Data encryption is a fundamental component of strategies to address security threats and satisfy regulatory mandates. While encryption is not in itself difficult to implement, managing the keys and other cryptographic objects is a really challenging problem.

This paper describes important concepts for cryptographic key management and how they are met by QuintessenceLabs key and policy management solutions.
Overview

Data encryption is a critical part of any strategy to respond to both security threats and regulatory mandates. However, while encryption is not in itself difficult to implement, managing the keys and other cryptographic objects is a really challenging problem.

This white paper describes best practices for cryptographic key management, drawing on recognized sources such as NIST SP 800-57 Part 1, NIST’s key management recommendations document. It also provides information on how these best practices are supported in QuintessenceLabs’ qCrypt key management products, and on additional features and capabilities of these products to enhance ease of implementation and security.

Performance:

- Implement separation of duties
- Require dual control for specific processes
- Use split knowledge to limit exposure of any parameter
- Support multiple encryption standards
- Centralize user profiles for authentication and access to keys
- Keep comprehensive logs and audit trails
- Use one solution to support fields, files, and databases
- Look for a solution that supports third-party integration
- Other important features

Implement Separation of Duties

What it is: This is a widely known control, set in place to prevent fraud and other mishandling of information. Separation of duties means that different people control different procedures so that no one person controls multiple, or all procedures. When it comes to encryption key management, the person who manages encryption keys should not be the same person who has access to the encrypted data.

QuintessenceLabs’ approach: qCrypt provides separation of duties for the two types of users of the product: administrators and clients.

Administrators are responsible for managing the key management platform. Duties of administrative users include: creating other administrative users; defining key management policies; configuring network interfaces; configuring system time and time zone; managing system credentials; configuring key store replication; managing key lifecycle; creating clients and groups; backup and recovery; and managing log files.
Administrative roles are defined by permissions. Several preset permission sets are available. It is possible to create roles made up of these preset permission sets and/or one or more individual permissions. It is recommended that roles be defined for each set of duties appropriate to an administrative user – consistent with operational needs and system security.

The second type of user – client – represents the end point that uses keys and invokes key management operations. A client may use symmetric keys, public/private key pairs, certificates, random objects, secret data objects, or other managed object types. Additionally, a client may request operations such as create a key, register a key, get a key value, assign attributes to a key, modify a key’s attributes, revoke a key, destroy a key, wrap or unwrap key, etc.

Usage and object policies for clients can be defined by an authorized administrator. These policies are enforced by qCrypt to ensure that only authorized clients are able to perform the specified operations on the specified objects. Quorum (also known as “m-of-n”) rules can also be defined. It is recommended that policies be defined for clients and client groups to control the operations and objects consistent with operational needs, and system security.

**Dual Control**

**What it is:** Dual control means that at least two or more people control a single process. In encryption key management, this means at least two people should be needed to authenticate the access of an encryption key, so that no one single person has access to an encryption key.

**QuintessenceLabs’ approach:** Dual control is implemented in qCrypt for managing key store master keys. Export and import of key store master keys requires that two administrators authorize the operations. Failure of two administrators to authorize an import or export operation causes the operation to fail.

Dual (two or more) control of client operations is managed by usage policies. This was discussed above in the section on separation of duties.

**Split Knowledge**

**What it is:** 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 must be present to create or re-create the encryption key or passcode.

An alternative approach to split keys is to use multiply wrapped keys. This approach allows the wrapping keys to be managed by different key management systems, with different levels of access control.
Additionally, this approach scales far better than split keys. Multiply wrapped data encryption keys can be stored outside the key management system, with only the wrapping keys needing to be managed on the key management systems. With hierarchical key wrapping, this can support an almost unlimited number of data encryption keys.

As a general rule, 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 wrapping.

### Support Multiple Encryption Standards

**What it is:** Even if you choose specific encryption standards for your organization, you may find that mergers and acquisitions or the need to work with business partners in your ecosystem will require support of other standards. Choosing a security solution that supports all industry-standard encryption algorithms ensures your organization will conform to government and regulatory requirements now and in the future.

**QuintessenceLabs’ approach:** qCrypt supports a large number of encryption key algorithms. It includes templates and object policies that provide easy to use ways for managing algorithm standardization and migration throughout an organization.

Where centralized control of algorithm usage, and organization wide management of algorithm migration are important, it is recommended that templates and object policies be used.

### Centralize User Profiles for Authentication and Access to Keys

**What it is:** A “user” is any application or person requiring access to sensitive data. Access to these resources should be based on user profiles in the key manager. Users can be assigned and issued credentials (for example, RSA certificates) to provide access to encryption resources associated with their user profile. User profiles are managed through an administrative role 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 above in the section on separation of duties, roles restricting operations and visibility can be defined and assigned to administrative users. In qCrypt, an administrative user is never permitted to access the actual value of any managed key.

Clients authenticate with qCrypt using mutually authenticated TLS. Client credentials can be created on and downloaded from qCrypt, or they may be imported into the system if an organization has a PKI infrastructure or service already in place.
Keep Comprehensive Logs and Audit Trails

What it is: Extensive audit logging that occurs in every component of the distributed architecture is an important component of key management. Every access to sensitive data must be logged with details about the function, the user (individual or application), the encryption resources utilized, the data accessed, and when the access took place.

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

Use One Solution to Support Fields, Files, and Databases

What it is: One benefit of the distributed execution model is that the security software doesn’t know or care what kind of data it is encrypting. To get started, define which fields need to be protected and specify how they are to be protected. Once activated, information is available based on user rights, allowing access (to the full value or a predefined masked value) or denying access.

QuintessenceLabs’ approach: qCrypt supports this top-down approach through the use of object and usage policies, as well as the ability to assign and manage attributes on keys that are specific to the end use device or application. This centralization of policy, object, attribute and lifecycle management for cryptographic key material ensures that consistent rules are applied, and communicated. Managed cryptographic objects can be assigned both global attributes, as well as individual attributes, allowing all objects to be consistent at a common level, but also carry application-specific information when required.

It is recommended that usage, and object policies, together with templates and client group definitions be employed to allow maximum flexibility as well as maintain consistency across all encrypting endpoints in an organization.

Look for a Solution that Supports Third-Party Integration

What is needed: Encryption solutions are often separate from the applications you need to use them with. Perhaps you want to use one solution with multiple types of applications. You may need to use APIs to integrate the encryption solution with your applications, so look for a solution that facilitates the integration.

QuintessenceLabs approach: qCrypt implements the OASIS Key Management Interoperability Protocol (KMIP) and is regularly interoperability tested with other vendors’ encryption products.
Other Important Capabilities

QuintessenceLabs qCrypt delivers many other key management capabilities to strengthen security. These include:

- **FIPS 140-2 Level 3 available**: certified security delivering the optimum security for the vast majority of uses. Includes measures to prevent any tampering with the device’s cryptographic module, and rendering it inoperable if it’s breached.
- **Multi master replication**: 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 delivering 1Gbit/sec at 100% entropy.
- **Virtual Machine capability**: qCrypt can be supplied with a virtual machine version as a stand-alone 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 our website at www.quintessencelabs.com or contact sales@quintessencelabs.com