



ENTRUST

SECURING A WORLD IN MOTION



Entrust Cloud Services Consultancy

Version control

Rev	Date	Author	Description of change
1.0	23-12-2025	EP	Initial Submission
2.0			
3.0			

Entrust contacts for this submission are:

Name	Title	Phone	Email
Eric Piroux	Sr Sales Exec - Digital Security		eric.piroux@entrust.com
Emeka Okoye	Tech Sales Consultant		emeka.okoye@entrust.com

Confidentiality statement

This document contains information proprietary to Entrust Corporation ("Entrust"), and whose unauthorized disclosure would cause damage to the interests of Entrust. Entrust reserves the right to require the return of the document, and the destruction of any copies or extracts of it made by the recipient. The right to copy and use this document is limited to that necessary for evaluating and submitting a proposal to the End Customer, and this document must not otherwise be used or disseminated without the prior written consent of Entrust. Requests for permission for wider use or dissemination should be made to an Entrust contact listed above.

© 2025 Entrust Corporation. All rights reserved.

Contents

1	Summary	1
1.1	Features of the PKI consultancy and CCOE.....	1
1.2	Entrust Cryptographic Centre of Excellence Overview	1
1.3	Core security assets require a strong crypto strategy:	2
1.4	Crypto Governance Consulting:	2
1.5	PKI Governance Health Check (Expert-by-your-side):	2
1.6	PKI System Health Check:	2
1.7	PKI Governance Consulting:.....	3
1.8	The Service Benefits.....	3
2	Why Entrust?	4
2.1	tScheme	6
2.2	On Boarding and Off Boarding Process	7
2.3	Data Protection, Location & Extraction/Removal Process	7
2.4	Data Centre Tier Rating & Overview	8
2.5	Security and Assurance.....	8
2.6	Backup & Disaster Recovery	9
2.7	Contacts	9
2.8	Ordering and Invoicing.....	9
2.9	Termination of Contract	10
Appendix A.	Entrust profile and history of innovation	11

1 Summary

Entrust consultancy is designed to provide consultancy support to both the Entrust SaaS entries and those of our partners on G-Cloud including Managed PKI, Managed Certificate Life Cycle, Key Control As A Service and PKI As A Service, now integrated as a unified platform “Entrust Cryptographic Security Platform” (CSP).

Also available as a specific package is a PKI discovery via Entrust’s Cryptographic Centre of Excellence (CCOE) whereby Entrust’s PKI experts will assess the customer’s current PKI deployment and produce a report with recommendations for improvements to the PKI. These improvements could be on a technology or policy basis, or both.

1.1 Features of the PKI consultancy and CCOE

- Proven methodology
- Engineers with SC Clearance
- PKI, Policy/Assurance, HSM, Cryptography and IDM specialists
- Reports that can help customers shape future PKI improvements and policy
- Market-leading expertise in Certificate Policy (CP), Certificate Practice Statement (CPS) and PKI technology

1.2 Entrust Cryptographic Centre of Excellence Overview

- Entrust, a leader in cryptographic security solutions, is the first certification authority (CA) to offer a Cryptographic Center of Excellence.
- It’s designed to help organizations balance the risk associated with IT practices that expand crypto use cases by accelerating a crypto strategy for enhanced digital security. We work alongside security, risk, and compliance teams as a trusted partner. Cryptography is dynamic, with changes taking place on various axes. New digital practices, such as DevOps, IoT, cloud, and multi-cloud environments, upcoming PQC migrations, exponentially increase risks that lead to business disruption and security threats.
- As enterprises adopt new IT practices that expand their crypto footprints, the need for a CryptoCoE has become essential for securing a broadening attack surface.

Regulations and compliance standards around the world require businesses to encrypt their customers’ personal and financial information. Also, as computing devices become more powerful, key lengths and algorithms must evolve to protect organizations from brute force attacks. The pace of change is accelerating, and new challenges arise daily. These dynamics disrupt traditional crypto and PKI planning, as organizations increasingly rely on those technologies to improve their overall security postures.

If not managed properly, crypto can expose critical infrastructure to vulnerabilities. As crypto evolves, particularly in relation to the forthcoming crypto-agility, policies and processes need to be amended to maintain compliance with updated security standards.

1.3 Core security assets require a strong crypto strategy:

A solid crypto and PKI management strategy can help security, compliance, and risk professionals lead their organizations in establishing a CryptoCoE. Crypto is critical infrastructure that requires expertise and dedicated resources to bring it under control and into compliance. It calls for a set of organizational standards and best practices to rein in rogue crypto and establish governance. The Entrust CryptoCoE encompasses five main pillars: (Discovery, Analysis, Remediation Strategy, Best Practices and Maintenance).

It's designed to augment operational cryptographic and PKI processes with tools and expertise providing increased insight into the cryptography that organizations rely on to maintain secure operations and comply with regulations that are applicable to their businesses.

These building blocks can be employed in a modular format to deliver a custom experience based on your organization's specific needs.

1.4 Crypto Governance Consulting:

Our crypto experts can supplement your team as trusted advisers to your organization. They deliver expert guidance and support on the policies, procedures, processes, and people who define and implement the controls surrounding your cryptographic systems. The consultancy culminates in a crypto roadmap on how to achieve your defined goals.

1.5 PKI Governance Health Check (Expert-by-your-side):

A proper PKI implementation goes beyond technology. It needs to demonstrate essential compliance standards for audits. In addition, your PKI should be built to support both current and future business requirements.

Our experts can review your PKI policy documentation (CP, CPS, RPS, PDS) and review the roles, processes, and policies that have been established for your organization. Our experts will compare those policies with best practices, standards, and your business use cases and applications.

Then, we will deliver actionable recommendations to provide you with clearly defined and formal documentation that's designed to close procedural gaps and reduce risk.

1.6 PKI System Health Check:

It's not uncommon for an organization to be operating a PKI that was originally deployed 10 or 20 years ago. This timeline typically surpasses resource tenure and creates a

knowledge gap. Over that time, an organization is likely to have increased its digital sophistication and its number of use cases.

It's important that the technology and software that comprise your trust environment is up to date and adapts to changes in your business. For example, modern digital ecosystems typically require a PKI that can grow and add capacity — or one that can seamlessly interact with remote apps and modern systems. We can help guide your teams by assessing the status of your existing PKI implementation – including the equipment and algorithms in use – to help ensure it meets both current and future business requirements.

1.7 PKI Governance Consulting:

A crucial step in the initial design and deployment of an effective PKI is the formal documentation and definition of the policies that will be used to govern your PKI. Our experts are readily available to support you by defining the policies, roles, and procedures according to best practices, so they can then be enforced within your organization.

Entrust builds trust through assessment and advisement. Our expert services help build confidence in your organization's crypto and PKI security posture so that we can help you maintain compliance, enforce policies, and deepen engagement with regulatory agencies. This can help you avoid failed audits, service outages, and non-compliance with regulations.

1.8 PQC readiness assessment

Entrust's PQC Readiness Assessment helps organizations understand their cryptographic posture and prepare for the transition to post-quantum cryptography. Delivered through the Cryptographic Center of Excellence, the assessment evaluates crypto-agility maturity, maps where PQ-vulnerable algorithms and dependencies exist, and identifies gaps that could impede migration.

It provides clear, actionable recommendations and a tailored roadmap so organizations can remediate risks, strengthen agility, and confidently plan their move to quantum-safe cryptography

1.9 The Service Benefits

- Reduces project risks, costs and timelines
- Proven many times so you are in safe hands!
- Services provided underpinned by our Assurance Framework

2 Why Entrust?

Entrust has been providing secure PKI and smart card based Services from its ISO27001, ex-military, ultra high-security data centre in Berkshire since 1998. We specialise in 'On Demand' services where extremely high security and compliance is mandatory. As such, we build and run CAs for many government and commercial organisations.

Entrust have built and operated over 100 audited and approved systems. Examples include PKIs for Public Services Networks, NHS, Defence, Finance, 4G/LTE PKI for Telcos, ePassport PKI for many countries including the UK, etc. All solutions are provided with bespoke policy documentation sets, under the appropriate legal jurisdiction and specific to the PKI requirements. Most are audited and accredited for PKI operations (via tScheme or ETSI).

As an established provider of PKI and Trust Services with a reputation for delivering reliable and cost-effective services that fit business needs, we believe that we have all the attributes to successfully build and manage a PKI Service, a BYOK service, a Root CA or a BYOK for government organisations of all kinds.

Entrust key competencies include:

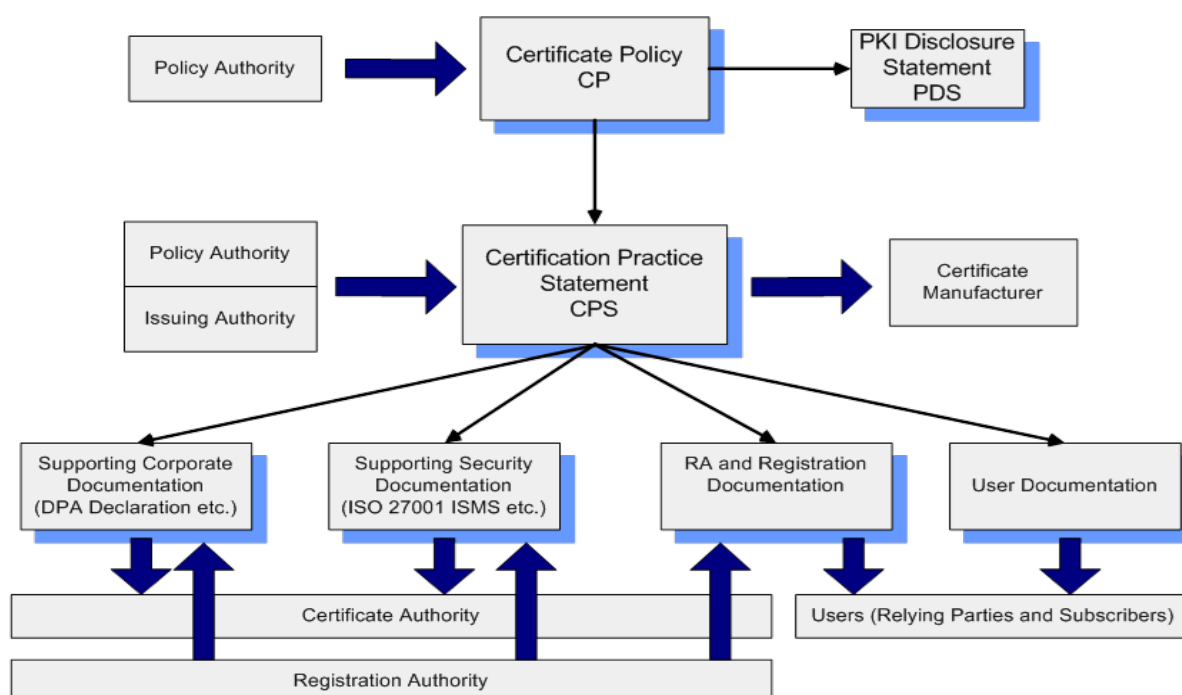
- PKI technology choice of Microsoft and/or Entrust software.
- We can offer "on premise" or managed service solutions as well as cloud services in Azure, AWS etc.
- We operate our Managed Services from UK locations under Policies controlled by our customers and under UK/European Law;
- Our entire operations are ISO27001 accredited;
- We have delivered many complex and large scale PKIs – many involving multinational and multijurisdictional elements that require special expertise in Policy, assurance and compliance;
- All PKI components hosted and controlled within the Entrust data centre are compliant with and therefore can easily attain internationally recognised criteria & approvals e.g. tScheme;
- All Entrust services are delivered to the most exacting levels of service, trust, compliance and assurance;

We use highly skilled personnel with high security clearances, who can deal with every aspect of PKI and security. Our staff are also SC cleared.

Our PKI builder methodology

When we build a PKI, we use our PKI Builder methodology, which exploits the Entrust Assurance Framework (EAF). The EAF is a fully developed and tested set of architectures, designs, baseline policies, procedures, and business practices that make up the components of a complete PKI system and can be used to jumpstart the development of a customised PKI. Importantly, PKI Builder delivers a standards compliant PKI that will satisfy customer requirements and the most rigorous regulatory requirements.

Figure 1. Fig 1 - The EAF policy component heavily exploits PKI Disclosure Statements to give flexibility and cost effectiveness to PKIs that have to fulfil compliance and assurances standards.



PKI Builder includes the assessment of the business requirements, dependent applications, host infrastructure, technology selection and design. This provides a firm foundation upon which physical design, compliance, processes and policies, testing and full deployment can be completed. All solution aspects such as backup systems and contingency arrangements are also addressed.

Technology

Entrust is vendor independent and product neutral; we implement systems using the most appropriate technology for the requirement.

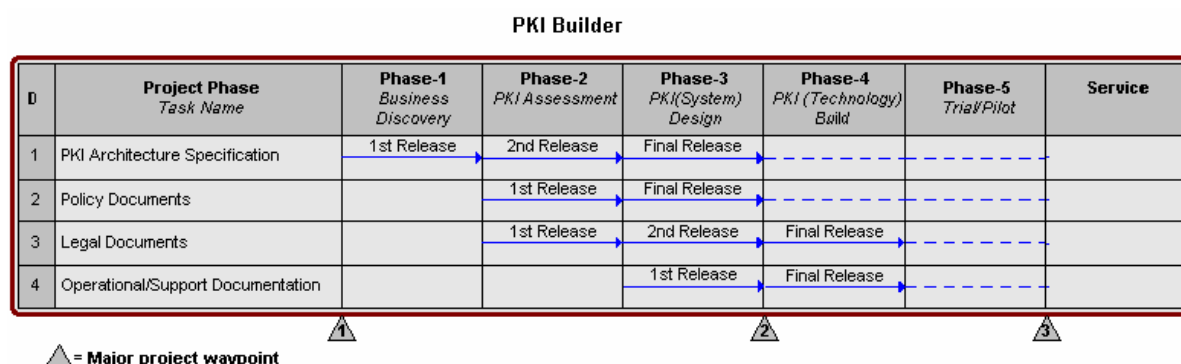
Project Management

Entrust manages and controls the PKI Builder process in accordance with timescales and other requirements agreed with the client. A project lead handles all coordination and control functions as well as maintaining close liaison and interface with the client.

Entrust apply action-centred project management throughout. The project plan, the controlling document for the project, is managed and controlled by the Entrust project manager. The main interface document for project control is the Project Status Report – typically produced fortnightly to coincide with project meetings, it is used for progress monitoring, issue resolution and planning.

We use control and quality processes throughout PKI Builder.

Figure 1. Fig 2 - PKI Builder Overview



Stages

Figure 2 illustrates the PKI builder process. Major milestones are shown at the bottom. It can be seen that key deliverables are developed iteratively. This is necessary as the process incorporates close involvement and liaison with the customer. It also allows PKI builder to be scheduled to match customer planning and resource availability. Thus, whilst a robust and complete methodology, PKI Builder can be adapted to suit any particular engagement.

The PKI design document forms the first major deliverable and a milestone early in the project. Other activities coincide with this step, for example, a project plan to align with customer requirements will be produced. This is undertaken so that all aspects of solution refinement are reflected in advance of system build stages.

The next component incorporates test system build, testing, piloting, application and integration, and shakedown of all aspects of the solution and supporting services. We use a formal change control process during this phase to ensure the customer is completely in control of any on-going refinement to the system. During this phase, policies are completed and procedures and operational details established.

We always advocate a period of trialing to ensure the PKI is exercised fully.

PKI Builder concludes with formal key signing (root and subordinates) of the operational system.

Thereafter, the system is deployed and operated to the defined standards of compliance.

2.1 tScheme

Entrust has helped more organisations achieve tScheme Approval than any other. Our standard PKI Builder approach strictly uses ISO27001 & tScheme best practices and assurance processes. Managed PKI Services running within the Entrust Secure Data Centre also comply with tScheme assurance profiles.



tScheme is an independent regulatory body publishing agreed best practice criteria for secure electronic transaction services. It grants approval to services that meet those strict criteria as shown by independent external assessment and publishes their details in its secure website Directory of Approved Services.

2.2 On Boarding and Off Boarding Process

These processes are specific to the solutions our consultancy team are assisting with. Please see additional Digital Marketplace entries for full information on these processes as they relate to the solutions themselves.

2.3 Data Protection, Location & Extraction/Removal Process

Where relevant and/or necessary, data will be retained by Entrust in accordance with the Policy and this retention period may be substantial. Entrust is fully compliant with the Data Protection Act and upholds, through our ISO27001, ISO9001 processes and publication of Policy and privacy information the HMG Information Principles.

The mechanisms, processes, risk assessments, systems, access controls, security governance and Policies required for the highest levels of protection of data for Entrust Managed Service delivery is encompassed within our company wide ISMS (Information Security Management System). We operate systems and services certified to best practice standards which include:

- ISO 27001
- tScheme
- ETSI
- ISO9001

Many of our services are for government departments and agencies, all of whom require specific and stringent data protection standards. Entrust uses a comprehensive set of security controls embracing physical, technical and personnel including:

- Secure Facilities: Military grade facilities with segregation and controlled access zones,
- Physical Access Control system - logging and auditing,
- CCTV,
- Specialist, qualified security staff including CLAS, CITP, and MSCE,
- Full background security and CRB checks. Many technical staff hold HMG clearances,
- Separation of duties. Security staff are segregated from operations with a direct reporting line to the Board,
- Regular internal / third party audits against certification standards,
- Penetration testing,
- Certified security equipment, e.g. Common Criteria, FIPS, BS, ETSI,

- Formal information security classification scheme.

These security controls are managed by our risk treatment process. This ensures the prescribed data protection is met for services we provide. The methodology is designed with flexibility so that new services are incorporated routinely.

2.4 Data Centre Tier Rating & Overview

Entrust operates its services from its Trust Service Centre (TSC) which is an ex-military Armoury. TSC is ideally suited to Cloud Services through a combination of extreme physical robustness, multiple approvals and certifications as well as Entrust's expertise.

The Entrust Data Centres are classed as Tier 2, they comply with the EU Code of Conduct on Data Centres Energy Efficiency and the primary Data Centre's capabilities include:

- Elastic/burstable resources:
 - 2 x dedicated WES circuits connected to geographically dispersed Points of Presence (POP)
- Guaranteed/non-guaranteed resources:
 - Entrust's connectivity to the Internet consists of redundant leased lines (2x in high availability mode). Bandwidth is fully allocated to Entrust with a 1 to 1 contention ratio.
- Persistence/non-persistence of storage:
 - Persistent storage for Virtual hosts is provided by redundant vSphere ESX servers hosted on two geographically dispersed locations. Local backups are to cartridges (rotated weekly with one cartridge stored off site). All critical Certificate data, where applicable, is backed-up to a contingency site on an hourly basis and stored on a backup server that is also backed up to cartridge. Business information is backed up nightly to a separate contingency site. All communication is via a VPN link.
- Type of Hypervisor:
 - Our VM environment Hypervisor consists of two components vSphere VM management controls the ESX server community and management of system backups is controlled by Veeam. All of our systems are also monitored by Opmanager.

2.5 Security and Assurance

The Entrust security model is based on fundamental good practices and ensures a high level of management control. It comprises a number of best practice elements for information security and continuity.

We operate established, approved and proven formal processes for the management and governance of managed services:-

- ISO 27001 controls through our Security and Quality Management process,
- tScheme use for compliance management,

- We can also accommodate additional customer specific audits insofar as they do not breach existing standards.

Entrust applies security and contingency controls to its entire operations, covering both the Trusts primary data centre and its geographically separate contingency site. Both locations have multiple levels of network and power contingency, together with a high level of systems contingency. Physical and logical access to both sites is strictly controlled and audited.

Entrust operations are also compliant with and audited to ISO9001 standards and are subject to a process of continual improvement. This is achieved by performance measurement and reporting against SLAs, risk assessments, internal and external audits, and other feedback mechanisms.

Governance resides in the Entrust quality and security committees which regularly meet to manage and enforce the policy, compliance standards (defined for our services), review performance and agree any necessary changes.

All Entrust personnel are highly proficient; all undergo security clearance and a continual programme of training. All are subject to performance review and awarded a formal approval status to work on managed services. Furthermore, all high level security processes are carried out under two-person control.

2.6 Backup & Disaster Recovery

Entrust operates a progressive business continuity approach. Layered backup services ensure data and applications can be recovered quickly and contingency hardware allows for rapid recovery from equipment failure. In addition to recovery for systems, the Primary Datacentre (DC) is a commercial Tier 3 DC, has separate independent network connections, site-wide battery-based UPS and a full service backup generators that can provide power for the entire DC in the event of a sustained power outage.

We operate a geographically independent contingency site in support of the Certificate Factory – the Trust Service Centre (TSC). This site is examined as part of all our compliance assessments. The contingency site benefits from similar facilities to the Primary DC in terms of networking and power. Contingency tests to confirm the ability to move operations to the site are conducted regularly.

An additional third secure site is used for storage of security components to ensure resilience and to support high availability services.

2.7 Contacts

Entrust Contact Details luke.niemiec@entrust.com

Tel: +44 (0) 7741 306362

2.8 Ordering and Invoicing

Entrust's PKI CONSULTANCY is available to order from the Digital Marketplace. Invoicing takes place upon completion of the agreed scope of work.

2.9 Termination of Contract

Using our SCS consultancy, an Exit Plan can be created if required. This is rarely relevant to consultancy.

2.10 Services schedules

<https://www.entrust.com/legal-compliance/terms-conditions/professional-services>

PKI governance is under PKI health check

For CSP, PS schedule can be found here: <https://www.entrust.com/legal-compliance/terms-conditions/cryptographic-security-platform>

Appendix A. Entrust profile and history of innovation

At every stage, Entrust has been there to keep you safe

Entrust Corporation (Entrust) was founded in 1969 and is a privately held, \$1B+ organization with its headquarters in Shakopee, Minnesota, USA.

We've established secure connections across the planet and even into outer space. We've enabled reliable debit and credit card purchases with our card printing and issuance technologies. Protected international travel with our border control solutions. And safeguarded networks and devices with our suite of authentication products.



Figure 2. Entrust by the numbers

Backed by more than 25 years of digital identity experience and 55+ years of security innovation, the Entrust team delivers world-leading products that follow the most stringent digital security standards.

- Approximately 100 million workforce and consumer identities are protected by Entrust
- 93% of our customers say they would recommend Entrust Identity to others

Entrust is an innovative leader in identity-centric security solutions, providing an integrated platform of scalable, AI-enabled security offerings. We enable organizations to safeguard their operations, evolve without compromise, and protect their interactions in an interconnected world. Entrust supports customers in 150+ countries and works with a global partner network.



Figure 3. Entrust has an unrivaled partner ecosystem.

Entrust keeps the world moving safely by enabling trusted experiences for identities, payments, and digital infrastructure

We offer an unmatched breadth of solutions that are critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption, and more.

Trusted infrastructure

Our solutions use trusted identities, applied cryptography, PKI, and other advanced security technologies to prevent cybersecurity threats, protect data, and enable digital life. The result is a foundation of trust that empowers organizations and end-users to adopt new technologies, solve business challenges, and drive transformation with confidence.

Digital Security portfolio

Trust Policy Management

An enterprise-wide approach to discovering, managing, protecting, and auditing crypto assets and their policies in hybrid and multi-cloud environments.

Multi-Cloud Security

Securing multi-cloud and hybrid environments with comprehensive protection for keys, certificates, VMs, containers, and data.

Application Security

Proven, foundational security for today's business applications on-premises and in the cloud.

Database Security

Unified database security platform ensures critical data is always secured and available for uninterrupted business.

Digital Signature

High-assurance digital signatures, document integrity and non-repudiation.

Digital Onboarding

Digital verification of financial customer credentials to support frictionless remote account opening and onboarding.

Identity & Payments portfolio

ID Issuance

Identification credentials that meet a full range of requirements, from basic photo ID cards to high- assurance identity credentials and government IDs.

Identity Verification

High-assurance digital verification of citizen identities for governments and travel service providers.

User Identity

Provides user authentication, authorization, and access control to the right resources, anytime, anywhere to enable Zero Trust approach.

Machine Identity

Scalable machine identity security practice, with trusted code signing, encryption, and identity – and the tools to manage those identities throughout their entire lifecycle.

Financial Issuance

Trusted digital and physical payment credentials for banks and credit unions.

110M+	87%	65%	202	20B	10B	60M+
protected workforce and consumer identities	of C-Suite and Executive Management trust Entrust	of the Fortune 500 companies are secured by Entrust	countries/nationalities that have had their citizen identities verified by Entrust	payment cards issued	ID cards activated for students, employees, and citizens	active certificates issued

Strong identities

We help establish and maintain trusted user and machine identities. This provides a strong foundation for experiences like hybrid work and frameworks like Zero Trust – all with the most advanced identity and encryption technology to help prevent evolving security threats.

Secure payments

We help secure modern payments with the issuance of secure digital and physical payment credentials so financial customers can pay how and when they like. Our unique portfolio includes digital card issuance, high-volume card issuance, and in-branch instant issuance of fully personalized cards.

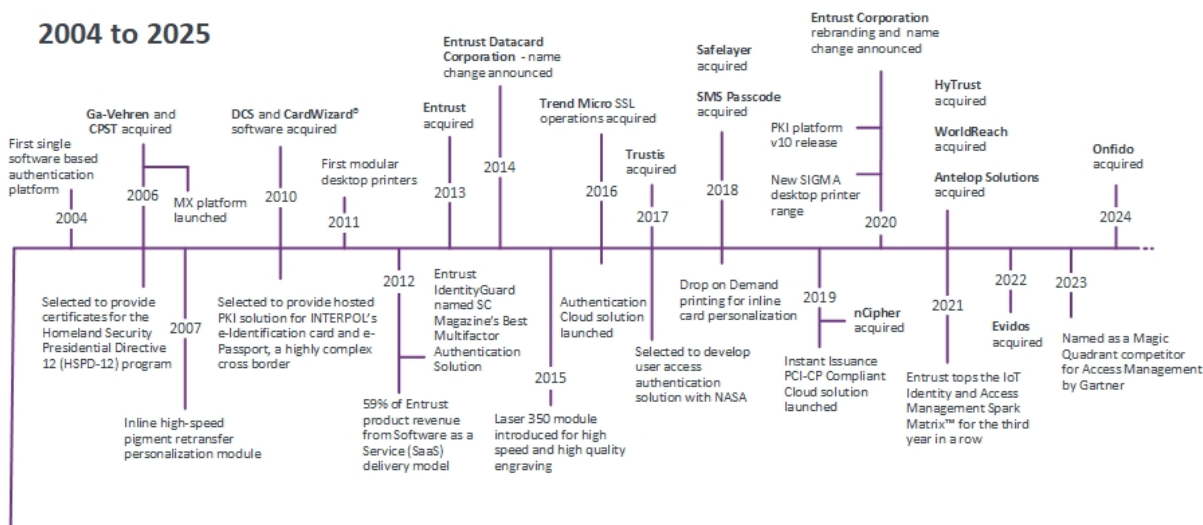
Entrust is a global company with a vast portfolio of accomplishments

Key statistics include:

5B financial and government cards issued annually	690K websites secured globally	24M+ SWIFT messages encrypted and secured daily	57 of Global Fortune 100 companies use our HSMs	45K+ instant issuance deployments worldwide	10B ID cards activated for students, employees, and citizens	202 countries/ nationalities which have had their citizen identities verified	10M+ secure identity and payment credentials issued daily	25 countries and global inter- governmental agencies use our PKI	100M+ protected workforce and consumer identities	95% of IT professionals say Entrust is highly respected	20B payment cards issued
---	--	--	--	--	--	---	---	--	---	---	--

Entrust History of Innovation Since 1969

2004 to 2025



1969 to 2003

