thalestct.com

THALES

Best Practices for Cryptographic Key Management

White Paper

The New Data Security Landscape

The proliferation of cloud applications, mobile devices and virtualization have created many shared environments and an unlimited number of endpoints, leaving data incredibly vulnerable. Escalating threats, compounded by expanding regulatory requirements, is altering the data security landscape. The best way to secure sensitive information is by placing safeguards around the data itself through encryption. As the use of encryption becomes more wide-spread and diverse, many organizations are recognizing the need to adopt a strategy that centralizes these accumulated 'encryption islands' and allows them to migrate to the cloud. It's reasonable to assume that new types of threats will emerge, leading to new types of encryption within new places. This is why organizations need to take the time to investigate any vulnerabilities within their environment and implement a 360-degree data protection plan that covers all security risk areas now and in the future.

Encryption
Whether you are reassessing your current security infrastructure (or putting one in place for the first time) encryption should be approached in the same way an organization establishes a security policy.

- Detect your threats and locate all sensitive information. First, conduct a risk assessment of the organization in order to understand what types of data are present, where the data is stored, and the flows or patterns of the data.
- Determine the level of encryption required: data in use (e.g. databases containing customer information), data at rest (financial information in file servers and back up in storage networks) and data in transit as it crosses the network to/from your public/private cloud-computing environment. You must consider all of the various threats that apply to data at different points within the lifecycle and then select the best encryption solution based on requirements and that given set of data.

What About the Cryptographic Keys?
Aside from implementing a strong method of encryption, it's crucial that your encryption keys are treated with the same level of care. Once data is encrypted, the only way to gain access is by decrypting or unlocking secret content using the key. Haphazardly protecting these keys negates the entire process of encryption and creates a false sense of security. Therefore, the security deployment should utilize best practices for both encryption and key management.

Deploying a Cryptographic Key Management Strategy
An effective cryptographic key management strategy should take a centralized approach to secure various types of data in different environments, combined with the management and maintenance of keys and crypto resources being utilized. In order to provide the consolidation, protection and flexibility that today's environment demands, a data protection strategy should incorporate the following five key areas:

High Assurance Cryptographic Key Protection
Secure cryptographic keys by storing them in a hardware security module or hardened virtual appliance.

Cryptographic Processing and Acceleration
Offload and accelerate crypto operations to improve performance.

Key Lifecycle Management
Manage cryptographic keys throughout their lifecycle.

Cryptographic Resource Management
Define access levels, manage and deploy cryptographic resources, and report on all activity.

Once these areas are factored into the strategy, organizations no longer have to rely on the bare minimum procedures established by their application vendors. They are free to build, maintain, and manage each area according to their specific use cases.

High Assurance Cryptographic Key Protection

The proliferation of encryption has created a situation where keys are stored in inconsistent states of security. Protection of cryptographic keys throughout their operational life is essential to the security of all encryption systems. Systems may use different types of keys, including symmetric and asymmetric keys. Some rely on a root key and a certificate, creating a trust link where keys involved are symmetrical, or identical, for both encrypting and decrypting a message. A more hybrid solution may rely on distinct, asymmetric key pairs using a working session key. Session keys live momentarily and are the last thing to encrypt, but the root key is the constant in the system and has to be the most secure.

The requirements of your use case(s) and environment will determine the keys' roles and ultimately how they are stored. Depending on the value of data being protected, and the variety of keys needing to be stored, organizations have the option of storing their keys within hardware or software. For keys that are trusted to protect highly sensitive data and applications, a centralized, hardware-based approach to key storage is recommended.

Centralized key storage (keys stored in hardware)
The highest assurance model when it comes to the security of your data is to store the key(s) within a hardware security module (HSM). An HSM is a specialized computing device that performs cryptographic operations and includes security features to protect keys and objects within a secure hardware boundary, separate from any attached host computer or network device.

With an HSM, nothing ever enters or leaves the tamper-resistant vault so keys are more isolated from traditional network attacks and should the HSM become compromised, the keys will zero out. This approach is required by several compliance mandates: The National Institute of Standards and Technology's Federal Information Processing Standard (FIPS) and The Common Criteria for Information Technology Security Evaluation. These certifications indicate that the appliance has been through stringent third-party testing against publicly documented standards.

Placing a gap between the threat vectors that have access to your data and the threat vectors that have access to the keys is best practice. Use cases (e.g. code signing, certificate validation, transaction processing, and Public Key Infrastructure) involving a limited number of applications, are an ideal fit for the centralized key storage model, which requires limited key distribution, used for one specific reason. Some applications will require a more distributed model, where cryptographic keys must exist in close proximity to the data and applications they secure.

Distributed key storage (keys stored at the endpoints)

Organizations trying to encrypt mass amounts of smaller sections of data, requiring high availability and usage, may gravitate toward this model. For instance, data within customer databases usually requires numerous keys moving across many applications. Keys are called upon to encrypt sensitive data and store it within applications as needed. Vast quantities of keys are required to accommodate seemingly unlimited transactions, and these keys are kept in proximity to the database for efficiency and convenience.

It's important to note that the security of the underlying master keys can impact the trust placed in thousands of distributed keys. Where possible, organizations are encouraged to generate keys using a highly secure master key stored in an HSM. These keys can then be wrapped, using algorithms designed to encapsulate cryptographic key material, and distributed to endpoints as needed. This allows organizations to maintain a high volume of keys and transactions necessary to conduct business while still ensuring all keys are protected to the utmost. Effective use of key management should also be used to alleviate some of the vulnerabilities of keys stored in a distributed fashion.

Crypto Processing and Acceleration

Take stock of the types of information you are currently encrypting or need to incorporate in order to achieve your goals. Ensure that cipher/algorithms are comparable with current industry standards and widely used, as the classification of 'strong' cryptographic algorithms can change over time. You may want to consider elliptic curve cryptography, which allows you to create strong keys that take up very little memory. Next, establish key lengths with the right combination of protection and flexibility. Compliance mandates can help guide best practices to follow.

Look at current workflows and applications. Where will encryption and decryption take place? Depending on where you want encryption to run, and the velocity, you may need to consider incorporating high-speed cryptographic processors. Appropriate offloading and accelerating crypto operations will help to avoid processing bottlenecks and increase system capacity.

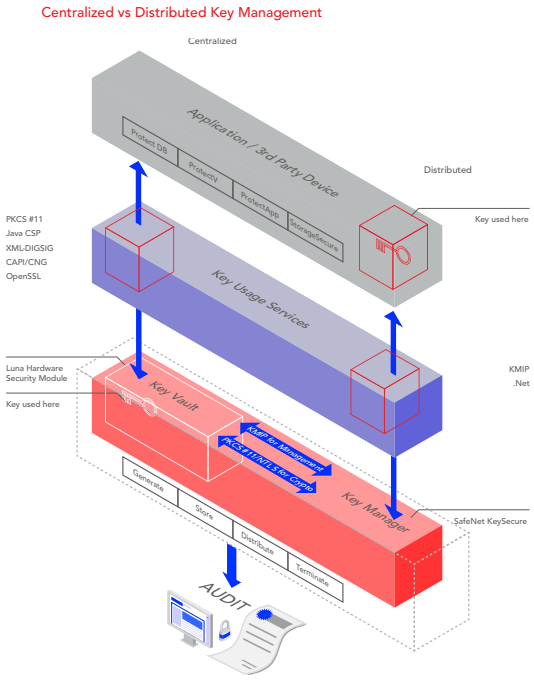
Intelligent load balancing ensures uninterrupted operation and highest availability. Hardware security modules can provide a solution for offloading cryptographic processes from application servers to dedicated hardware.

The key is to find a solution that can be easily implemented and supports industry standard APIs out of the box, which can greatly simplify integration. Having the flexibility in performance, scalability, usability, and security will ensure your cryptographic key management infrastructure is able to support both mission and security goals.

Key Lifecycle Management

Successful key management can be challenging because it involves an integrated approach around generating, storing, distributing, rotating, revoking, suspending, and terminating keys for devices and applications. More than likely, various encryption solutions have been deployed and accounting for all of those affiliated keys and disjointed systems becomes unsustainable. The stakes are high and mismanagement of keys could lead to exposed data.

Effective key management is particularly needed when keys are stored in the distributed model. An organization warranting high volume, velocity, and variety of keys might consider investing in a system that



specializes exclusively on key management duties. This centralized management platform will perform all key-related tasks and tie back to other systems or HSMs that are performing cryptographic operations using those keys.

Understanding the various key lifecycle states is important to properly plan key management requirements:

Key generation and certification

Since a key is used to encrypt and decrypt vital data, make sure the key strength matches the sensitivity of the data. In general, the length of the key coupled with how randomly unpredictable keys are produced are the main factors to consider in this area. The greater the key length, the stronger the encryption. The strength of the key is essential to the mitigation of the threat of brute force attacks.

Enterprise-wide encryption policies should also be established. Security administrators should define a standard set of criteria and mandate a standard set of tools to meet the requirements wherever encryption is required.

Key distribution

Before being distributed, a key must be associated with a particular user, system, application, or policy. The association will determine the requirements to secure the key, and ultimately the method used to secure it while in transit. The type of cryptography used will determine the appropriate method of key distribution. In symmetric key cryptography, secret keys must be securely exchanged between parties. Wrapping these keys prior to distribution can provide security as they travel through otherwise insecure networks. In public key cryptography, private keys must be stored securely, while public keys may be widely distributed without fear of data loss.

Lastly, the ability to differentiate access between the administrator creating the key and the person using it is vital. By having this separation of duties, business owners can be confident that they have minimized the risk of unauthorized users getting access to confidential information.

Key storage

For keys that are trusted to protect highly sensitive data and applications, a centralized, hardware-based approach to key storage is recommended. Some applications will require a more distributed model where cryptographic keys must exist in close proximity to the data and applications they secure.

Key rotation
Depending on the algorithm and organizational need, each key should be designated a crypto period with the ability to change that key on demand. It's important to limit the amount of data encrypted with a single key because using the same key over a long duration of time increases the chances that the key will be compromised. Furthermore, it can be impossible to tell when keys are lost, stolen, or copied, so rotating keys regularly ensures stolen keys are only useful for a specific time period. Once rotated with a new key, the existing data should be rekeyed. Rekeying is the process of decrypting data and re-encrypting it with a new key in order to protect it from any undetected compromise of older keys.

Key back-up and recovery
If the key storage mechanism fails or is compromised, there must be a way to restore the keys. Otherwise, the data is encrypted and lost forever. Backup copies of cryptographic keys should be kept in a storage mechanism that is at least as secure as the original store, so keys can be restored and data decrypted and re-encrypted with a new key. Ideally, using an offline storage container, such as a FIPS validated card, appliance or token is best practice. Be sure to document concrete procedures to handle a key compromise as well.

Key revocation, suspension, termination
Every organization needs the ability to revoke, destroy, or take keys offline. In the event of a compromise, an organization can delete the keys associated with the compromised systems or data and, by doing so, ensure unauthorized users will never get the keys required to decrypt sensitive assets. Depending on the circumstance, there may be the need to take a key out of the lineup but not terminate it. For instance, data subject for litigation will need to be recalled upon and therefore should only be suspended.

Crypto Resource Management
In order to ensure consistent policy enforcement, provide transparency, and maintain the health of your system, every organization should have one, easy-to-use interface to administer, monitor and provision all cryptographic resources.

Deploy resources
Provision and de-provision cryptographic resources for HSMs, automate client provisioning based on partitioning capabilities and create multi-tenant, tiered security administrator access levels. Organizations have multiple stakeholders, which take part in the key management lifecycle. Control of the cryptographic keys should be established so that System Administrators and Security Officers can perform their duties without compromising the Application Owner duties of access and control over the keys.

Configure policy
Determine how many keys can be generated, and where they are stored. Continue to update variables in the system, such as back-up networks and users. Establish a policy for key usage, defining application, device access levels, and to what extent they can each perform. For instance, only users who are highly trusted and trained to perform key custodian duties should be able to recover the key in case of a loss.

Monitor and report
Secure, automated, and unified logging and reporting are absolutely crucial to maintain requisite risk and compliance posture. Key ownership must also be clearly defined, and all modifications recorded and securely stored in order to provide an authentic and trusted audit trail of key state changes.

- Proper monitoring indicates how keys are being used, as well as identifies failures in the cryptographic devices and unmanaged endpoints.
- Reporting capabilities securely track and store audit trails to be signed for non-repudiation. Automated reports and email alerts may be set-up based on a number of cryptographic management criteria.

By leveraging a cohesive, centrally managed platform, IT and security teams can become much more nimble in adapting to changing requirements and challenges. New encryption services can be rolled out quickly and effectively, and data is free to move throughout the enterprise to support mission objectives, without compromising security.

Conclusion
Roots of trust, as defined by the Cryptographic Technology Group at the U.S. National Institute of Standards and Technology (NIST), are components that are inherently trusted to perform one or more security-critical functions. Three examples are: protecting cryptographic keys, performing device authentication, and verifying software.

These components must be secure by design and, according to NIST, are ideally implemented in or protected by tamper-resistant hardware.

In the public cloud, there is a very real challenge to implementing hardware-based roots of trust when the cloud is so dependent on the virtualization and functionality that is often completely defined by software.

About Thales Trusted Cyber Technologies
Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com

©2019 SafeNet Assured Technologies, LLC. 11.21.19