BEST PRACTICES
Enterprise Encryption Key and Digital Certificate Management
VENAFI IS THE INVENTOR OF AND MARKET LEADER IN ENTERPRISE KEY AND CERTIFICATE MANAGEMENT (EKCM) SOLUTIONS. VENAFI DELIVERED THE FIRST ENTERPRISE-CLASS SOLUTION TO AUTOMATE THE PROVISIONING, DISCOVERY, MONITORING AND MANAGEMENT of encryption keys and digital certificates, built specifically for encryption management interoperability across heterogeneous environments.

This document provides an introduction to EKCM best practices that Venafi has developed while working for nearly a decade with Global 2000 organizations. The best practices in this document apply directly to the management of certificates and their associated private keys.

For a much more in-depth version of these best practices, visit www.venafi.com/best-practices.
Before starting to implement best practices, it helps to understand why a best practices approach is important. Certificates and private keys play a critical role in securing data and systems across all types of organizations. The following table shows some of the challenges that can arise when they’re not properly managed.

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downtime and System Outages</td>
<td>Certificates that are not renewed and replaced before they expire can cause serious downtime and outages.</td>
</tr>
<tr>
<td>Private Key Compromise</td>
<td>Private keys used with certificates must be kept secure or unauthorized individuals can access confidential information.</td>
</tr>
<tr>
<td>Compliance Violations</td>
<td>Compliance assessors are increasingly scrutinizing management practices for encryption keys.</td>
</tr>
<tr>
<td>High Administrative Costs</td>
<td>The average certificate and private key require four hours per year to manage, costing hundreds of thousands of dollars per year for many organizations.</td>
</tr>
</tbody>
</table>
It is critical to understand why encryption is being used within your organization as well as the risks of that security being compromised. The risks presented by poor management of encryption may seem obvious, but time spent capturing the specifics will be helpful when working with cross-functional teams.

Gather information on the costs of the current process, including the costs associated with outages. Use this information to build the business case for implementing these best practices.

Getting support from executives in your organization for implementing EKCM best practices is critical due to the cross-functional nature of key and certificate management in most organizations. Also, be sure to also identify all the individuals and teams that play a role in the process, as their cooperation will be necessary.
There are many areas to define polices for EKCM. This section highlights some of these and makes specific recommendations of many critical enterprise systems.

ESTABLISHING ENTERPRISE KEY AND CERTIFICATE BEST PRACTICES

3

CERTIFICATE AUTHORITIES AND TEMPLATES

Select the specific certificate authorities (CAs) and certificate templates that are approved for particular use cases such as externally- and internally-facing systems. Use publicly trusted CAs for external facing systems and private CAs for internal and test/development systems.

ADMINISTRATOR ACCESS TO PRIVATE KEYS

Direct administrative access to private keys should be eliminated wherever possible. If access is required, that access should be closely monitored to prevent the possibility of a copy of the private key being made. All private key access should be logged. Every time a system’s administrator is changed, the private key and corresponding certificate should be changed.
The validity period is the time window a certificate is valid and consequently the period during which you must ensure the secrecy of the certificate’s private key. Resist the urge to use longer certificate validity periods – they create a false sense of operational benefit while greatly increasing the risk of data exposure. Wherever possible, use one year validity periods.

Many keystores rely on a password to protect private keys. Establish policies for minimum keystore password length and complexity. Wherever possible, use passwords of at least 12 characters with a combination of lower and uppercase characters with at least one number and one non-alphanumeric symbol. Keystore passwords should be changed each time a certificate and private key are replaced/renewed.

Define a minimum number of days prior to expiration that the certificate renewal must begin. Use 30 days as a benchmark and adjust accordingly for your organization. You’ll start sending notifications prior to this window, but this defines when the process will start.

The current minimum recommended key length by the U.S. National Institute of Standards and Technology (NIST) is 2048-bits. Assure that all smaller certificates and keys are proactively replaced immediately. Determine whether there are any applications or devices that do not support 2048-bit keys.
PRIVATE KEY DISTRIBUTION

Every time private keys are accessed in order to transfer them from one location to another, it dramatically increases the risk of a key compromise. Private keys must be securely wrapped during transport. Use a password encrypted file (e.g. PKCS#12 or PEM) or a wrapping key from the target device. Ideally, use a system that eliminates administrative handling of private keys during distribution. If this isn’t possible, require that two individuals each type in half of the wrapping password. This reduces the possibility that a single person could gain access to the private key.

DUAL CONTROL

The establishment and enforcement of clear dual control policies is critical in the context of certificate and private key management in order to prevent a single individual from performing unauthorized actions. The specific operations that require dual control should be driven by an analysis of specific security risks and threats as well as governance oversight requirements (such as Sarbanes-Oxley).

AUDIT LOGGING

Audit logging is important for your certificates and, especially, private keys. However, collecting all of the events related to managing certificates and private keys into a single log is challenging due to the technologies traditionally used to manage keys and certificates. Nonetheless, you need to develop a strategy for collecting and securing log information for all certificate and key management operations, especially for any access to private keys.
The critical starting point in any certificate and private key management strategy is to create a comprehensive inventory of all certificates, their locations and responsible parties. This is not a trivial matter because certificates are deployed in a variety of locations by different individuals and teams – it’s simply not possible to rely on a list from a certificate authority. Take a multi-pronged approach to ensure that no certificates are missed.
The first step is to gather what you already know about the certificates from existing certificate authorities. It is very dangerous to assume that an import from your known CAs will provide an accurate inventory of all certificates; it’s merely a starting point that must be augmented by discovery.

Next, perform a network discovery to find certificates that are present on a listening port such as HTTPS. Start by gathering your network address ranges and then collect a list of ports to check. You can initially check on port 443, but there are many ports on which certificates are commonly presented.

Many certificates are not discoverable via network ports, such as client-side certificates used for mutual authentication on SSL. Finding these certificates typically involves performing file system scans on server and client systems with a locally-installed agent.

Network and agent-based discoveries can take time and it may not be possible to perform them in all corporate locations. That makes it critical to educate administrators and make sure they are proactively reporting any certificates they are aware of and adding them to the inventory.

Be aware that performing an inventory is not a one-time event. You should repeat the steps above weekly to keep the inventory up to date.
As you develop your inventory, analyze the data you’ve collected. Here are some of the things to look for:

- **ANALYZE YOUR INVENTORY**
- **EXPIRATION DATES**: Immediately begin evaluating and tracking expiration dates to assure that any certificates brought into the inventory that expire in less than 30 days are flagged for renewal.
- **CAs IN USE**: Determine which CA issued each certificate so that you can identify CAs that are not approved or certificates that are self signed.
- **KEY LENGTHS**: Note certificates with noncompliant key lengths and replace immediately.
- **VALIDITY PERIODS**: Flag all validity periods longer than 1 year and remediate.
RESPONSIBLE GROUPS
Analyze and collate certificates according to responsible teams.

MANAGEMENT PROCESSES
Review and document current key and certificate management processes for each group where they’re in use.

As you analyze your inventory, determine whether any of the policies you’ve defined should be adjusted in order to address the specific needs of your organization.
Once you’ve identified the compliance gaps between your policies and your current environment and processes, educate your organization on operational best practices. Wherever possible, leverage management tools to reduce operational risks and improve security while reducing operational overhead.

As you’re developing your inventory, start establishing a correlation of who the contacts and owners are for certificates. Wherever possible assign groups as the contacts instead of individuals to avoid a single point of failure. Some helpful sources include certificate authorities, tracking spreadsheets, and even a CMDB. Define clear responsibilities for maintenance of certificate contact information.
An important method for preventing in-service expirations is to establish a central monitoring function that ensures certificates are replaced prior to expiration by automatically notifying responsible groups. Only when the new certificate has been installed and the application has been reset to use the new certificate prior to the time of expiration is the risk of downtime averted.

Expiration reports should be sent to certificate owners each month that show a list of all certificates expiring in the next 90 days. Individual expiration notifications should be sent if action has not been taken on an individual certificate within 30 days of expiration. If action has not been taken within 20 days prior to expiration, escalation to additional parties should be added. At 10 days from expiration, notifications should be sent to a NOC or other corporate group that is responsible to respond to the crisis until it is resolved.
Establish standard practices for enrollment and provisioning that maximize reliability and repeatability, ensure security and compliance to policy, and minimize load on your administrators. There are easily 20 or more steps involved in issuing or renewing a certificate. These steps must be standardized and implemented in compliance with policy every time. Errors are inevitable when these steps are performed manually. In addition, confidently ensuring the security of the private key is very challenging when these operations are performed manually.

Prudent organizations will evaluate automated methods of certificate enrollment and provisioning.

For more detailed steps and recommendations for each of these areas of best practice, visit www.venafi.com/best-practices.