CHIFFREMENT POST-QUANTIQUE SOUVERAIN

AllEyes Resilient

Première plateforme de chiffrement réseau post-quantique
certifiable ANSSI CSPN en France

`ML-KEM-1024` `ML-DSA-87` `AES-256-GCM` `FIPS 203/204` `CPU-Blind` `IPsec/IKEv2`

6.4 Tbps	800 Gbps	< 1 µs	CSPN
par serveur — stackable	par carte FPGA	latence chiffrement	objectif Q3 2026

L'ordinateur quantique brisera RSA et ECDH avant 2035. Les données interceptées aujourd'hui seront déchiffrables rétrospectivement — **Harvest Now, Decrypt Later**. CryptOps chiffre vos liens critiques avec des algorithmes post-quantiques standardisés NIST, dès aujourd'hui, sans modification de votre infrastructure réseau.

Performance

6.4 Tbps par serveur
Latence < 1 µs
Stackable — scalabilité linéaire

Souveraineté

100 % français
Stack Rust auditée
Zéro dépendance US

Certification

CSPN objectif Q3 2026
ANSSI — CEA-Leti CESTI
NIS2 / DORA natif

Architecture conçue pour les Opérateurs d'Importance Vitale et infrastructures critiques européennes.

01 — CONTEXTE

Pourquoi le chiffrement post-quantique ?

⚠️ Menace quantique

Les calculateurs quantiques briseront RSA, ECDH et les courbes elliptiques d'ici 2030-2035. Toutes les communications chiffrées aujourd'hui avec ces algorithmes deviendront lisibles.

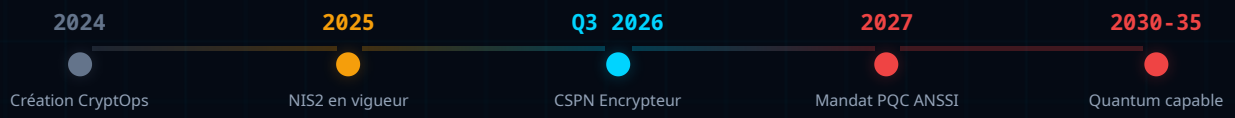
🗄️ Harvest Now, Decrypt Later

Des acteurs étatiques interceptent et stockent massivement le trafic chiffré dès aujourd'hui. Lorsque le quantique sera disponible, ces données seront déchiffrées rétrospectivement — y compris les secrets d'État et données bancaires.

📋 Mandat ANSSI 2027

À partir de 2027, l'ANSSI exigera que tous les produits qualifiés intègrent du post-quantique. Les produits non conformes perdront leur qualification. La transition doit commencer maintenant.

TIMELINE RÉGLEMENTAIRE



TROIS PILIERS CRYPTOPS

Performant

6.4 Tbps par serveur en chiffrement post-quantique. Architecture stackable pour une scalabilité linéaire. Latence inférieure à 1 microseconde.

Certifié

CSPN ANSSI en cours d'évaluation. Conformité native NIS2, DORA, SecNumCloud. Évaluation par le CEA-Leti, CESTI agréé ANSSI.

Souverain

100 % français. Stack Rust auditée. Zéro composant US dans la chaîne de confiance. Hébergeable on-premise ou SecNumCloud.

02 — PRODUITS

Portefeuille produits

Cinq form factors pour couvrir du datacenter souverain à la sous-station SCADA. Même chiffrement post-quantique, même firmware durci, tous interopérables.

RÉFÉRENCE	FORMAT	DÉBIT	USAGE CIBLE
AllEyes Resilient 4U	4U rack datacenter	Jusqu'à 6.4 Tbps	Datacenter souverain, trading haute fréquence
AllEyes Resilient 2U	2U rack compact	Jusqu'à 3.2 Tbps	Backbone régional, PoPs opérateurs
Agent PQC-WAN 1U	1U télécom (NEBS Level 3)	10 Gbps	Opérateurs télécom, PoPs
Agent PQC-WAN Compact	1U ultra-compact	10 Gbps	Agences bancaires, micro-sites
Edge E300	Boîtier industriel 3.4 kg	10 Gbps	SCADA, sous-stations, -40/+70°C

Encrypteurs : chiffrement FPGA hardware · Agents : chiffrement logiciel · Tous interopérables nativement

SERVICES LOGICIELS

GARANCE PKI

Infrastructure de certificats post-quantique. Signatures ML-DSA-87, révocation OCSP/CRL temps réel, audit trail immutable. 100 % souverain.

GLUON Agent

VPN mesh post-quantique. Chiffrement point-à-point, déploiement zero-touch, interopérable avec les encrypteurs AllEyes.

SPÉCIFICATIONS CLÉS

5	2	100%	Rust
form factors	certifications CSPN	AMD — CPU + FPGA	firmware audité

03 — SÉCURITÉ

Architecture de sécurité — CPU-Blind

Les clés de chiffrement ne transitent **jamais** par le CPU. Six domaines d'isolation indépendants garantissent qu'un attaquant doit compromettre au minimum trois composants hétérogènes pour accéder aux clés.

D1
CPU AMD EPYC
Orchestration uniquement — ne voit jamais les clés

D2
FPGA Chiffrement
AES-256-GCM hardware — isolation totale

D3
FPGA Firmware
Négociation PQC — firmware Rust audité

D4
Secure Element
Clés maître — EAL6+ certifié

D5
HSM Backup
Redondance clés — hardware indépendant

D6
Kill Switch
Zéroisation < 100 ms — indépendant du CPU

6	71	CPU-Blind	< 100 ms
domaines d'isolation	canaux d'exfiltration analysés	clés jamais sur le CPU	zéroisation hardware

CANAUX D'EXFILTRATION COUVERTS

Électromagnétique 12 EMI, TEMPEST, fuites RF	**Temporel** 18 Timing, Spectre, cache side-channel	**Puissance** 14 SPA/DPA, injection de fautes
Mémoire 11 Cold boot, DMA, Rowhammer	**Réseau** 9 MITM, replay, analyse de trafic	**Physique** 7 Tampering, JTAG, sondes

04 — CAS D'USAGE

8 secteurs, une même promesse

📡

TELECOM

Backbone & PoPs Télécom

Chiffrement post-quantique des backbones optiques et PoPs d'interconnexion télécom.

800 Gbps/carte | <1 us

🏦

BANQUE / FINANCE (DORA)

Conformité DORA -- Chiffrement inter-sites bancaire

Chiffrement inter-sites bancaire conforme au règlement DORA RTS Art. 6.

Art. 6 Couvert | 10G-800G selon lien

⚡

ENERGIE / EAU / TRANSPORT (NIS2)

SCADA & Sous-stations électriques

Protection des réseaux SCADA et sous-stations électriques avec chiffrement post-quantique.

DIN Rail mural | -40/+70 C

☁️

CLOUD SOUVERAIN

Isolation crypto inter-tenant cloud souverain

Isolation cryptographique entre tenants dans un cloud souverain.

100% crypto | SecNumCloud ANSSI

🛡️

DEFENSE

Déploiement défense air-gapped

Chiffrement post-quantique en mode autonome pour réseaux de défense air-gapped.

Standalone Air-gapped | <100 ms

🔗

INTERCONNEXION DC

Chiffrement P2P transparent sur fibre

Chiffrement point-a-point transparent sur fibre noire ou DWDM.

Layer 2 Transparent | <1 us

🏥

SANTE / HDS

Imagerie médicale & réseaux hospitaliers

Chiffrement post-quantique des flux DICOM et réseaux inter-hospitaliers conformes HDS et NIS2.

Complète NIS2 + RGPD | <1 us

📈

FINANCE / HFT

Trading ultra-basse latence sécurisé

Chiffrement post-quantique intégré au FPGA de trading. Crypto certifiée + IP métier dans le même hardware.

<1 us | Double Crypto + Métier

Cas d'usage détaillés disponibles sur cryptops.fr/cas-usage

05 — CERTIFICATIONS

Roadmap certification ANSSI

Q3 2026
CSPN Encrypteur
Mode Standalone — CEA-Leti CESTI
35% avancement

Q4 2026
CSPN Agent
Après cert. encrypteur — CEA-Leti
10% avancement

2027
Common Criteria
EAL4+ — Architecture complète
Planifié

2027+
Qualification ANSSI
Niveau standard — ISO 27001
Planifié

CONFORMITÉ RÉGLEMENTAIRE

✓ NIS2	Chiffrement obligatoire pour les opérateurs essentiels (Art. 21)
✓ DORA	Chiffrement inter-sites bancaire + audit trail (RTS Art. 6)
✓ SecNumCloud	Isolation cryptographique inter-tenant qualifiable
✓ RGPD	Chiffrement données personnelles en transit (Art. 32)
✓ IEC 62443	Cybersécurité systèmes industriels (SL2)

⚠️ Mandat ANSSI 2027

À partir de 2027, tous les produits qualifiés ANSSI devront intégrer du chiffrement post-quantique pour conserver leur qualification. CryptOps est conçu dès le départ pour ce standard — pas de migration nécessaire.

06 — TARIFICATION

Offres commerciales

Starter

Proof of Concept

Sur devis

- ✓ 2× encrypteurs AllEyes
- ✓ 1 tunnel chiffré PQC
- ✓ Support email 5j/7
- ✓ 1 journée formation
- ✓ Durée : 90 jours
- — Dashboard temps réel
- — SLA garanti
- — GARANCE PKI

Recommandé

Pro

Déploiement opérationnel

Sur devis

- ✓ 10× encrypteurs AllEyes
- ✓ Tunnels illimités
- ✓ Dashboard CryptOps temps réel
- ✓ Support 24/7 — SLA 4h
- ✓ CSPN ANSSI (objectif Q3 2026)
- ✓ Conformité NIS2 / DORA
- — GARANCE PKI dédiée

Enterprise

OIV / Défense

Sur devis

- ✓ Encrypteurs illimités
- ✓ Architecture souveraine on-premise
- ✓ GARANCE PKI ML-DSA-87 incluse
- ✓ Contrôleur GLUON dédié
- ✓ Audits NIS2 trimestriels
- ✓ Équipe support dédiée
- ✓ EAL4+ (objectif 2027)

PARTENAIRES TECHNOLOGIQUES

AMD FPGA & Computing	**Supermicro** Serveurs haute densité	**Avnet Silica** Distribution EMEA
OVHcloud Cloud souverain FR	**Scaleway** Cloud européen	**Dassault Systèmes** Outscale SecNumCloud

Tarification détaillée sur demande — contact@cryptops.fr

Contactez-nous

Prenez rendez-vous pour une démonstration personnalisée ou recevez les spécifications techniques complètes sous NDA.

Fabrice Langlois
CEO & Fondateur
fabrice.langlois@cryptops.fr

Commercial
Demande de démo
contact@cryptops.fr

Technique
Spécifications & NDA
cryptops.fr/contact

TLS 1.3 · ML-KEM-1024 · FIPS 203/204 · CSPN cible Q3 2026 · NIS2 · DORA

Spécifications techniques complètes disponibles sur demande — contact@cryptops.fr