



SOLUTION BROCHURE

Entrust PKI Hub

All-in-one container-based PKI virtual appliance for simplified, scalable, and secure PKI and certificate lifecycle management deployable in the cloud or on-premises



ENTRUST

SECURING A WORLD IN MOTION

BUSINESS CHALLENGE

PKI's Ever-Expanding Footprint

Over the past 25 years, public key infrastructure (PKI) has evolved and expanded, playing a critical role across a wide range of applications – from the cloud and edge networks to IoT, modern citizen identities, and digital signatures.

PKI's footprint continues to grow as it adapts to increasingly complex use cases, becoming a central component of our digital lives. However, as PKI scales and its use becomes more complex, a significant challenge emerges: the lack of clear ownership and responsibility for managing these changes. Without visibility and understanding of how to control PKI in these new contexts, organizations struggle to maintain their security posture and infrastructure as they once did.

As PKI deployments continue to diversify and scale, another issue arises: The previous solution has often been to add another CA or source for certificates within the organization, but this approach has led to widespread certificate sprawl, creating a large maintenance problem and massive management overhead.



SOLUTION OVERVIEW

Comprehensive Yet Simplified PKI

Entrust PKI Hub is a comprehensive, high-performance, container-based PKI, certificate lifecycle management, and automation solution. It comprises all the components required to run a secure, quantum-ready PKI, deploy in a range of applications, and expand on demand.

Deployed as a pre-packaged virtual appliance, it enables customers to streamline PKI and CLM while providing the flexibility to scale across enterprise and cloud environments.

HOW IT WORKS

Pre-Packaged With All the Components You Need

A complete PKI involves an integration of software, policies, and procedures that collectively establish and manage public key encryption. Entrust PKI Hub comes as a pre-packaged virtual appliance with all the components required to:

- Run a secure and quantum-ready PKI
- Deploy anywhere and however you need it
- Scale on demand

Those components include:

PKI Hub Certificate Authority

Entrust PKI Hub provides a robust, scalable, secure solution for issuing digital certificates to ensure trusted identities across your organization. Deployed in a virtualized environment, this appliance streamlines certificate lifecycle management, supports compliance with regulatory requirements, and ensures secure communications.

- Multi-CA support for enterprise PKI deployments with automation of certificate lifecycle management for DevOps and microservices
- Two-tier CA hierarchy
- Dual-CA strategy enables your organization to seamlessly transition from Microsoft CAs to a modern, adaptable enterprise PKI
- Supports Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) for real-time certificate validation
- Integration with external databases and hardware security modules (HSMs) enhances security of private keys to align with industry compliance standards like FIPS

Entrust PKI Hub includes these components:

- PKI Hub Certificate Authority
- Automated certificate lifecycle management
- Enrollment services
- Online Certificate Status Protocol (OCSP)
- Timestamping
- RESTful API (Entrust CA Gateway)
- Management console

Certificate Lifecycle Management (CLM) Across Your Organization

Thanks to advanced reporting, PKI Hub helps you discover all the users' and machines' digital identities across your organization from multiple CAs, includes comprehensive automation capabilities, and provides a simple and intuitive "single pane of glass" view.

- Certificate discovery via network scanning and automated import from CA databases and cloud services
- Centralized management of certificate policies, issuance, renewal, and revocation, regardless of CA vendor
- Ability to push certificates and manage key rotations and certificate profiles across endpoints
- Certificate import methods include:
 - Discovery scanner
 - Bulk import through import API
 - Manual upload through UI
 - Source sync with CA databases
- Convenient admin controls, reporting, and notifications
- Role-based access control with customizable roles to help you with regulatory compliance, separation of duties, and delegation of responsibilities; authorization tags provide even more granular access

Enrollment Services (ES)

Our registration authority module for automated certificate enrollments and renewals supports Microsoft Active Directory auto-enrollment and all major industry protocols, including:

- Intune MDM
- ACMEv2
- Simple Certificate Enrollment Protocol (SCEP)
- EST
- CPMv2

Online Certificate Status Protocol (OCSP)

Real-time certificate validation via OCSP is built into the appliance. This validation authority supports third-party CA status checking and is designed to:

- Provide reliable information on the status of a digital certificate
- Process information from one or multiple CAs using CRLs or CA databases

Timestamping

Get maximum security and trustworthiness for your digital identities with verifiable, RFC3161-compliant timestamping of digital transactions and documents.

RESTful API (Entrust CA Gateway)

Entrust PKI Hub's RESTful API is a powerful interface that enables full certificate lifecycle management, reporting, trust policy, and operational management to the PKI Hub CA and third-party CAs.

Management Console

Our centralized interface for deployment, configuration, and monitoring of all PKI Hub components simplifies and streamlines management tasks for IT teams.

DID YOU KNOW ...

Entrust introduced the world's first commercially available public key infrastructure in 1994.



KEY BENEFITS

360° Degree PKI, CLM, and Automation

All PKI and CLM functions integrated in a single product including third-party integration and automation.

Deploy Anywhere

PKI solution deployed anywhere with the same ease and flexibility for cloud or on-premises environments.

Small Footprint

Minimize infrastructure footprint and reduce time and costs by deploying an unlimited number of private CA instance deployments on a single server, while scaling horizontally as needed.

High Scalability and Transactions per Second

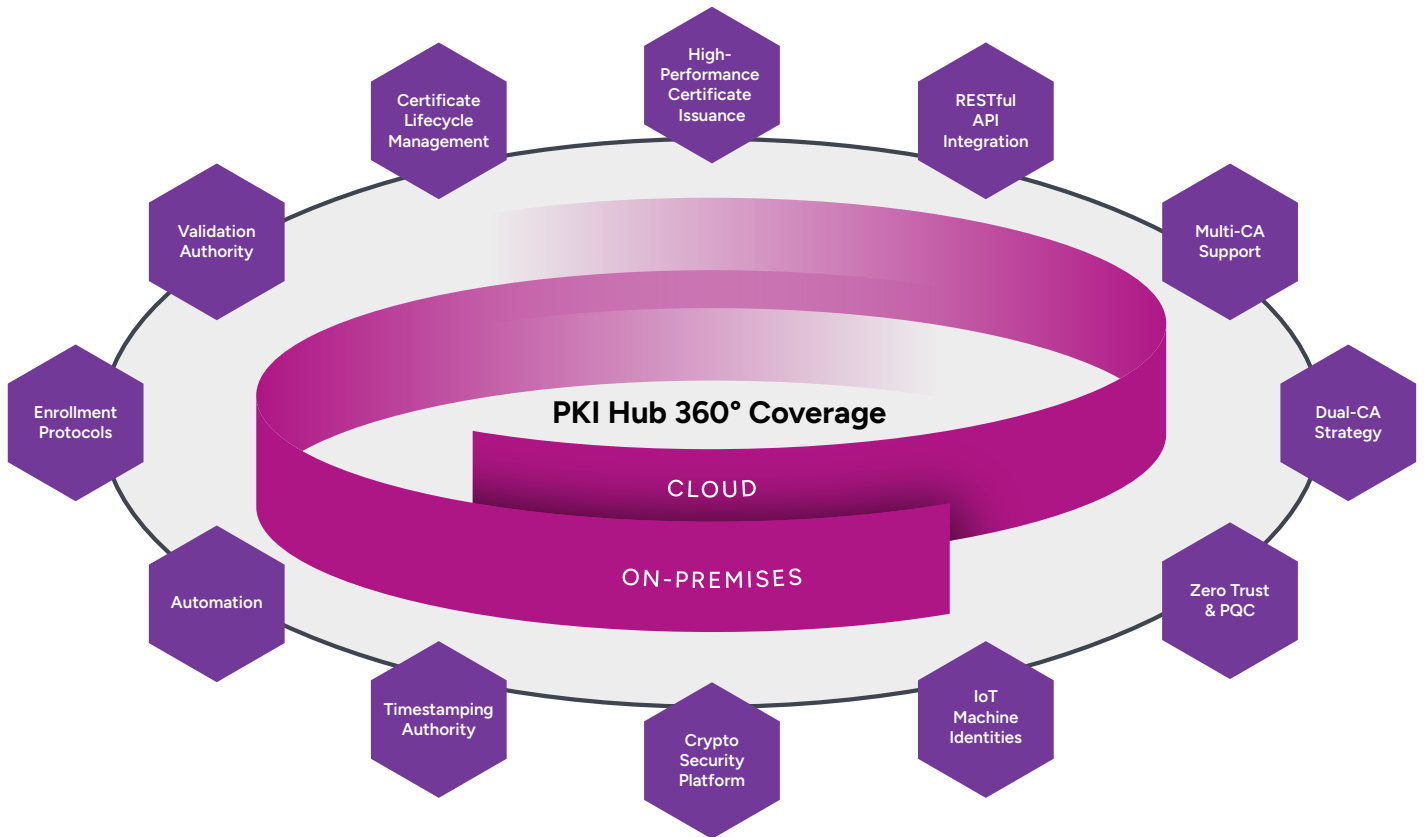
For IoT, connected services, and on-premises PKI systems that grow with scalable capacity for multi-CA deployments.

Simplified

Managed components and turnkey approaches to use cases make it simple to deploy and adaptable. Straightforward, simple licensing and pricing.

Entrust E2E Cryptographic Security

The assurance you expect from Entrust with dedicated CAs and protection of your keys by Entrust nShield HSMs out of the box.



KEY FEATURES



Complete Technology Stack

Entrust PKI Hub minimizes the complexity of configuring and managing your organization's PKI. It includes a full software stack that includes:

- PKI Hub Certificate Authority
- Automated certificate lifecycle management
- Enrollment services
- Online Certificate Status Protocol (OCSP)
- Timestamping
- RESTful API (Entrust CA Gateway)
- Management console with support for network-attached HSMs



Multi-Platform Support

Entrust PKI Hub is compatible with any virtualization platform, including but not limited to VMware, Hyper-V, cloud platform providers (Azure, AWS), and Kernel-based Virtual Machine (KVM). This ensures seamless integration into your existing IT infrastructure without additional configurations or adaptations.



Flexible and Quick Deployment

Whether on-premises or in the cloud, Entrust PKI Hub offers deployment flexibility for diverse IT environments. Minimal setup time is required to configure and integrate into the enterprise infrastructure.



Intuitive User Interface for Simplified Management

Streamline certificate management and policy enforcement with a single, unified platform. The intuitive UI simplifies configuration and ongoing operation.



High Availability

Entrust PKI Hub's cluster configuration ensures your PKI solution remains operational – even during maintenance or unexpected failures – providing robust fault tolerance and business continuity.



Secure

Integrated security features such as HSM support, OCSP, and timestamping help ensure that your certificates and data remain safe.

SPECIFICATIONS

Supported Integrations

Entrust PKI Hub runs on an Entrust operating system, providing certificate issuance, renewal, and revocation through a single-pane-of-glass interface to support a wide range of applications.

| | |
|--|--|
| Certificate Authorities | <ul style="list-style-type: none">• PKI Hub Certificate Authority• Entrust Certificate Authority• Entrust Public Trust Certificate Authority (Entrust Certificate Solutions CA)• Microsoft Certificate Authority• Standalone Microsoft Certificate Authority |
| Enrollment Protocols | <ul style="list-style-type: none">• Microsoft Active Directory auto-enrollment• ACMEv2• EST• INTUNE• MDMWS• SCEP• CMPv2 |
| External and Third-Party API Integrations | <ul style="list-style-type: none">• CA/Enrollment Gateway• IoT Agent• IT Agent (Windows/Mac)• RESTful APIs• CertManager• ServiceNow• Device Authority• Ansible |
| KMS and Vaults | <ul style="list-style-type: none">• Entrust Vault (KeyControl)• Azure Key Vault• HashiCorp Vault |
| Servers/Load Balancers, Etc. | <ul style="list-style-type: none">• Apache• F5 BIG-IP• Java• NGINX |
| Deployment Platforms | <ul style="list-style-type: none">• VMware• AWS• Azure |

Supported Databases

| Database | Component |
|----------------------|--|
| PostgreSQL | Certificate Authority, OCSP, Certificate Hub |
| Microsoft SQL Server | OCSP |
| Oracle | OCSP |

Supported Platforms

| Platform | Description |
|-------------------------|---|
| Bare-metal machine | PKI Hub can be installed directly on physical hardware using an ISO image, ensuring high performance and resource optimization. |
| Virtualization platform | Compatible with any virtualization platform, including but not limited to VMware, Hyper-V, and Kernel-based Virtual Machine (KVM) |
| Cloud-hosted machine | Tested on the Amazon Web Services (AWS) and Microsoft Azure cloud providers |

Supported HSMs

| HSM | Component |
|----------------------------|---|
| Entrust nShield 5C | Certificate Authority, OCSP, Timestamping |
| Entrust nShield Connect XC | Certificate Authority, OCSP, Timestamping |
| Thales Luna Network HSM | OCSP, Timestamping |

Supported Cryptography and Technology

- RSA and ECDSA keys
- CNSA-compliant and RFC5280-compliant X.509 certificates and CRLs
- PKCS#10, PKCS#12, JKS, PEM, and PKCS#11 keystores
- RFC6960-compliant OCSP

THE ENTRUST DIFFERENCE

Empowering Modern Enterprises With Next-Generation PKI Solutions

Entrust brings more than 30 years of expertise and innovation in PKI to meet the evolving security needs of modern enterprises. In fact, we built and sold the first commercially available PKI back in 1994.

As a trusted leader in identity and security solutions, Entrust has continuously innovated to address the growing complexity of digital environments, including cloud services, IoT, and remote work. With a deep understanding of the critical role PKI plays in securing machine identities, user authentication, and data integrity, we provide scalable, flexible solutions to help ensure seamless integration and robust protection.

Whether for traditional on-premises deployments or cloud-first strategies, our PKI solutions are designed to meet the demands of today's dynamic security landscape, enabling organizations to maintain the highest standards of trust to reduce risk while simplifying compliance and management.



Learn more about Entrust PKI Hub at
[entrust.com/products/pki/pki-hub](https://www.entrust.com/products/pki/pki-hub)



ABOUT ENTRUST

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 – so they can transform their businesses with confidence. Entrust supports customers in 150+ countries and works with a global partner network. We are trusted by the world's most trusted organizations.