



VENAFI, INC.

2011 ENTERPRISE ENCRYPTION KEY AND DIGITAL CERTIFICATE MANAGEMENT MARKET OUTLOOK

RESEARCH REPORT REVEALS IMPACT OF INCREASED
ENCRYPTION USE IN TODAY'S ORGANIZATIONS

Eliminating unquantified and unmanaged risk—
Millions of encryption keys and digital certificates at a time

Copyright © 2011 Venafi, Inc. All rights reserved. Venafi, the Venafi logo and Systems Management for Encryption 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 Patent #7,418,597, #7,568,095, #7,650,496, #7,650,497 and other patents pending

Executive Summary

When organizations rely on the Internet and their corporate networks to conduct global business and facilitate worldwide communications, they deploy multiple layers of IT security hardware and software technologies — all designed to protect networks from unauthorized intrusions, cyber attacks and regulatory compliance violations.

Key to any effective IT security and compliance program are encryption key and digital certificate technologies. These indispensable tools allow systems and servers to authenticate with one another, secure data, and validate that only authorized users and systems are conducting incoming and outgoing communications and business transactions. Sensitive, regulated information would be completely exposed without digital certificates and encryption keys.

All organizations that rely on electronic communications and authentication — regardless of size or industry — utilize encryption keys and digital technologies in some form. Many of the world's Fortune-ranked organizations utilize thousands and even hundreds of thousands of encryption keys and digital certificates across their global networks. Without automated management processes, solutions and best practices, organizations will never gain complete control of their key and certificate inventories, resulting in significant unmanaged and unquantified risk within organizations, including unauthorized access, failed security audits and unplanned system downtime.

Venafi is providing this free report to the market in general to demonstrate the challenges organizations are facing when it comes to data protection, encryption key and digital certificate management. Based on extensive survey data, the report draws conclusions regarding why problems exist and provides direction on steps organizations can take to eliminate unquantified and unmanaged risk.

This report and its conclusions are based on a number of research data points:

- A 2011 survey of 471 enterprise-class organizations
- Research reports and opinions from noted analysts and firms
- Intimate interactions with customers, prospects and partners
- Prior market surveys

Conclusions

This report provides a number of salient conclusions:

- Organizations are deploying increasing numbers of digital certificates and encryption technologies.
- These security assets are also becoming lost, stolen and unaccounted for in epidemic proportions.
- These security assets become dangerous liabilities when they go missing, expire or find their way into the wrong hands.
- Reliance on antiquated, resource-intensive manual management processes is not only exacerbating security and compliance problems but also leaving expired certificates in place, which lead to costly systems downtime and outages.
- There is a lack of understanding and guidance when it comes to available best practices and solutions that can eliminate unquantified and unmanaged risk.
- Deployment of an encryption key and digital certificate management solution that automates processes, such as Venafi's, can eliminate unquantified and unmanaged risk, costly manual processes, and expired certificates and systems downtime.
- As recognized by Gartner in the Cool Vendors in 'Data and Infrastructure Protection, 2010,' Venafi's "cool factor" lies in its neutral relationship with the many vendors and services it interfaces with, and in its simplification of complex cryptographic management activities. In the case of X.509 certificates, the Venafi solution supports the autodiscovery, registration and management of all certificates issued to devices, applications and services.

Research information sources included but were not limited to the following:

- Venafi 2011 Market Survey, which polled 471 management and C-level respondents — 59 percent of the respondents surveyed worked in organizations with more than 5,000 employees. Respondents' organizations spanned a wide range of industries, including high tech, telecommunications, banking/financial services, energy/oil and gas, government, aerospace, manufacturing and retail. Among the respondents was one of the world's largest food distributors and consumer retailers.
- Oct. 2010 Security and Availability: SSL Certificate and Key Management survey conducted at the Gartner IT Expo, Florida. Venafi invited the 150-plus registrants from the world's largest

companies to weigh in on the market problem of downtime caused by the increase in encryption deployments, coupled with an acute lack of enterprise management controls.

- 'Gartner Cool Vendors in Data and Infrastructure Protection, 2010,' available at www.venafi.com/cool
- Insight from industry pundits, including Richard Stiennon, noted author, speaker and principal analyst at IT Harvest.
- Intimate contact and consulting sessions with customers, prospects and partners — including a case study with Zions Bancorp.
http://www.venafi.com/Collateral_Library/Zions_Bancorp_Success_Story.pdf

Venafi 2011 market survey results:

- 51 percent stated they had experienced either stolen or unaccounted-for digital certificates, or that they were uncertain if their organizations had lost, stolen or unaccounted-for digital certificates in general.
- 54 percent stated they had experienced either stolen or unaccounted for encryption keys, or that they were uncertain if their organizations had lost, stolen or unaccounted for encryption keys in general.
- 46 percent of organizations are managing at least 1,000 digital encryption certificates; 20 percent are managing more than 10,000.
- 83 percent of organizations are managing technologies from at least two different CAs; 18 percent are dealing with more than five.
- 88 percent of organizations have multiple administrators managing encryption keys; 22 percent have more than 10.
- 42 percent of organizations manage encryption technologies from at least four vendors; 8 percent are dealing with more than 10.

Oct. 2010 Security and Availability: SSL Certificate and Key Management survey results:

- Organizations anticipate a 27 percent year-over-year certificate and key inventory growth rate.
- 85 percent of organizations manage encryption certificates and private keys manually via spreadsheets and reminder notes.

- 78 percent of organizations have experienced system downtime due to encryption failures in the past 12 months.
- 96 percent of organizations use certificate-based server-to-server and/or server-to-client mutual authentication for secure communications inside the firewall.
- 71 percent of organizations have regulatory auditors assessing against private and asymmetric key management.