White Paper

Finding the RESTful Path to Certificate Lifecycle Automation and Integration

PKI REST API provides simple, trusted security

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

INTRODUCTION

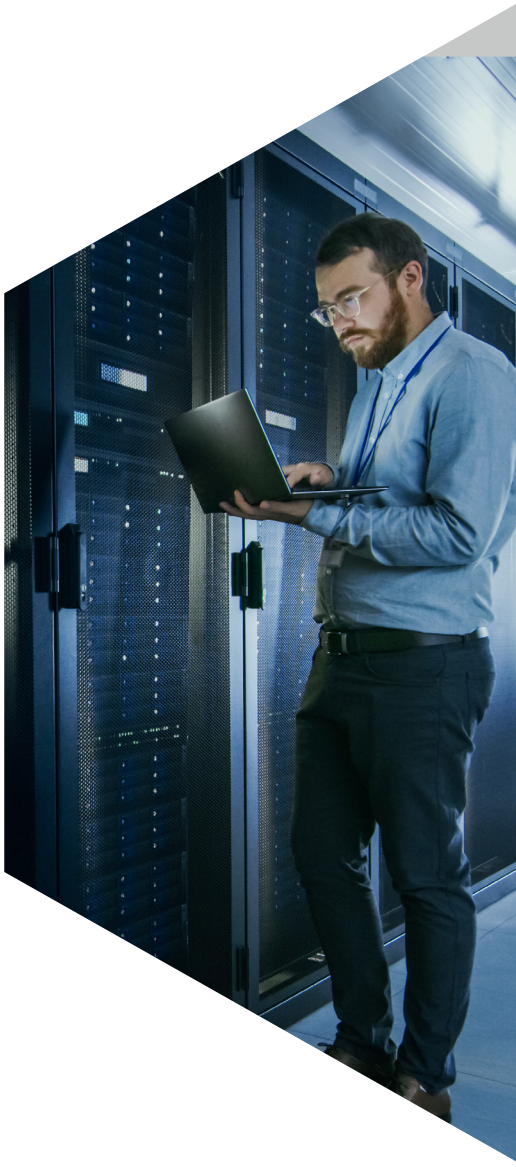
Entrust PKI REST API

Certificate Authority Gateway (CA Gateway) is Entrust's REST API offering for PKI automation. It provides a CA-agnostic, powerful REST-based API interface as well as a frontend for the highly scalable PKI as a Service (PKIaaS) from Entrust and 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 your CAs.

Simple, trusted security

Not everyone is a PKI expert. Whether you're developing a platform or an application, your focus needs to be on the key functionality that is core to your business yet you understand the importance of leveraging PKI. In order to not be slowed down by learning 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.

Cloud-based PKI as a Service support — CA Gateway acts as a frontend for the highly scalable PKIaaS from Entrust that can allow a turnkey PKI setup and issuance, management, and validation services at scale.

Hybrid PKI support — The CAGW, when network connectivity allows, can also support a hybrid scenario where both on-premises and Entrust managed 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.

Non-Entrust PKI support — CA Gateway is CA-agnostic and therefore supports non-Entrust Certificate Authorities.

Better than toolkits

Unlike traditional toolkits, the CA Gateway 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.

APPLICABLE TO A VARIETY OF USE CASES

Certificate Lifecycle Management	Perform basic certificate operations, like issuance, search, renewal, and revocation, as well as more complex operations, like key recovery.
Business Workflow Integration	Integrate administrative actions – like request, approval, and reporting – into your organization's existing business workflows. Make certificate management easy and centralized to help eliminate shadow IT problems.
DevSecOps Orchestration	Support DevOps CI/CD automation through plugin integration to orchestration frameworks that create and destroy container certificates as needed for the enterprise, either on-premises or in-cloud.
Device Cert Provisioning and Management	Our collection of APIs and complementary protocols provides tremendous scope and allows for automation, efficiency, and reduction of human error. Complement industry-standard protocols, like SCEP, EST, and CMPv2. Central management of devices and credential revocation when devices are decommissioned or compromised. Augment device enrollment mechanisms with API-based configuration of enrollment shared secrets.
Secure Trust Management for Custom Mobile, Desktop, and Server Applications	Provide a centrally controlled and compliant trust management infrastructure for developers to leverage in the app-oriented economy. Implement state-of-the art trust management between application components without having to be security experts, allowing you to use highly trusted certificates to authenticate and secure interactions.
System Monitoring	Perform periodic monitoring of the PKI system health. Particularly useful in combination with other applications above.

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.

ACTOR	OBJECT			
	CA	**Policy**	**Entity**	**Certificate**
Operator – Hosts an instance of the system	Create/Deploy CAs	Set/Query global policy	Manage integrators and tenants	Issue credentials to integrators
Integrator – Provides services or capabilities to customers	Create/Deploy and query CAs	Set/Query tenant policy	Manage tenants	Issue credentials to tenants
Tenant – Consumes services provided by the operator or integrator		Define policy within set limits set by integrator and/or operator	Enroll end entities Hold/Revoke account	Issue credentials to end entities Hold/Revoke certificates
End Entity – Person or thing that needs a certificate				Request and self-manage credentials

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

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

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. With more than 2,800 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com