



RED HAT CERTIFICATE SYSTEM

A SCALABLE, SECURE PLATFORM FOR PUBLIC KEY INFRASTRUCTURE

WHAT IS IT?

Red Hat Certificate System provides a powerful security framework to manage user identities and ensure privacy of communications. Handling all the major functions of the identity life cycle, Red Hat Certificate System simplifies enterprise-wide deployment and adoption of a Public Key Infrastructure.

WHAT DOES IT DO?

Red Hat Certificate System works behind the scenes to issue, renew, suspend, revoke, and manage single and dual-key X.509v3 certificates needed to handle strong authentication, single sign-on, and secure communications.

Support for Global Platform permits direct communication between a registration authority and a smart card for key management tasks such as enrollment and PIN reset. As a result, Red Hat Certificate System now provides the first end-to-end smart card solution throughout the user management life cycle.

WHY SHOULD I CARE?

With Red Hat Certificate System your network applications, data devices, and users operate within a security framework to ensure that the right resources are accessed only by authorized users.

Overview

- Supports all aspects of deploying and maintaining a Public Key Infrastructure (PKI) for managing user identities
- Integrates easily with third-party security software and existing applications through published APIs
- Allows administrators to request and install certificates on smart cards, in real time, with minimal interaction from end users
- Scales to manage millions of digital certificates
- Supports key recovery for retrieval in the case of lost encryption keys
- Supports distributed architecture for high availability
- Supports cross-certification with other PKI deployments
- Supports use of Global Platform compliant smart cards (tokens) to simplify key management
- Supports enrollment of routers and devices via SCEP
- Auto Enrollment Proxy integrates seamlessly with Microsoft Windows Active Directory environments.

Strong authentication

Unlike passwords, certificates can't be easily reproduced. Issued by a trusted authority, digitally signed certificates provide a reliable method of verifying user identity and preventing identity theft.

Enables Single Sign-On

Single sign-on is the ability for a user to log in once, using a single password, and get authenticated access to all servers that user is authorized to use—without sending any passwords over the network.

Single sign-on has immediate benefits for both the user and administrator. Users can gain access to multiple resources with a single login. For administrators, single sign-on simplifies maintenance across servers. It can also lower enterprise help desk costs by reducing the volume of calls concerning lost passwords.

Digital certificates issued by Red Hat Certificate System and tied to entries in a corporate LDAP directory provide a reliable way to support single sign-on. Also, this release supports Global Platform compliant smart cards, meaning you can distribute your certificates on portable smart cards that automate single sign-on from any computer within an organization.

Enables secure communications

Protecting mission-critical information is an important requirement to security-conscious companies. Red Hat Certificate System issues X.509v3 certificates that allow an enterprise to encrypt both critical network-based information and confidential email traffic.

Flexible deployment

Red Hat Certificate System allows for flexible deployment, adaptable to enterprise security policies and existing investments in security solutions. Easy configuration and installation allow enterprises to tailor deployment for use with a variety of extranet and intranet applications. Features available include off-the-shelf integration with third-party products; customization application programming interfaces (APIs) for authentication, policy modules, and custom extensions; and an authorization framework that allows IT administrators to assign access controls to groups and administrative users.

High scalability and manageability

Red Hat Certificate System provides a distributed, high-performance architecture that is designed to support large deployments across employees, partners, and customers. It includes a centralized, web-based administration tool that helps administrators manage roles, logs, users, and groups. A command-line interface is also available for easy automation of common tasks.

Cloning features allow Red Hat Certificate System to be deployed with multiple Certificate Authorities (CA) for high availability and increased scalability while maintaining a distributed architecture.

Advanced security features

Red Hat Certificate System uses FIPS 140-2 Level 2-validated security libraries and can be used with Level 3-validated hardware. Hardware signing protects the highly sensitive CA signing key, keeping it off any easily accessible desktop machine.

Integrated Applications

Red Hat Certificate System enables enterprises to deploy web-based authentication, form signing, virtual private networks, routers, and S/MIME. It is fully integrated with Red Hat Directory Server as well as other security solutions such as SecurID, allowing enterprises to easily leverage existing investments in security solutions.



FEATURES:

Software signing

- Signs certificates using industry-standard RSA digital signature (RSA signature with SHA-256 or SHA-512 hash)
- Supports signed audit logs

Flexible policies

- Permits hierarchically organized certificate authorities
- Includes customizable policy templates that can be adapted for unique enterprise certificate management policies
- Supports automated online authentication checks against existing credential databases through a published API
- Supports cross-certification with other PKIs, allowing a CA to create and sign cross-signed certificates for another CA

Reduced administration

- Requests, delivers, and installs certificates over a network using web protocols, such as HTTP, HTML, and SSL
- Distributes certificates and certificate revocation lists to LDAP-compliant directory services
- Enables remote administration of the Red Hat Certificate System from various computers on the network using SSL's encryption, message integrity, and authentication services
- Features tight integration with Red Hat Directory Server
- Provides an authorization framework that allows administrators to assign access controls

Integrated applications

- Enables certificate-based applications that require strong authentication, signing, and/or encryption, including web-based form signing and S/MIME
- Integrates with existing security environment through authentication plug-ins
- Works with various browsers to allow management of personal certificates
- Integrates with NSS Security Toolkit to allow developers to add Public Key Infrastructure (PKI) support in custom applications

Flexible architecture

- Enables corporations to issue, renew, suspend, revoke, and manage single and dual-key certificates
- Supports certificate requests from clients, servers, and network devices, such as virtual private network clients and routers
- Supports key archival for long-term storage of encryption keys
- Modular system design allows components, including Registration Manager, Certificate Manager, Data Recovery Manager, and OCSP Manager, to run on multiple systems (such as a cluster configuration) to support delegated registration authorities and increased scalability
- Allows for cloning of certificate authorities for scalability without creating subordinate certificate authorities
- Encrypts communication between all components using SSL client authentication with optional hardware acceleration for increased performance
- Allows installation of user certificates to a browser or smart card



- Provides a customizable Enterprise Security Client—a user interface for desktop key management tasks that facilitates use of Global Platform protocols for communication between a registration manager and individual user tokens. The Enterprise Security Client provides a simplified interface for supporting desktop management tasks like PIN resets. It also enables fully configurable enrollment using deployment-customized information.

Extensible solution

- Delivers APIs and tools to develop custom plug-ins for authentication, policy, and certificate extensions
- Enables integration of existing custom business logic and legacy applications
- Provides registration templates that collect user ID, password, and PIN information. HTML-based templates may be easily customized to collect specific information for other authentication modules.

Open standards support

- Issues certificates for use with SSL-compliant clients and servers
- Issues certificates for use with S/MIME

- Formulates, signs, and issues industry-standard X.509v3 public-key certificates
- Supports DSA and RSA public-key algorithms for encryption, hashing, and signatures
- Supports certificate requests using standards such as PKCS #10, CRMF (with proof of possession) and CMC
- Allows clients and servers to communicate with Red Hat Certificate System via Online Certificate Status Protocol (OCSP) for revocation checking
- Issues certificate revocation lists (CRLs) at specified intervals that are downloadable by certificate-aware clients and servers.
- Includes a built-in OCSP responder that is tightly integrated with the entire Certificate System architecture. This allows clients and servers to communicate to Certificate Management System via OCSP for revocation checking.
- Supports Global Platform compliant smart cards, greatly simplifying all key management tasks, such as initial enrollment, key archival, PIN reset, and key recovery.
- Supports SCEP enrollment protocol for routers and other devices.

SUPPORTED PLATFORMS AND SYSTEM REQUIREMENTS

HARDWARE	ARCHITECTURE	OPERATING SYSTEM	SERVER MEMORY	DISK SPACE
Sun	SPARC 64bit	Solaris 9	256 MB (required)	400 MB (minimum)
Intel / AMD	i386 and x86_64	Red Hat Enterprise Linux 4, 32- and 64-bit versions	256 MB (required)	400 MB (minimum)