SEQURE QUANTUM

SeQRNG - Expansion

We don’t just generate randomness — we prove it.

Verifiable quantum entropy for KMS, HSM, VPNs, firewalls, encryptors and post-quantum architectures — on-prem and across AWS, Microsoft Azure and Google Cloud.

PRODUCTS
SeQRNG · verifiable quantum entropy | Expansion · FIPS 140-2 high-volume DRBG

STANDARD
ETSI GS QKD 014 · mTLS over PQC TLS 1.3

DOCUMENT
Solution & Integration Brochure · 2026

Verifiable Quantum Entropy

We don't just generate randomness — we prove it.

In the next generation of cybersecurity, it is no longer enough to assume that randomness is trustworthy. As artificial intelligence, quantum computing and the digitalisation of critical infrastructure advance, security increasingly depends on the ability to prove that the entropy behind every cryptographic key is truly unpredictable.

At Sequre Quantum we don't just generate quantum randomness — we verify it. Through the SeQRNG, our quantum random number generator with real-time self-certification, we introduce a new category of security: verifiable quantum entropy. And through Expansion, our FIPS 140-2 high-volume DRBG, that same entropy can be delivered at gigabyte-per-second scale.

This brochure presents the use cases where Sequre Quantum strengthens critical cryptographic infrastructures, integrating with KMS, HSM, VPNs, firewalls, encryptors, cloud platforms and post-quantum architectures — both on-premise and across hyperscalers (AWS, Google Cloud, Microsoft Azure).

More than an additional component, Sequre Quantum positions itself as a foundational layer of trust for modern cybersecurity: one where it is no longer enough to encrypt — you must also prove the quantum origin of the entropy that protects every system.

The SeQRNG

True quantum entropy, delivered over a standard interface.

What it is

The SeQRNG is a hardware quantum random number generator that produces true random numbers from active quantum photonics. Unlike first-generation QRNGs that rely on assumptions about internal device parameters, the SeQRNG implements a device-independent self-certification protocol — entropy quality is proven continuously from observed quantum measurement statistics alone, without trusting the device's own characterisation. This means the entropy lower bound H_min is certified in real time under worst-case adversarial assumptions: any degradation, tampering, or detector attack is detected and compensated before a single weak bit is released. The device continuously monitors its operational health and delivers output through a REST API, including native support for the ETSI GS QKD 014 standard.

Performance & certification (key specs)

- Quantum entropy source rate: > 8 MHz (typical).
- Certified private randomness: > 3 Mbps**, autocertified in real time
- 256-bit key generation: > 8,000 keys/second.
- Compliance: ITU-T X.1702 (QES2), NIST SP800-22; GLI certified (RN-523-LCN-23-01).
- Form factor: 19" rack 1U, 4.2 kg; dual RJ-45; < 130 W; AC 100–240 V.

Standard integration interface — ETSI GS QKD 014

The SeQRNG natively exposes ETSI GS QKD 014, the European standard for quantum-key delivery over a REST API. Any compliant device — a Thales HSE, a FortiGate, or a custom ETSI client — requests keys from the SeQRNG over mutual TLS (mTLS) and is identified by a SAE ID. The mTLS channel itself runs TLS 1.3 with the X25519MLKEM768 hybrid key exchange, so the key-distribution channel is post-quantum protected end-to-end. Each key delivery is logged with SAE ID, key ID, timestamp, and status, providing native audit and forensic trail.

How customers consume it

- Entropy-as-a-Service (EaaS): managed REST API + ETSI 014 endpoint.
- On-prem appliance: rented unit inside the customer's data center. Used when regulation, sovereignty, or air-gap rule out cloud delivery.

The SeQRNG is not a replacement KMS, HSM, firewall, or VPN concentrator — it is the certified entropy and key-material foundation those systems depend on. Customers keep the vendors they have selected; we make the keys those vendors generate quantum-safe.

***Scalable from ~3 Mbps to 2.8 GB/s, while preserving the quantum origin of the seed. See Expansion*

Do your systems require high volumes of verifiable, quantum-origin randomness?

SeQRNG Expansion

FIPS 140-2 high-volume entropy on top of SeQRNG.

What it is

Expansion is a complementary service that turns the SeQRNG's certified quantum entropy into a high-throughput stream of FIPS-compliant random bytes. It pairs the SeQRNG with an OpenSSL 3.0 FIPS-certified DRBG (HMAC-DRBG SHA-256 / CTR-DRBG AES-256), and exposes a simple HTTP REST API. Customers can saturate any cryptographic workload — token farms, signing platforms, blockchain, large-scale TLS.

Why it matters

Expansion enables customers to consume gigabytes per second of cryptographically secure random bytes while the SeQRNG periodically re-seeds the DRBG, maintaining the quantum origin of the seed throughout the process. This preserves end-to-end entropy integrity, without making throughput the bottleneck.

Key specifications

- FIPS 140-2 compliant via OpenSSL FIPS Module 3.0; 256-bit security strength with prediction resistance.
- Throughput: up to ~2.8 GB/s (CTR-DRBG AES-256 with thread pool and pre-fetch ring) in benchmarks; ~250 MB/s sustained in CPU-bound co-located deployments.
- Entropy lifecycle: 10 MB pool refilled in 1 MB batches when depleted; auto-reseed every 300 s or 100,000 requests, per NIST SP 800-90A.
- HTTP REST API (port 8000) — output as base64, hex or binary. POST /api/v1/generate with size and format.
- Fully containerised (Docker / Podman). No host-side dependencies. Deployable on a dedicated server, on the customer's machine, or co-located with the SeQRNG hardware for zero network latency on refills.

How it pairs with SeQRNG

Expansion never weakens the quantum guarantee — every reseed and pool refill consumes real SeQRNG entropy. It simply amplifies it: the SeQRNG remains the source of truth for randomness, and Expansion makes that randomness available at the volume modern workloads require.

Technology Partners

We strengthen the security stack from inside — validated by the people who own it.

Sequre Quantum's only formal technology partnership is with Thales, where our SeQRNG and Expansion services are validated as a foundational entropy and key-material layer across the Thales encryption stack. Beyond that partnership, we deliver validated integrations with the vendors and platforms our customers already operate — they keep their existing stack; we make the cryptography it generates verifiable, quantum-safe and high-volume.

FORMAL TECHNOLOGY PARTNER

Thales

Validated quantum-entropy integrations across the Thales encryption stack: HSE CN6140 high-speed encryptors, CipherTrust Manager (KMS), and Luna HSM. ETSI GS QKD 014 deployed in production design.

Beyond that partnership, Sequre Quantum delivers validated integrations with the vendors our customers already run. With Palo Alto Networks, the SeQRNG feeds the PAN-OS 12.1+ Quantum Security feature: the firewall acts as the SAE device and fetches quantum keys from the SeQRNG (KME) for hybrid post-quantum IKEv2 VPNs. With Fortinet, the FortiGate (FortiOS 7.4+, validated on 7.6.6) pulls quantum-seeded key material over ETSI GS QKD 014 for hybrid post-quantum IKEv2 / IPsec VPNs. Juniper (Junos OS, RFC 8784 PPK) is supported over the same ETSI 014 path. Across cloud, BYOK is in production with AWS and Google Cloud, with Microsoft Azure BYOK on the roadmap, while OS-level entropy reinforcement on Red Hat Enterprise Linux remains exploratory. Where a vendor does not yet expose ETSI 014 natively, Sequre delivers entropy through its REST / KMIP / SDK interfaces.

Integrations

01 · Cloud KMS — BYOK / HYOK with Quantum Entropy & Rotation Policy

Any cloud-KMS user with sovereignty, compliance or audit requirements — e.g. banking, finance, healthcare, government, regulated SaaS

PAIN / RISK

Cloud KMS services (AWS KMS, Azure Key Vault, GCP Cloud KMS) generate keys from the provider's own entropy pool. BYOK and HYOK schemes give the customer back ownership, but the entropy source still comes from a deterministic system — and rotation policy is rarely operationalised beyond defaults. The result: weak entropy assurance, lock-in to provider-defined cycles, and audit gaps.

VALUE PROPOSITION

We provide quantum entropy at the BYOK import point or directly inside the customer's HYOK HSM, so every cloud key is seeded from a true quantum source. We also help the customer design and operate a rotation policy that is aggressive enough for compliance and operationally feasible — frequency, key versioning, fall-back behaviour, audit evidence.

CUSTOMER BENEFITS

True quantum entropy at the foundation of every cloud key (BYOK + HYOK); customer-defined rotation policy with quantum re-seeding on every cycle; auditable evidence per key delivery (SAE ID, key ID, timestamp); compatibility with AWS XKS, Azure Key Vault EKM, GCP Cloud EKM. No vendor lock-in.

REFERENCE ARCHITECTURE

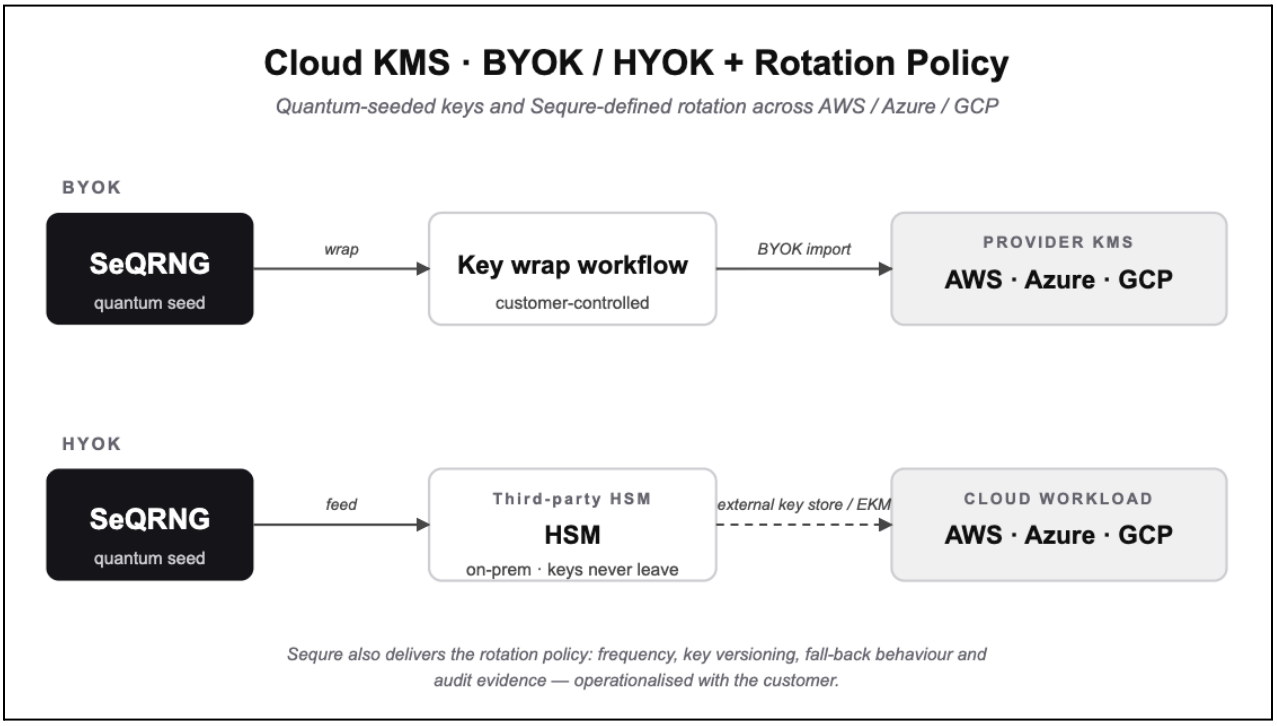
The SeQRNG exposes an API REST. In BYOK, the customer's import workflow calls the SeQRNG to seed the key wrapper; the wrapped key is then imported to AWS KMS, Azure Key Vault, or GCP Cloud KMS. In HYOK, the on-prem HSM (e.g. Thales Luna) requests quantum keys from the SeQRNG at creation and at every rotation event. Sequre provides the rotation playbook and audit hooks.

VENDOR STACK

Sequre SeQRNG + customer's KMS / HSM — validated paths into AWS KMS (XKS), Azure Key Vault (EKM), GCP Cloud KMS (EKM), Thales CipherTrust Manager, Thales Luna HSM, and digital-signature platforms (e.g. e-Sign).

EFFORT & INVESTMENT

2–4 weeks (cloud or on-prem). Customer involvement: CISO / CTO with KMS access; cloud architect for XKS/EKM wiring; risk/compliance owner for rotation policy.



02 · Site-to-Site & IPsec VPNs (multi-vendor)

Any organisation operating site-to-site or remote-access IPsec VPNs — e.g. banking, government, defence, critical infrastructure, large enterprise.

PAIN / RISK

Site-to-site and remote-access IPsec VPNs are exposed to harvest-now-decrypt-later: classical IKEv2 with PSK or PKI authentication will not survive a cryptographically relevant quantum computer, and recorded VPN traffic can be decrypted retroactively. Replacing the VPN concentrators outright is expensive, slow and disruptive.

VALUE PROPOSITION

We strengthen any IPsec VPN with quantum-derived key material delivered to the customer's existing concentrators — Fortinet FortiGate, Palo Alto NGFW, Juniper SRX — over the standard ETSI GS QKD 014 protocol. The VPN keeps its topology, vendor, and management plane; we make every key it negotiates quantum-safe.

CUSTOMER BENEFITS

Quantum-safe site-to-site and remote-access VPNs with no rip-and-replace; vendor-neutral via ETSI 014; hybrid PQC IKEv2 (ADDKE on Fortinet, Quantum Security on PAN-OS, RFC 8784 PPK on Juniper); auditable key delivery per SAE ID; mixed estates supported (Fortinet + Palo Alto + Juniper from a single SeQRNG hub).

REFERENCE ARCHITECTURE

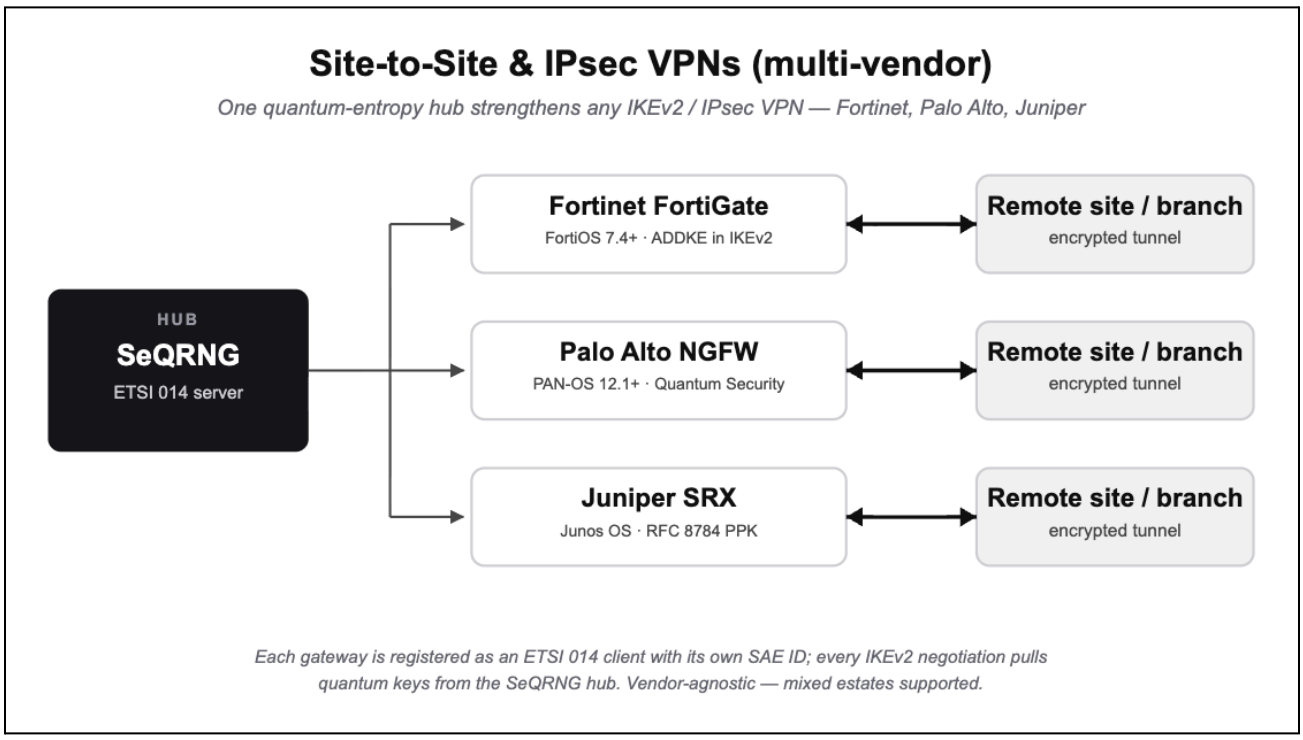
Each VPN endpoint registers as an ETSI 014 client of the SeQRNG with its own SAE ID. At every IKEv2 negotiation, the endpoint requests quantum keys from the SeQRNG over mTLS / TLS 1.3 X25519MLKEM768 and incorporates them into the IPsec SA as additional entropy alongside classical DH and post-quantum KEM/signatures. The SeQRNG hub can serve dozens of endpoints; HA available with load balancer.

VENDOR STACK

Sequre SeQRNG + Fortinet FortiGate (FortiOS 7.4+) + Palo Alto NGFW (PAN-OS 12.1+) + Juniper SRX. Vendor-agnostic via ETSI 014.

EFFORT & INVESTMENT

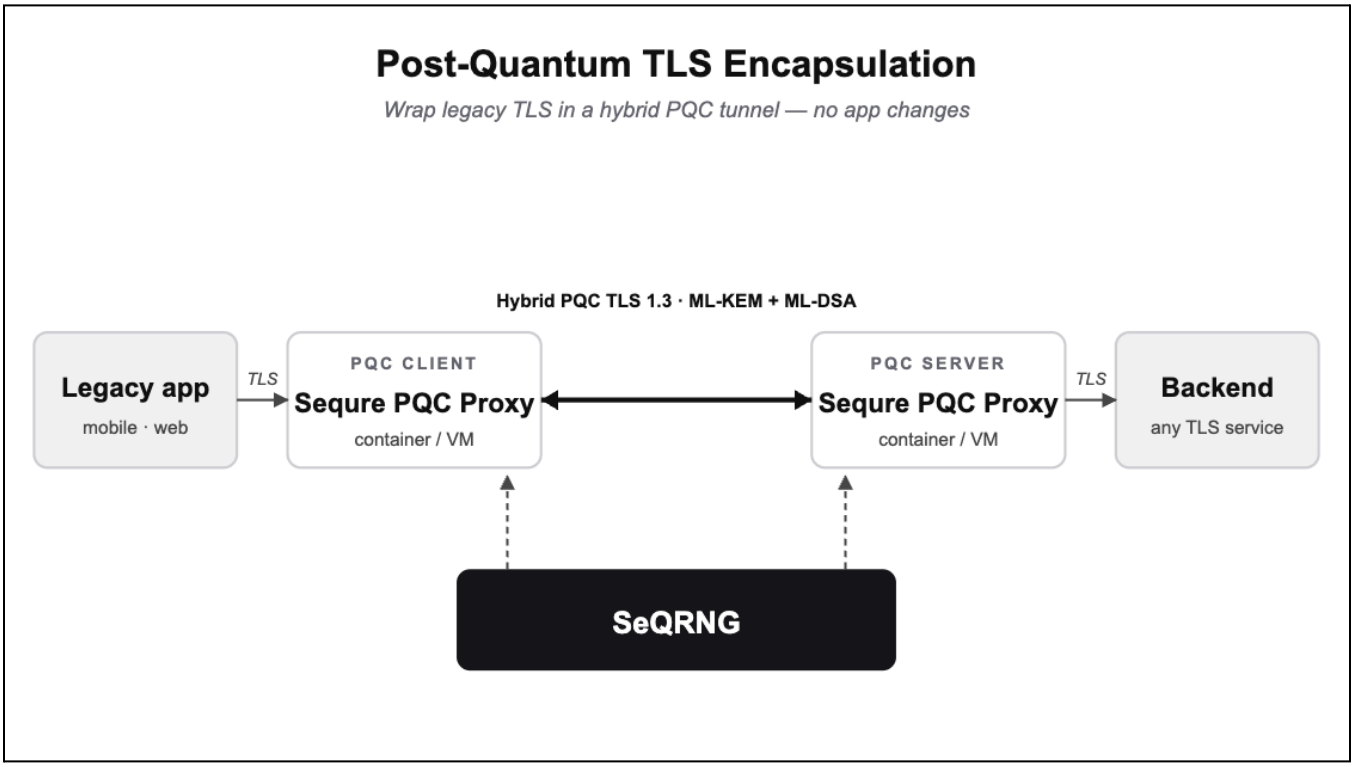
2–4 weeks per endpoint pair; faster on cloud / containerised deployments. Customer involvement: network/security architect; firewall admin; certificate management.



03 · Post-Quantum TLS Encapsulation

Any organisation with legacy TLS estates that needs to migrate to PQC — e.g. banking, healthcare, government, large enterprise

PAIN / RISK Legacy infrastructure/applications rely on classical TLS that cannot easily be migrated to post-quantum standards. Re-architecting them is expensive, slow, and risky — but leaving them in place means they will fall behind compliance and threat baselines.	**VALUE PROPOSITION** We wrap legacy normal TLS traffic inside a quantum-safe tunnel using our PQC Proxy, with no changes required to applications or infrastructure. Customers achieve quantum-safe communications without re-architecture, on a predictable timeline.
CUSTOMER BENEFITS Quantum-safe communications without changes to apps or architecture; fast path to PQC compliance for legacy estates; transparent to upstream and downstream systems; ideal for omnichannel banking (mobile + web ↔ score / offer / identity systems).	**REFERENCE ARCHITECTURE** A PQC Proxy Client and PQC Proxy Server are deployed at each endpoint. The agent establishes a hybrid TLS 1.3 tunnel using ML-KEM for key exchange and ML-DSA for authentication, encapsulating the legacy TLS session inside a quantum-safe channel. SeQRNG seeds the key material.
VENDOR STACK Sequre PQC Proxy + SeQRNG (deployable alongside any vendor stack).	**EFFORT & INVESTMENT** 2–3 weeks (faster on cloud / containerised). Customer involvement: infrastructure and architecture (deployment topology, network rules).



04 · Data-at-Rest Protection

Any organisation handling regulated data at rest — e.g. banking, finance, healthcare, pharma

PAIN / RISK

Critical and regulated data (PII, PHI, financial records) is exposed to breach, ransomware, and harvest-now-decrypt-later attacks. Standard encryption keys are generated with classical entropy and may be vulnerable as quantum capability matures.

VALUE PROPOSITION

We protect data at rest with encryption and keys seeded with quantum entropy from the SeQRNG, delivered through a partnership with Thales CipherTrust Manager. The result is encryption that is quantum-safe by design.

CUSTOMER BENEFITS

Regulatory compliance (financial, health, data-protection regimes); reduced exposure to ransomware and exfiltration; long-term protection against harvest-now-decrypt-later attacks; centralised policy and key lifecycle management.

REFERENCE ARCHITECTURE

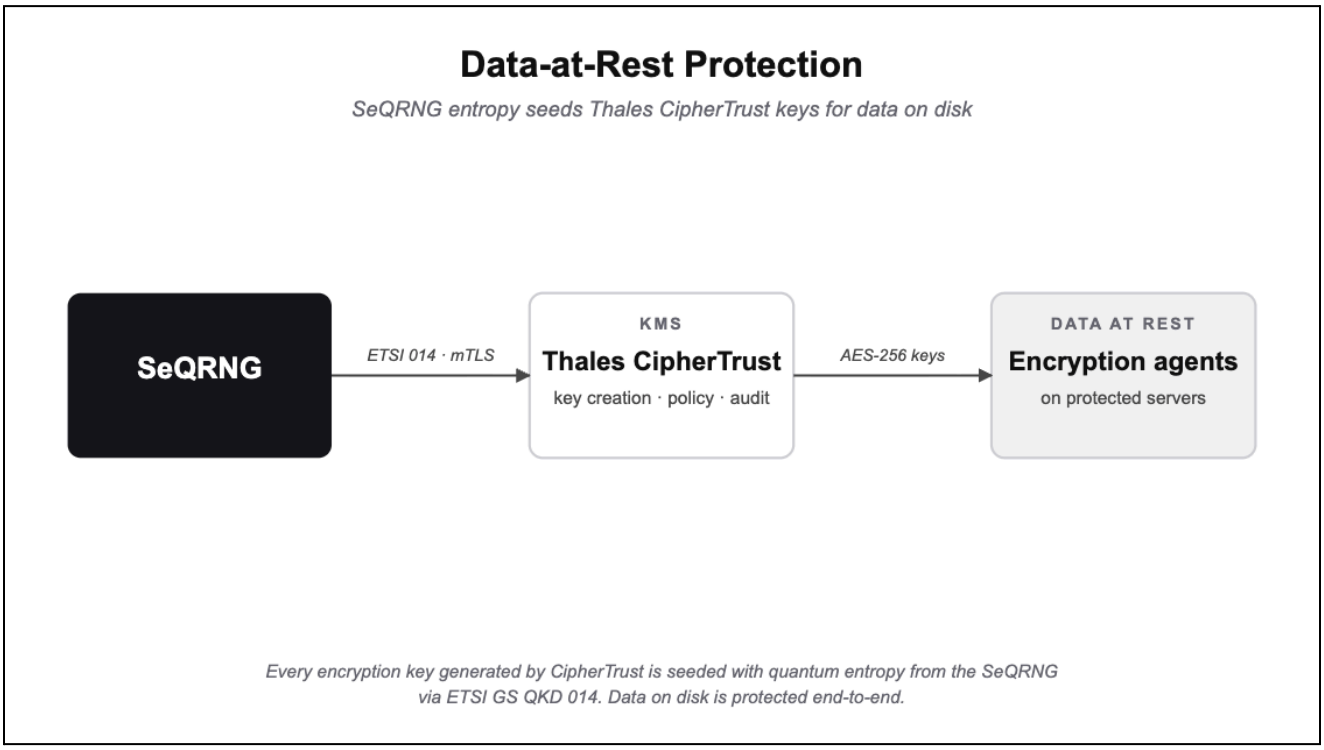
A lightweight encryption agent is installed on each protected server. The agent connects to the Thales CipherTrust Manager (KMS), which calls the SeQRNG entropy service to seed every key it generates. Access policies are managed centrally in CipherTrust.

VENDOR STACK

Sequre SeQRNG + Thales CipherTrust Manager (KMS).

EFFORT & INVESTMENT

2–4 weeks depending on server count and policy scope. Customer involvement: CISO / security team, infrastructure, architecture. Investment: USD 900 – 10,000 / month depending on number of servers and cloud vs. on-prem.



05 · Data-in-Transit Protection (HSE via ETSI 014)

Any organisation with mission-critical multi-site operations — e.g. government, defence, energy, telco backbones, critical infrastructure

PAIN / RISK

Mission-critical communications between sites, data centres, or command nodes are vulnerable to interception. Today's TLS will not survive a cryptographically relevant quantum computer, and recorded traffic can be decrypted retroactively.

VALUE PROPOSITION

We secure point-to-point links by feeding certified quantum entropy into the Thales HSE CN6140 high-speed encryptors via the ETSI GS QKD 014 standard. Each pair of HSEs derives its session keys from SeQRNG-generated quantum keys, eliminating dependency on PRNG-only key material and resisting harvest-now-decrypt-later attacks.

CUSTOMER BENEFITS

Reinforced confidentiality of critical data in transit; resilience against present and future quantum threats; standards-based key delivery (ETSI 014) — no proprietary KDK over SSH; full audit trail per key (SAE ID, key ID, timestamp).

REFERENCE ARCHITECTURE

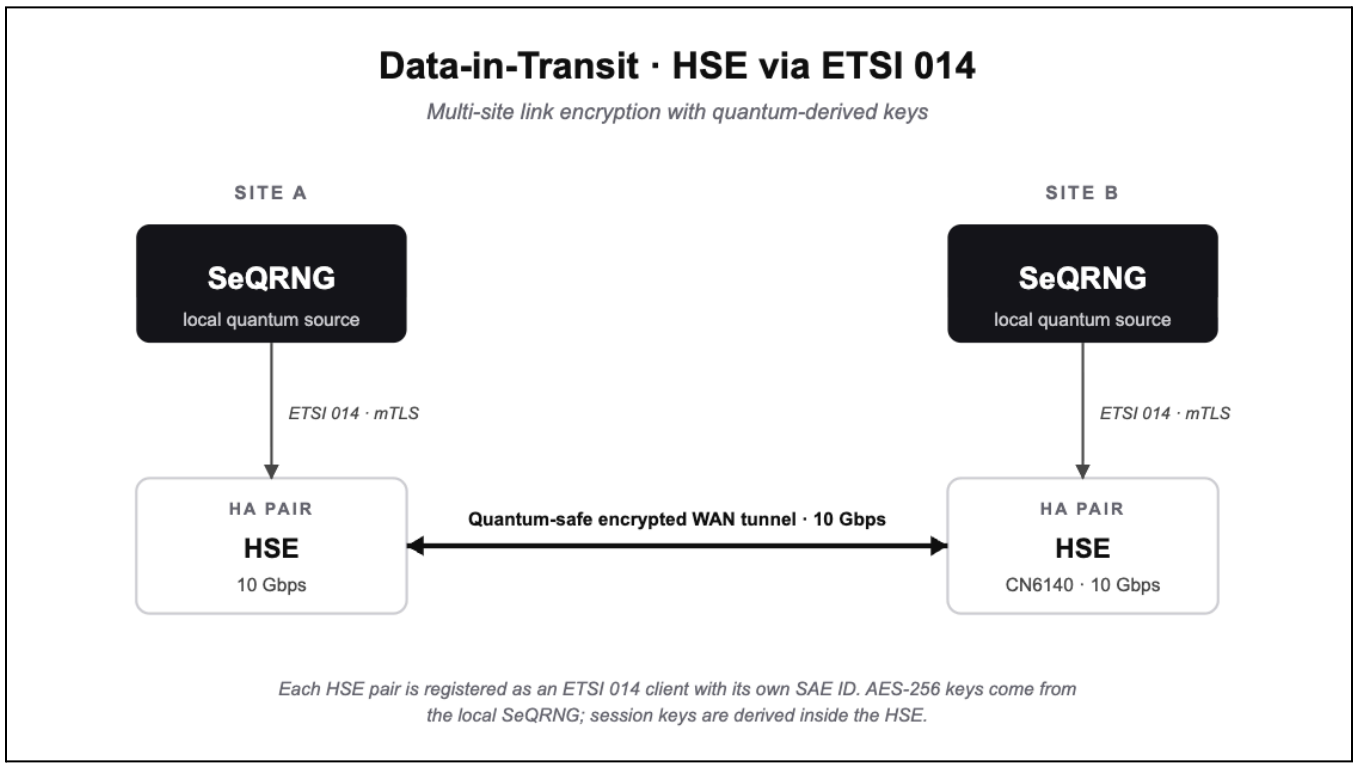
Thales HSE CN6140 deployed at each site (HA active/standby). Each HSE registers as an ETSI 014 client of the SeQRNG with a unique SAE ID, requests AES-256 quantum keys, and uses them to derive session keys for the encrypted WAN tunnel. mTLS over TLS 1.3 with X25519MLKEM768 protects the key-distribution channel.

VENDOR STACK

Sequre SeQRNG (ETSI 014 server) + Thales HSE CN6140 + Thales CipherTrust Manager (key policies & audit).

EFFORT & INVESTMENT

3–6 weeks per multi-site deployment; HSE coordination required. Customer involvement: network/architecture/infrastructure; data-centre access; IP planning; HSE certificates.



Additional integrations

Specialised and emerging use cases, beyond the five core integrations.

Beyond the five integrations above, the SeQRNG is also deployed or in validation in three further scenarios. Their fit and maturity vary by customer, so we scope and position them per engagement.

Certified Random Draws & Lotteries (In production)

Certified, auditable quantum-random numbers delivered in real time through a simple REST API. Each draw is provably based on quantum entropy, with a per-draw audit log that gives regulators and oversight bodies forensic evidence. Deployed today with lottery operators. Vendor stack: Sequre SeQRNG (direct REST API). Typical effort: 2–4 weeks.

Column-Level Database Encryption (MySQL) (Beta)

A PQC Proxy SQL sits in front of the database and encrypts / decrypts only the columns defined as sensitive (PII, account numbers, clinical data), seeded with quantum-safe keys. Applications and DBAs keep interacting with the database as usual. Currently available for MySQL as a beta; additional engines on the roadmap. Vendor stack: Sequre PQC Proxy + SeQRNG. Typical effort: 3–4 weeks.

OS-level Entropy Reinforcement on Red Hat (Roadmap)

A lightweight Sequre daemon seeds /dev/urandom on RHEL hosts with quantum entropy from the SeQRNG, so SSH keys, X.509 certificates and TLS sessions inherit a quantum-safe seed with no application, library or container changes. Earlier co-development with Red Hat is currently on hold; the capability is exploratory and not yet in production. Vendor stack: Sequre SeQRNG + Red Hat Enterprise Linux.

Vendor integration matrix

Where the SeQRNG plugs into the security stack you already operate.

Each Sequre solution is delivered through a combination of the SeQRNG and a set of validated vendor integrations. The matrix below summarises the role each vendor plays and the use cases it enables.

Vendor / Stack	Integration via	Role of the SeQRNG
Thales HSE CN6140	ETSI GS QKD 014 (mTLS · TLS 1.3 X25519MLKEM768)	The SeQRNG strengthens the entropy seeding every AES-256 key, so each session key the HSE derives is quantum-seeded.
Fortinet FortiGate (SD-WAN / ADVPN 2.0)	ETSI GS QKD 014 (FortiOS 7.4+, validated on 7.6.6)	The SeQRNG strengthens the entropy that feeds every IKE key the FortiGate generates, delivering quantum-seeded hybrid PQC defense-in-depth.
Palo Alto Networks NGFW	ETSI GS QKD 014 (PAN-OS 12.1+)	The SeQRNG strengthens the entropy of those keys: PAN-OS acts as SAE device and pulls quantum-seeded material from the SeQRNG (KME) at every negotiation.

Vendor / Stack	Integration via	Role of the SeQRNG
Juniper SRX	ETSI GS QKD 014 (Junos OS, RFC 8784)	The SeQRNG strengthens the entropy of the PPK material (RFC 8784) injected into each SA — so every site-to-site tunnel carries quantum-seeded keys.
Red Hat Enterprise Linux (roadmap)	/dev/urandom seeding (co-development)	The SeQRNG strengthens the kernel entropy pool, so every consumer of /dev/urandom on a Sequre-strengthened RHEL host inherits a quantum-seeded random stream.
Thales CipherTrust Manager	KMS API + ETSI 014 / KMIP	The SeQRNG strengthens the entropy used at every key creation, so every policy-managed key — and the encryption that follows — is quantum-seeded.
Thales Luna HSM	Luna SDK over PQC tunnel + ETSI 014	The SeQRNG strengthens the entropy injected into every key creation event, so every Luna-issued key is quantum-seeded.
AWS · Azure · GCP cloud KMS	BYOK import + XKS / EKM hooks	Via BYOK, the SeQRNG strengthens the entropy of the keys you wrap and import; via HYOK (AWS XKS · Azure Key Vault EKM · GCP Cloud EKM), the customer's on-prem HSM serves quantum-seeded keys to the cloud workload. Sequre also delivers the rotation policy..
Sequre PQC Proxy	Native (Sequre product)	The SeQRNG provides the quantum-seeded entropy for every key exchange and signature inside the tunnel. Used in TLS encapsulation and DB column-encryption use cases..
Digital-signature platforms (e.g. e-Sign)	REST / KMS API over PQC tunnel	The SeQRNG strengthens the entropy used to generate every signing key, raising the assurance level of every signature, certificate and timestamp the platform issues.

ETSI GS QKD 014 is now the de-facto industry standard for quantum-key delivery — adopted in GA software by Palo Alto Networks, Fortinet, Juniper, Thales, Senetas, Toshiba and ADVA. The SeQRNG plugs into any of them as an interchangeable QRNG / QKD source. Channel security throughout: mTLS over TLS 1.3 with X25519MLKEM768 hybrid key exchange. Where a vendor does not yet expose ETSI 014 natively, Sequre delivers the entropy through its REST / KMIP / SDK interface.

Deployment, effort & investment

What the customer commits, and what they get back.

Two deployment models

Every SeQRNG-based solution is available either as a managed service or as an on-prem deployment. The right model depends on the customer's regulatory environment, data-sovereignty requirements, and operational preferences. A typical engagement starts on the managed service, then migrates one or more workloads on-prem as scope grows.

Typical implementation timelines

- Entropy-as-a-Service integration: 2–4 weeks.
- PQC TLS encapsulation (per link): 2–3 weeks.
- Data-at-rest encryption (per cluster): 2–4 weeks.
- Database column encryption (per database): 3–4 weeks.
- Site-to-site link with HSE + PQC Proxy: 3–6 weeks.

Who participates from the customer side

CISO / security team for policy and scope. Infrastructure and architecture for deployment topology and network rules. Application or database owners for the systems being protected. Specific use cases (signing, draws, database column encryption) also involve the relevant business owner — DPO, lottery operations, signing-platform owner.

Why Sequre Quantum

Production deployments with regulated customers, validated vendor integrations, and a single accountable partner.

Production references

The five core use cases in this brochure are not roadmap — they are deployed and in use today; the additional integrations note their maturity individually. Active customers and prospects span banking (Banco Estado, Scotiabank Cencosud), healthcare (MMrad), defense and intelligence, and lotteries (Lotería de Concepción, Lotería de Misiones).

Single accountable partner

Customers contract one party — Sequre Quantum — for the entropy source, the integration with their existing vendors (Thales, Fortinet, Palo Alto, AWS), and the operational support of the resulting solution. We own the integration: the customer does not have to assemble it themselves.

How to start

- Pick the use case closest to your current pain (the matrix on the previous page is a good starting point).
- We run a 1-hour scoping session with your security and infrastructure teams to size the engagement.
- We propose a 2–6 week pilot on a managed-service model. From there, we scale into on-prem or production as required.