Charting Your Path to Enterprise Key Management

WHITE PAPER

Steps to Take Today for a More Efficient, Secure Key Infrastructure

Executive Summary

The increasingly prevalent use of data protection mechanisms in today's enterprises has posed significant implications. One of the most profound challenges relates to key management, and its associated complexity and cost. Written for business leadership and security architects, this paper looks at the past, present, and future of key management, revealing how emerging trends and approaches will ultimately enable enterprises to optimize both efficiency and security in the management of key materials.

Introduction

Enterprises today need to balance several equally critical business mandates:

- Strengthen security. Businesses need to enhance data security to minimize the risk of loss or breach of sensitive, personally identifiable information of patients, customers, or employees. Companies must also protect intellectual property, such as legal records, files and correspondence associated with mergers and acquisitions, trademarked digital media, and much more. This sensitive information can be found in structured systems, such as databases, as well as in unstructured files like word processing documents, spreadsheets, images, designs, and PDFs. As part of this effort, security teams need to consistently enforce corporate security policies, while at the same time contending with increasingly dynamic infrastructures, workforces, outsourcing relationships, and organizational structures.

- Ensure regulatory compliance. It is incumbent upon organizations to comply with all relevant without impacting the user experience or affecting their performance regulations, whether that means organizations following regional privacy and breach notification rules, including U.S. state laws and the E.U. data protection directive; retailers adhering to the Payment Card Industry Data Security Standard (PCIDSS); financial organizations complying with Sarbanes- Oxley; or healthcare organizations meeting standards set forth in the Health Insurance Portability and Accountability Act (HIPAA). Compliance with relevant regulations is not a one-time, static event, but rather a continuous endeavor, which means organizations must nimbly adapt to changing standards, definitions, and auditor findings.

• Manage costs and leverage investments. In an uncertain, tough economic climate, costs need to be managed closely, and businesses need to wring maximum value out of their investments. In this environment, organizations are increasingly relying on cloud-based and outsourced services to improve agility, scale operations and reach, and reduce capital and operational expenditures. For internal infrastructures, closed, proprietary systems are increasingly at odds with an organization's financial and administrative goals. Protecting, managing, and leveraging a heterogeneous environment requires a combination of integration flexibility and interoperability through open standards.

Business Mandates Led to Increased Reliance on Encryption

In recent years, encryption has become increasingly prevalent. This is in direct response to two of the business mandates above, namely security and compliance, with both security best practices, competitive demands, and compliance mandates dictating encryption of credit cards, personally identifiable information, and other private information, wherever those sensitive data assets may reside.

This increased adoption of encryption has often run directly counter to the business' other chief objectives, namely cost reductions and interoperability. Initial forays into encryption have often been tactical in nature, for example, responding to a breach or rushing to prepare for an upcoming audit. Often, these efforts were driven by a department or workgroup rather than corporate initiative. Consequently, these efforts tended to be costly, both in initial expenditures and in terms of ongoing maintenance and overhead. In addition, in these scenarios organizations typically employed point solutions that don't provide full data protection. For example, an encryption solution may protect data when held within a specific platform or device, such as a database, but not when that data flows between different systems within the organization.

Key Implications of Encryption Adoption

Key management is one of the areas in which encryption's ongoing cost and effort is most pronounced. When encryption is employed, cryptographic keys must be safeguarded—if not, the entire encryption infrastructure can be compromised. Further, key administration entails such tasks as ongoing rotation, deletion, and creation—sensitive, potentially time-consuming tasks that can also present security vulnerabilities and devastating business impact, if they are not managed correctly. For example, loss of keys is a primary concern: If keys are lost, so is the encrypted data.

This paper looks at the evolution of key management in the enterprise, outlining some of the specific stumbling blocks of early encryption efforts. It then describes how more advanced encryption approaches are mitigating many key management challenges. The paper then looks at enterprise key management, describing how this will be the ultimate path for enterprises looking to optimize both efficiency and security in the management of their cryptographic keys. Finally, the paper explores some practical approaches businesses can take today to prepare for an enterprise key management program.

Early Key Management

As mentioned above, initial forays into encryption were largely more tactical, short-term efforts. Following are some common scenarios:

- In order to prepare for an upcoming PCI audit, a database administrator (DBA) is asked to deploy encryption on the company's customer database.
- After an employee in finance loses a laptop containing employee records, and the breach is widely reported, the company deploys whole disk encryption of the finance team's laptops.
- After an offsite tape storage facility misplaces backup tapes containing a retailer's financial records, including sensitive customer details like credit card data, the company employs encryption of the files before backing up to tape.

In a large enterprise, these disparate efforts add up, with dozens of distinct implementations being common. In many organizations, the amount of key material—keys, digital signatures, certificates, and so on—is doubling every year. As the number of these deployments grow, so too do the challenges:

- **Administration.** While these initial deployments may be expensive in their own right, it is after deployment that IT management begins to realize how truly expensive they are. Because these implementations have been done in an ad hoc, disparate fashion, they must also be managed that way. Efforts like backing up, rotating, and revoking keys must be done on each point system, and so begin to consume increasing chunks of administrators' time, and the time spent only grows as encryption grows more widespread.
- **Poor availability and performance.** The availability of cryptographic keys is vital; if they are unavailable, the data and assets they protect will be too. Additionally, tokenization solutions also requires administration for key management to map the token data vault to the associated ciphertext. Often, when early encryption approaches are employed, cryptographic keys end up on servers that don't have robust backup mechanisms in place, so they are subject to inadvertent deletion and outages. Further, they can be on general purpose servers that have many other competing processing demands, which can lead to unpredictable or slow response.
- **Complex auditing and logging.** With keys managed in a disparate fashion, so too are auditing, logging, and remediation, which represents long-term, ongoing administrative complexity, higher costs, and slower response to security breaches and threats.
- **Security gaps.** Because keys are held on disparate, general purpose systems—often on the very systems containing the sensitive data—they are vulnerable to theft and misuse. And the more locations keys reside in, the more pervasive an organization's risks. In addition, as keys are backed up, if they are, they often aren't secured in transit, which leaves them further exposed.

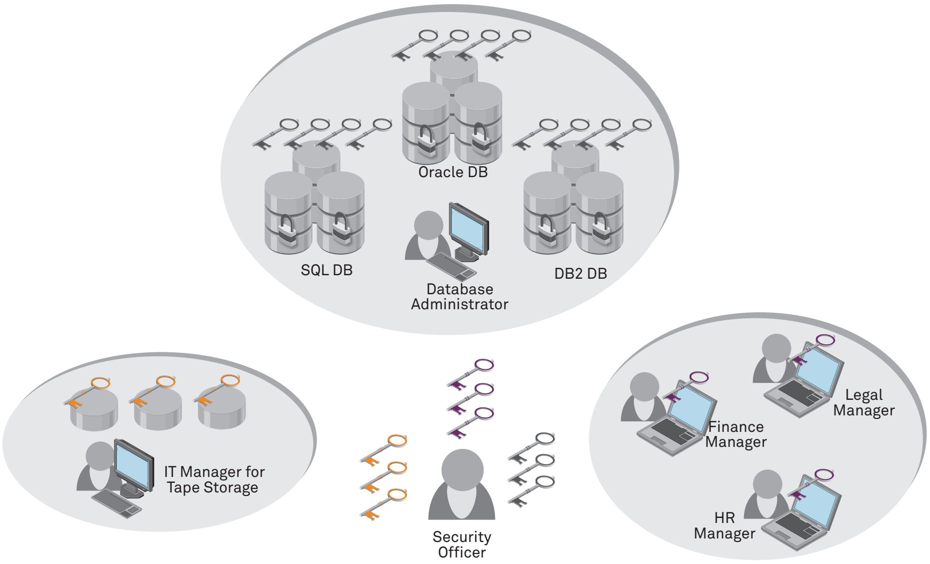

Figure 1: Disparate Key Management

Today's Key Management

In recent years, organizations have adopted more advanced security solutions that offered many advantages compared to the tactical approaches of the past.

These solutions offered more comprehensive lifecycle key management capabilities, which means they were purpose built to support keys throughout their lifecycle, including creation, rotation, storage, backup, and deletion. Often these solutions were more centralized in nature, which meant keys were more consistently, and efficiently managed and secured. However, these approaches could present challenges if employed in silos. Here are some suggestions to minimize the impact of those challenges:

- Select key management tools that cover the broadest range of usage scenarios to limit the number of silos, and therefore reduce the administrative overhead, points of vulnerability, and cost.
- Create a master report to summarize logs from various data protection solutions to help streamline proof of compliance and identify trends across the organization.
- Leverage lessons learned from siloed solutions to determine best practices for access policies and the management of the key lifecycle in anticipation of eventually incorporating a true enterprise key manager.

Key Life Cycle (NIST SP800-57)

A Key's access policies change as the key progresses through life cycle!

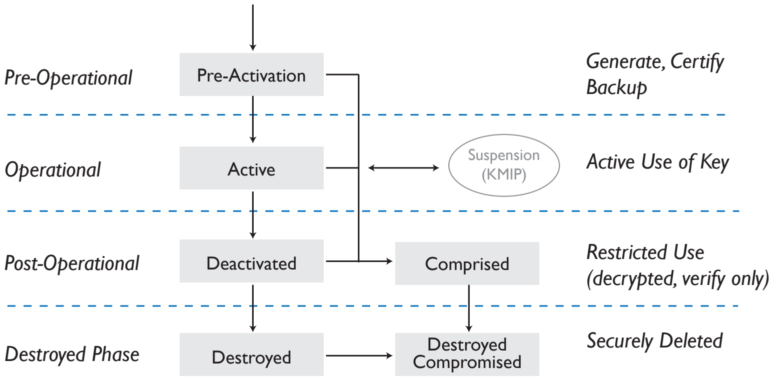

Figure 2: The Lifecycle of Cryptographic Keys

Enterprise Key Management: What It Is

Enterprise key management represents a centralized approach for the control of all cryptographic keys—across an entire enterprise. Enterprise key management constitutes the protection of all of an organization's key materials, essentially the governance of all the "secrets" relating to cryptography. This includes the following key materials:

- **Identities.** This includes end users, endpoints, and services. These are the public key infrastructure secrets in use when asymmetric cryptography is employed.
- **Information**. This includes data, and the containers and media that contain this data. In this case, protection secrets for symmetric cryptography are being managed.

Inherent in enterprise key management is standardization and centralized management, so security teams can get better visibility and control of previously disparate key management deployments and approaches. True enterprise key management will mean that all the secrets related to every digital protection system based on cryptography will be managed in a single, unified manner. Within this context, digital protection is defined as data encryption, communications encryption, and identity keys.

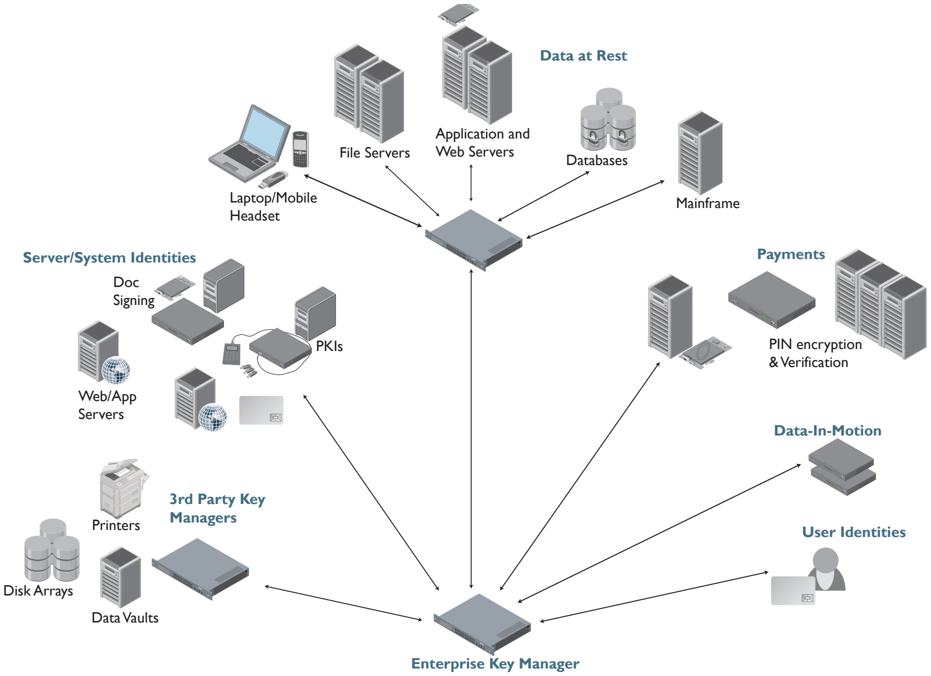

Figure 3: The Enterprise Key Management Infrastructure

Enterprise Key Management: Still a Nascent Market

While the theory of enterprise key management is very compelling, the reality hasn't taken hold in most enterprises to date. Why is this thecase?

The industry as a whole has been hindered by a lack of common standards, which are an essential ingredient to interoperability of solutionsfrom multiple vendors. Initially, the Institute of Electrical and Electronics Engineers (IEEE) made great strides in establishing standards for key management. The IEEE 1619.3 key management project was started in early 2007, and the standard developed was intended to define the "methods for the storage, management, and distribution of cryptographic keys used for the protection of stored data." However, these standards were quite comprehensive and therefore difficult to implement in practice.

In early 2009, the OASIS "Key Management Interoperability Protocol" (KMIP) Technical Committee was created. The KMIP group is leveraging some of the work that the IEEE 1619.3 group produced, while keeping the initial target release focus more narrow, so that a standard could be published sooner to address some immediate use cases, particularly in the storage area. Consequently, KMIP promises to provide a standard that will be easier to implement and manage in real-world situations. As of the publishing of this document, KMIP 1.0 is slated for release in the mid-2010 timeframe. As a result, the market is still waiting for this simpler standard.

Finally, it is important to note that one key driver for key management standards was to address the demand for managing identities. As the use of data encryption continues to grow, the need for enterprise key management, and the need to use standards broad enough to cover a wide array of asset types, as well as identities, will become increasingly critical. Therefore, market demand will foster the adoption of enterprise key management capabilities in the very near future.

Keys to Effective Lifecycle Key Management Today—and a Successful Enterprise Key Management Future

Focus on Comprehensive, Proactive Security

As outlined above, prior security investments and deployments have often been reactive in nature, responding to a breach, preparing for an upcoming audit, or modifying policies to map to changing regulations. As enterprise security teams evolve, so too will their initiatives and approaches. Given that, enterprise key management will be part of a holistic, strategic security plan that is based on best practices and optimal security, rather than a series of ongoing, tactical responses to issues and regulations. As part of this transition, security teams will be much more empowered and effective, focusing on the most critical efforts and assets in order to ensure optimal security is being realized.

Persistent, Data-centric Approach

Historically, many encryption solutions have offered a binary, either/or approach to securing resources. In the case of storage encryption, for example, this meant that solutions would enable security teams to encrypt and decrypt only an entire backup tape or backup job on a tape. In the case of laptop encryption, an entire hard drive would be encrypted. However, organizations have encountered significant limitations with many of these types of solutions because an entire tape or system would need to be decrypted any time data is needed. Further, point solutions used in these tactical deployments often only deal with one specific threat. For example, a tape encryption solution will only guard against loss or theft of tapes and full disk encryption will only guard against loss of disk. Today, more persistent and granular, asset-based encryption alternatives will need to be adopted. Persistent encryption offers a way to, with a comprehensive solution, guard against a broad range of threats and risks. These encryption mechanisms need to enable administrators and end users to employ encryption in a granular way, both by user and group permissions, asset type, and specific asset. This means not only being able to decrypt a credit card column in a database, but encrypting an excel spreadsheet with sensitive payroll information. An added benefit of this approach is that the more granular encryption, the more granularan audit trail is for compliance, monitoring, and remediation.

Following are several encryption requirements:

- **Persistent.** Encryption needs to be enforced persistently, so that, if a sensitive file is e-mailed, saved to a flash drive, stored in a cloud-based application, or transported anywhere else, security policies will remain in effect.
- **Top-down policy enforcement.** Administrators need to enforce policies in a top-down manner, so corporate-wide policies can be applied consistently and cohesively across the enterprise, and down to the specific asset and user level.
- **End user transparency.** To maximize adoption, enterprise key management will employ encryption regardless of whether encryption or tokenization is chosen as the method of data protection in a way that is completely transparent to end users, ensuring optimal security and productivity.

As more granular encryption alternatives are adopted, enterprise key management will become an increasingly urgent need. Modern key management approaches will both help facilitate and support the above objectives.

Centralize Key Management and Policy Enforcement

To be practical, enterprise key management needs to represent a move to a point in which keys are centrally managed across the enterprise, including across heterogeneous database platforms, application environments, endpoints, and more. Following are several benefits of this approach:

- **Decreased exposure of keys.** Centralizing key management offers fundamental advantages in security as it limits the number of locations in which keys reside, minimizing the potential for exposure.
- **Consistent policy enforcement.** Centralized key management makes it practical for administrators to more consistently enforce corporate standards and policies across the organization. For example, an administrator can set user credentials and policies around a specific asset once, and then ensure those policies are effectively employed, whether that data is saved to a database server, mainframe, or laptop.
- **Streamlined administration.** At the same time, centralized key management also streamlines administration, enabling administrators to make changes and updates once and have them propagated across all pertinent areas.
- Encryption efficiency. This also represents a more efficient model: As opposed to point encryption, where data on one platform would have to be decrypted and re-encrypted when it is transmitted to another platform, a specific asset can be encrypted once and distributed to multiple systems, and only need to be decrypted when an authorized user needs access to it.
- **Unified auditing and remediation.** Finally, having all keys centralized can significantly streamline auditing and remediation by housing auditlogs that encompass all key-related activities.
- **Tokenization Support.** With the emergence of tokenization as a viable option for protecting structured data accessed by some applications as a means to reduce the scope of compliance, centralized key management plays an essential role in consistently enforcing access policy between encryption and tokenization.

Guard Against Insider Threat

In order to guard against insider threats, it is vital for organizations to reduce the circle of trust, minimizing the number of employees who could potentially compromise or exploit cryptographic keys.

While access to keys should be restricted to the fewest number of security team members, organizations should also ensure that no single user has “super user” administrative privileges. Instead, security teams should enforce separation of duties, so, for example, one administrator is authorized to do network configuration, while another user might only be given access to certificate management. In addition, systems should allow administrators to continue to do their jobs unabated, which often means working with sensitive data, while restricting their ability to access sensitive data in the clear. In this way, IT can manage the data resources—without accessing the information inside the data files.

Further, all interactions with sensitive data should be logged. As organizations move to enterprise key management, and so centralize more key management control, this capability to guard against insider threats will grow even more critical.

Leverage Purpose-Built Security Products and Services

To maximize the protection of the key management infrastructure, organizations need to move key management off general purpose systems. For example, a software-based key manager saves keys on the same location as the encrypted data. This can pose availability risks, for example, if a system crashes, both keys and data will be lost. Further, it can pose a security risk as these software-based mechanisms are often easy for lots of internal users to access.

Instead, organizations need to ensure keys are housed and managed within infrastructures designed specifically with security in mind. For cloud providers and enterprises, this will mean employing software, hardware, and services that offer off-the-shelf compliance with relevant mandates, such as Common Criteria and the Federal Information Processing Standard (FIPS).

In the case of hardware, this requires tamper-proof hardware security modules, which ensure key materials can't be stolen by removing physical key storage devices from appliances. For example, an enterprise looking to leverage a cloud providers' elastic storage capabilities can encrypt sensitive assets and retain the associated cryptographic keys in a purpose-built hardware security module, before the data is migrated to the cloud, and so ensure that access policies are enforced, even as data moves outside of the enterprise.

Further, purpose-built systems and solutions should support an organization's ability to demonstrate and ensure compliance.

Maximize Investments through Broad Integration

Key management is an underlying linchpin to the entire security and IT infrastructure, and as a result, key management technologies and processes intersect with a broad array of systems and services across an enterprise. Enterprise key management represents an approach in which keys are centrally and cohesively managed across an entire organization. Preparing for this requires investing in solutions that offer the broadest integration in a range of areas:

- **Key management for point solutions.** Point encryption technologies, such as native database encryption solutions that only work on a specific database platform, are being used pervasively in many enterprises, and most likely will continue to be for some time. Organizations need to be able to leverage a solution that centrally manages key and policy management while securely protecting the keys. This offers advantages in both administrative efficiency and security.

- **Integrate with IT systems.** Enterprise-wide control over keys can only be realized through broad, effective integration with associated IT systems, including ID management, asset management, global policy administration, public key infrastructures, and token management. The deeper and more seamlessly key management is integrated with related systems, the more cohesively keys can be managed within a security framework.

- **Support for heterogeneous environments and assets.** Enterprise IT infrastructures continue to be more, not less, heterogeneous in nature. In a given enterprise, myriad platforms, operating systems, servers, and device types are in use and must be secured. Data is housed in an array of virtualized and cloud-based environments. Further, sensitive information is everywhere—databases, mobile devices, unstructured files, mainframes, and backup tapes. Key management needs to support the security of this breadth of standards and asset types.

Glossary

Lifecycle key management.
Capabilities for managing keys throughout their lifecycle, including creation, rotation, storage, backup, and deletion.

Enterprise key management.
A centralized approach for the governance of all cryptographic keys, across an entire enterprise.

Persistence.
Continuous security of assets, regardless of the location or state of that asset.

Transparency.
Minimizes the impact of encryption on users and associated systems.

Data centricity.
The approach of securing specific data assets, such as a file or column in a database, rather than entire systems.

Secrets.
The private materials associated with cryptography, including passwords, private keys, etc.

Key material
Includes cryptographic keys, identities, digital signatures, and algorithms.

Where are the exposure points for data?

	Inside Network	Partners' & Interagency Networks	Consultant/ Contract Networks	Outside the Network (Cloud/ SaaS)
Databases	🟪	🟧	🟧	🟧
Laptops	🟩	🟪	🟧	🟧
Desktops	🟩	🟪	🟧	🟧
Mobile Devices	🟪	🟧	🟧	🟧
Removable Devices	🟩	🟪	🟧	🟧
CDs/DVDs	🟪	🟧	🟧	🟧
File Servers	🟪	🟧	🟧	🟧
NAS/SAN Devices	🟩	🟧	🟧	🟧
Log Files	🟧	🟧	🟧	🟧
Excel Spreadsheets	🟧	🟧	🟧	🟧
PDFs	🟩	🟧	🟧	🟧
Word Docs	🟧	🟧	🟧	🟧
Image Files	🟩	🟧	🟧	🟧
PowerPoint Presentations	🟧	🟧	🟧	🟧
Email Text	🟧	🟧	🟧	🟧
Email Attachments	🟩	🟩	🟧	🟧
Instant Messages	🟩	🟪	🟧	🟧

Everywhere!

🟧 Exposed 🟪 At Risk 🟩 Safe

Figure 4: Enterprise Key Management Represents a Way to Secure All Sensitive Data across an Enterprise,While Centrally Managing and Securing Cryptographic Keys

Conclusion

Approaches to encryption and key management have evolved a great deal in recent years. However, to be sustainable from a cost and administrative standpoint, and to ultimately deliver the cohesive security required, encryption and key management will need to evolve further. Toward that end, organizations need to plan and prepare for enterprise key management—realizing a single, cohesive means for governing all cryptographic keys.
To get ready for this future, organizations need to employ approaches and solutions that offer open standards and flexible integration, granular and persistent controls, and central administration.

About SafeNet Key Management

SafeNet data encryption and control solutions focus on sensitive data, providing persistent protection throughout its lifecycle, wherever it resides. Information is protected at every moment—when it is created by an employee on a company laptop, shared with a business partner by e-mail, stored in an enterprise database, processed by an application, and accessed by a field employee on a mobile device. Data encryption and control solutions cover data center protection for databases, applications, and mainframes, as well as endpoint protection for files and full disk encryption.

In addition, SafeNet Hardware Security Modules (HSMs) provide reliable protection for applications, transactions, and information assets for enterprise and government organizations to ensure regulatory compliance, reduce the risk of legal liability, and improve profitability. SafeNet HSMs are the most secure and highest performance solution for the protection of cryptographic keys, the provision of encryption, decryption, authentication and digital signing services, as well as the protection of payment transactions and PIN generation.

About SafeNet

SafeNet is a global leader in information security, founded more than 25 years ago. The Company protects identities, transactions, communications, data, and software licensing through a full spectrum of encryption technologies, including hardware, software, and chips. More than 25,000 corporate and government customers in 100 countries trust their security needs to SafeNet. In 2007, SafeNet was acquired by Vector Capital, a $2 billion private equity firm specializing in the technology sector. For more information, visit www.safenet-inc.com.

Contact Us

Corporate Headquarters:
4690 Millennium Drive
Belcamp, Maryland 21017 USA
Tel: +1 410 931 7500 or 800 533 3958
Email: info@safenet-inc.com

EMEA Headquarters:
Tel: +44 (0) 1276 608 000
Email: info.emea@safenet-inc.com

APAC Headquarters:
Tel: +852 3157 7111
Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit **www.safenet-inc.com**

Follow Us:
www.safenet-inc.com/connected

WP-Charting Your Path to Enterprise Key Management(EN)-08.10.10