CERTIFICATIONS

QUINTESSENCELABS PRODUCT STANDARDS, COMPLIANCE AND CERTIFICATIONS

Quintessence Labs

Trusted Security Foundation® (TSF®) Key & Policy Manager

COMMON CRITERIA CERTIFICATION

The Common Criteria (CC) consists of cybersecurity requirements that address encryption, auditing, security updates, and other related topics. The Network Device Collaborative Protection Profile (NDcPP) is a compilation of CC requirements specifically designed for network devices. Conformance with the NDcPP is verified through independent testing conducted at NIAP-accredited laboratories.

The TSF is currently under evaluation for compliance with NDcPP – see https://www.niap-ccevs.org/products, group *Products in Evaluation*, VID 11518.

FIPS 140 USE CASE

The QuintessenceLabs' TSF 400 key and policy manager generates, imports, and manages cryptographic keys for network-attached clients. Embedded within the TSF is an Entrust nShield XC FIPS 140-3 Level 3 validated Hardware Security Module (HSM). The HSM serves as a root of trust, ensuring the protection of sensitive data and facilitating cryptographic operations.

The HSM is used to provide FIPS 140-approved protection in three areas:

1. Protection of Managed Key Material

Client keys can be either generated on the TSF, utilizing the NIST SP 800-90B entropy source, or imported into the TSF over a secure channel. In both scenarios, the keys are securely wrapped within the HSM using a wrapping key that is generated within the HSM.

2. TLS Handshake

TLS provides secure channels for client-server, server-server, and admin-server communications. Server-side TLS private keys are generated, stored, and used within the HSM. TLS cryptographic handshake operations are performed inside the HSM.

3. Internal Public Key Infrastructure

The TSF includes an embedded Public Key Infrastructure (PKI) service. The local private Certificate Authority (CA) key is generated within the HSM. All operations performed using the private key are performed within the HSM. This includes the creation of PKI credentials on behalf of external users, the creation of PKI credentials for internal use, and certificate signing operations performed within the HSM.

Use of the integrated HSM is conformant with the FIPS 140-3 Security Policy for the HSM.

NIST SPECIAL PUBLICATION 800-57

The Trusted Security Foundation Key & Policy Management application is 100% compliant with NIST Special Publication 800-57, where applicable.

Key Management | CSRC (nist.gov) – NIST Special Publication 800-57 offers guidance on cryptographic key management and is divided into three parts. Part 1 provides general guidance and best practices for managing cryptographic key material. Part 2 offers guidance on policy and security planning requirements for U.S. government agencies. Finally, Part 3 provides guidance for using the cryptographic features of current systems.

COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSFC)

Commercial Solutions for Classified Program (CSfC) – The Commercial Solutions for Classified (CSfC) program is a key component of NSA's commercial cybersecurity strategy aimed at providing secure cybersecurity solutions leveraging commercial technologies and products. Established to enable the use of commercial products in layered solutions, NSA's CSfC Program protects classified National Security Systems (NSS) data.

The TSF 400 has been reviewed by NSA validating conformity with the CSfC KGS Approval Criteria and the Symmetric Key Management (KM) Requirements Annex for the use of Symmetric Pre-Shared Keys to deliver quantum-resistant cryptographic protection for classified information within properly configured, maintained, and monitored CSfC solutions.

KGS solutions meeting the CSfC KGS Approval Criteria and the Symmetric Key Management (KM) Requirements Annex must still obtain approval for use through the CSfC solution registration process.

VMWARE CERTIFICATION

The Trusted Security Foundation Key & Policy Management application is a VMware Certified Key Management Server (KMS).

KMS Compatibility Guide – This document lists Key Management Servers, also referred to as KMS, developed and released by security and cloud vendors for encryption in virtualized environments. The KMS listed have passed VMware's KMS Certification tests, which allows these certified KMS to provide a measure of reliability and stability of the end solution in customer deployments. All the tests contained in the KMS Certification plugin are meant to verify that the vendor's KMIP-compliant KMS works with the vSphere VM Encryption feature.

VMware by Broadcom is also an OEM partner of QuintessenceLabs, licensing the qClient KMIP Client for the vSphere VM Encryption feature.

qStream™ Quantum Random Number Generator (QRNG)

NIST SP 800-90B CERTIFIED

The NIST SP 800 Series provides guidelines and recommendations on deterministic random bit generator (DRBG) mechanisms, entropy sources, and construction principles for RBGs. The series consists of three main parts:

- SP 800-90A – Recommendation for Random Number Generation Using Deterministic Random Bit Generators, details mechanisms for generating random bits using deterministic methods. NIST is in the process of revising SP 800 90A to ensure consistency with SP 800-90C.
- SP 800-90B – Recommendation for the Entropy Sources Used for Random Bit Generation, outlines the design principles and requirements for the entropy sources used by RBGs, as well as the necessary tests for validating these entropy sources.
- SP 800-90C – Recommendation for Random Bit Generator (RBG) Constructions (4th Public Draft), specifies constructions for implementing RBGs.

The qStream 100 QRNG is NIST SP 800-90B certified.
Entropy Certificate #E145 – Cryptographic Module Validation Program | CSRC

Additionally, the qStream 100 complies with NIST SP 800-90A and SP 800-90C, certification only available with NIST 800-90B.

DIEHARDER TEST

qStream QRNG is a validated True Random Number Generator, making use of the Dieharder Tests, which include not only the Dieharder tests but other tests from the NIST statistical test suite and others. https://webhome.phy.duke.edu/~rgb/General/dieharder.php

Dieharder Tests are a battery of statistical tests for measuring the quality of a random number generator. They include Birthday spacings test, Overlapping 5-permutation test, Binary rank matrices test, Bitstream test, OPSO, OQSO & DNA test, Count-the-1's test, Parking lot test, Minimum distance test, 3D spheres test, Squeeze test, Overlapping sums test, Runs test, and Craps test.

FOR MORE INFORMATION VISIT
www.quintessencelabs.com/compliance-and-certifications
or contact info@quintessencelabs.com.

Quintessence Labs

AUSTRALIA
Unit 11, 18 Brindabella Circuit
Brindabella Business Park
Canberra Airport ACT 2609
+61 2 6260 4922

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

www.quintessencelabs.com

Document ID: 6969-01