



ENTRUST



Entrust Instant ID Government

An enterprise-class platform for establishing trusted identities, issuing secure credentials, and lifecycle management

Entrust Instant ID Government software revolutionizes the issuance and management of highly secure passports, national IDs, PIV cards, and other secure government credentials. It streamlines every step of the process — including enrollment, identity verification, application approval, document issuance, and post-issuance management. As a standards-based platform, it replaces the typical delays and cost overruns of custom software development with the certainty of a preconfigured software solution. It manages the capture of biometrics and biographic information, then validates individual identities by interfacing with recognized authorities and registries. It also prepares identity attributes for issuance and allows users to update existing credentials, which can eliminate costs associated with physically re-issuing cards, passports, or other documents.

SOFTWARE BUILT FOR SECURITY

Entrust Instant ID Government offers an enterprise solution for issuing a variety of credentials, including driver's licenses, passports, national IDs, secure employee badges, and entitlement cards.

Secure Enrollment. Capabilities include biographic and biometrics capture and breeder document verification.

Identity Management. The software interfaces with external identity sources to verify and manage secure identities.

Credential Management. The platform includes business rules, profiles, and data preparation capabilities.

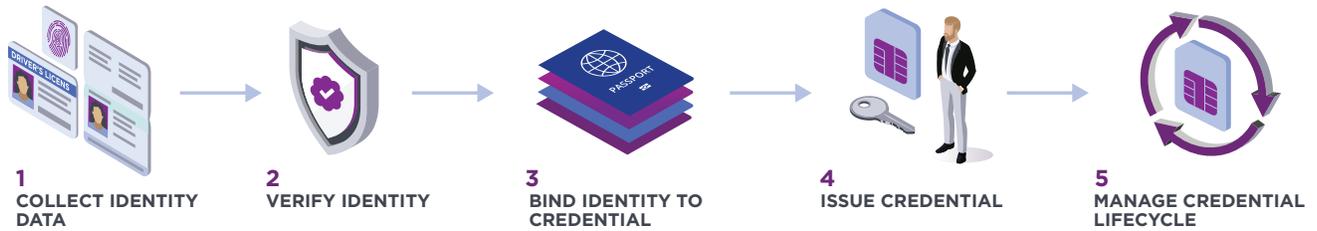
Issuance. Users can choose central, distributed, or mobile issuance models — or a hybrid solution.

Post-Issuance. The platform enables effective management of credentials after issuance.

- Faster implementation
- Reduced program risk
- Technology interoperability
- Investment protection
- Physical and logical security



Entrust Instant ID Government



Establish Trusted Identities. Instant ID Government empowers end-users to collect identity data, such as facial images, fingerprints, or iris images. It also verifies identities by interfacing with biometrics matching systems, such as AFIS and watch lists. Verified identities are securely bound to credentials.

Issue Secure Credentials. The software manages the data preparation process, including physical attributes on cards or passports and electronic data on smart cards. Issuance options include central, instant, mobile, or hybrid models.

Manage Issued Credentials. Post-issuance capabilities allow end-users to reissue, renew, or revoke credentials. Other post-issuance capabilities include activation, deactivation, PIN management, and certificate renewal.

Decades of trusted government solutions

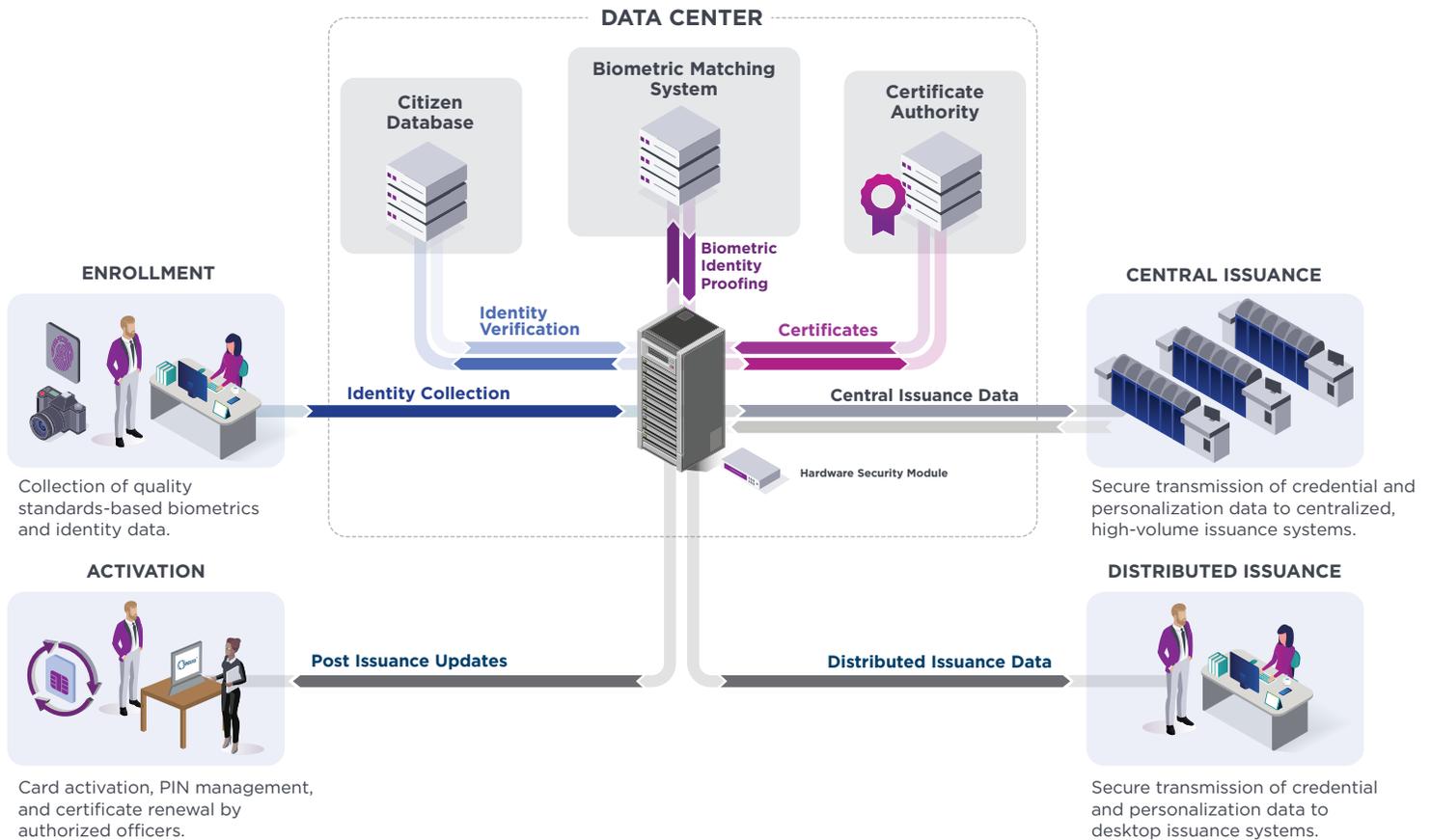


Expert deployment, minimized risk

Entrust participates in industry organizations and standards groups such as ISO. Our deep understanding of industry standards and best practices results in secure identity solutions that meet both technical and market requirements. Our experience implementing secure credential programs around the world allows us to help customers deploy secure and efficient programs — and minimize program risk. Every day our solutions are used to issue more than 15 million cards and smart cards and tens of thousands of passports.



Entrust Instant ID Government



Identity Collection. Collect facial images, fingerprints, iris scan, biographic data, and supporting documents.

Identity Verification. Interface with identity sources such as central database and biometric matching systems.

Certificates. Create certificate profile requests. Receive the certificates and bind them to specific identities.

Credential Issuance. Securely issue credentials with central, distributed, or hybrid models.

Post-Issuance. Card activation, PIN management, and certificate renewal.



Entrust Instant ID Government

Designed to address key identity issues

Government agencies face a host of challenges when it comes to secure identity programs. In addition to preparing for escalating physical security threats, governments must develop logical infrastructures that integrate with an evolving identity infrastructure – which includes elements such as watch lists, certificate authorities, and biometrics. Most existing identity systems are not designed to accommodate this increasingly digital and highly connected world.

Instant ID Government is designed specifically to empower government agencies to successfully manage passport, national ID, driver's license, healthcare, and benefits programs in this challenging environment. It provides an enterprise-class platform for establishing trusted identities and issuing secure credentials. It also enables management of secure credentials after they have been issued.

Adherence to industry standards and a web-based open architecture allows for fast, predictable deployment. The flexibility of the software also makes it easy to scale up or down to accommodate program changes – such as growing populations, the addition of new technologies, or the creation of new document types.

Integrated with Datacard® issuance systems

Instant ID Government offers built-in compatibility with the complete portfolio of Datacard® card and passport issuance systems. You can choose from high-volume central issuance systems or desktop systems for distributed issuance.

Government agencies can choose to create a centralized issuance program, which provides exceptional control over key program elements – including data, cardstock, blank booklets, issuance systems, personalization supplies, and finished credentials.

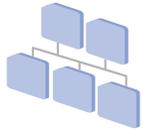
Instant ID Government also enables distributed issuance, which allows government agencies to produce identification cards and passports in multiple locations. Distributed issuance is ideal for producing credentials in remote areas or issuing credentials at embassies or consulates.

In addition to software and issuance systems, Entrust also offers a complete portfolio of card delivery systems, consultative services, technical support, secure laminates, and program supplies.



Entrust Instant ID Government

KEY ADVANTAGES



Workflows

BPMN 2.0 standards-based preconfigured workflows for common processes. Flexibility to customize workflows.



Lifecycle Management

Built-in lifecycle management for credential issuance, reissuance, renewal, and revocation.



Secure Issuance Anywhere

Robust and secure issuance – choice of central, distributed, and hybrid issuance models.

PROGRAM BENEFITS

Fast Deployment

Instead of custom development, government agencies and system integrators can leverage preconfigured workflows for faster deployment.

Reduced Risk

Adherence to industry standards and reduced need for customization minimize the risk of cost and time overruns.

Interoperability

Standards-based architecture streamlines integration with other systems and minimizes the risk of becoming locked into proprietary products.

Future-Proof

Flexibility and compatibility make it easy to expand the platform and incorporate new technologies as they become available.

Layered Security

The platform provides strong lines of defense for data-in-motion and data-at-rest. Role-based access controls, audit trails, strong encryption, and multi-factor authentication.



Entrust Instant ID Government

KEY FEATURES

Credential Lifecycle Management

- Preconfigured workflows for managing issuance, reissuance, and renewal processes
- Credential business rules
- Credential types management
- Preconfigured support for ICAO LDS 1.7, ISO DL 18013, and FIPS 201 based data preparation
- EAC/BAC/AA standards support
- Post-issuance capabilities

Secure Issuance Anywhere

- Central issuance support for ID cards and passports
- Distributed (desktop) issuance of passports and ID cards
- Hybrid (central and distributed) issuance model support
- Batch and route to central or distributed issuance systems
- Key management capabilities

Integration

- Preconfigured integration with leading capture devices, AFIS, PKI, and cards
- Web services APIs for integration
- Tools for adding support for new capture devices
- Tools for importing enrollment and credential data from external systems

Security

- Role-based access control
- Data-in-motion and data-at-rest protection
- Strong encryption
- Tamper-evident audit logs
- Multi-factor authentication

Workflows

- BPMN 2.0 standards-based workflows
- Preconfigured workflows for common processes
- Flexible workflows for easy configuration and customization

Enrollment

- Preconfigured enrollment workflow for capturing facial images, fingerprints, signatures, and documents
- ICAO- and PIV-compliant biometrics capture and processing
- Flexible and configurable enrollment workflows

Customization Toolkit

- Web services APIs
- Data mapping tool
- User interface customization
- Sample code and documentation
- Designer and developer tools

Standards

- ICAO 9303, FIPS 201, ISO DL 18013
- LDS 1.7, BAC, EAC
- ISO 19794-4, ISO 19794-5, INCITS 378/385
- JPEG 2000, JPEG, WSQ
- BPMN 2.0, Web Services, XML, CSV



Learn more at
entrust.com



ENTRUST