

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 o ering 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 o ering

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 e ort between Entrust, vendors, other entities, and our customers, and is dependent on various other factors, we make many e orts 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

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

Protecting the application that processes the data

IIDaaS provides the following application



Entrust and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation