RED HAT CERTIFICATE SYSTEM

DATA SHEET

WHAT IT IS

The Red Hat Certificate System is an enterprise software system designed to provide a scalable, secure framework to establish and maintain trusted identities and ensure the privacy of communications.

Red Hat Certificate System is designed to provide Certificate Life Cycle Management – issue, renew, suspend, revoke, archive/recover, and manage single and dual-key X.509v3 certificates needed to handle strong authentication, single sign-on, and secure communications.

The Certificate System servers include six subsystems:

- Certificate Authority (CA)
- Registration Authority (RA)
- Data Recovery Manager (DRM), sometimes referred to as a Key Recovery Authority (KRA)
- Online Certificate Status Protocol (OCSP) Responder
- Token Key Service (TKS) and Token Processing System (TPS) for smart card management

Certificate System integrates these subsystems to simplify certificate issuance and validation, smart-card management, and key back-up for public key infrastructure (PKI) deployments.

WHAT IT DOES

- Supports all aspects of deploying and maintaining a 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 corrupted 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.

STRONG AUTHENTICATION

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

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

SINGLE SIGN-ON

Digital certificates issued by Red Hat Certificate System can be tied to entries in a corporate LDAP directory. This provides a reliable way to support single sign-on. Additionally, support for Global Platform-compliant smart cards makes it easy to distribute certificates on portable smart cards that automate single-sign on from any computer within an organization.

SECURE COMMUNICATION

Red Hat Certificate System issues X.509v3 certificates that allow an enterprise to encrypt both critical network-based information and confidential email traffic.

ADVANCED SECURITY FEATURES

Red Hat Certificate System supports FIPS 140-1 Level 2-validated tokens 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 and can be easily integrated with

RED HAT CERTIFICATE SYSTEM

other security solutions, like mobile devices, allowing enterprises to leverage existing investments.

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 ECC 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
- Allow clients and servers to communicate securely with up-to-date certificate status checking via Online Certificate Status Protocol (OCSP) for revocation checking
- Issues certificate revocation lists (CRLs) at specified intervals that are download-able by certificate-aware clients and servers.
- Supports Global Platform-compliant smart cards, simplifying all key management tasks, such as initial enrollment, key archival and recovery, PIN reset, and key recovery
- Supports certificate issuance for routers and other devices using SCEP

SUPPORTED PLATFORMS

Red Hat Certificate System Subsystems (CA, KRA, OCSP, TKS, TPS)
Red Hat Enterprise Linux 7.1 and later (x86_64, 64 bit)

Enterprise Security Client (ESC) Supported Platforms
Red Hat Enterprise Linux 7.1 and later (x86_64, 64 bit)
NOTE: ESC is also supported on latest versions of Enterprise Linux 5 and 6, but Red Hat Enterprise Linux 5 and 6 do not support Red Hat Certificate System 9, but those clients can be used against the TMS system in Red Hat Certificate System 9.

Supported Web Browsers by Platform		
Platform	**Agent Services**	**End User Pages**
Red Hat Enterprise Linux	Firefox 38 and later	Firefox 38 and later
Windows 7	Firefox 40 and later	Firefox 40 and later
		IE 10
WindowsServer 2012	Firefox 40 and later	Firefox 2.x

SUPPORTED SMART CARDS

The Enterprise Security Client supports Global Platform 2.01-compliant smart cards and JavaCard 2.1 or higher. The Certificate System subsystems have been tested using the following tokens:

- Gemalto TOP IM FIPS CY2 64K token, both as a smart card and GemPCKey USB form factor key
- SafeNet Smart Card 650 (SC650), with support for both SCP01 and SCP02

NOTE: All versions of SC650 require the Omnikey 3121 reader. Legacy smart cards can be used with the SCM SCR331 CCID reader.
The only card manager applet supported with Certificate System is the CoolKey applet, which is part of the pki-tps package in Red Hat Certificate System.

SUPPORTED HSM

Red Hat Certificate System 9 has been tested to support two hardware security modules (HSM):

- nCipher NShield connect 6000
- Gemalto SafeNet Luna SA 1700.

www.redhat.com
Sep 2015
For external / internal usage.