KYC Registration and Verification

From online application to secure verification.

A complete national platform for onboarding and verification, applicable for:

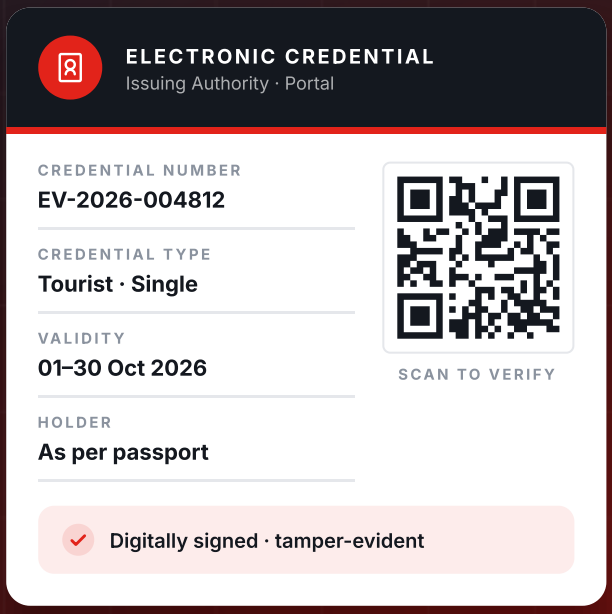
Financial Services · Telecommunications · Education · Events · Public Security · eVISA / ETA

Including KYC application, payment, officer decision, digital credential issuance and secure verification.

Deploy in weeks. Built on 15+ years of identity expertise.
Government control retained throughout.

ONE PLATFORM · FIVE STAGES

1. Online application
2. Integrated payment
3. Officer decision
4. Digital credential issuance
5. Secure verification



Secure Identity. Trusted Digital Future.

IDMETRIX s.r.o. · Your Partner for Identity Solutions.

www.idmetrix.eu

THE VALUE

Modernisation without the multi-year overhaul

Digitalisation is inevitable. The real question is how to achieve it without a multi-year, high-risk IT transformation.

Digital access

Citizens apply, upload documents, pay and receive their credential entirely online, reducing reliance on in-person application processes.

Operational efficiency

Structured digital workflows carry every application from submission through review, decision and issuance.

Government control

Officer-led decisions and full authority over policy, data and issuance. Your officers approve, reject and revoke.

Secure verification

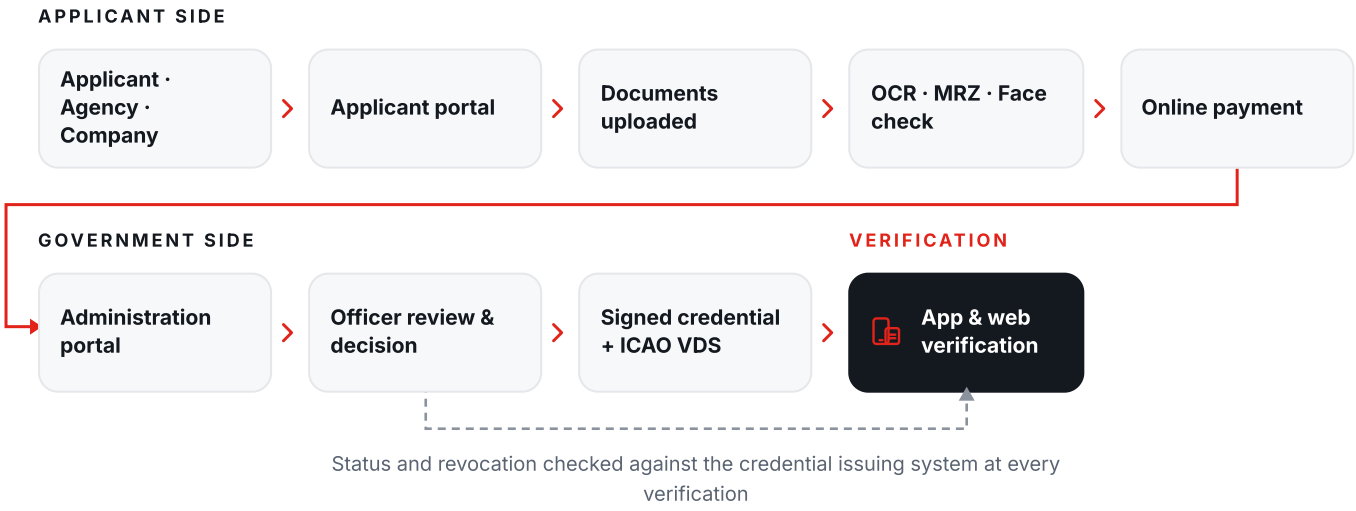
Digitally signed eCredentials with an ICAO Visible Digital Seal (VDS): authenticity and issuing authority verified by the officer.

Start with a working national platform.

Add integrations and automation as requirements evolve, on your existing infrastructure.

HOW IT WORKS

One flow from application to verification

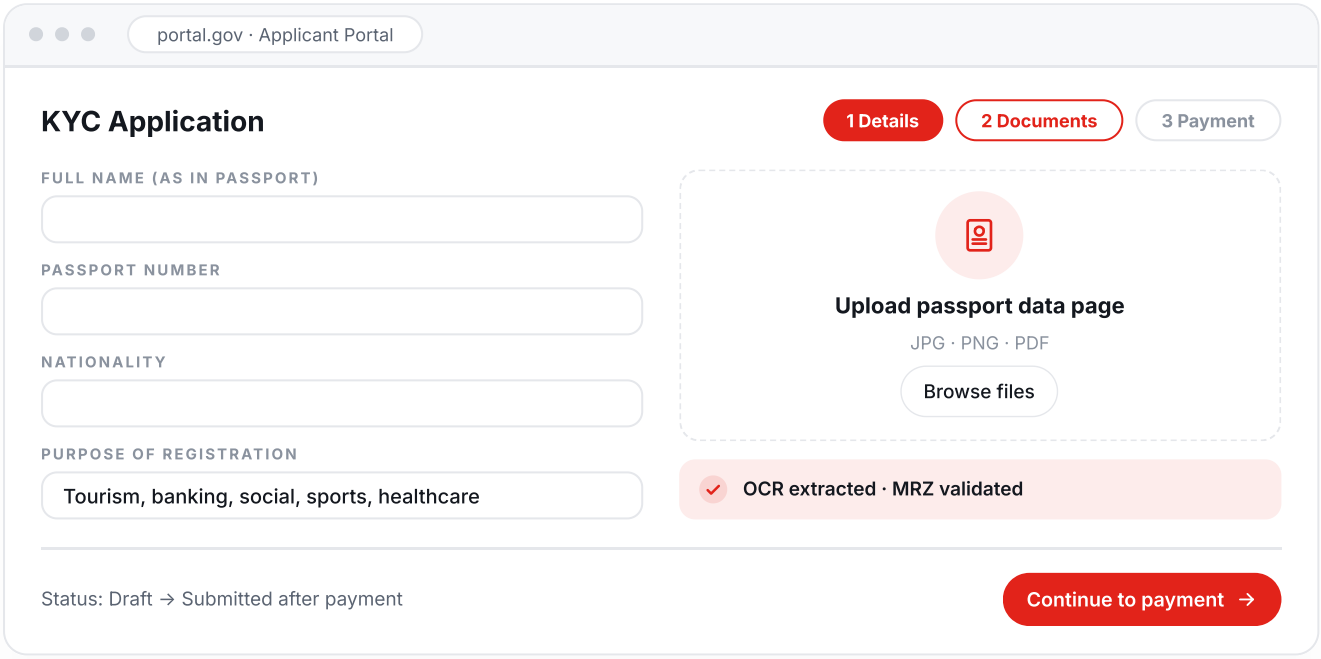


THE SOLUTION

One platform for digital credential issuance and its lifecycle

A web-based, payment-enabled platform, from the applicant's first click to verification.

APPLICANT PORTAL



PLATFORM CAPABILITIES

Online application
Individuals, agencies, companies

OCR + MRZ validation
Passport data read and checked

Face matching + liveness
Passport photo vs live selfie

Integrated online payment
Via third-party payment providers

Officer review workflow
Structured review and decision

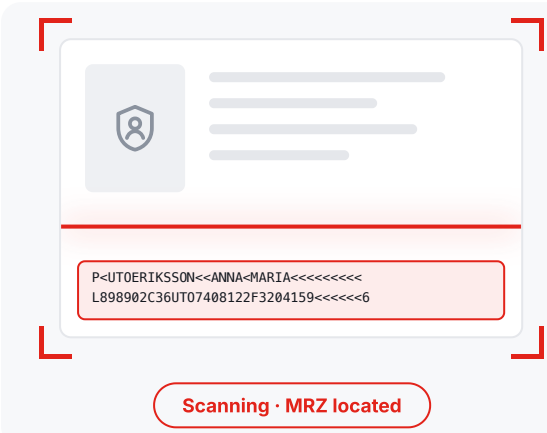
Signed eCredential
Tamper-evident secure PDF

ICAO VDS verification
Authenticity and issuer confirmed by the verifier app

Payment supports international card schemes (Visa, Mastercard, American Express, UnionPay) and local payment methods where required.

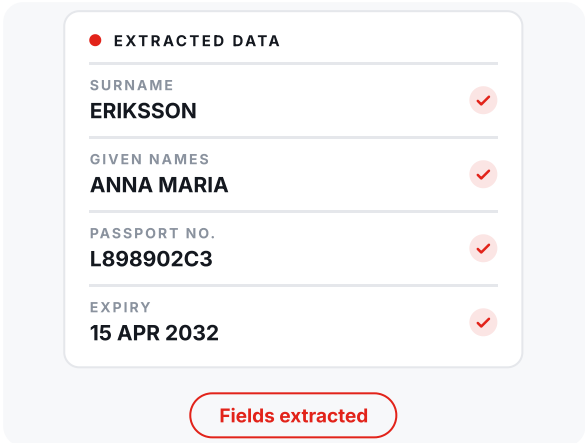
ZOOM INTO THE VERIFY STEP

How every application is checked



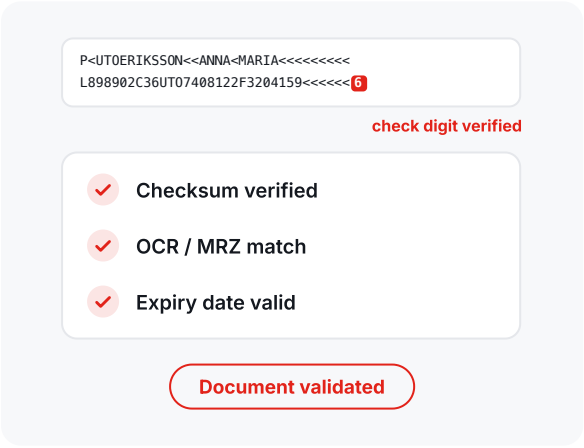
01 Passport scan

Data page captured; machine-readable zone located.



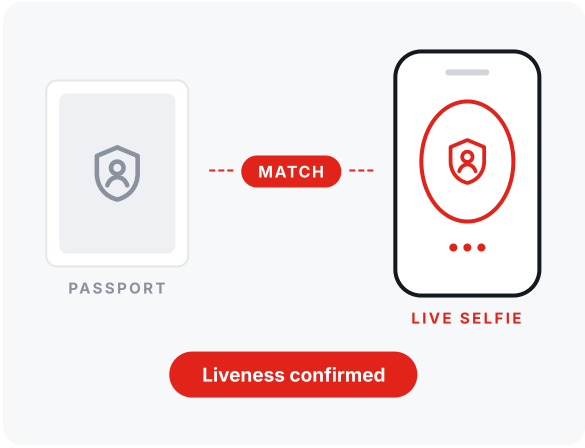
02 OCR extraction

Passport fields read automatically from the data page.



03 MRZ validation

Check digits verified; OCR and MRZ cross-checked; expiry confirmed.



04 Face match + liveness

Passport photo compared with a live selfie; liveness confirmed.

The final solution scope, configuration and integrations are defined according to the requirements of each government project.

GOVERNMENT CONTROL

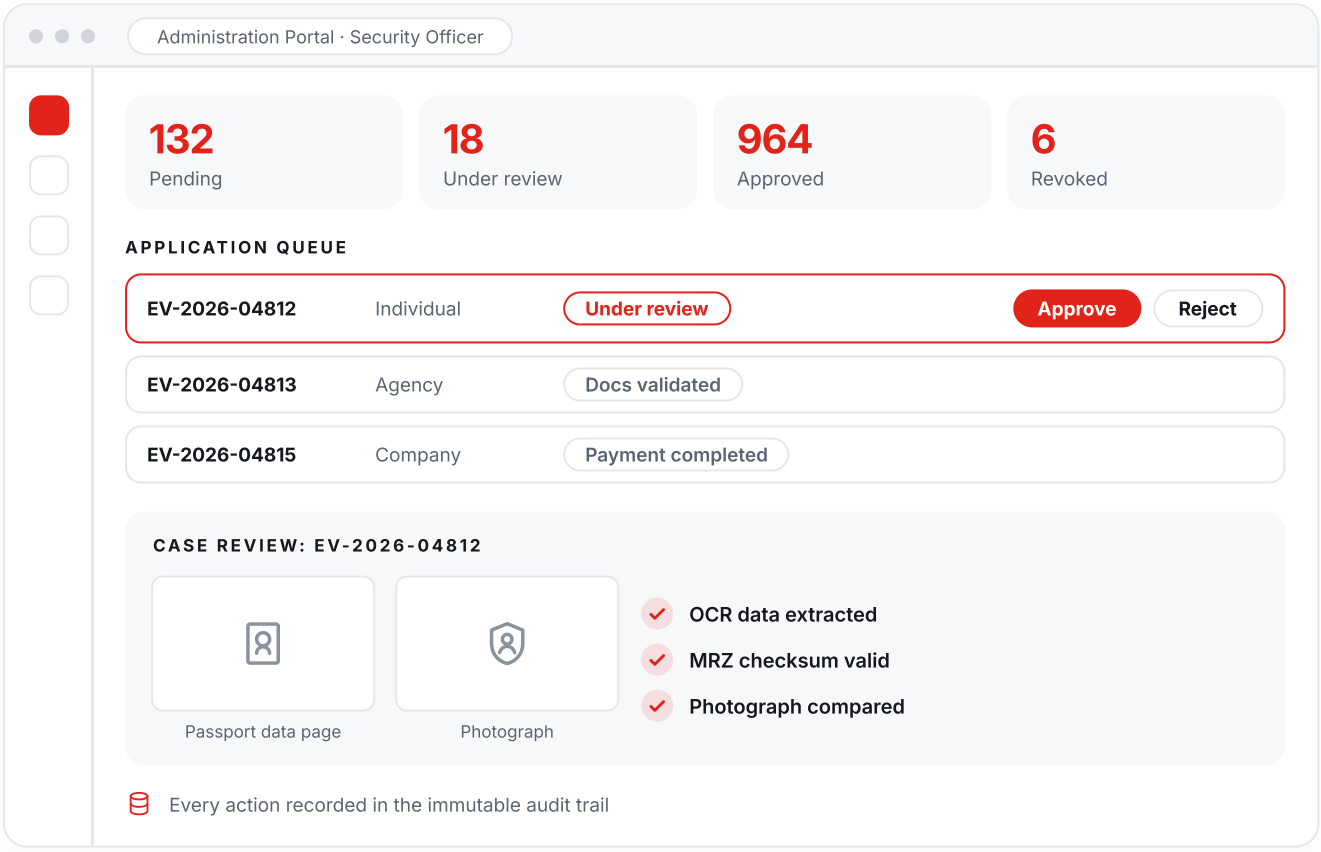
State officers stay in control at every step

YOUR OFFICERS DECIDE

- Structured review of every application
- Approve, reject or request more information
- Issue and revoke, with full case history
- Roles and permissions defined by the authority

Policy, data ownership and final credential decisions remain with the issuing authority.

ADMINISTRATION PORTAL



TRUST AND VERIFICATION

Security you can verify

Every credential is checked on two independent layers: the authenticity of the document itself, and its current status in the issuing system.

LAYER 1 · DOCUMENT AUTHENTICITY

Digital signature
Tamper-evident: any modification is revealed.

ICAO VDS
Enables verification of document authenticity and the issuing authority.

LAYER 2 · CURRENT STATUS

Validity
Current validity checked against the credential issuing system.

Revocation status
Revoked credentials are identified at every verification.

ISSUED CREDENTIAL

ELECTRONIC CREDENTIAL
Issuing Authority · Portal

SCAN TO VERIFY

CREDENTIAL NUMBER
EV-2026-004812

CREDENTIAL TYPE
Tourist · Single entry

VALIDITY
01 Oct 2026 – 30 Oct 2026

HOLDER / PASSPORT
As per passport

Digitally signed · tamper-evident

Immutable audit trail. Every action is logged; records cannot be modified.

PLATFORM STANDARDS

TLS	**At rest & in transit**	**Role-based**	**24×7**
ENCRYPTION	DATA ENCRYPTION	ACCESS CONTROL	AVAILABILITY

DEPLOYMENT MODELS

One platform. Three deployment models.

The same core registration process supports three different deployment models, selected by the responsible authority to fit its regulatory, operational and security requirements.

1 OPTION

Biometric Digital Registration

FACE-BASED IDENTIFICATION · POWERED BY IDMETRIX ABIS

- Facial recognition is the sole biometric identification modality
- Facial biometric enrolled into the authorised facial database
- Officer captures the person's face via a mobile or web application
- IDMETRIX ABIS searches the facial database; a match identifies the registered record
- The officer receives the information authorised for their role
- A unique registration number / reference is issued and can be delivered electronically, e.g. by email, and retained on a mobile device

No QR code. No physical card required: the face is the identification modality.

2 OPTION

Digitally Signed VDS Credential

SECURE PORTABLE QR CREDENTIAL

- Visible Digital Seal (VDS) issued as a protected QR credential
- Digitally signed using a certificate issued under the issuing authority's Certificate Authority (CA)
- The issuing authority is established as the trusted issuer
- Origin of the signed credential can be verified; integrity of signed data can be checked
- Unauthorised modification of signed data is detectable
- VDS data content configurable per project

A portable digital credential backed by cryptographic trust.

3 OPTION

Physical Citizen Credential

PLASTIC CARD · SMART CARD

- Plastic ID card or smart card, where required by legislation
- Visible identification information on the credential
- Optional machine-readable or electronic functionality
- Issued from the same registration platform
- Backed by the same central digital identity record

A physical credential supported by the central digital record.

COMMON FOUNDATION Digital registration + Passport OCR & MRZ validation + Facial biometrics + Central record

ONE REGISTRATION PROCESS: THREE DEPLOYMENT MODELS

Start with biometric registration → **Add a digitally signed VDS credential** → **Extend to physical or smart cards**

The responsible authority selects the model that best fits its regulatory, operational and security requirements.

DELIVERY

From decision to deployment

Target deployment: approximately eight weeks.

WEEKS 1–2
Configure
Credential types, fees, workflows and portal branding set up to your policy

WEEKS 3–5
Integrate
Payment provider, email / SMS notifications, environments prepared

WEEKS 6–7
Validate
User acceptance testing, administrator training, runbooks and handover

WEEK 8
Go live
Production cutover with engineering support from the IDMETRIX team

Using existing infrastructure where appropriate. Indicative target, subject to agreed scope, infrastructure readiness, third-party access and customer approvals.

Reuse existing infrastructure. Runs in your data centre or preferred hosting: software-led modernisation rather than heavy replacement.

Local-partner delivery model. Local partners lead customer relationships and first-line support; IDMETRIX provides the platform, training and engineering escalation.

GROWTH PATH

Start standalone. Scale on your terms.

TODAY — INITIAL SCOPE

A complete working system
- Application, payment and notifications
- OCR, MRZ, face matching and liveness
- Officer-led review and decisions
- Signed digital credentials with ICAO VDS, audit trail

NEXT — FUTURE INTEGRATIONS

Automate the checks
- Automated watchlist screening
- National registry integration
- ABIS / external biometric systems
- Semi-automated approval workflows

BEYOND — FUTURE EXTENSIONS

Connect the ecosystem
- Airline and border-management APIs
- Electronic travel authorisation (ETA)
- Mobile verification and analytics
- Connection to social programmes
- Connection to healthcare systems
- Connection to the population registry

API-first, modular architecture. Integrations are additions, not a rebuild.

WHY IDMETRIX

Secure identity is at the core of IDMETRIX's business

15+ years

of eID and digital identity expertise, proven in government identity programmes worldwide

10+ specialists

in identity and software engineering, with dedicated project management, training and knowledge transfer

Government focus

eID, ePassports, secure documents, biometrics and border management, including ICAO-aligned travel document expertise

Partner delivery

Local partners lead customer relationships and first-line support; IDMETRIX provides the platform, training and engineering escalation

Let's discuss your digital verification programme.

IDMETRIX can review your existing registration process, infrastructure and integration requirements, and define an appropriate phased deployment approach.

ask@idmetrix.eu

www.idmetrix.eu

Lermontovova 911/3, 811 05 Bratislava – Old Town, Slovakia