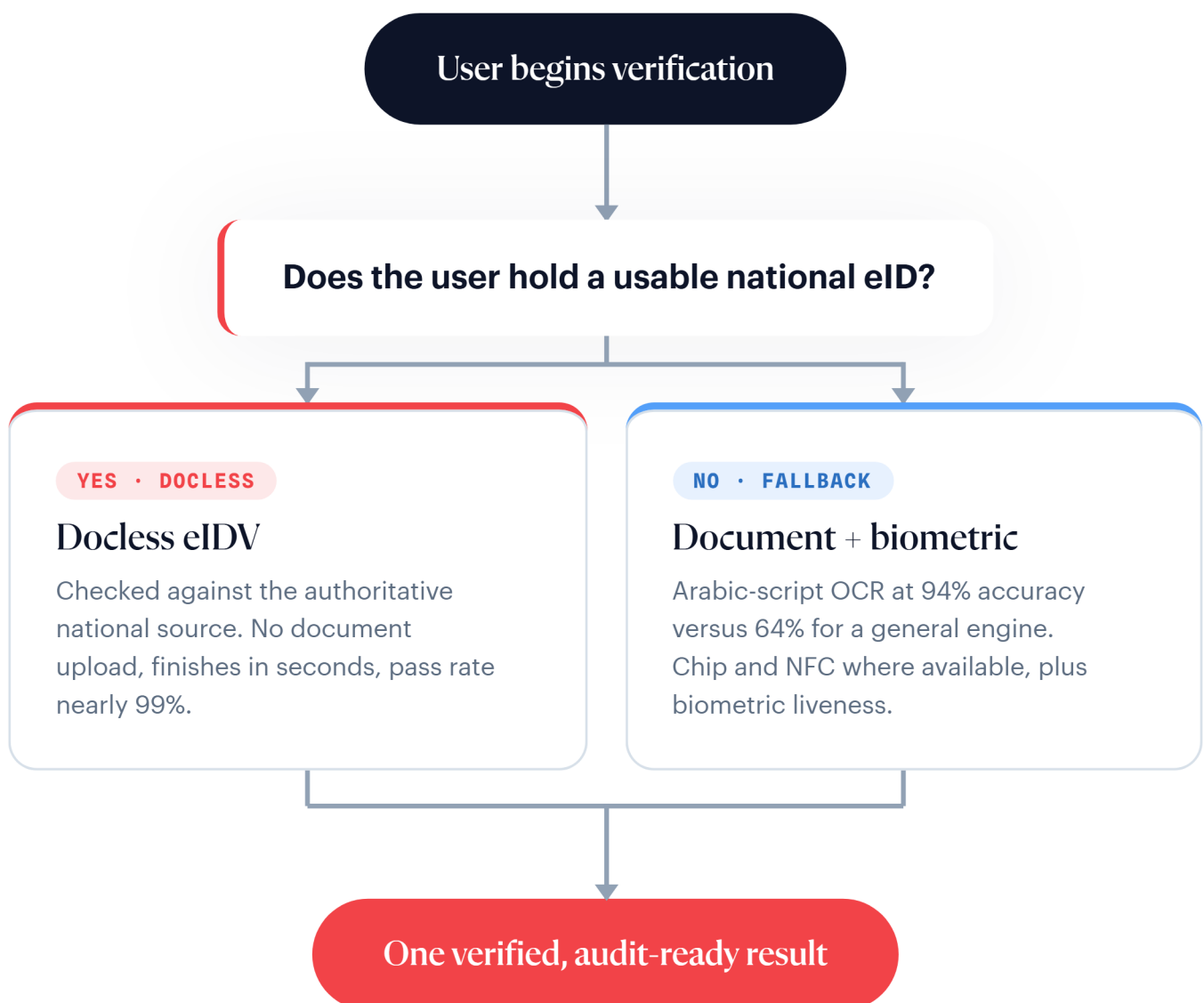


Figure 02 · Routing is per user, not per market. Where national-eID adoption is high the docless path carries most users; where it is still building the document path does, with docless applied for those who can use it. The same integration covers both.

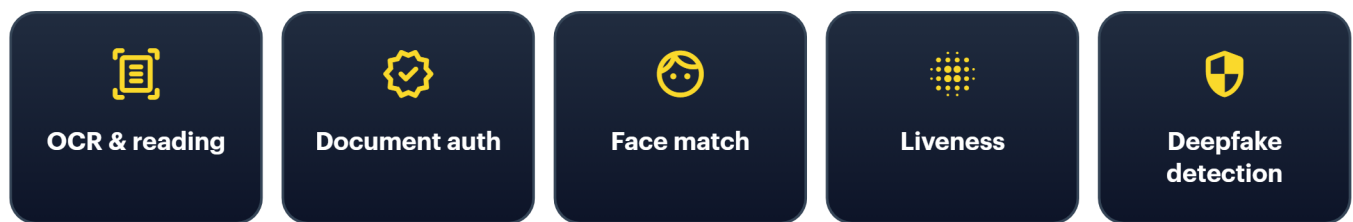
09 WHAT THE RIGHT IDV FOUNDATION LOOKS LIKE

Owned end to end, built for the region it serves

The verification problem in this region is not solved by a longer feature list. It is solved by an architectural decision: own the core verification technology end to end, accept the full range of identity inputs the region actually uses, and be deployable where each regulator needs the data to sit.

This is what flattens the curve in *Figure 01*: one owned, jurisdiction-aware platform that takes on a new market as a configuration change, not a rebuild. The same platform decides the route per user rather than per market, so a holder of a usable national eID goes through the docless route first while anyone else is sent automatically to document and biometric verification (*Figure 02*).

OWNED END TO END · ONE ROADMAP



DEPLOYABLE WHERE THE DATA MUST LIVE · ONE API



Shufti's approach

Document reading, document authentication, biometric matching, liveness, and deepfake detection are all developed in-house, on one roadmap. Shufti actively verifies 10,000+ document types each month across 240+ countries and territories, with proprietary OCR reading 150+ languages including Arabic, and no human fallback for low-confidence reads. A Saudi deployment can keep processing in-Kingdom while a Dubai deployment runs differently, without standing up a second vendor.

“ One platform, fully owned technology, deployable where the data must live, rather than a stack assembled from parts no one fully controls. ”

10 CERTIFICATIONS THAT MATTER TO COMPLIANCE

Shufti's certifications and external validations

Shufti's platform is independently validated against the security, privacy, and biometric standards that matter to regional compliance, product, and risk teams. Current certificates and audit letters are available on request.



Verification built for the region it serves.

If your team is onboarding across the Middle East, or running into the gaps this guide describes in your current setup, the honest comparison starts with a short conversation about your own onboarding data, market by market.

Book a 20-minute demo →

Docless Identity Verification in the Middle East · © Shufti 2026

SHUFTIPRO.COM · SUPPORT.SHUFTIPRO.COM

