

qClient™

qClient SDK | KDP

Key Management-Focused Software Development Kit

Enables the implementation of strong key and policy management

Works with third-party products and platforms throughout your organization

Straightforward API integrates with existing security systems

Overview

qClient is a highly capable and vendor neutral client software development kit, which provides an ideal solution for developers wanting to integrate powerful cryptographic key and random number management.

Integrating Key Management

qClient enables developers to integrate QuintessenceLabs' key and policy manager and true random number generator to deliver the strongest foundation for the most demanding encryption needs. It comes with all the components required for fast and efficient integration including libraries, header files and sample source code.

The OASIS Key Management Interoperability Protocol (KMIP) is a communication protocol to allow the manipulation of keys on a key management server. It facilitates the deployment of secure encryption across an organization by allowing cryptographic key management and random number management to be quickly and easily integrated into any application.

qClient supports a general purpose key management API for full KMIP functionality. Developers don't need to be KMIP experts to take advantage of qClient – the main API has a concise number of functions for acquiring, creating, checking and otherwise maintaining managed keys, certificates and related data.

qClient Deployment

qClient SDK: qClient can be delivered as a standalone interoperable client to allow developers to integrate key and random number management.

qClient is also a component product of the QuintessenceLabs data production platform, included in all qStream or qCrypt deployments.

qClient KMIP Development Platform (KDP): This combines qClient SDK with a not-for-resale license for the qCrypt 200V virtual machine.

qClient Capabilities

Proven compatibility with KMIP servers lets qClient take the guesswork out of interoperability, while a powerful key management API lets developers work without losing functionality. qClient comes with all the components required for fast and efficient integration, including binary libraries, header files, additional APIs for key management and PKCS#11, plus source code samples and detailed documentation.

qClient is designed to be embedded in applications, cross-platform interfaces, and platform-specific implementations. It can operate with secure transport, synchronous and asynchronous operations, and file system and network I/O.



SPECIFICATIONS

qClient™**qClient SDK | qClient KDP**

	qClient SDK	qClient KDP	
Key Features	<ul style="list-style-type: none"> Implements OASIS Key Management Interoperability Protocol (KMIP) Interoperates with third-party servers Facilitates rapid development, relieving developers of the need for deep KMIP knowledge Enables implementation of general-purpose key management 	<ul style="list-style-type: none"> Includes not-for-resale qCrypt 200V virtual machine license* 	
KMIP & PKCS#11	<ul style="list-style-type: none"> Basic and advanced KMIP profiles: Secret Data, Storage Encryption, Symmetric Key, Asymmetric Key PKCS#11 Baseline and Extended Provider profiles 		
Languages	<ul style="list-style-type: none"> qClient is implemented in C API for .NET; Java (<i>Other APIs available on request</i>) 		
Supported Managed Object Types	Certificate Opaque Object Private Key	Public Key Random Object Secret Data	Symmetric Key Template
Supported Managed Object Attributes	Activation Date Always Sensitive Application Archive Date Bit Length Certificate Issuer Certificate Length Certificate Subject Compromise Compromise Date Contact Information Cryptographic Algorithm Cryptographic Domain Parameters Cryptographic Length Cryptographic Parameters Cryptographic Usage Mask Custom Attribute Deactivation Date Destroy Date	Digest Digital Signature Algorithm Entropy Quality Extractable Fresh Hash Initial Date Last Change Date Lease Time Link Name Never Extractable Object Group Object Type Occurrence Date Offset Operation Policy Name Personalization String Process Start Date Process Stop Date	Random Number Generator Revocation Reason Rewind Allowed RNG Retrieve RNG Seed Sensitive Specific Information State Unique Identifier Usage Limits X.509 Certificate Identifier X.509 Certificate Issuer X.509 Certificate Subject
Supported KMIP Operations	Activate Add Attributes Archive Cancel Check Create Create Key Pair Decrypt	Delete Attribute Destroy Encrypt Get Get Attributes Get Attributes List Get Usage Allocation Locate	Modify Attribute Obtain Lease Poll Query Recover Register Re-Key Revoke

* Please see qCrypt 200V data sheet for more information



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: 1989