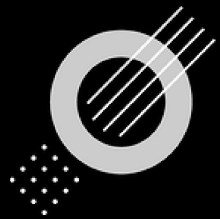


QUINTESSENCE LABS & ENGAGE BLACK PARTNERED TSF SERVER SOLUTION

ENGAGE BLACK

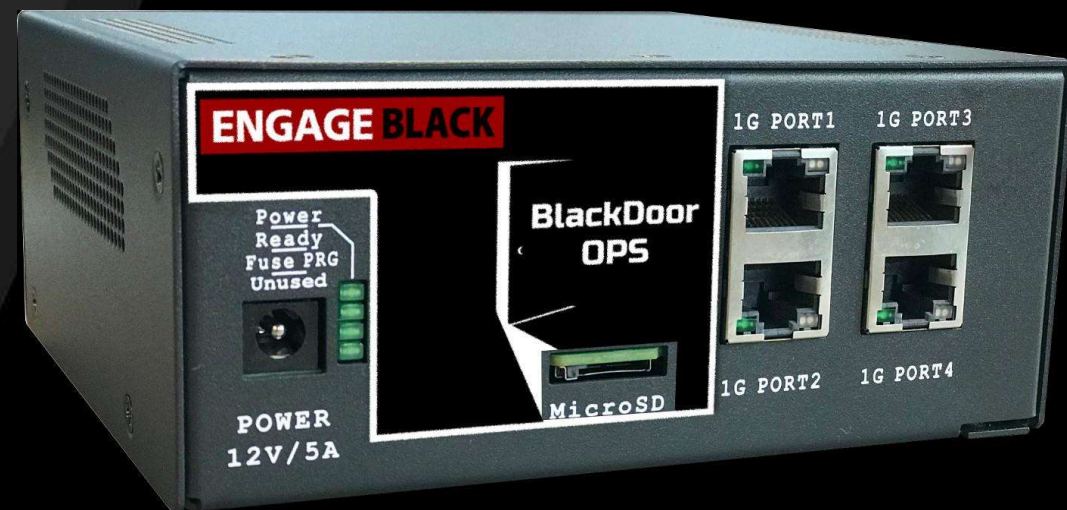


Quintessence
Labs

Strong protection for today, quantum
resilience for tomorrow

The BlackDoor OPS

- Supports ETSI QKD Standard GS QKD 014
- Four 10/100/1000 Base T Encrypt Voice, Video, & Data at Gigabit Speeds
- Encrypt Layer 2 / 3 / MPLS Payloads
- Secure Proprietary Information
- Point-to-Point or Multipoint Architecture
- FIPS approved symmetric encryption algorithm used by U.S. Government organizations to protect sensitive information



Designed for gigabit wireline or wireless backbone configurations.

The BlackDoor DUO

- Supports ETSI QKD Standard GS QKD 014
- Two 10/100/1000 Base T
Encrypt Voice, Video, & Data up to
200 Mbps Speeds
- Encrypt Layer 2 / 3 / MPLS Payloads
- Secure Proprietary Information
- Point-to-Point or Multipoint Architecture
- FIPS approved symmetric encryption
algorithm used by U.S. Government
organizations to protect sensitive
information

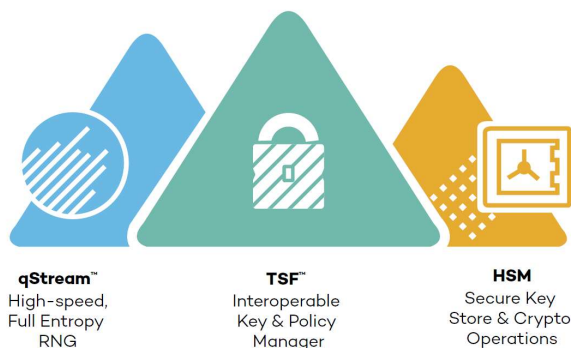


Encrypts Layer 2/3 MPLS Payloads and supports Point to Point and Multipoint information assurance configurations with unique dynamic keys.

PROTECTING DATA TODAY WITH THE TRUSTED SECURITY FOUNDATION®

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

Centralized and vendor-neutral key and policy management solution, designed to easily address the toughest challenges in data protection.




TSF APPLIANCE
(virtual or physical)

Strong protection for today, quantum resilience for tomorrow:

- Replication network protected by long symmetric keys
- Standards-based interfaces and protocols
- Crypto-agile key management to manage new, quantum resilient encryption keys
- VMware KMS Certified
- Integrated HSM (optional)
- Embedded high speed QRNG (optional)



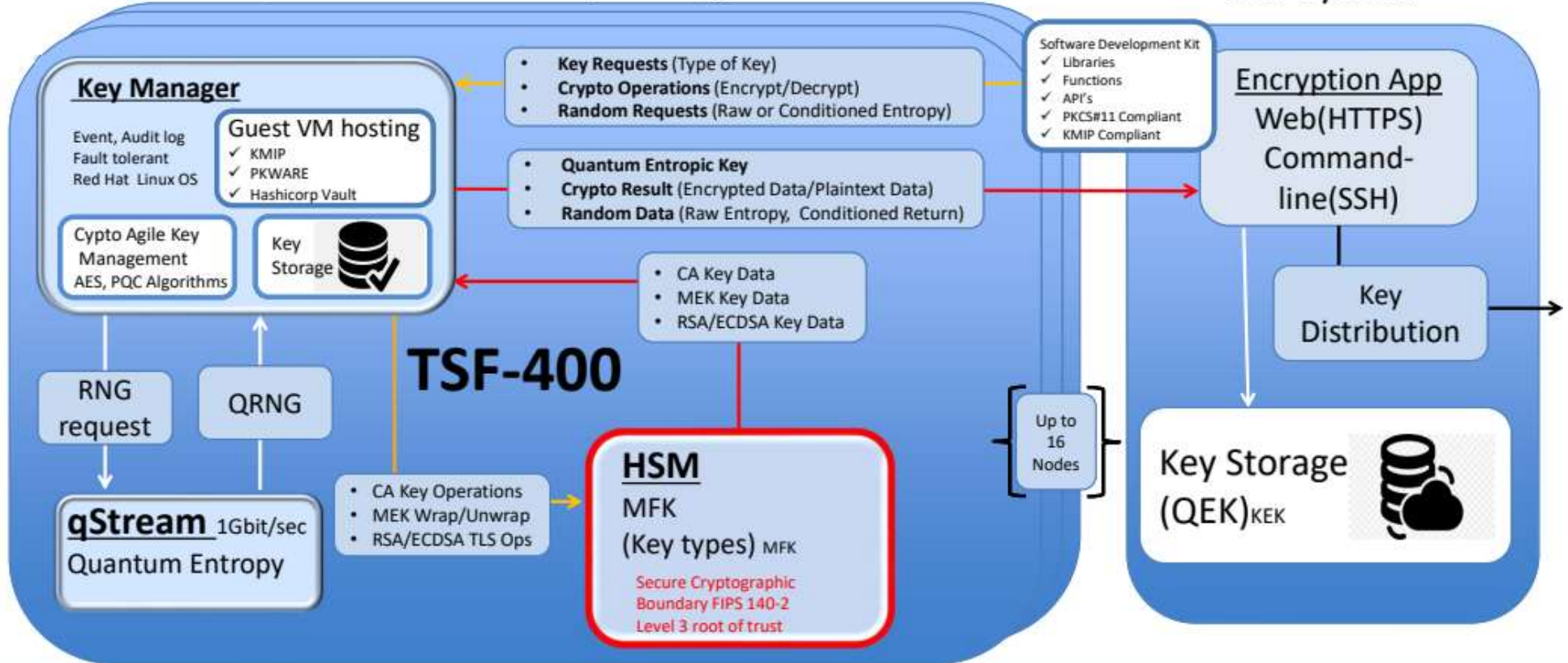
TSF: A SECURE FOUNDATION FOR MANAGING CRYPTOGRAPHIC KEYS, OPERATIONS AND POLICIES

- 
- Cryptographic policy management
 - Cryptographic key lifecycle management
 - Key management and cryptographic operations auditing
 - Hardened platform for creating, storing and managing key material
 - Highest quality key material generated from a quantum entropy source
 - Standards based interfaces – KMIP, PKCS #11 and RESTful API
 - High availability – hardware and system redundancy, active-active clusters
 - Supports hosted applications on the same hardware platform
 - Post quantum ready



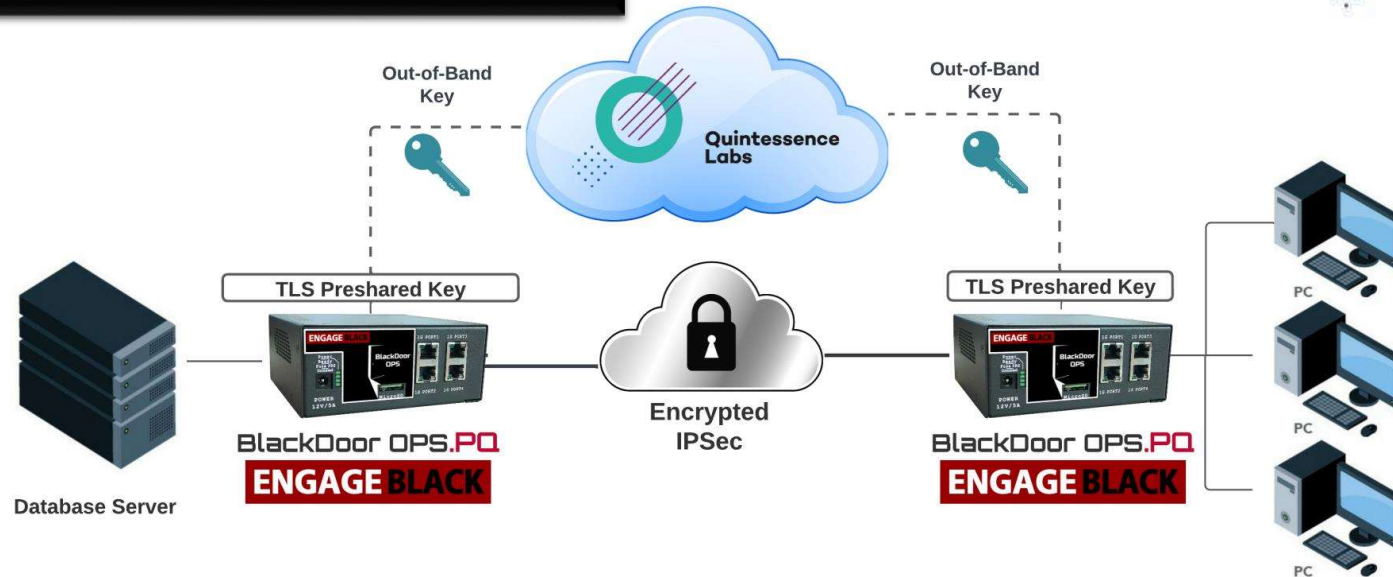
TSF-400 Quantum Enabled Key Management Platform

Your System



Post Quantum Ethernet Encryption OPTION with Trusted Security Foundation

ENGAGE BLACK



ETSI-QKD

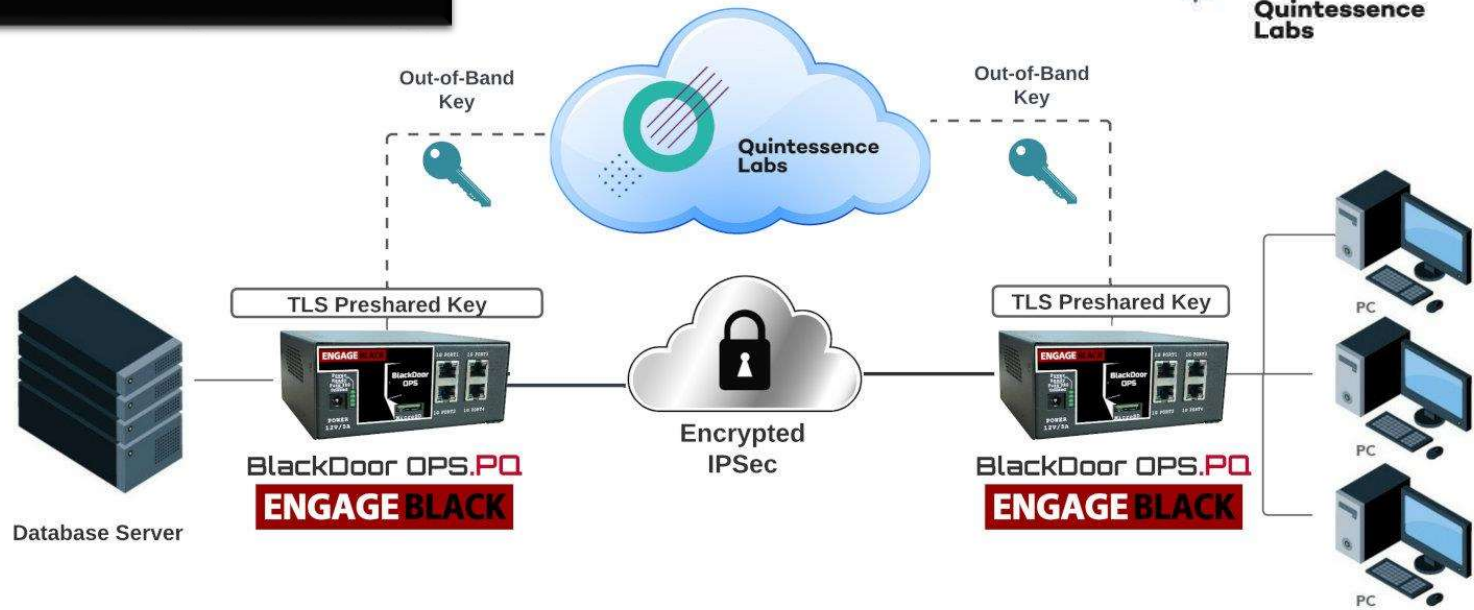
The ETSI QKD Standard GS QKD 014 is a communication protocol and data format for a Quantum Key Distribution (QKD) network to supply synchronized IPsec Session keys.

Hybrid-Key

An additional layer of Security to the BlackDoor is added by combining the IPsec session key with the Out-of-Band Key.

Post Quantum Ethernet Encryption OPTION with TSF Server

ENGAGE BLACK



Utilizes Quantum-Safe Out-of-Band Key Distribution to deliver Session Keys to the BlackDoor over an encrypted out-of-band connection utilizing ETSI QKD Standard GS QKD 014 protocol.

Quantum-Safe Out-of-Band Key
A **TLS Pre-Shared Key (PSK)** connection to the Key Management Server provides *Out-of-Band* quantum-safe key transport. AES 256-bit **PSKs** are able to protect the connection against a large-scale quantum computer.

"Symmetric Pre-Shared Keys (PSKs) may be used instead of X.509 v3 authentication certificates to provide quantum resistant cryptographic protection of classified information"
– NSA SYMMETRIC KEY MANAGEMENT REQUIREMENTS ANNEX V2.0





END_

Aptos, California USA
www.engageblack.com
info@engageblack.com

ENGAGE BLACK

**Impregnable Cryptographic
Solutions that protect against
the cyber threats of today and
the future.**

