Quintessence Labs

WHITE PAPER

Key Management Best Practices

Data encryption is a fundamental strategy to address security threats and satisfy regulatory mandates. By itself, implementing encryption isn't difficult, but managing encryption keys and other cryptographic objects is where the challenges lie.

> This paper describes important concepts for cryptographic key management and how they are met by QuintessenceLabs' key and policy management solutions, drawing from recognized sources including NIST SP 800-57 Part 1, a key management recommendations document from the U.S. National Institute of Standards and Technology.

Introduction

Despite the difficulties in implementing encryption key management, there exist recommendations and best practices from throughout the cybersecurity space. We've outlined the most important ones below.

Implement Separation of Duties

What Is It? Separation of duties is a widely-known control used to prevent fraud and other mishandling of information. Separation of duties means that different people control different procedures, making sure no one person controls multiple, much less all, procedures. In terms of key management, the person managing the encryption keys shouldn't be the same as the person who can access the encrypted data.

QuintessenceLabs' Approach: qCrypt provides separation of duties for administrators and clients, the two types of users.

Administrators are responsible for managing the key management platform, and their duties include creating other admin users; defining key management policies; configuring network interfaces; configuring the system clock; managing system credentials, configuring keystore replication; managing key lifecycles; creating clients and groups; backup and recovery, and log file management. Admin roles are defined by permissions, and qCrypt has several preset permission sets. It's recommended that roles be defined for each set of duties appropriate for an administrative user, consistent with operation needs and system security.

Client users represent the endpoint that uses keys and invokes key management operations. Clients may use symmetric keys, public/private key pairs, certificates, random and secret data objects, and other managed object types. Clients may also request key operations such as creating, registering, getting values, assigning/modifying attributes, revoking, destroying, and wrapping or unwrapping.

An authorized administrator can define the usage and object policies for clients. These policies are enforced by qCrypt to ensure that only authorized clients can perform specified operations on specified objects. Admins can also define quorum (or "m-of-n") rules. Policies should ideally be defined for clients and client groups to control the operations and objects consistent with operational needs, and system security.

Require Dual Control in Specific Processes

What Is It? Dual control means that at least two people control a single process. For key management specifically, at least two people should be needed to authenticate the access of an encryption key so that no one person can access it alone.

QuintessenceLabs' Approach: Dual control is implemented in qCrypt for managing keystore master keys. Importing or exporting the master keys requires two administrators to authorize the operations. Failure of two administrators to authorize causes the operation to fail. Client operations can also employ dual control, managed by usage policies.

Use Split Knowledge to Limit Exposure of Parameters

What Is It? Split knowledge prevents any one person from knowing the complete value of an encryption key or passcode. Two or more people should know parts of the value, and all persons should be present to create or re-create the key/passcode.

An alternate approach is to use multiple-wrapped keys, allowing such keys to be managed by different systems with different levels of access control. Notably, this approach scales much better than using split keys. Multiple-wrapped data encryption keys can be stored outside the key management system, with only the wrapping keys needing to be managed within the system. With hierarchical key wrapping, this can support an almost unlimited number of encryption keys.

Split keys should be used when m-of-n access is required, and wrapped keys should be considered when there are large numbers of data encryption keys.

QuintessenceLabs' Approach: qCrypt supports both split keys and key wraps.

Support Multiple Encryption Standards

What Is It? Even when an organization chooses an encryption standard, various events can upend their plans – mergers, acquisitions, or business partners that require support of other standards. Choosing security solutions that support all industry-standard encryption algorithms will ensure the organization will conform to government and other regulatory requirements now and in the future.

QuintessenceLabs' Approach: qCrypt supports many encryption algorithms. It includes templates and object policies that provide easy-to-use ways to manage algorithm standardization and migration throughout an organization. Wherever it's important to have centralized control of algorithm usage and managing algorithm migration throughout an organization, it's recommended to use templates and object policies.

Centralize User Profiles for Authentication and Key Access

What Is It? A "user" is defined as any person or application requiring access to sensitive data. Access to such resources should be based on user profiles within the key manager. From there, users can be assigned and issued credentials – for example, RSA certificates – to provide access to the encryption resources associated with their user profile. The profiles are managed through an administrative role, again in the key manager. In compliance with the PCI DSS mandate and as a best practice, no single administrator or user has access to the actual keys themselves.

QuintessenceLabs' Approach: As described in the above section on separation of duties, admin users can be defined and assigned roles restricting operations and visibility. In qCrypt, the administrative user is never permitted access to the actual value of any managed key. Clients can authenticate in qCrypt using mutually authenticated TLS. The client credentials can be created within and downloaded from qCrypt, or potentially imported into the system if an organization has a PKI infrastructure or service already in place.

Keep Comprehensive Logs and Audit Trails

What Is It? It's important to have extensive audit logging that occurs in every component of the distributed architecture of key management. Every access to sensitive data must be logged with details about the function, the user (individual or application), the encryption resources used, the data access, and when the access occurred.

QuintessenceLabs' Approach: qCrypt records all administrator and client access attempts and their operations. In addition, each subsystem of the product records activities in the log file. Logs can be configured to be pushed to external log management systems or SIEM tools. Log records include time and date of activities, process involved, user information, and the nature of the activity (e.g., login, key creation, importing credentials, etc.).

Use One Solution to Support Fields/Files/Databases

What Is It? One benefit of a distributed execution model is that security software doesn't know or care what kind of data it encrypts. Define which fields need to be protected and specify how they'll be protected. Once activated, information is available based on user rights, allowing or denying access to a key's full value or a predefined masked value.

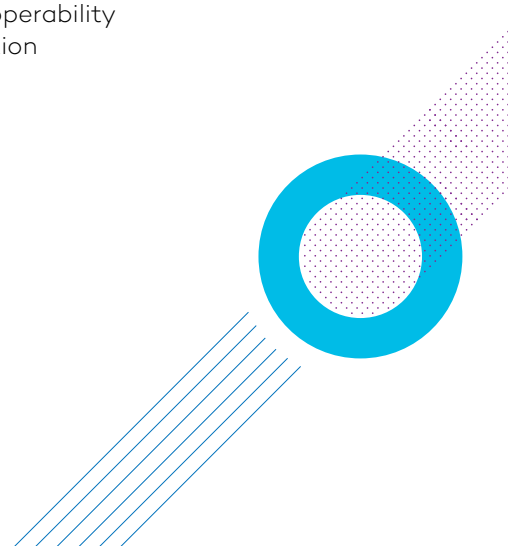
QuintessenceLabs Approach: This top-down approach is supported in qCrypt using object and usage policies, as well as the ability to assign and manage attributes of keys specific to the end-use device or application. Centralizing the management of policies, objects, attributes and lifecycles of key material ensures that consistent rules are applied and communicated. Managed crypto objects can be assigned both global or individual attributes, allowing all objects to be consistent at a common level, yet carry application-specific information when required.

It's recommended to employ usage and object policies together with templates and client group definitions. This will allow maximum flexibility, as well as maintain consistency across all encrypting endpoints in an organization.

Look for Solutions Supporting Third-Party Integration

What's Needed? Encryption solutions are often separate from the applications needed to use them. Suppose you want to use one solution with multiple types of applications – you may need to use APIs to integrate the encryption with your applications, so it's important to seek solutions facilitating the integration.

QuintessenceLabs' Approach: qCrypt implements the OASIS Key Management Interoperability Protocol (KMIP) and is regularly tested for interoperability with other vendors' encryption products.



Other Important Capabilities

qCrypt from QuintessenceLabs delivers many more key management capabilities to strengthen security, including:

- FIPS 140-2 Level 3 compliance: Delivers the optimum security for the clear majority of uses. Includes measures to prevent any tampering with the device's cryptographic module, and rendering it inoperable if breached
- Multi master replication: A method of replication for optimum redundancy and security, which allows data to be stored by a group of devices and updated by any member of the group. All members are responsive to client data queries
- Entropy source: High-speed true random entropy from a physical quantum source that delivers at 1Gbit/sec
- Virtual machine capability: qCrypt is offered as a virtual machine, either standalone or in complement to the hardware version for increased redundancy and maximum flexibility

For more information on the full feature set of QuintessenceLabs' qCrypt product suite, visit **quintessencelabs.com** or contact **info@quintessencelabs.com.**

Quintessence Labs

AUSTRALIA
Unit 1, Lower Ground
15 Denison St
Deakin, ACT 2600
+61 2 6260 4922

UNITED STATES
175 Bernal Road
Suite 220
San Jose CA 95119
+1 650 870 9920

www.quintessencelabs.com

Document ID: 2030