



ENTRUST

Entrust On-Premises PKI

Essential security and enablement for the evolving enterprise

HIGHLIGHTS

Securing and enabling your evolving enterprise

The new age of connectivity drives powerful growth opportunities for the modern enterprise. But it also requires critical changes in the way you protect information, networks, and devices. Entrust Security Manager, the world's leading PKI solution, provides an advanced PKI solution for security-minded organizations – delivering full in-house control over PKI infrastructure, governance, and compliance, and simplifying the identity management process.

Simplified certificate management

Manage digital identities for enterprise-wide security, without burdening administration. Deployed at the server level, Entrust Security Manager software enables valuable security capabilities to be applied across a wide variety of enterprise, IoT, LTE, and ePassport use cases:

- Permission management
- Digital signature
- User and device authentication
- Encryption

Seamless mobile security

Mobile operating systems inherently have the ability to store certificate-based credentials and make them available to applications that run on the device – such as VPN clients and email software. Entrust Security Manager issues certificates to mobile devices, enabling organizations to efficiently protect their mobile networks.

Easy & transparent for users

Simplify the user experience. Automatic and transparent key and certificate management means users do not need to understand public keys and certificates to add security to communications, mobile devices, and transactions. The platform even provides key history, backup, and recovery features so encrypted information will not get lost should users misplace their keys.

High availability

With native support for multi-node or “hot/hot” deployment, Security Manager provides organizations with the confidence to deliver the required service levels by dramatically reducing downtime.

LEARN MORE AT [ENTRUST.COM](https://www.entrust.com)



Entrust On-Premise PKI

KEY FEATURES & BENEFITS

- Experience you can trust – Entrust deployed the first commercially available PKI and brings more than 25 years of PKI experience to every engagement
- Reduce the number of credentials you need to purchase and manage
- Simplify PKI deployment and management to a broad range of users and connected devices
- Centralize control of your PKI – Manage multiple use cases with a single CA
- Leverage existing investments – High interoperability includes enhanced integration with Microsoft, Android, Apple and more

HOW IT WORKS

Enterprise use cases

Managing identities and devices across multiple locations and reducing Shadow IT requires PKI capabilities. Businesses are challenged to offer secure access to a broader array of services, applications, and physical locations while guarding against increasingly sophisticated threats. Entrust enterprise PKI solutions support IT agility and help organizations securely adapt to multiple use cases.



Private Networks and VPN Security

Establish a trusted network environment by issuing digital certificates to VPN gateways, remote access clients, and routers.



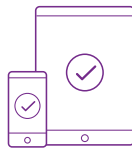
User Authentication

Give authorized users one simple and secure way to log into networks and cloud-based apps from desktops, laptops, or mobile devices.



Mobile Authentication

Remove administrative obstacles for mobile workers while actually improving security – enable the powerful concept of mobile as the new desktop.



Device Authentication

Simplify Shadow IT and embrace its advantages – manage the identities of all users and devices across your enterprise from a single platform.



TLS/SSL Certificates for Websites and Services

Enable security capabilities at the server level – including permission management, electronic signature, digital receipt, and encryption – to be applied across a variety of enterprise applications.



Email Security

Simplify secure communication with comprehensive, standards-based email encryption capabilities.



Entrust On-Premise PKI

Elements of PKI



Identification and Authentication

Digital Certificates - Trusted Identity for People and Devices

Digital certificates contain information detailing the identity of a person, device, or application, and a public/private key pair associated exclusively with the person, device, or application.



Integrity, Authenticity, and Non-repudiation

Digital Signatures - Non-Repudiation for Secure Transactions

Electronic signatures that verify term acceptance or transaction authorization are impossible to forge, which makes them even more secure than signatures on paper.

Message Hashing - No Information Tampering

This technique applies a digital fingerprint to encrypted messages. Attempts to alter message content are easily detected.



Confidentiality

Encryption - For Your Eyes Only

Encryption algorithms transform characters into unreadable code that can only be decrypted by authorized users with secure keys.

Public and Private Key Pairs

All parties in an encrypted transaction have an assigned key pair - one public and one private. Senders use the public key unique to the recipient to encrypt messages. Recipients use their private key to decrypt the message.



Entrust On-Premise PKI

THE ENTRUST DIFFERENCE

Nothing builds trust like Entrust PKI

We bring over 25 years of PKI leadership. Our first public key infrastructure – the world’s first commercially available PKI – was released in 1994. Today, our 10th generation technology is the industry’s most trusted PKI solution.

Trusted around the world

Using Entrust PKI, our ICAO-compliant ePassport solutions provide integrity and authenticity to citizen information written in 50% of the world’s passports.

800+ PKI deployments worldwide

- 18 of the top 20 eGovernments
- 20 of the top 20 finance companies
- 8 of the top 10 telecom companies
- 7 of the top 10 pharmaceutical companies
- 5 of the top 5 petroleum companies
- 8 of the top 10 aerospace companies

OUR OFFERINGS

Entrust PKI portfolio

Entrust Security Manager

Helps organizations easily manage their security infrastructures and allows simplified management of digital keys and certificates.

Entrust Administration Services

The Registration Authority that works with the Entrust Certificate Authority.

Entrust Security Manager Proxy

Allows communication with Security Manager using standard internet protocols without making changes to existing firewall settings.

Entrust Managed PKI

Offers the convenience and security of a full PKI without the expense of infrastructure investment or in-house experts.

Entrust Certificate Hub

A single portal where you can find, control, and automate the management of your public and private certificates.

Entrust CA Gateway

REST API enabling customers, integrators, and alliance partners to develop certificate-enabled solutions.

Entrust ePassport Solutions

Proven solutions for Basic Access Control and Extended Access Control environments.

Entrust Citizen ID Solutions

Used for a variety of citizen e-ID, national ID, and civil authentication requirements.

Entrust Discovery Scanner

Find, inventory, and manage digital certificates across diverse systems to prevent outages, data breaches, and compliance issues.

Entrust Entelligence™ Agent

Allows organizations to use a single digital identity to add security capabilities beyond authentication to applications such as email or file encryption.

Entrust Validation Authority

Provides a high-performance OCSP responder enabling PKI relying parties to easily validate the status of their digital certificates.



Learn more at
[entrust.com](https://www.entrust.com)



ENTRUST