Finding the RESTful path to certificate lifecycle automation and integration

PKI REST API provides simple, trusted security
# Table of Contents

Introduction........................................................................................................... 3  
Simple, trusted security ......................................................................................... 4  
Support for Entrust Managed PKI, Cloud and On-Premises .......................... 5  
Better than toolkits............................................................................................... 6  
The PKI RESTful API ............................................................................................. 7  
How to get started ................................................................................................. 8
INTRODUCTION

Entrust PKI REST API

The PKI REST API is Entrust’s latest offering for PKI automation. It allows for rapid integration with Entrust PKI services. The gateway provides a powerful RESTful interface that enables full certificate lifecycle management, reporting, trust policy, and operational management across all of your Entrust-supported CAs.
Simple, trusted security

Not everyone wants to be a PKI expert. Whether you’re developing a platform or an application, you want to focus on the key functionality that is core to your business. You don’t want to be distracted by having to learn the nuts and bolts of security and trust management. You just need a PKI API that:

• Gives you assurance your system is secure without having to spend an inordinate amount of time in security implementation and evaluation.

• Insulates developers/integrators from the nuances of PKI by abstracting the complications of certificates and trust management away from your implementation.

• Makes it easy to integrate trust management into your apps/solutions in a way that is aligned with your workflow and logic — with the confidence that Entrust expertise is built into the programming model.
Support for Entrust Managed PKI, Cloud and On-Premises

Since the API abstracts the PKI away from your applications and integrations, you can use either cloud-managed PKI, on-premises PKI, or a combination of both. The gateway can act as a single distribution and access point for all of your certificate needs.

**Managed PKI support** — Hosted and maintained by Entrust, our mPKI customers can benefit from gateway services for both test and production instances while allowing Entrust engineers to manage patching and deployment. The standard interface across test and production environments allows for rapid integration validation and “go live” timelines.

**On-Premises PKI support** — On-premises customers can obtain and run the CA Gateway (CAGW) component, which implements the PKI REST API as part of their infrastructure.

**Hybrid PKI support** — The CAGW, when network connectivity allows, can also support a hybrid scenario where both on-premises and Entrust CAs are accessible from a single CAGW instance provided from the Entrust mPKI environment. This hybrid environment leverages the benefits of Entrust’s continuous innovation and release in the API, with on-premises hosting of the CAs and data.
Better than toolkits

Unlike traditional toolkits, the PKI REST API is language-independent, giving you the freedom to choose your implementation language. It doesn’t require you to license and distribute any Entrust-supplied components, and there’s no need to plan for the subsequent component upgrades. Plus, the gateway separates your application from our services, isolating problems and making for easier troubleshooting.

<table>
<thead>
<tr>
<th>APPLICABLE TO A VARIETY OF USE CASES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certificate Lifecycle Management</strong></td>
</tr>
<tr>
<td><strong>Business Workflow Integration</strong></td>
</tr>
<tr>
<td><strong>DevSecOps Orchestration</strong></td>
</tr>
<tr>
<td><strong>Device Cert Provisioning and Management</strong></td>
</tr>
<tr>
<td><strong>Secure Trust Management for Custom Mobile, Desktop, and Server Applications</strong></td>
</tr>
<tr>
<td><strong>System Monitoring</strong></td>
</tr>
</tbody>
</table>
The PKI RESTful API

The PKI API is a RESTful web service API that provides flexible capabilities for certificate lifecycle automation, integration, and extension to new use cases. It virtualizes the underlying PKI by presenting a consistent programming model of the PKI policy, operations, and data that is independent of underlying PKI infrastructure.

The API framework supports a matrix of roles (actors) operating against the elements of PKI (objects).

A client of the API can:

- **Manage CAs and policy**: Catalog certificate authorities (CAs) and query CA artifacts, such as certificate chains, certificate revocation lists (CRLs), and certificate profiles

- **Issue certificates**: Submit enrollment requests for certificates for both client-generated and server-generated key pairs

- **Manage certificate lifecycle**: Renew, revoke, or hold certificates and recover keys

- **Report**: Query the CA for certificates based on certificate attributes, metadata attributes, and status changes

Enhancements are planned to allow active management of the PKI policy and infrastructure.

<table>
<thead>
<tr>
<th>ACTOR</th>
<th>OBJECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Policy</td>
</tr>
<tr>
<td>Operator – Hosts an instance of the system</td>
<td>Create/Deploy CAs</td>
</tr>
<tr>
<td>Integrator – Provides services or capabilities to customers</td>
<td>Create/Deploy and query CAs</td>
</tr>
<tr>
<td>Tenant – Consumes services provided by the operator or integrator</td>
<td>Define policy within set limits set by integrator and/or operator</td>
</tr>
<tr>
<td>End Entity – Person or thing that needs a certificate</td>
<td>Request and self-manage credentials</td>
</tr>
</tbody>
</table>

LEARN MORE AT ENTRUST.COM
How to get started

Integration to the API is straight-forward and is supported with online API documentation and a number of developer aids.

- **API documentation:** View documents at: https://api.managed.entrust.com/doc/

- **How to get connected:**
  - Managed PKI customers: To access the API, you must obtain API access keys for your existing mPKI test CA. Contact our operations team through your normal channels.
  - On-premises customers: Contact your Entrust account manager.
  - Technical Alliance Partners: We have sandbox environments available to support you in your development. For more information or to request environment setup, contact our Technical Alliance Team.

- **Professional services team:** Fully trained in API development, our team can help you with training and/or implementation.

- **General contact information:** entrust.com/contact
ABOUT ENTRUST CORPORATION

Entrust secures a rapidly changing world by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they’re crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it’s no wonder the world’s most entrusted organizations trust us.