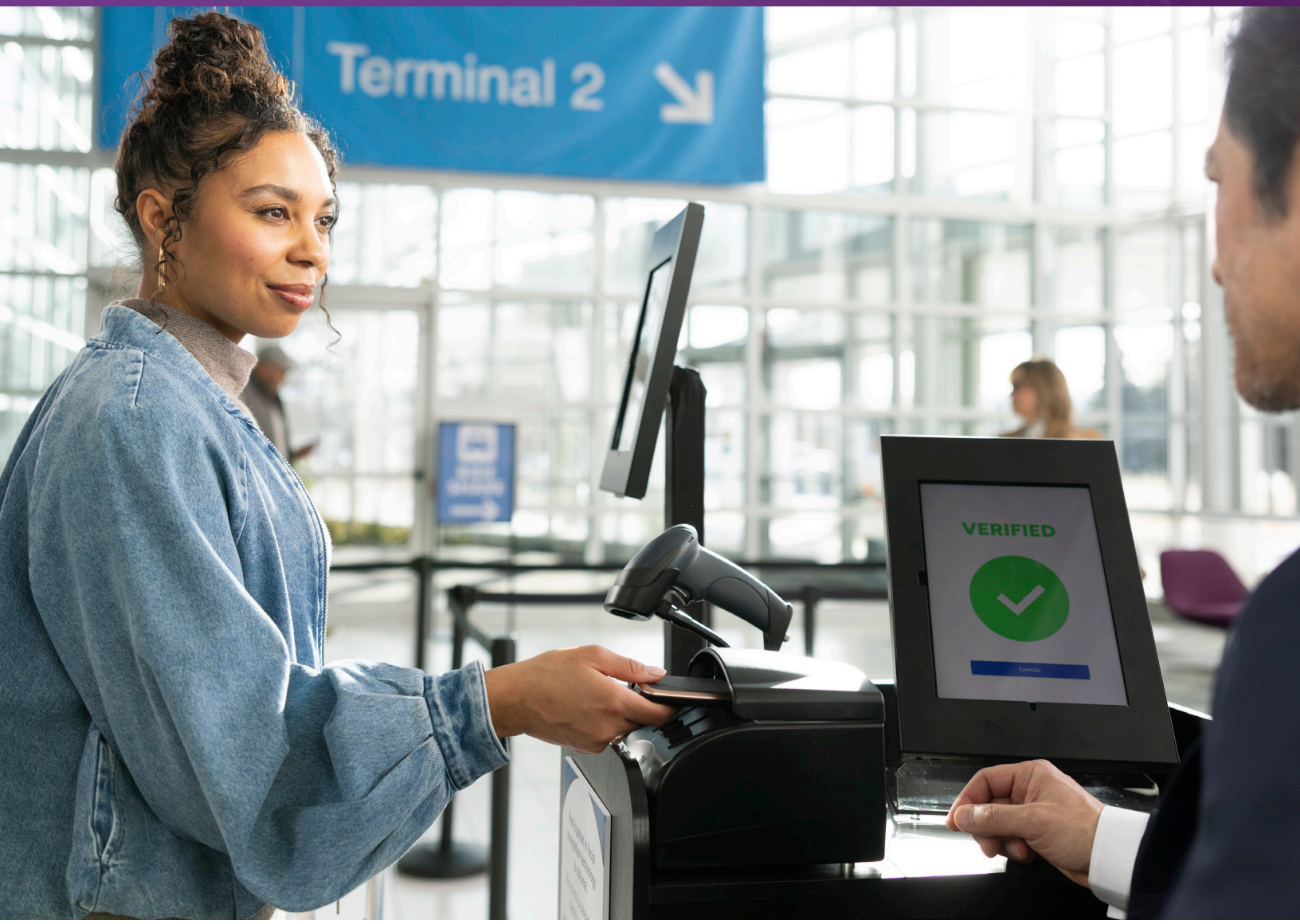
IDENTITY VERIFICATION FOR GOVERNMENT

Delivering Secure, Trusted, and Connected Digital Experiences



ENTRUST

SECURING A WORLD IN MOTION

Citizens and travelers increasingly expect seamless and intuitive digital experiences, driving global demand for streamlined, digital-first government processes. From accessing public services to moving through airports and borders, government agencies need to enable efficient digital interactions at scale, while delivering trust, security, and convenience. This imperative is reinforced by expanding global regulations for digital identity, privacy, and data protection, making identity a critical foundation for both service access and cross-border mobility.

At the same time, identity fraud is getting more sophisticated, with the proliferation of AI-generated deepfakes and morphed identity documents. Government agencies, in particular, face the daunting task of processing large volumes of citizen transactions while safeguarding national security and minimizing fraud.

The right identity verification solution helps government agencies keep services secure and user-friendly. It enables trusted access to services, seamless travel, and better fraud prevention through secure and connected digital journeys.

Purpose-Built for High-Assurance Identity Programs

Entrust Identity Verification for Government ensures:

Global Standards Compliance Support: Maintain data sovereignty and regulatory alignment and support interoperability across ecosystems with privacy-first design and adherence to ICAO, ISO, NIST, and ETSI standards.

User-Friendly Experience: Deliver intuitive, guided mobile and web journeys with multilingual support, enabling fast, touchless verification and low-friction experiences for citizens, residents, and travelers at scale.

Scalable Performance: Handle population-scale workloads with resilient, cloud-hosted deployments that maintain high throughput and continuity during peak demand or disruption scenarios.

Ease of Integration: Fit seamlessly into existing enrollment and IAM or CIAM workflows, with multiple deployment options that simplify interoperability and accelerate government digital transformation initiatives.

Intelligent Insights: Use built-in analytics and monitoring to track performance, optimize operations, and continuously strengthen security across identity programs.

Enhanced Security: Automate low-risk case processing with high assurance at the first touchpoint, enabling agencies to focus resources on higher-risk cases through centralized, real-time reporting.

Discover how Identity Verification for Government solutions helped the UK Home Office digitize its border control to help enhance security and streamline travel authorization.

Comprehensive Identity Verification for Government Programs

Entrust Identity Verification for Government is a comprehensive solution that orchestrates best-of-breed microservices to meet diverse policy, risk, and regulatory requirements underpinning government and travel processes. These microservices include document verification, biometric facial matching, liveness detection, photo QA (quality assessment), and device intelligence integrated into an IDV workflow. By corroborating evidence across multiple checks, the solution produces a risk-based identity assessment of more than 250 data points that support confident, real-time trust decisions.

This approach delivers highly accurate identity proofing at scale, helping governments digitally transform citizen- and traveler-facing initiatives.

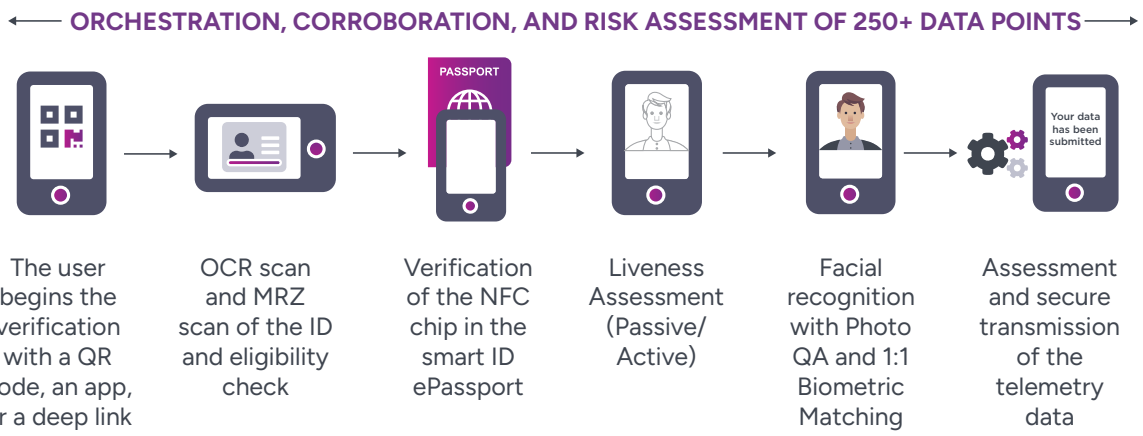
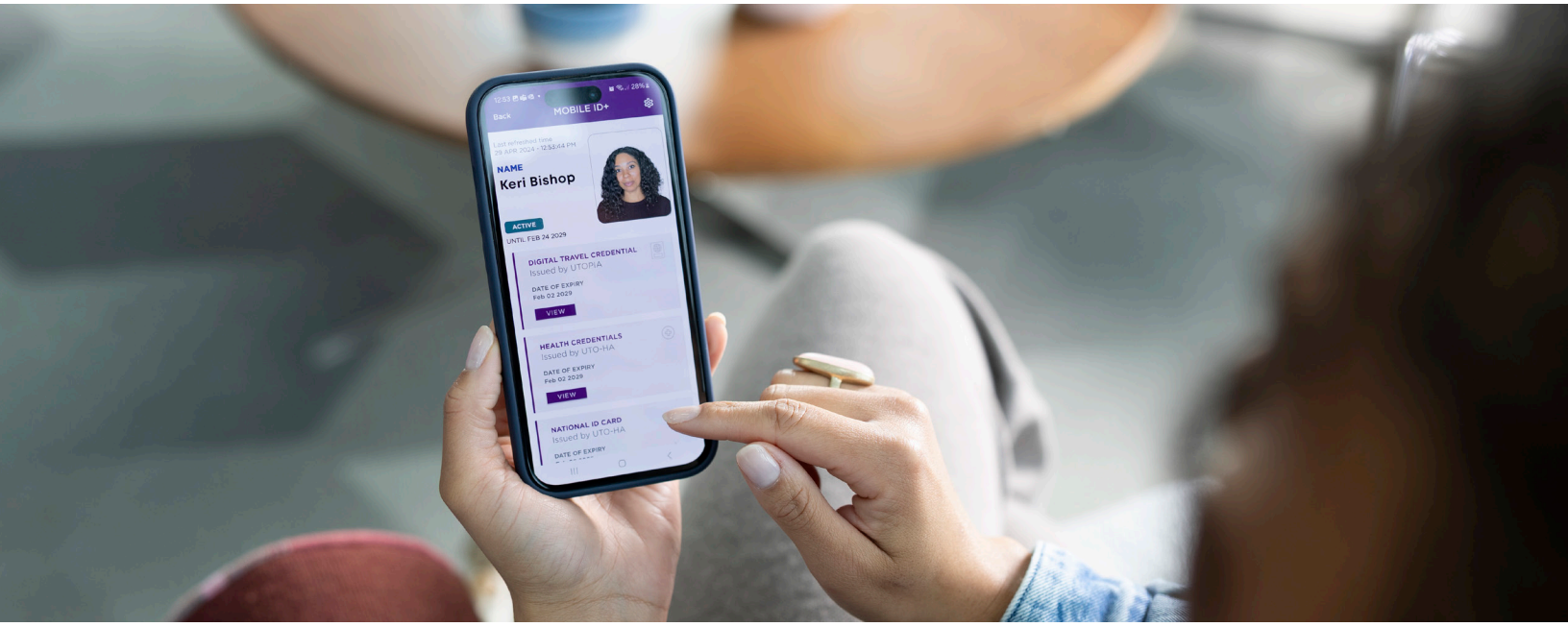


Figure 1: A Typical Identity Verification Workflow



Key Functionalities

Document Verification: Document verification validates the authenticity of government-issued documents. Using OCR and forensic analysis, this microservice examines the visual inspection zone, extracts data from the machine-readable zone, and assesses the document against a global library of eligible IDs. Captured data can be used to autofill forms, reducing manual entry errors and improving user experience.

NFC Chip Read: NFC chip verification is the gold standard for confirming document authenticity and claimed identity, making it ideal for border control, immigration, and other high-risk government scenarios. The solution auto-detects NFC chips in ePassports and smart ID cards and guides users through the scanning process. Using a smartphone's native NFC reader it validates chip authenticity and matches the encrypted data with the physical document and the holder, adding a strong layer of assurance.

Liveness Assessment: Liveness assessment protects against deepfakes, presentation attacks, and injection attacks by confirming the individual is who they say they are and physically present during verification. Entrust supports both active and passive liveness methods conformant with ISO 30107-3 and is also independently certified. The solution adapts to user context and device capabilities, minimizing friction while protecting against impersonation and advanced identity fraud.

Advanced Facial Recognition: Entrust Identity Verification for Government uses advanced facial recognition ranked among the top 5 globally in recent NIST FRTE evaluations. It verifies individuals through guided selfie capture that adapts to real-world conditions. A 1:1 biometric comparison matches live selfies with trusted ID portraits. Anti-bias AI training minimizes demographic bias, while optional photo quality assessment aligned with ISO/IEC 19794-5 and morph detection further improves accuracy and reduces failures across diverse populations.

Multi-Modal Biometrics Support: Entrust supports integration of physiological biometrics beyond facial recognition to deliver higher assurance where required. Technologies such as fingerprint and palm or finger-vein recognition can be incorporated into the IDV process. By combining multiple biometric modalities, agencies can match authentication strength with each individual's risk profile.

Device Intelligence: Device intelligence enhances fraud detection by adding risk signals captured from the device to the IDV process. Assessment of passive non-document and non-biometric signals helps detect sophisticated fraud without added user friction. These signals include device integrity, IP, geolocation data, and visual fraud detection.

Configurable Workflows: Entrust Identity Verification for Government enables agencies to configure IDV workflows to match program-specific requirements. Verification steps, decision logic, rules, and risk thresholds can be tailored for different user groups, regulatory environments, or service types. This flexibility ensures consistent eligibility checks, approvals, and referrals across agencies while maintaining a common trust framework and simplifying operations.

Flexible Deployment: Entrust Identity Verification for Government offers flexible deployment models that align with existing technology environments and modernization strategies. Agencies can embed verification into web, iOS, or Android applications using SDKs that integrate with backend systems. For faster deployment, ready-to-use native mobile applications are available without SDK implementation. All options support white-label branding to deliver a consistent user experience.

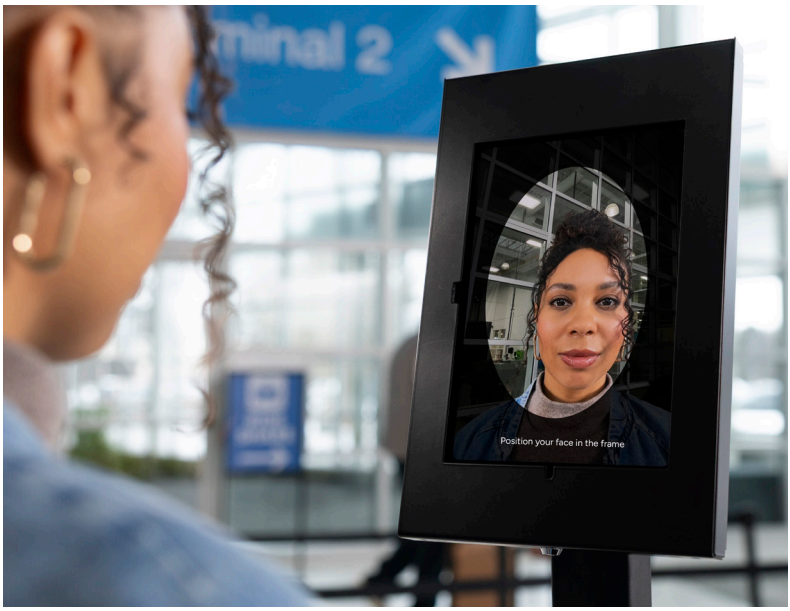
How IDV Helps Governments Uphold Security and Convenience

Entrust Identity Verification for Government supports a range of critical government programs where secure, remote identity verification is essential, including:

Digital Travel Authorizations (eVisa and eTA): Verify traveler identity remotely by corroborating passport data, biometrics, and liveness signals. This enables real-time, risk-based eligibility decisions before traveling, reducing fraud and improving border throughput without increasing operational burden.

Remote ePassport Renewal: Enable secure remote ePassport renewal by validating applicants through high-assurance document, NFC, and biometric checks. This reduces in-person workloads, shortens processing times, and lowers costs while delivering an improved citizen experience.

Touchless Biometric Corridors: Establish trusted digital identities in advance to support touchless biometric corridors, increasing passenger flow rates while maintaining strong security controls and regulatory compliance.



Social Security and Benefits Fraud Reduction: Ensure benefits are issued only to verified, eligible recipients through continuous identity validation, significantly reducing fraud, leakage, and improper payments.

Online and In-Person Test Integrity: Verify candidate identity at registration and at critical checkpoints, preventing impersonation and reducing administrative oversight costs across digital and physical testing.

Take the Next Step to Secure Your Organization

Embedding identity verification into digital transformation initiatives can be straightforward, but sustaining resilience, scalability, and long-term security amid evolving identity threats is far more complex.

Agencies need the flexibility to scale, modify, or extend capabilities of their digital-first programs. Entrust Identity Verification for Government is designed for incremental modernization and modular orchestration, offering government agencies a reliable technological foundation.

Visit Entrust.com for more information on Identity Verification for Government solutions.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION