ENTRUST

Entrust Instant ID

Data and Information Security

Security overview

The following highlights our commitment to security and the key benefits of using Instant ID. Although a robust security posture is a collaborative effort between Entrust, vendors, other entities, and our customers, and is dependent on various other factors, we make our best efforts possible to secure the product.

KEY FEATURES & BENEFITS
Protecting physical access

Our state-of-the-art card production applications contribute to the following protections:

- Cards using strong cryptography for tamper resistance

- Protection against duplication of cards in possession

These protections provide peace of mind by securing access to valuable assets like schools, universities, and sensitive areas within a building.

Protecting data

Data breaches can be expensive - one estimate pegs the average cost at around $4M US.[1] A simple internet search for, "university data breach," can show the extent of recent breaches.

Instant ID provides the following to help secure customer data through the lifecycle:

- **Data Creation:** When data is created by the user in a browser environment, we support technologies like content security policy to leverage features of modern browsers to enhance data protection.

- **Data in Transit:** We support industry standard protocols such as TLS 1.2. Instant ID provides features to encrypt the channels through which data flows, between users, services, databases, authentication systems, and more, thereby reducing the possibilities of man-in-the-middle attacks. Our enhanced cipher list provides features like Perfect Forward Secrecy.

[1]https://www.ibm.com/security/data-breach

Learn more about Instant ID Software at entrust.com

Instant ID Data and Information Security

- **Data at Rest:** We provide users the ability to encrypt the datastores used by the application with strong crypto algorithms and keys such as AES-256. We also provide a way for customers to encrypt the file system used by the application.

Protecting the application that processes the data

Instant ID provides the following application security features:

- **Authentication:** We provide our users the ability to configure strong password requirements. Our authentication mechanisms extend beyond the human users and extend into service endpoints to protect from insider attacks and also avoid relying exclusively on firewall protections.

- **Multi-Factor Authentication (MFA):** Everyone these days is rightfully concerned about phishing attacks and other password compromises. Instant ID provides the ability to configure strong, risk-based, multi-factor authentication systems including SAML 2.0 support to mitigate such issues.

- **Authorization:** We provide fine-grained control for the admin users to fine-tune the permissions for different types of users such as operators, designers, and admins. This helps control the access level on an as-needed basis.

- **Audit Logs:** DB-based audit logs provide information to identify any possible attacks on the system, by tracking important events like failed login attempts and cards issued.

- **Cryptography:** Our smart cards employ strong cryptography.

- The Instant ID team follows recommendations proposed by industry standard organizations like OWASP and NIST in improving our application security.

The above features help in reducing insider attacks, which could lead to things like unauthorized issuance of cards and exfiltration of sensitive data.

One size does not fit all, so Instant ID provides UI-based security configurations for our customers to match the application settings to their individual security needs.

Capture Manager (the component used by Instant ID that captures images) provides the following security features:

- Encrypted connection between Capture Manager and Instant ID server

- Accepts authenticated requests with strong tokens

Security practices at entrust

As a global company offering multiple products and solutions centered around information security, Entrust is in a unique position to cross-pollinate best security practices across multiple product lines.

- Entrust follows a rigorous secure development lifecycle process.

- This involves performing automated scans for vulnerabilities in open source and proprietary software and performing remediations as appropriate.

- We perform targeted ethical hacking against our products to proactively find issues.

- A team dedicated to security assurance helps us build security into the DNA of our offerings.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223