Scalable and secure PKI operations and certificate management

KEYFACTOR
SECURE EVERY DIGITAL IDENTITY

According to Gartner there will be 7.3 billion smartphones, tablets and PDAs in the marketplace by 2020. Dwarfing that number is the 26 billion Internet of Things (IoT) devices that will communicate across an open and common medium. Cyber threats, outages, and data breaches pose real risk to enterprises, and can have a significant impact on both revenue and reputation of businesses worldwide.

As the IoT grows, so do security risks. The use of PKI and digital certificates can help mitigate risk and keep threats at bay.

Getting ahead of security risks using certificates for identification and authentication

The underlying mechanism that ensures secure identity is a cryptographically sound public key infrastructure (PKI). A robust implementation of certificates allows for digital identities to be integrated into business processes and workflows, significantly improving both the security posture of an enterprise, as well as end-user experiences. Deploying certificates and managing them across internal and external workloads throughout their lifecycle is a complex process. The margin of error is slim and the impact of miscalculation can be costly.

Keyfactor Command and Entrust nShield HSM deliver proven, highly scalable, and secure enterprise PKI operations management

Keyfactor Command simplifies the identification, cataloging, monitoring, issuance, and revocation of digital certificates across multiple enterprise platforms. Keyfactor Command is uniquely designed and implemented to address complex PKI environments that include both public SSL certificates, as well as multiple private certificate authorities and their associated internal workloads. Designed specifically for making the issuance, revocation, and lifecycle of all certificates in an organization scalable and highly secure, the Keyfactor platform brings IT professionals everything they need to manage their infrastructure at scale — enabling on-device support for iOS, Mac, Linux, Java, and Windows certificate processes, including a rich reporting and alerting infrastructure.

Combined with Entrust nShield® Connect hardware security modules (HSMs), Keyfactor Command delivers a high assurance PKI implementation in an economically efficient and highly scalable model. Keyfactor and Entrust provide a proven, agile platform from which your identities and information can be secured.

LEARN MORE AT ENTRUST.COM/HSM

Scalable and secure PKI operations and certificate management

Secure even more: an additional layer of security by using an HSM

Critical PKI keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack or other form of compromise. HSMs are considered by analysts and technology leaders to be a best practice for root and issuing CA private key protection providing certified, auditable security. nShield Connect HSMs integrate with Keyfactor Command to provide comprehensive logical and physi- cal protection. The combination delivers an auditable method for enforcing security policies that underpin critical components of the enterprise PKI.

Working together, Keyfactor Command and nShield allow you to:

- Enable highly scalable, comprehensive enterprise PKI management
- Establish an IoT directory for device authentica- tion and authorization
- Offer hassle-free enterprise PKI managed services in the Cloud or on-premises
- Provide centralized control and management of every certificate's lifecycle
- Simplify security auditing and reduce compliance risk

And more:

- Secure CA root and issuing private keys within a carefully designed cryptographic boundary
- Protect keys using robust access control mechanisms, so keys are only used by authorized personnel for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed by the PKI
- Provide a hardened, tamper-resistant environ- ment for performing secure cryptographic processing, key protection, and key management including code signing keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, and CNG)

About Keyfactor

Keyfactor is a leading provider of secure digital identity management solutions that enables organizations to confirm authenticity, and ensure the right things are interacting in the right ways in our connected world.

Learn more

For more detailed technical specifications, visit **www.keyfactor.com**

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com