Trusted Cyber Technologies

THALES

Fortify your Red Hat Public Key Infrastructure

The Challenge

Red Hat Certificate System provides a powerful and comprehensive security framework to manage user identities and ensure communication privacy. Handling all the major functions of the identity life cycle, it easily facilitates enterprise-wide deployment and implementation of a public key infrastructure (PKI). Red Hat Certificate System subsystems include a Certificate Authority, Key Recovery Authority, Online Certificate Status Protocol server, Token Key Service, and Token Processing System.

Red Hat Certicate System 9.4 has also been awarded NIAP certification for compliance with the Common Criteria Protection Profile for Certification Authorities (v2.1) and also appears on the National Security Agency's Commercial Solutions for Classified (CSfC) Components Llist as an approved Certificate Authority (CA). With a dedication to security, Red Hat has numerous software modules validated to FIPS 140-2 Level 1. In the Level 1 solution, however, the private keys and certificates for the various subsystems are stored in Red Hat's native Network Security Services key store, which is a software-secured storage area. Many federal organizations mandate a higher level of FIPS 140-2 assurance and require hardware security module (HSM)-based protection of the most critical keys in the PKIhigh-value crytographic keys. In addition, for CSfC registration, a Red Hat-based certificate CA solution must be paired with an HSM approved by the NSA for use in the National Security Systems Public Key Infrastructure (NSS PKI).

The Solution

Thales Trusted Cyber Technologies' (TCT) Luna Hardware Security Module (HSM) family is not only validated to FIPS 140-2 Level 3, but the HSMs are also approved by use in the NSS PKI by the National Security Agency (CNSS Memorandum 063-2017). By using a Thales TCT Luna HSM, organizations can be assured the most critical keys in their PKI are generated and stored in a validated and trusted HSM designed and built in the United States for specifically for that purpose. Private keys generated in the HSM never leave the hardened appliance and are utilized by Red Hat Certificate System subsystems via cryptographically secured communication links. At no time are these critical keys exposed to threats that exist in the external operating environment.

By utilizing an integrated Red Hat Certificate System and Thales TCT Luna HSM solution, federal organizations can build a Public Key Infrastructure meeting the most stringent of security standards and also work with two companies dedicated to providing robust and certified security solutions to the U.S. Federal Government.

Red Hat Certificate System Key Benefits

- NIAP evaluated and NSA approved as a CSfC component
- Support for all PKI functions including signing, revoking, renewing, publishing certificate revocation lists, and verifying certificate status
- Support for archiving and recovering escrowed encryption keys
- Multifactor authentication capabilities via an included card management system
- High availability and scalability

Thales TCT Luna HSM Key Benefits

- Provides centralized lifecycle management of cryptographic keys in a purpose-built, FIPS 140-2 Level 3 validated appliance approved by NSA for the NSS PKI
- Offloads and accelerates cryptographic operations to a dedicated cryptographic processor
- Available in multiple form-factors, including a USB-attached model ideal for offline root CAs
- Can be grouped together to provide high availability for critical PKI applications
- Developed, manufactured, and supported solely within the boundaries of the U.S., thus providing a completely trusted U.S.-based source

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business unit of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com