



Issuing CA

Automated certificate operations for enterprise PKI

Automate Certificate Issuance, Renewal, Revocation, and Status Operations

Futurex Issuing CA gives PKI teams a controlled way to manage operational certificate authority workflows beneath the trusted root of the PKI hierarchy. Teams can process certificate signing requests, issue TLS, S/MIME, client, X.509, and document signing certificates, renew expiring certificates, revoke certificates when trust changes, and maintain certificate status across enterprise environments.



Unified Control for Certificate Operations

- HSM-Backed CA Signing: protect CA private keys throughout certificate issuance, renewal, revocation, and signing operations.
- Policy-Based Certificate Workflows: apply certificate policy across CSR processing, issuance requirements, validation checks, and operational controls.
- Status Validation Services: manage CRLs, CRL distribution points, and OCSP-based status checking for timely trust validation.

Issuing CA Capabilities

Automated CSR Processing

Process certificate signing requests through validation workflows, certificate policy controls, and security checks.

Certificate Issuance

Issue certificates for enterprise workloads, users, applications, web servers, secure email, client authentication, and document signing.

Policy Enforcement

Apply certificate policy across issuance requirements, validation workflows, and operational controls.

Certificate Type Support

Support TLS, S/MIME, client, X.509, and document signing certificate workflows across enterprise PKI deployments.

Renewal and Expiration Monitoring

Track expiration dates, trigger renewal workflows, and reduce disruption from expiring certificates.

Revocation and Status Services

Manage certificate revocation lists, CRL distribution points, and OCSP-based status checking.

Audit Trails and Access Controls

Track certificate details, policy actions, lifecycle events, administrative activity, role-based access controls, and multi-factor authentication for sensitive operations.



Built for Operational Certificate Control

Issuing CA operations often span CA servers, directory services, web server teams, trust stores, and manual approval steps. Futurex Issuing CA gives PKI teams a defined issuing layer for repeatable certificate operations, protected CA signing keys, current status data, and documented certificate activity.

What Does Futurex Issuing CA Do for You?

Futurex Issuing CA helps PKI teams coordinate certificate requests, signing operations, status services, integrations, and audit records across the systems that depend on enterprise trust.

• Control Certificate Requests

Route CSR processing through validation workflows, policy checks, and issuance controls before certificates are issued.

• Certificate Policy Controls

Publish revocation and status changes through CRL management, CRL distribution points, and OCSP-based validation.

• Connect Enterprise PKI Systems

Support certificate workflows across Active Directory, Windows Server, web servers, enterprise applications, operating systems, and trust stores.

• Support Network Enrollment

Use SCEP-based enrollment for Cisco, Palo Alto, and Aruba environments where network device certificate workflows apply.

• Document Certificate Activity

Track issued certificates, revoked certificates, policy actions, lifecycle events, administrative activity, and access controls for audit review.

Built for Enterprise PKI Environments

Defined Issuing Layer

Use an issuing CA service for CSR processing, issuance, renewal, revocation, and status management

Chain and Trust Management

Manage subordinate and intermediate CA operations, certificate chain validation, and trust chain maintenance

Network Device Enrollment

Support SCEP enrollment for Cisco, Palo Alto, and Aruba environments

Certificate Policy Controls

Apply validation and issuance controls across operational certificate workflows

Enterprise Integrations

Connect issuing workflows to Active Directory, Windows Server, web servers, enterprise applications, operating systems, and trust stores

About Us

For over 40 years, Futurex has been an award-winning leader and innovator in the encryption market, delivering uncompromising enterprise-grade data security solutions. Over 15,000 organizations worldwide trust Futurex to provide groundbreaking hardware security modules, key management servers, and cloud HSM solutions.

Futurex is headquartered outside of San Antonio, Texas, with regional offices worldwide and over a dozen data centers across five continents, Futurex delivers unmatched support for its clients' mission-critical data encryption and key management requirements.



864 Old Boerne Road,
Bulverde, Texas 78163

