

Venafi Encryption Director Certificate Manager™

DISCOVERY | MONITORING | VALIDATION | ENROLLMENT | PROVISIONING



WHAT IT DOES

Venafi Encryption Director Certificate Manager enables organizations to rapidly inventory, monitor and provision digital certificates across their enterprise environments through:

- Continuous Discovery
- Monitoring & Alerts
- Validation
- Extensive Reporting
- Enrollment
- Provisioning



WHY IT'S VALUABLE

Simplify the management of digital certificates across the enterprise environment and reduce the unquantified and unmanaged risks that result in data breaches, failed security audits and unplanned system downtime.

SECURITY, AVAILABILITY AND EFFICIENCY

Encryption has become ubiquitous in today's IT infrastructure and is critical in any security strategy. Digital certificates are a core component of the larger encryption landscape for securing communications and authenticating users and systems for protocols such as SSL and IPSEC.

While certificates and their associated private keys are leveraged heavily for mission-critical applications, they do not come without overhead. First, the trust and validity of a certificate is time limited—typically valid for one year—and must be renewed before the lifecycle period expires or system outages and downtime occur. Second, although the public portion of a certificate is freely transmitted, the private portion must be kept secret and properly managed to avoid data or system compromise. Finally, the certificates and private keys must adhere to current encryption standards and best practices.

Expiration Risk

Once a certificate is installed and in use, it is easy to forget about, lose track of, or have the responsible administrator move on to another project or position. All certificates have expiration dates. Applications and processes that rely on the certificate for security or trust stop functioning when a certificate expires. Because most corporations have hundreds or thousands of certificates in use that are being managed manually, unplanned system outages are increasingly common and can have disastrous effect.

Security Risk

A certificate's private key protects access to the information it secures and is used to decrypt confidential data or authenticate users or systems. Thus, strict security of the private key is critical to ensure data and system protection during its lifespan. As a result of the manual-management practices used in many organizations, numerous administrators have unfettered and unmonitored access to private keys. This represents unmanaged risk in organizations.

Administrators who have had access to a certificate's private key during its lifecycle can easily use it for nefarious purposes and compromise the data it protects. Organizations must minimize the number of adminis who have access to private keys and ensure proper separation of duties and access controls.

Compliance Risk

Regulations and standards are requiring increasingly stringent management practices and compliance reporting of cryptographic keys. For example, PCI-DSS requires separation of duties, dual control, and other processes to ensure keys used for protecting credit card data are properly secured. The National Institute of Standards and Technology (NIST) has issued recommendations SP 800-57 and 131A, which call for all certificates and private keys to be 2048-bits or larger.

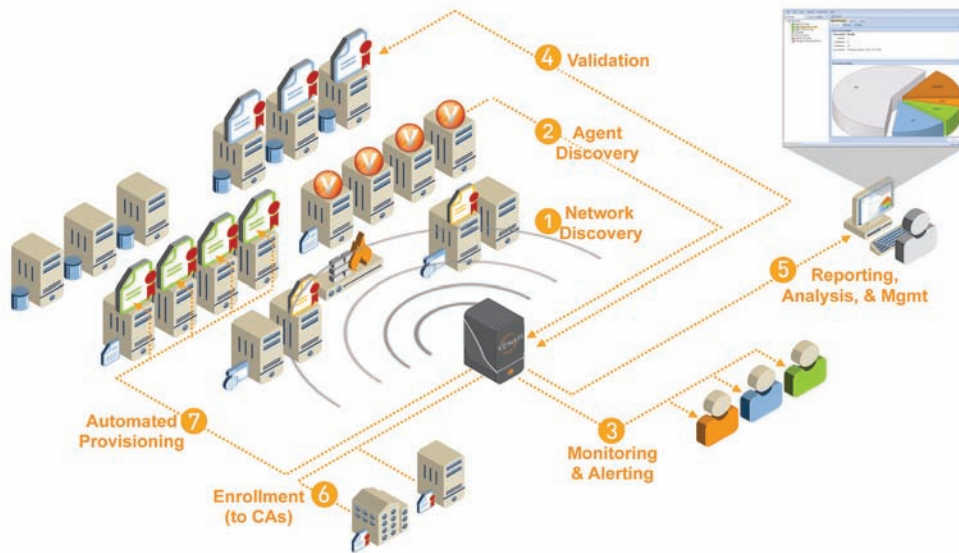
Compliance with these requirements necessitates maintaining an inventory of all keys to ensure sufficient key strengths, sound enforceable management practices, and compliance reporting. Many organizations are at risk of audit failures due to poor key and certificate management practices and rapidly expanding use of certificate-based encryption.



VENAFI ENCRYPTION DIRECTOR CERTIFICATE MANAGER

Venafi Encryption Director™ Certificate Manager™ (Director Certificate Manager) enables organizations to rapidly develop an accurate certificate inventory and identify security and operational risks. Additionally, organizations can quickly evaluate their compliance with corporate and regulatory policies and establish a concise methodology to ensure compliance. With built-in management and policy best practices, Director Certificate Manager helps eliminate data breaches, security audit failures and unplanned system outages.

Director Certificate Manager enables organizations to quickly quantify their certificate- and private key-related risk. Once quantified, it is possible to manage that risk and drastically reduce exposure. Director Certificate Manager is built on the Director platform, which for nearly a decade has enabled many of the world's largest organizations to manage their encryption environments effectively.

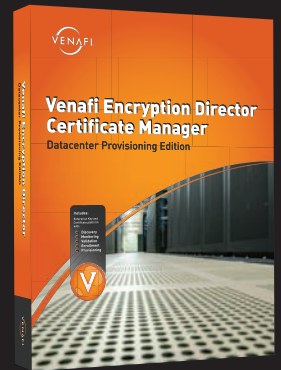


Director Certificate Manager manages hundreds of thousands of keys and certificates for some of the largest organizations in financial services, healthcare, retail, aerospace, and other industries. Director's third-generation architecture supports multiple certificate authorities, heterogeneous platform deployments and various encryption types, and has proven scalability in some of the world's largest deployments. Director Certificate Manager provides out-of-the-box automated management capabilities that eliminate unquantified and unmanaged risk, including:

- Develop an inventory: Remove guesswork and get a clear picture of your encryption landscape through automated discovery. Rapidly identify where risk exists and take action.
- Monitor certificate expiration: Alert administrators before problems wreak havoc in your environment, escalate if timely action is not taken.
- Reduce private key access: With secure and automated remote generation and provisioning of keys and concise separation of duties, you can minimize private key access. Ensure that those with knowledge of a key's credential do not have access to the stored key.
- Get compliant: Compare assets to standards and measure reality versus objectives. With policy-based automated enrollment and provisioning, ensure that mission-critical encryption assets meet the standards you must comply with, while reducing administrator workload.

With Venafi Encryption Director, you can ensure that your encryption systems provide the security they are designed to deliver while at the same time reducing operational risk and administrative workload. Secure your organization with Venafi Encryption Director Certificate Manager today and dramatically minimize your risk profile. Learn more at www.venafi.com/Director.

Copyright © 2011 Venafi, Inc. All rights reserved. Venafi and the Venafi logo are trademarks of Venafi, Inc. in the United States and other countries. All other company and product names may be trademarks of their respective companies. This datasheet is for informational purposes only. Venafi makes no warranties, express or implied, in this summary. Covered by United States Patents #7,418,597, #7,568,095, #7,650,496, #7,650,497, #7,698,549 and other patents pending. Part number: 4-0007-0211



SUPPORTED SYSTEMS

Web Servers:

- IBM® HTTP Server
- IIS
- Apache
- Oracle® iPlanet

Application Servers:

- IBM WebSphere Application Server
- Oracle WebLogic

Middleware:

- IBM WebSphere MQ Server
- IBM WebSphere MQ Client
- IONA Artix

SSL Accelerators:

- F5® Big-IP®
- Citrix® NetScaler
- Cisco® ACE
- Cisco CSS
- Brocade® Foundry

Other:

- IBM Tivoli® Access Manager
- PKCS (#7 & #12)
- PEM
- IBM Global Secure Kit (GSK)
- Java keystore

The above is not an exhaustive list of supported systems. Director supports thousands of platforms and applications out of the box. Supported versions are subject to change without notice. Contact a Venafi Sales Representative for a current list of supported platforms.



Contact **Venafi** at:

Worldwide: +1 801 676 6900
EMEA: +31 641 789 667
info@venafi.com

www.venafi.com