KEYFACTOR

Keyfactor® Command

CLOUD-HOSTED PKI AS-A-SERVICE

Keyfactor Command is the only solution that delivers integrated certificate lifecycle automation and PKI as-a-Service into a single cloud-hosted platform.

The platform enables enterprise IT to discover, monitor, and automate the lifecycle of keys and certificates across their environment, while eliminating the need to manage and run their PKI in-house. Extensive integrations with public and private CAs, network and cloud infrastructure, and security platforms enables you to extend automation and protection across your entire environment.

Keyfactor Command runs in a dedicated cloud-hosted environment, hosted and managed on your behalf by Keyfactor with stringent security controls including multi-part authentication, FIPS 140-2 Level 2 HSMs, a dedicated firewall, and robust backup and failover.

Proven in environments with more than 500M certificates, the platform enables you to easily scale PKI operations as your business demands grow, while retaining complete governance and control.

KEY BENEFITS

- Prevent costly certificate-related network and application outages

- Enforce consistent security policies and prevent the risk of key and certificate misuse

- Maximize crypto-agility to respond and remediate security incidents quickly

- Save time and prevent errors for network, infrastructure, and application teams that routinely request certificates

- Reduce costs and complexity by eliminating the need for HSMs, hardware, software, and specialized PKI training in-house

- Free up IT staff from resource-draining PKI maintenance tasks

A Powerful Combination

PKI AS-A-SERVICE

Get all the benefits of private PKI, without the operational complexity and cost of managing the software and hardware required to run it. You maintain control over day-to-day decisions while offloading backend tasks to our PKI experts.

CERTIFICATE LIFECYCLE AUTOMATION

Discover, manage, and automate the entire lifecycle of keys and digital certificates across your private and publicly rooted PKI to effectively prevent certificate-related outages and breaches.

✓ DISCOVERY & MONITORING

Discover all certificates, monitor their status, and set automated alerts to renew certificates before expiration.

✓ POLICY & WORKFLOW

Simplify certificate requests and approvals via self-service portals, REST APIs or custom automation workflows.

✓ END-TO-END AUTOMATION

Manage and automate the lifecycle of keys and certificates from issuance, provisioning, renewal, and revocation.

✓ EXTENSIBLE ORCHESTRATION

Extend orchestration capabilties to load balancers, web servers, firewalls, and multi-cloud environments.

✓ REST API INTEGRATIONS

Integrate with existing systems such as ITSM , PAM, SIEM, MDM, and DevOps tools like HashiCorp Vault

✓ ROBUST, DEDICATED PKI

State-of-the-art cloud-hosted PKI with a dedicated root CA, monitored 24/7 to ensure high security and availability.

Keyfactor Command Hosted Components
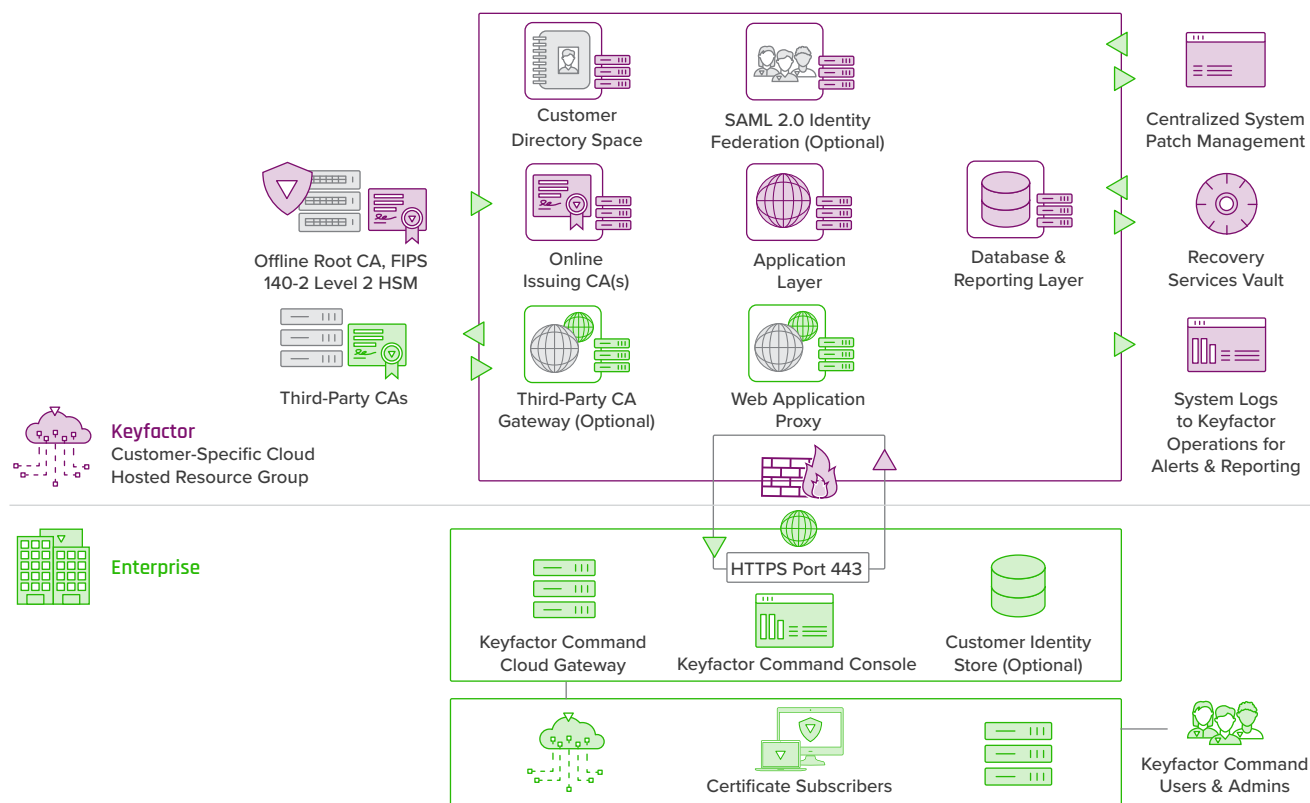
- **Offline Root Certificate Authority:** The cryptographic "trust anchor" for your Keyfactor solution. Hosted and managed on your behalf by Keyfactor with stringent security controls including multi-part authentication requirements on a FIPS 140-2 Level 2 hardware security module.

- **Dedicated Cloud Hosting Environment:** Your Keyfactor Command environment in the cloud is single-tenancy, with no customers coexisting within the same resource space. A dedicated firewall is employed with a "least-privilege" access model.

- **Online Issuing (CAs):** Online certificate authorities serve the certificate requests behind your on-premise Keyfactor Command Cloud Gateway. Optional cloud-based hardware security module (HSM) key protection is available.

- **Keyfactor Command Application and Data Layers:** Keyfactor Command is the world's most complete and scalable cloud-based certificate management platform, providing the freedom to secure every identity across the enterprise.

- **Optional Identity Federation:** Keyfactor Command supports SAML 2.0-based identity federation for secure authentication and ease of administration.

- **Keyfactor Command Cloud Gateway:** The Keyfactor Command Enrollment Gateway is installed on a physical or virtual server in your environment, and connects to your cloud backend security via TCP port 443. It "looks and feels" like an on-premise enterprise CA.

- **Operational Controls:** Your Keyfactor Command Hosted environment employs centralized systems patch management, backup and recovery via Azure Recovery Services Vaults, and monitoring, logging, and alerting processes within our operations and support ecosystem.

This document is intended for general reference information only, does not alter any contractual agreement or statement of work, and is subject to change.