Symantec™ Certificate Lifecycle Platform

Data Sheet: Authentication

Identity protection, privacy concerns, regulatory compliance, and national security issues drive governments, and other large institutions, to seek ways to secure sensitive information. This is a world-wide phenomenon, and to properly address these concerns, trust-based security measures need to be implemented to authenticate users (for example, confirm someone is who they say they are), restrict access to confidential information (for example, grant appropriate access to the right people), and verify ownership of sensitive documents (for example, ensure a piece of content has been authored and/or approved by a given individual).

A Public Key Infrastructure (PKI) platform enables this level of security by making it possible for individuals with no prior contact to be authenticated with each other, maintain confidentiality, and establish the integrity of a message. PKI platforms accomplish this by employing a Certification Authority (CA), which issues, renews, revokes, and manages digital certificates to deliver:

- Strong authentication (also known as “two-factor” authentication).
- Encryption.
- Secure digital signing.

Symantec™ Certificate Lifecycle Platform

Symantec™ Certificate Lifecycle Platform provides a scalable CA service platform, and is designed for large on-premise configurations where a hosted and managed PKI solution is not appropriate due to regulatory, or other factors. The product enables governments, and other large institutions, that cannot outsource any aspect of their PKI operations to have complete end-to-end control over their PKI infrastructure. Certificate Lifecycle Platform is capable of supporting millions of end-user digital certificates on a global scale.

Certificate Lifecycle Platform architecture

Certificate Lifecycle Platform is derived from Symantec’s PKI infrastructure that has been delivering hosted and managed security to thousands of commercial and government customers since it went into operation in 1995. Its architecture is a combination of highly-integrated hardware, software, and processes that are protected in a secure data facility. This environment functions as a primary CA to provide the full range of services to the organization and its clients.

The organization operating the Certificate Lifecycle Platform is responsible for providing the secure facility, trusted employees, hardware, and underlying system software. Certificate Lifecycle Platform delivers the specifications, PKI software, and secure policies and procedures that complete the PKI platform infrastructure.

The front-end of this PKI environment hosts a combination of Web servers and certificate registration servers, which validate enrollment data prior to issuing digital certificates, to support incoming requests. The back-end includes a set of application servers that oversee the processing of requests among a variety of other important back-end servers, including:

- Database servers that track and archive digital certificate data.
- Signing servers, which are responsible for creating the signed digital certificates.

Symantec™

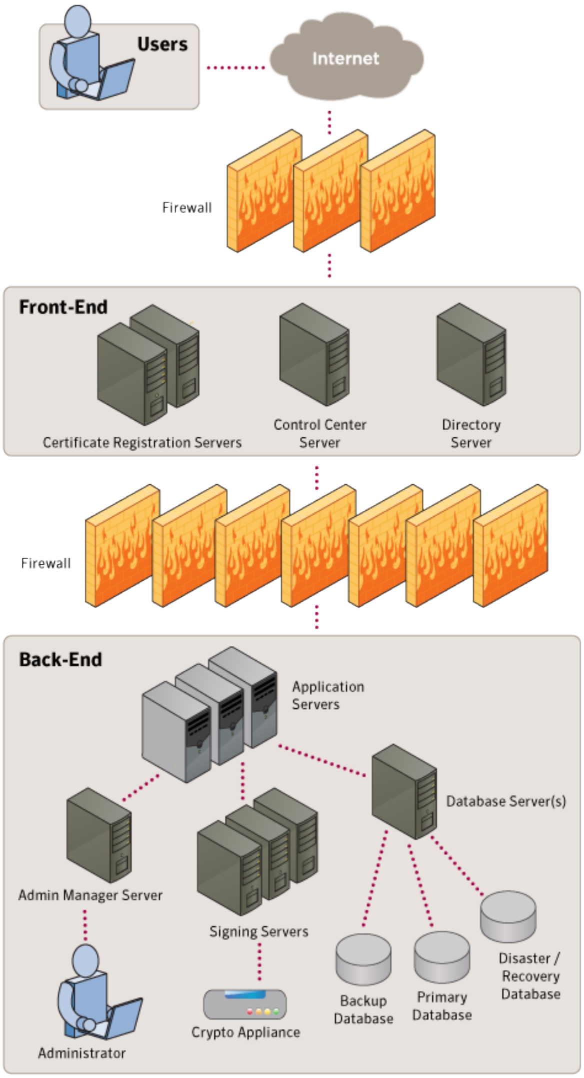

Figure 1: Certificate Lifecycle Platform Architecture

Features & benefits

The Certificate Lifecycle Platform high-performance transaction engine delivers the following features and benefits:

Feature	Benefit
Certification authority (CA)	Operate an on-premise PKI environment by delivering the following functionality: • Generate CA key pairs. • Activate and deactivate CA certificates. • Maintain Certificate Revocation Lists (CRLs) with configurable expiration periods. Supports validation of a digital certificate's status using Online Certificate Status Protocol (OCSP) standards.
Registration authority (RA)	Allows administrators to: • Authenticate, approve, or reject certificate requests from prospective subscribers and revoke certificates. • Generate reports on certificate activity.
Complete certificate lifecycle management	Certificate issuance to internal and external users, Web servers and devices.

Feature	Benefit
Key management service (KMS)	Allows an administrator to control the backup and recovery of user private keys, with minimal risks and minimal security costs. This solution has three main functions: • Generate and distribute end-user keys and certificates. • Backup private encryption keys. • Recovery of those key and certificates. The KMS works with leading messaging solutions.
Carrier-class scalability	Architected to support the highest volume and peak load requirements in the industry. • Overall system architecture is designed to support the issuance and management of more than 100 million certificates per year. • Symantec diagnostic procedures, security practices, operational policies, and infrastructure have been tested and proven over time and designed with scalability in mind.
Archive	An Oracle® database tracks and saves information regarding administrative activities performed against a certificate. • Serves as an audit trail.
Business system API	Enables integration with business system applications to allow validation and digital certificate issuing functions.
Monitoring	A set of software tools to monitor and manage critical system processes and applications. These monitoring tools can generate email, alphanumeric pager messages, and console notifications.
Database mirroring	Enables disaster recovery.
Standards-based	Symantec has a strong commitment to open standards, innovative technology, and strategic collaborations to enable the flexibility and ease-of-use that enterprises require. • Supports standard certificate types, including: S/MIME, SSL, and IPSec, as well as PKI industry standards such as X.509 v3, LDAP, PKCS #7, PKCS #10, and PKCS #12. • Symantec's open approach to security enables organizations to operate freely in diverse environments, and maximize return on, and preservation of, existing investments.
Proven, best-of-breed technology and practices	Inherits the rich functionality and robust architecture that Symantec employs for thousands of customers desiring a managed PKI service (for example, one where Symantec hosts the PKI infrastructure on behalf of the customer).
Deployed by organizations from around the globe	Certificate Lifecycle Platform has been selected by numerous leading-edge government organizations that require end-to-end control of a military-grade PKI solution to secure sensitive information. Applications include: military, government ID programs, and intelligence operations. Certificate Lifecycle Platform has also been implemented in dozens of environments around the globe as part of joint sales operations with regional partners.

More Information

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

21195848-2 07/14