

# Verified PKI as a Service

Help meet compliance mandates and reduce your dependency on public trust with a cloud PKI service built on a WebTrust-audited infrastructure.

## OVERVIEW

With the increasing operational risks of public trust certificate management and the growing compliance requirements around private PKIs, managing digital certificates is becoming more complex to manage than ever.

Entrust Verified PKIaaS was specifically designed to help you outsource all three components, with a PKI that goes under the same audit that is required to run a publicly trusted certification authority and that already meets multiple compliance mandates.

## BENEFITS

Reduce your dependency on WebPKI with a ready-to-use service that operates under best practices.

Entrust Verified PKIaaS can help you transition some of your use cases away from public trust without the need to build and operate your own PKI.

### **Align to critical PKI compliance requirements.**

Entrust Verified PKIaaS is a WebTrust-audited cloud PKI, with offline roots. Our service can help you meet compliance requirements such as WebTrust, HIPAA, and PCI DSS.

### **Meet CISOs' demand for enhanced security.**

Chief Information Security Officers (CISOs) are increasingly tasked with managing a complex threat landscape. They recognize that a properly managed PKI is a powerful tool for mitigating risk, but also that it requires specialized skills and mature processes.

## Benefits at a glance

- De-risk your digital certificate estate by reducing your dependency on public trust
- Get an alternative to WebPKI for your business-critical use cases that still carries trust thanks to audits
- Rely on mature processes by implementing best-practice identity verification, issuance, and revocation procedures.
- Help meet key compliance requirements such as HIPAA and PCI DSS
- Delegate CA operations, RA operations, and standards-based compliance to Entrust
- Switch away from a "one-size-fits-all" PKI architecture that requires too many resources

# Why choose Entrust Verified PKI as a Service?

## HIGHLIGHTS

### **A PKI in the cloud, with offline roots**

Entrust Verified PKIaaS delivers a fully managed PKI hosted in the cloud, backed by offline root CAs in FIPS 140-2 Level 3 certified HSMs. This approach provides security, scalability, high availability, and faster deployment, reducing operational complexity and overhead.

### **Security aligned to WebPKI best practices but with more flexibility on certificate issuance**

The service is audited under the WebTrust program, an independent validation that the PKI is operated to the highest standards. But the certificate lifetimes and certificate profiles from Verified PKIaaS do not have the same constraints as WebPKI, and certificates issued are not logged into any certificate transparency (CT) log.

### **Comprehensive CP and CPS documentation**

Entrust Verified PKIaaS comes with full CP and CPS documentation, all defined and managed by Entrust, and aligned with WebPKI best practices. You benefit from standards-based policies without the need to build and maintain your own.

### **Dedicated intermediate CAs under your name**

Operate under your own branded intermediate CAs, backed by Entrust's secure infrastructure. Get greater control, trust, and flexibility for business-critical PKI use cases without the complexity of managing hardware or audits.



### **Registration authority (RA) services**

Entrust agents perform identity and domain validation on your behalf, in alignment with WebPKI requirements, ensuring accurate and secure certificate issuance. This delegation reduces your internal workload and minimizes the risk of validation errors.

### **Certificate lifecycle management (CLM) features**

Our service can help you automate workflows for issuance, renewal, and revocation to streamline certificate management and reduce human error. Policy-driven processes such as role-based access control (RBAC) and automated key verification ensure tight visibility and control of your cryptographic assets.