DATA SHEET

# Drive the Adoption of Digital Government Services

Secure, efficient interactions between governments, citizens, and businesses.

## HIGHLIGHTS

Elevating citizen experiences when interacting with the public sector is a critical outcome for eGovernment.[1] In the context of the citizen, "onboarding" refers to registering and verifying individuals and businesses to facilitate service access and manage personal data.

The onboarding experience directly impacts the rate of adoption of digital services and influences public trust. Onboarding can be done in-person or remotely via digital channels. In-person onboarding is often required by policy when it's important to authenticate the identity at the outset, e.g., enrolling in national ID systems, applying for a passport, driver's license, etc.

Yet increasingly, governments are moving toward digital onboarding. It offers a more streamlined user experience, greater security, improved operational efficiency, reduced processing timelines, and lower cost of service delivery.

## THE SOLUTION

### Composable Onboarding

Entrust offers a flexible approach to onboarding that can be adapted for in-person, digital, and hybrid onboarding, while ensuring maximum data security and privacy.

Identity proofing, a process to match the claimed identity of the individual to their actual identity, is a critical component of onboarding. The user simply provides their identification credentials or ID and performs a selfie check using their smartphone.

The onboarding module of the Entrust Citizen Identity Orchestration (CIO) solution takes care of the back-end processes with the help of composable building blocks that support data collection, document verification, biometric capture, and database checks. The onboarding journey can be delivered as a mobile or web-based application, or as an API gateway with third-party systems.

1: 2025 Gartner CIO and Technology Executive Survey

ENTRUST
SECURING A WORLD IN MOTION

ONBOARDING PROCESS

## Here's a Typical Onboarding Workflow Facilitated By Our CIO Solution:

### 1. User Registration

- **User Initiation:** The user is registered at a brick-and-mortar enrollment center, or accesses the digital government portal via its website or mobile app.
- **Information Gathering:**
  - **Data Entry**: Users provide basic biographical information such as their name, email address, phone number, and sometimes a username or password.
  - **Document Upload**: Users provide identification like government-issued IDs, passports, utility bills, or other relevant documents. The data collected at this step is used to auto-fill forms.

### 2. Identity Verification

- **Document Verification:** The uploaded documents are typically subjected to automated or manual checks to verify their authenticity. This step can optionally include NFC chip scanning and verification of the eID or ePassport.
- **Biometric Verification:** Facial recognition or fingerprint scanning determines the presence of a real, live person and matches the user to their ID. This includes an active or passive liveness check to detect spoofing, deepfakes, and other fraudulent attempts.

**3. Identity Vetting:** An optional step, this ensures the verified identity is valid for the given context. Identity vetting can be automated but is usually performed by a designated vetting officer.

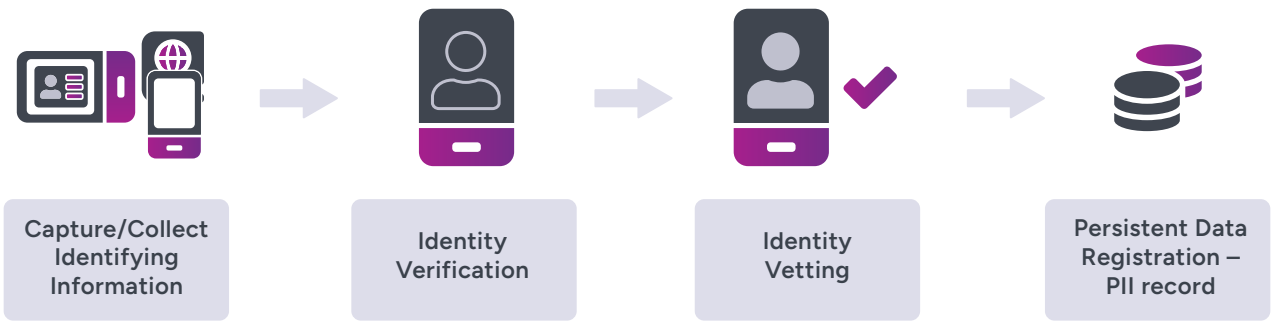
**4. Persistent Data Registration:** Non-volatile data that needs to be stored, such as the record of the identity credential, audit trail, logs, and data storage in the IT management system to facilitate future transactions.

### Enhancing Onboarding

A composable software approach also simplifies the process of adding functionalities that further enhance the user's onboarding experience.

Most onboarding processes require the user to sign documents. With the Entrust Citizen Identity Orchestration Solution you can add an eSignature workflow to sign the document through digital signing and timestamping building blocks.

## Fig. 1: Key Components of Onboarding



## BENEFITS

Entrust's onboarding solution ensures your citizens and residents gain seamless access to services, improving the rate of adoption of digital services and enhancing public trust.

- **Fraud prevention:** Accurately establishes an individual's identity from the outset, reducing the risk of fraud, including account takeover (ATO) and synthetic identity fraud.
- **Operational efficiency:** Provides time and cost savings by reducing manual reviews, eliminating paper-based processes and improving accuracy with automated form fills.
- **Improved risk posture:** Better risk assessment and management with business intelligence dashboards that ensure data security and adherence to regulations.
- **Enhanced flexibility:** The composable design architecture provides maximum control and flexibility, avoiding vendor lock-in tied to monolithic biometric platforms.

# Use Cases

Using our comprehensive CIO Solution, you can register or enroll individuals to establish their identity and eligibility to unlock various services and/or functionalities as below:

| Use Case | Description |
|---|---|
| Credential issuance | Providing secure digital or physical credentials (e.g., ID cards, digital IDs) after establishing a secure and verifiable identity for individuals or entities. |
| Service access | Streamlining access to public and private services by enabling individuals to reuse verified identity information across multiple platforms. |
| Age verification | Confirming an individual's age to ensure eligibility for age-restricted services or benefits. |
| Proof-of-life | Verifying that an individual is alive to continue receiving benefits such as pensions or Social Security. |
| Travel authorization | Granting permission for individuals to travel across borders or within restricted zones based on identity and eligibility. |
| Biometric corridor access | Allowing seamless and secure movement through checkpoints using biometric recognition technologies. |
| eSignature enablement | Allowing users to sign documents digitally using verified identity credentials. |
| Consent management | Enabling individuals to control and manage how their personal data is shared and used across services. |
| Address verification | Confirming the residential or business address of an individual or organization for service eligibility or compliance. |

## Security is our priority

Our solution is built with security at its core, adhering to a comprehensive set of global standards and regulations to support compliance, risk mitigation, and seamless deployment. These include:

- **ISO/IEC 27001:** Information security management
- **ISO 27701:** Global privacy standard for the protection of PII
- **ETSI TS 119 461:** Biometric identity proofing
- **ETSI EN 319 401:** Trust service provider policy and security requirements
- **GDPR:** General Data Protection Regulation for data privacy
- **NIST Guidelines:** Standards for digital identity proofing

Entrust also supports:

- BIPA: Biometric Information Privacy Act
- Web Content Accessibility Guidelines or, WCAG 2.1 (W3C Recommended Guidelines)
- iBeta PAD Level 1 and Level 2 for Android and iOS: For Presentation Attack Detection (PAD) based on the ISO 30107-3 standard

In addition, the Entrust Citizen Identity Orchestration solution aligns with several regional and industry-specific regulations, ensuring robust protection and operational readiness across diverse environments.



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

ENTRUST
SECURING A WORLD IN MOTION