Entrust Identity as a Service
Security Whitepaper – Confidential
Last Revised April 2025

Introduction

Entrust's mission is clear— we are relentlessly focused on securing a world in motion by enabling strong identities, secure payment issuance, and trusted infrastructure. It energizes us as an organization, to continuously improve our solutions, enhance our capabilities, expand strategic relationships, and increase our leadership position within the market.

Entrust combines technology, people, and process with expertise to produce world class innovations in trusted identity and secure transaction technologies.

Who Entrust is today?

Since our early days pioneering high-volume card issuance machines, we've continually advanced and innovated to become one of the world's leading providers of cybersecurity solutions. We are privately backed and owned by the same long-term investors for 40 years. We serve customers on every continent, and the innovations we bring to market are expanding our reach and driving strong growth.

Security and Risk Management Organization

Entrust has a dedicated team of security professionals focused on security and compliance, based on ISO 27001 and Cloud Security Alliance frameworks.

Working across all organizations within the business, Entrust maintains ISO 27001 certification. The Entrust Information Security Program includes Governance Risk and Compliance (GRC), Threat and Vulnerability Management (TVM), Secure Software Development Lifecycle (SSDLC), Security Architecture, Defensive Cyber Ops, and Security Incident Response.

Governance, Risk, and Compliance

Entrust maintains compliance with federal, financial, international, and industry regulations and policies, including ISO 27001, NIST 800-53, NIST CSF, FISMA, and Certificate Authority Browser (CAB) Forum WebTrust. ENTRUST also keeps in alignment with FFIEC and PCI DSS. ENTRUST manages controls using the Unified Control Framework (UCF).

At Entrust our senior leadership is engaged in the Information Security Management System (ISMS), chaired by the Chief Information Security Officer and ISMS manager. The Chief Information Security Architect is engaged across all business and technical organizations, leveraging a security reference architecture based on the Cloud Security Alliance. An Enterprise Risk Management team performs internal audits, providing additional attention to risk from a business perspective.

Threat and Vulnerability Management

The Entrust Information Security Program has a primary goal of protecting the confidentiality, integrity, and availability of information in all forms. Threat and Vulnerability Management (TVM)

is essential in reducing the overall risk to Entrust information systems presented by known vulnerabilities. The TVM program coordinates the measurement and remediation of vulnerabilities within deployed applications (developed in-house and consumer off-the-shelf), storage services, operating systems, network devices and perimeters, data centers, and other IT services. Scanning includes measuring compliance of systems to the ENTRUST policies and standards.

The program also provides Static and Dynamic Application Security Testing (SAST/DAST) for use in all software development, requiring that threats are addressed prior to production release. Additionally, periodic third-party penetration is performed by third parties to verify the effectiveness of the overall Information Security program.

Secure Software Development Lifecycle

Software development is a critical component of the Entrust business model. Accordingly, the Information Security Program has a vested interest in assuring that the product reinforces the foundation tenets of preserving the Confidentiality, Integrity and Availability of information assets. Documented standards and guidelines set forth the requirements for the mitigation of information security risks that are discovered in the development of software. Software assurance processes are reviewed within the scope of annual ISO 27001 audits.

Security Architecture

A team dedicated to security architecture actively engages across all business and technical projects, maintaining a security reference architecture to facilitate design and to communicate strategy across the organization. Security architecture review is required for all projects, ensuring alignment with best practices and company policies and standards. The team provides architecture patterns and solutions to address threats consistently.

Security architecture ensures that projects are designing with consideration of security practices and controls, including:

- Authentication: employing standards, verifying user claims across zones, properly handling sessions, etc.
- Authorization: organizing access control business logic manageably, reviewing policy closely, aiming for consistent execution of policy, and leveraging verified identities from authentication processes.
- Accountability: granular traceability, system event logging, authorization decision logging, centralized log management, monitoring, and alerting.
- Confidentiality: TLS 1.2 or greater for data in-motion AES 256 for data at-rest.
- Integrity: X.509 signature validation (and TLS).
- Password escrow: service credentials deployed out-of-band and protected with encryption, file integrity monitoring, and process isolation in production environment.
- Isolation: strict isolation of development and production environments, leveraging logical and physical network segmentation, multi-tenant and multi-instance isolation strategies, bastion hosts for production administrative access, privileged access management.

- Input validation: addressing OWASP Top 10 threats in code, assessment processes, and using Web Application Firewalls.
- OS Hardening: Center for Internet Security (CIS) benchmarks are used where applicable guided by security professionals, trained in threat analysis and exploitation techniques.
- Architecture design: actively engaging Solution Architecture in the selection and design of secure platforms, libraries, algorithms, systems, physical and virtual infrastructure, and communication flows.

Defensive Cyber Ops and Security Incident Response

A dedicated team focuses on monitoring the state of all environments, actively watching for anomalous activities. A Security Incident and Event Monitoring system is used to collect logs from all critical systems, alerting the Security Operations Center team to analyze events to determine whether the dedicated Security Incident Response team should escalate.

Additionally, the team anticipates attacks using active threat intelligence subscriptions tuned to Entrust and its customer threats. Dedicated professionals actively consume and monitor feeds, providing early warning, keeping the Information Security Program and network teams on alert when threats are observed.

AWS Security

The Identity as a Service (IDaaS) product leverages Amazon Web Service (AWS) platform services to support a Secops strategy.

- IDaaS is built in Amazon Web Services (AWS) cloud – IDaaS uses four data centers in different regions, which are North America, Brazil, Germany, and Ireland.
- The solution is securely positioned in AWS cloud and Entrust employs end-to-end encryption on all data in motion and data at rest.
- Distinct AWS accounts are used to isolate production environments from pre-production systems and activity.
- Access to production follows separation of duties principles while adding a hardened bastion host for any administrative activities.
- Host images are hardened following CIS guidelines and tested for vulnerabilities prior to approval for production use.
- AWS Config Rules are employed to monitor and automatically remediate deviations from baseline, monitoring host images, NACLs, VPC, and Security Groups.
- AWS VPC and NACLs are used to isolate application layers and reduce attack surface.
- AWS Web Application Firewall (WAF) is used to address common application threats and to reduce bot traffic.
- AWS KMS is used to encrypt data at-rest.
- All backend traffic is protected with Virtual Private Network access.
- The system is designed with limited to no need for human operational administration.

IDaaS Security

- Authentication tokens are used for all API calls.
- Authorization policies and entitlements are granular.
- Customer level encryption of data further segments customer data.
- Data at Rest: Entrust uses strong crypto algorithms and keys to protect data.
- When data is created by the user in a browser environment, Entrust supports technologies like content security policy to leverage features of modern browsers to enhance data protection.
- Data in Transit: Entrust supports industry standard protocols such as TLS (Transport Layer Security). IDaaS 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.

Certifications and Privacy Notices

Certifications and Privacy notices referenced in this document are located on Entrust's website:

- ISO Certifications https://www.entrust.com/legal-compliance/iso-certifications
- Information Security Documentation https://www.entrust.com/legal-compliance/security