Security Practices: Instant ID as a Service

Entrust follows a rigorous secure development lifecycle process for Instant ID as a Service.

Security practices

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, including:

- Performing automated scans for vulnerabilities in open source and proprietary software and performing remediations as appropriate
- Performing targeted ethical hacking against our products to proactively find issues
- Having a dedicated security assurance team builds security right into the DNA of our offering

Security overview

The following highlights our commitment to security and the key benefits of using Instant ID as a Service (IIDaaS). 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 many efforts to secure the product.

Protecting physical access

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

- Cards that use strong cryptography for tamper resistance
- Prevention of duplication of cards in possession
- Secure access to valuable assets like schools, universities, and sensitive areas within a building

Learn more about Instant ID as a Service at Entrust.com

Security Practices: Instant ID as a Service

Securing the printer as a secure IoT device

- The Sigma printer TPM2 is used to store the Crypto keys and it is used as a cryptographic engine for encrypting/decrypting crypto keys during TLS operations in-system.
- Secure Boot: With the Secure Boot, the firmware shall ensure that only authentic firmware images are used to boot the printer by validating their digital signatures.

Protecting data

IIDaaS 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. IIDaaS provides features to encrypt the channels through which data flows between users, services, databases, authentication systems, and more, reducing the possibilities of man-in-the-middle attacks.
- Data at Rest: We use strong crypto algorithms and keys to protect data.
- Printer to Message Broker: In IIDaaS printer to message broker, communications are encrypted using TLS to provide confidentiality. Printer to Broker authentications are enforced by JSON Web Token (JWT) authentication mechanism using strong cryptography. This prevents rogue clients from being able to subscribe and publish to sensitive topics in Broker. In addition, authorization controls are employed by the Broker. This provides tenant data separation and allocates privileges to internal services on an as-needed basis.

Securing data connection to an on-premises database

Employ secure on-prem gateways that sit between the IIDaaS and customer database. These gateways use TLS to encrypt the communication with IIDaaS and secure credentials to connect. They can also be configured to use an encrypted channel to communicate with the on-prem database.

Learn more about Instant ID as a Service at Entrust.com

Security Practices: Instant ID as a Service

Protecting the application that processes the data

IIDaaS provides the following application security features:

- Authentication: We provide our users the ability to configure strong authenticators, e.g., OTP and strong passwords.
- Multi-Factor Authentication (MFA): People are rightfully concerned about phishing attacks and other password compromises. IIDaaS provides the ability to configure strong, MFA systems 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.
- Audit Logs: DB-based audit logs provide information to identify possible attacks on the system, by tracking important events like failed login attempts and cards issued.
- The IIDaaS team follows recommendations proposed by industry standard organizations like Open Web Application Security Project® (OWASP) and National Institute of Standards and Technology (NIST) in improving our application security.

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

Securing the application in the cloud

IIDaaS provides the following application security features to secure the application in the cloud:

- Threat & Vulnerability Management (TVM) scan is performed every release
- Entrust subscribes to AWS security bulletins, all of which are reviewed and, if relevant, applied as recommended
- All changes are reviewed by the Change Advisory board, including the security team
- Administrative access to deployed environment must pass through multiple access levels
- IIDaaS releases are fully automated
- IIDaaS deployments follow the blue-green deployment approach
- IIDaaS leverages AWS platform provided security and availability features

Security Practices: Instant ID as a Service

Security breach notification process

Security is in our DNA and it's infused into our software products in many ways, including:

- We conduct security software scans using third-party tools
- We proactively test our applications for potential security issues
- If any vulnerabilities are identified, depending on the nature of the vulnerability, a Security Bulletin will be issued. The typical route for notification would be via email, but alternative means of communication can be agreed to within the contract
- Entrust provides required notifications without undue delay and in accordance with applicable regulatory requirements and contractual terms.

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