Quintessence Labs

qClient™

100 | 200

Key Management-Focused Software Development Kit and KMIP Development Platform

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

QuintessenceLabs' 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

The qClient software development kit 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 that allows 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.

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

QCLIENT CAPABILITIES

Proven compatibility with KMIP servers lets the qClient software developer kit take the guesswork out of interoperability, while a powerful key management API lets developers work without losing functionality. The qClient software developer kit 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.

The qClient software developer kit 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.

QCLIENT DEPLOYMENT

qClient 100: The qClient 100 software development kit can be delivered as a standalone interoperable client to allow developers to integrate key and random number management. The qClient 100 software development kit is also a component product of the QuintessenceLabs' data production platform, included in all qStream™ quantum random number generator and Trusted Security Foundation® (TSF®) key and policy manager deployments.

qClient 200: The qClient 200 KMIP development platform combines qClient 100 software development kit with a not-for-resale license for the TSF® 100 key and policy manager virtual machine.

SPECIFICATIONS

qClient™

	qClient 100	qClient 200
Key Features	• Allows for rapid development of key management applications • Supports OASIS KMIP and PKCS#11 protocols • Interoperates with the Trusted Security Foundation (TSF) key and policy manager and compliant third-party key management servers • Facilitates rapid development, relieving developers of the need for deep KMIP or PKCS#11 knowledge	
	N/A	Includes not-for-resale TSF 100 virtual machine license*
KMIP & PKCS#11	• OASIS KMIP: Conformant with standards 1.0/1.1/1.2/1.3/1.4/2.0 • Supports all KMIP profiles and transport protocols: TTLV, TTLV over HTTPS, JSON, XML • PKCS#11 version 2.40, Baseline Provider and Extended Provider profiles, Authentication Tokens	
Languages	• qClient 100 is implemented in C • .NET and Java APIs • Other APIs available upon request	
Supported Platforms	• 32 bit Windows 7, 8+, Server 2008 R2+ • 64 bit Windows 7, 8+, Server 2008 R2+ • 32 bit Linux x86 Kernel 2.6+ • 64 bit Linux x86_64 Kernel 2.6+ • ARMv8 Debian 4.9.130 • 64 bit ESXi 6.5, 6.7	
Supported KMIP Managed Objects	– Certificate – Public Key – Symmetric Key – Opaque Object – Random Object – Template – Private Key – Secret Data	
Supported KMIP Managed Objects	– Objects Establishment – Attribute Management – Discovery – Object and Attribute Retrieval – Object Renewal – Crypto Operations – Object and Operation Accessibility – Asynchronous Operations – Split Key Operations – Object Lifecycle – Server Initiated	
Supported KMIP Profiles	– Baseline – Advanced Symmetric Key Foundry – Opaque Managed Object – Symmetric Key Lifecycle – Asymmetric Key Lifecycle – Storage Array with Self-Encrypting Drives – Basic Symmetric Key Foundry – Basic Cryptographic – Tape Library – Intermediate Symmetric Key Foundry – Advanced Cryptographic – RNG Cryptographic	
Supported KMIP Profiles	– Baseline Provider – Extended Provider – Authentication Token ("KMIP", "Keystore software" provided with support for customers to provide their own token)	

* Refer to the TSF 100 product sheet for more information