sysnet TELEMATICA

NEL FUTURO DELLE TELECOMUNICAZIONI

QuantumCrypt SCS

Quantum Safe Communication System

- Real time encryption data, voice and video up to 1Gbps (2Gbps throughput)
- Key Management Server appliance with Quantum Random Number Generator and HSM
- Key Management Server virtual appliance with High Entropy Number Generator
- Hybrid key, out-of-band composite key and KMIP/QKD distribution
- P2P/P2MP with HA/DR
- L2/L3/VLAN/MPLS Encryption
- CE, IEC60950, EMC - CFR 47 Part 15 Sub Part B:2002, EN55022:1994+A1&A2, EN55024, ICES-003 1997, CISPR 22 Level A

Cybersecurity

QuantumCrypt SCS

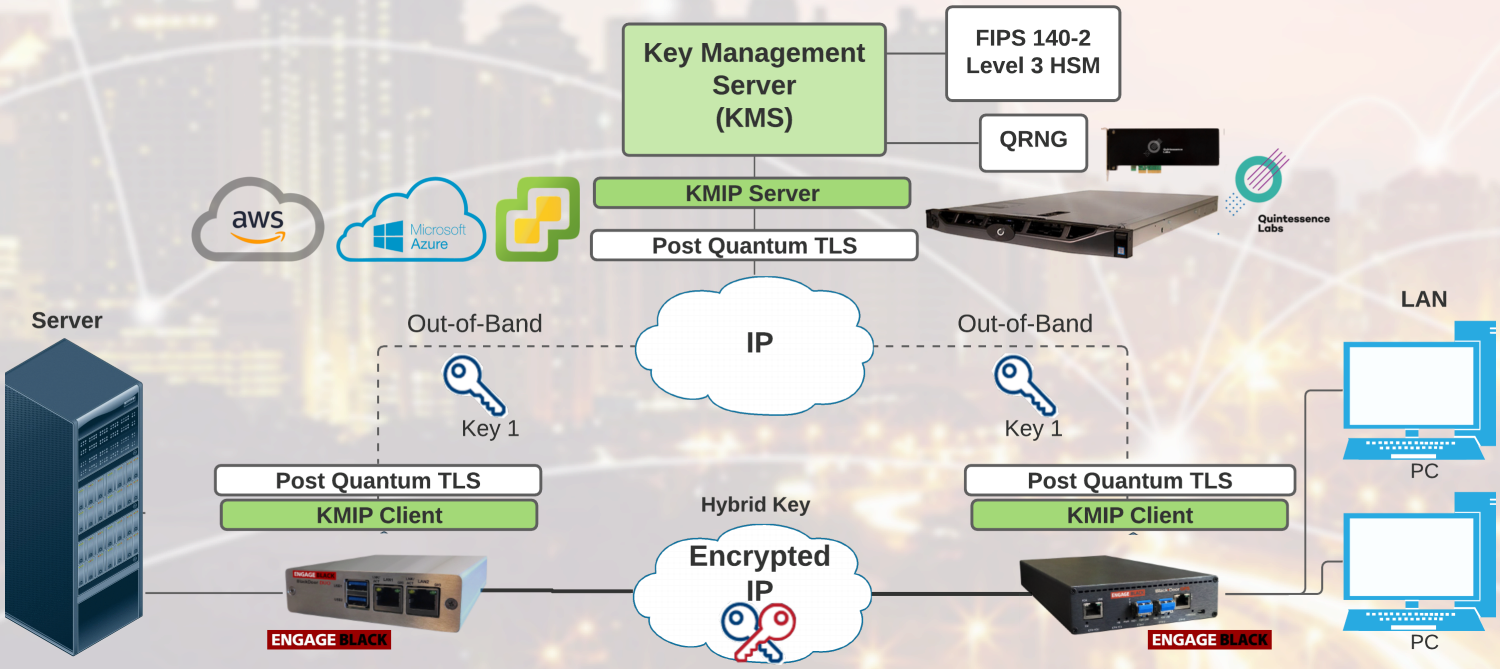
Quantum computers are very different to classical computers.
While classical computers encode data into binary digits (bits) that are either a “0” or a “1”, quantum computers use quantum bits, or qubits, which can represent a “0” and a “1”, simultaneously.
Their **processing power increases exponentially** with the number of these qubits, promising to give them extraordinary capabilities that will revolutionize computing.
Of significant concern, **they will also have impacts on cybersecurity that require us to change how we protect our data.**

Algorithms such as RSA are used to share symmetric encryption keys which in turn protect data.
The **security is founded on the huge processing time that classical computers would require to break** these asymmetric algorithms.
Indeed, **quantum computers will be able to break in seconds** the math behind encryption.

The way we currently exchange encryption keys – as well as digital certificates, blockchain and cryptocurrencies — **will no longer be safe**.

Timing: when to Worry?
Guesses range from **3 to 5 years**,
That means we should expect the **total breakdown of all currently used key exchange systems within a few years**, and **put in place a strategy early enough** that will allow us to implement quantum resilient in time to protect sensitive data for its full security life.

Adopt now our Quantum Safe Communication System made by the following blocks:



QSCS QRNG (Quantum Random Number Generator): the building blocks of cybersecurity lie in random numbers and truly random numbers remove vulnerabilities, building quantum resilience today.

QSCS Crypto-Agile KMS (Key Management Server): a secure platform for generation, distribution, storage, management and control of cryptographic objects, including quantum resistant keys and other cryptographic material.

QSCS KMIP/QKD Distribution: the forefront of QKD development, delivering high and cost-effective deployments using standard networking components.

Encryptors

The **Black Door DUO/OPS KMIP** are Ethernet Encryptors that employ a **Hybrid Encryption Key**, a secret combination of an in-band key and a KMIP sourced out-of-band key, to encrypt.

The **Black Door DUO/OPS KMIP** support wireline or wireless backbone networks with Point to Point and Multipoint configurations.

The **Key Management Interoperability Protocol (KMIP)** is an extensible communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server.; this facilitates data encryption by simplifying encryption key management.

A **Post Quantum Cryptography TLS** connection to the KMIP server provides quantum resistant key transport. Protecting against a large-scale quantum computer requires using a post-quantum key exchange algorithm during the TLS handshake.

A **Hybrid key exchange** performs two independent key exchanges during the TLS handshake and then cryptographically combines the keys into a single TLS session key.

Post Quantum TLS is a feature that adds new, post-quantum cipher suites to the protocol. The cipher suites specify a key exchange that provides the security protections of both the classical and post-quantum schemes.

BlackDoor DUO KMIP (20Mbps / 200Mbps)

BlackDoor OPS KMIP (2Gbps)

Encryption Algorithm
Hybrid Keying: In-Band and Out-of-Band
AES 256-bit (GCM)
Full Duplex real time encryption
Interfaces
Two 10/100 Base T, Optional 1000 Base X
Auto negotiation
Configured Speed and Duplex
Protocols
IP, TCP, UDP, ICMP, SSH
Post Quantum KMIP
Post Quantum TLS
Architectures
Point-to-Point, Point-to-Multipoint
Performances
100Mbps Full Duplex (200Mbps throughput)
1Gbps Full Duplex (2Gbps throughput) (OPS)
Low latency (< 1ms)

Regulatory:
CE, Safety -IEC60950, EMC - CFR 47 Part 15 Sub Part B:2002, EN55022:1994+A1&A2, EN55024, ICES -003 1997, CISPR 22 Level A
Management:
Console Port for Out of Band Management
SMNPv3· SSH support for Remote config., monitoring, & reset
Power
12-30 VDC, 1.0A., Locking Connector, Optional -48V 0.25 Amp, Hot Standby
Dimensions
Dimensions: 102 x 153 x 26 mm (4 x 6 x 1in)
Environmental
0° to 132° F (-10° to 50°C) operating temperature
Up to 90% operating humidity (non-condensing)
Optional Extended Temperature Range available

KMS (Key Management Server)

The **Quintessence TSF KMS/QRNG** delivers secure, centralized, and highly interoperable key and policy management across any organization, as either a **virtual machine or hardware appliance**.

TSF uses quantum technology to capture a level of randomness only seen in nature, resulting in perfectly unpredictable random numbers.

TSF® 100 | 200 | 300 | 400

	100	200	300	400
Configuration & Dimensions	Virtual Machine	Appliance	Appliance w/QRNG	Appliance w/HSM+QRNG
	N/A	• 1RU: H: 4.28 cm (1.69"), W: 48.20 cm (18.98"), D: 80.85 cm (31.83") • Weight: 22 kgs (48.50 lbs) • Support for running multiple Virtual Machines (VMs)		
Power Supply	N/A	1RU: Dual, redundant, hot-swappable, 550W		
Cryptography & Security	• Supports non-embedded FIPS 140-2 Level 3 cryptographic module • Supports one-time pad, symmetric key and asymmetric key ciphers, key derivation, random objects, certifications and some cryptographic operations • Support for Bring Your Own KEY (BYOK) operations with AWS and MS Azure • Granular, hierarchical and auditable access control • Supports both attended and unattended secure start-up • Event log, audit log, date and time of transaction, management and user reports • Thousands of end-client systems per node, 8,000 key requests/minute per node			
	N/A	N/A	N/A	FIPS 140-2 Level 3 HSM root of trust
Replication	• Secure replication of policies and managed cryptographic objects — up to 16 nodes per replication group • Supports both synchronous and asynchronous replication			
Random Number Generator	N/A	N/A	• QRNG included • Up to 1Gbit/sec true random stream • Conforms with NIST SP 800-90 A, B, and C (draft) • Satisfies NIST SP 800-22 (NIST STS) and Dieharder tests • Fully independent output for each user, audit trail from hardware through to consumer • RESTful API support for delivering random data	
Standards & Interoperability	• OASIS KMIP: Conformant with standards 1.0/1.1/1.2/1.3/1.4/2.0 • Fully implements all requirements in NIST SP 800-57 Part 1 • Common Criteria EAL 2 certified (does not apply to TSF 100) • Supports PKCS#11 over KMIP			
Administration & Management	• Web (HTTPS) or command-line (SSH) management interfaces • Purpose-built QRE secure operating system • Delivered with qClient™ 100 • Support for 10 Gbit/sec Ethernet			

UNI EN ISO 9001:2015 CERTIFICATION™
Intertek
Certificato
nr. 1316007-01

Sysnet Telematica S.r.l. - Viale Berbera 49 - 20162 - Milano
Web: http://www.sysnettelematica.it
E-mail: sales@sysnettelematica.it
Tel: (+39) 02.64.73.021

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI