< GROUPE DE TRAVAIL CRYPTOGRAPHIE POST-QUANTIQUE >

< Panorama des outils de migration vers la cryptographie post-quantique >

< Panorama des outils de migration vers la cryptographie post-quantique >

A l'heure où la cryptographie post-quantique s'impose comme une priorité stratégique de cybersécurité, la communauté PQC menée au Campus Cyber propose un ensemble de livrables voués à aider décideurs, RSSI et opérationnels à orienter leurs décisions en matière de migration vers des systèmes résistants à la menace quantique. Les annonces passées par l'ANSSI, le NIST ou encore le BSI convergent vers la nécessité d'entreprendre dès aujourd'hui des processus de migrations dans chaque entreprise ou organisation devant sécuriser ses échanges et ses données sensibles sur le moyen et le long terme. Dans ce cadre, ce document propose un panel d'outils nécessaires dans les différentes étapes d'une migration post-quantique.

Le Panorama met délibérément en exergue les solutions françaises et européennes, en cohérence avec l'approche de souveraineté numérique suivie par le Campus Cyber, alliant sécurité de la donnée et efficacité des outils retenus. Ces choix seront facilement identifiables dans ce document. Si cette information permet aux lecteurs de faire le choix de la souveraineté numérique européenne plus aisément, cela ne signifie en revanche pas que les autres solutions sont techniquement moins intéressantes ou nécessairement à écarter. Elles sont également listées dans chaque onglet, à la suite des solutions françaises ou européennes. Le classement des solutions est réalisé par ordre alphabétique par nom de fournisseur.

Dans ce document, nous listons les premières briques utiles pour démarrer une migration vers une infrastructure résistante aux attaques quantiques. Cela inclut des éléments permettant d'avoir un inventaire de la cryptographie existante (e.g. inventaire et CLM) ainsi que les premiers composants à migrer, comme ils fournissent les éléments clés pour la cryptographie (i.e. librairies, HSM et PKI). D'autres solutions peuvent évidemment s'ajouter à cette étude. Ce document ayant pour but d'être mis à jour régulièrement, le groupe de travail a décidé de commencer par les éléments principaux et d'autres types de composants pourront s'ajouter au fur et à mesure des évolutions des produits (et des annonces dans le domaine de la PQC).

Le groupe de travail a rassemblé les connaissances disponibles à date, dans un domaine qui évolue très vite et à tous les niveaux. Les choix retenus sont cohérents au moment de la publication.

Le Campus Cyber remercie les contributeurs et contributrices de ce livrable pour leur expertise et leur investissement.

Rubrique	Résumé
Introduction	Présentation du document
Guide et glossaire	Sommaire & glossaire
Inventaire	Outils d'aide à l'inventaire de la cryptographie
CLM	Outils aidant la gestion des certificats utilisables dans le cadre d'un inventaire
HSM	Dispositifs matériels sécurisés pour protéger et gérer des clés cryptographiques ainsi que réaliser des opérations cryptographiques
Librairies	Librairies et SDK fournissant des briques cryptographiques
PKI	Offres PKI complètes (i.e. solutions n'offrant pas uniquement des briques cryptographiques mais aussi la structure d'une PKI : CA, gestion des certificats, etc.)
Contributeurs	Liste des entreprises ayant contribué à ce livrable

Auteur : Groupe de travail PQC Campus Cyber
Version : 1.0
Date de mise à jour : mai 2026

CAMPUS CYBER

Le document est organisé en plusieurs rubriques :

- **INVENTAIRE :** contient les outils permettant de faire un inventaire du patrimoine cryptographie selon differents paramètres : type d'assets à inventorier (clés, certificats, algorithmes etc), type de capteurs (e.g. scan du code source, scan du réseau, etc...), etc.
- **CLM :** contient les outils permettant de gérer et monitorer des certificats pendant toute leur durée de vie.
- **HSM :** contient les offres HSM existantes.
- **LIBRAIRIES :** contient les librairies (open source ou commerciales) existantes offrant des briques cryptographiques.
- **PKI :** contient des offres PKI complètes, c'est-à-dire les solutions n'offrant pas uniquement des briques cryptographiques. Pour ceci, le lecteur est invité à regarder la partie «librairies», mais aussi la structure d'une PKI (CA, gestion des certificats, etc.).

< Glossaire >

ASIC (Application-Specific Integrated Circuit)	Circuit intégré dédié à une application spécifique, souvent pour accélérer la cryptographie.
CA (Certificate Authority)	Autorité de certification délivrant des certificats numériques.
CA connectors	Connecteurs pour relier un CLM à d'autres autorités de certification.
Capteur	Logiciel ou composant matériel qui collecte et transmet des informations sur un système ou un réseau.
Catalyst / Composite	Une méthode d'hybridation pour intégrer plusieurs signatures (classique + PQC) dans un certificat (IETF "composite", "catalyst" = schémas alternatifs).
CBOM (Cryptographic Bill of Materials)	Inventaire structuré des artefacts et primitives cryptographiques utilisés dans un système.
Certificat	Mécanisme permettant de garantir l'authenticité d'une clé publique, i.e. certifier qu'une clé publique appartient à son entité présumée.
Certifications de sécurité	Normes et reconnaissances de sécurité attribuées à une solution ou une entreprise.
CI/CD (Continuous Integration/Continuous Delivery)	Pratiques et outils d'automatisation pour le développement, les tests et le déploiement de logiciels.
CLM (Certificate Lifecycle Management)	Outil de gestion du cycle de vie des certificats numériques.
Code signing	Signature numérique de logiciels ou de code.
Common Criteria (CC) EALx	Certification internationale de sécurité.
Crypto-agilité	Désigne les capacités nécessaires pour remplacer et adapter les algorithmes cryptographiques des protocoles, applications, logiciels, matériels et infrastructures sans interrompre le fonctionnement d'un système en cours d'exécution, afin d'en garantir la résilience. [NIST CSWP39]
Cryptographie classique	Cryptographie symétrique et asymétrique reposant sur des algorithmes traditionnels (RSA, ECC, AES, etc.).
Cryptographie post-quantique (PQC)	Ensemble d'algorithmes cryptographiques reposant sur des "nouveaux" problèmes mathématiques réputés résistants aux attaques d'un ordinateur quantique, conçus pour remplacer les algorithmes classiques vulnérables (RSA, ECC, DH).
CSPN (Certification de Sécurité de Premier Niveau)	Certification de sécurité de premier niveau des produits des technologies de l'information délivrée par l'ANSSI.
CycloneDX	Format standardisé d'échange de SBOM/CBOM.
Data-at-rest	Données stockées sur disque ou autre support.
Data-in-transit	Données en transit sur le réseau.
Docker, Kubernetes	Plateformes de virtualisation et d'orchestration de conteneurs.
EDR (Endpoint Detection and Response)	Outils de détection et de réponse aux menaces sur les terminaux.
EST (Enrollment over Secure Transport)	Protocole sécurisé d'enrôlement de certificats.
FIPS (Federal Information Processing Standards)	Ensemble de standards publiés (et parfois développés) par le gouvernement américain pour des applications non classifiées (non militaires).
FPGA (Field-Programmable Gate Array)	Circuit intégré programmable pour des applications matérielles spécialisées.
HSM (Hardware Security Module)	Dispositif physique permettant de générer des clés cryptographiques, de les stocker, et d'effectuer des opérations sensibles tout en garantissant la confidentialité de ces clés.
Hybridation	Approche consistant à combiner des algorithmes classiques (de type RSA, ECC...) avec des algorithmes post-quantiques (ML-DSA, SLH-DSA, ...). L'objectif est d'assurer un niveau de sécurité même si l'un des deux schémas est compromis. Plusieurs solutions d'hybridation sont possibles: composite, catalyst.
ISAE 3402	Contrôle de sécurité et gestion des risques (audit).

< SUITE >

ISO 27001	Norme internationale pour la gestion de la sécurité de l'information.
JSON (JavaScript Object Notation)	Format de données structuré pour les échanges de données.
KDF (Key Derivation Function)	Fonction servant à générer des clés à partir d'un secret.
KEM (Key Encapsulation Mechanism)	Sert à établir une clé symétrique qui sera ensuite utilisée. Remplace DH en PQC.
Keystore	Base de données sécurisée contenant des clés cryptographiques.
KMS (Key Management Service)	Service de gestion centralisée des clés cryptographiques.
MIP (Modules In Process list)	Module en attente de certification (en contexte FIPS).
MPC (Multi-Party Computation)	Cryptographie multipartite permettant à plusieurs parties de calculer une fonction sans révéler leurs entrées respectives.
Multi-CA	Gestion de certificats émis par plusieurs autorités de certification.
Multi-tenancy / Multi-tenant	Capacité à gérer plusieurs clients ou entités sur une même plateforme.
NIST SP 1800 / NIST SP 800-90A/B/C	Série de guides pratiques de cybersécurité publiés par le NIST / standards pour les générateurs de nombres aléatoires.
NITES	Certification de sécurité de Singapour.
OCSP / OCSP Responder	Online Certificate Status Protocol, vérification du statut de validité des certificats.
PCAP (Packet Capture)	Fichiers contenant des traces de trafic réseau capturées.
PCI DSS, PCI HSM, PCI PTS HSM, PCI PIN, PCI P2PE, PCI-SLC	Normes de sécurité pour le secteur des paiements.
PKCS#11	Standard d'API pour l'accès aux HSM et aux jetons cryptographiques.
PKI (Public Key Infrastructure)	Infrastructure de Gestion de Clés publiques (IGC) : ensemble organisé de composantes fournissant des services de gestion des clés publiques cryptographiques et de leurs certificats.
POC (Proof Of Concept)	Prototype ou démonstration pour valider une technologie.
QSCD	Qualified Signature Creation Device (dispositif conforme eIDAS).
SAST (Static Application Security Testing)	Outils de test de sécurité de code source.
SBOM (Software Bill of Materials)	Inventaire structuré des composants logiciels d'une application.
SOC 2	Certification de conformité sur la sécurité et la confidentialité.
TLS (Transport Layer Security) / SSL	Protocoles de sécurité pour les communications sur Internet.
TRL (Technology Readiness Level)	Niveau de maturité technologique.
VS-NfD	Certification allemande pour l'utilisation dans des environnements classifiés.
X.509	Standard de format de certificats numériques.

< Inventaire >

< INVENTAIRE : contient les outils permettant de faire un inventaire du patrimoine cryptographie selon différents paramètres : type d'assets à inventorier (clés, certificats, algorithmes etc), type de capteurs (e.g. scan du code source, scan du réseau, etc...), etc. **>**

	Nom de l'outil	Produit par	Pays	Licence	Certifications	Support d'algorithmes PQC ?	Type de capteurs inclus dans l'outil (analyse code source / binaire / autre manière ?)	Possibilité d'ajou-ter des capteurs	Possibilité de fournir des sources externes de données	Politique de sécurité configurable ?	Liste des protocoles analysables (ex : TLS, IKEv2, SSH, etc)	Compatibilité de l'outil : quels formats en entrée et en sortie (tableau, analyse, CBOM...?)	Stockage de ces données générées par l'outil	Où est faite l'analyse ?	Commentaires
FR / EU	CryptoBOM-Forge	Banco Santander	Espagne	Open Source	Non	Non	Analyse de code	Oui	Non, prend en entrée juste l'output de CodeQL	Oui	Non applicable,inventaire uniquement dans le code	Entrée : CodeQL multi-repository analysis report Sortie : CBOM (CycloneDX)	Local	On-prem	https://github.com/Santanderse-curityresearch/cryptobom-forge/tree/dev
	Compass	Cryptonext Security	FR	Propriétaire	Non	Oui	Aucun par défaut	Oui	Oui	Oui	TLS, IKEv2, SSH	Compatibilité : Architecture ouverte permettant d'intégrer à l'envie capteurs tiers et nouveaux formats de données. Entrée : dépendant du capteur (PCAP, XML, CBOM, SBOM, flux Kafka...). Sortie : exports sous forme de tableaux (csv), CBOM, rapports analytiques.	Base de données relationnelle locale.	On-prem	
	Pcert Scanner	Datawarehouse	Allemagne	Propriétaire		Non	Scan de endpoints (trustore, keystore, certificats), scan de registre et scan réseau				Network share HTTPS, FTPS, SSH, LDAP, NMAP, LDIF, Keystores	Dashboard/Excel, CBOM, SBOM	Local pour On-prem/Sur leur serveur pour SaaS	On-prem/SaaS	https://datawh.info/en/pcert/
	SSHerlock	SSH.com	Finlande	Propriétaire		Oui	Agent/script, s'appuie sur les données système et les requêtes du protocole SSH	Non	Non	Non	SSH	Entrée : gathered automatically by the tool Sortie : Detailled report (PDF, HTML)		Hybride	
	QCBOM	Synergy Quantum	Suisse+Inde	Propriétaire		Oui	Analyse binaire, et divers types de fichiers	Non	Oui	Non	TLS, SSH, VPNs;	Entrée : CycloneDX, CSV, JSON Sortie : Dashboard, CBOM, CSV, PDF	Cloud pour les déploiements SaaS, onPrem possible.	Déploiement SaaS : cloud. OnPrem possible.	TRL 9
	AgileSecGlobal	InfoSecGlobal (KeyFactor)	Canada	Propriétaire		Oui	Sonde réseau, analyse de code, analyse de binaire, intégration avec Solution de détection existente tel que Qualys		Oui, données brutes, image d'application, etc	Oui (RBAC)	Tous	Dashboard/Excel, production CBOM prévu pour S1 2026	Local pour On-prem/Sur leur serveur pour SaaS	On-prem/SaaS	PQC Assessment Tool | PQC Readiness with Cryptographic Visibility
	AVX ONE PQC As-sessment Tool	AppViewX	USA	Propriétaire	SOC2, ISO27001, PCI DSS	Oui	Analyse de code, configurations et certificats		Oui	Oui	TLS, SSH, VPN	Entrée : code, packages/deps, configs, certificates. Sortie : CBOM (CycloneDX) ou CSV	Local pour On-prem/Sur leur serveur pour SaaS	On-prem/SaaS	PQC Assessment Tool | PQC Readiness with Cryptographic Visibility
	Transparency Platform	Binarly	USA	Propriétaire		Oui	Plateforme SaaS d'analyse des fichiers binaires	Oui (via règles custom/ intégration YARA)	Oui (analyse binaire)	Oui		Entrée : fichiers binaires. Sortie : CBOM	Cloud	SaaS	L'inventaire de ressources crypto'est pas la fonctionnalité centrale de la plateforme
	Mercury	Cisco	USA	Open Source	Non	Non	Sonde réseau	Non, à part en développant son propre capteur	Limité aux trafics réseaux. Live packets streams ou fichiers PCAP	Non	TLS,/SSL, DTLS, SSH, HTTP, TCP	Entrée : Live network interface ou fichiers PCAP Sortie : JSON	Local	On-prem	https://github.com/cisco/mercury/ L'inventaire de ressources crypto n'est pas la fonctionnalité centrale de la plateforme, il est majoritairement utilisé pour lire les paquets réseau
	Key Insight	Fortanix	USA-Inde	Propriétaire		Oui						Sortie : CBOM		On-prem (databases, file systems, other internal resources) + multi-cloud (AWS-KMS; Azure Key vault) environments	Key Insight fait l'inventaire vraiment très détaillé des clefs d'un système, in situ ou dans un cloud multiple. De là l'outil peut détecter les algos pré-quantiques et identifier les vulnérabilités cryptographiques.
	IBM Quantum safe advisor	IBM	USA	Apache Licence 2.0		Oui	Code source, CBOM	n. a.	Oui, (analyse de code source + CBOM externe)	Oui	Java (JCA, BouncyCastle lightweight API), Python (pyca/cryptography)	Entrée : code source. Sortie : CBOM	Local	On-prem	Utilise Sonar Cryptography Plugin (analyse de code source, génération de CBOM), inclut en plus une interface graphique (visualisation de CBOM)
	Sonar Cryptography Plugin	IBM	USA	Apache Licence 2.0		Oui	Code source	n. a.	Oui, (analyse de code source)	Oui, programmation de règles	Java (JCA, BouncyCastle lightweight API), Python (pyca/cryptography)	Entrée : code source. Sortie : CBOM	Local	On-prem	

Nom de l'outil	Produit par	Pays	Licence	Certifications	Support d'algorithmes PQC ?	Type de capteurs inclus dans l'outil (analyse code source / binaire / autre manière ?)	Possibilité d'ajouter des capteurs	Possibilité de fournir des sources externes de données	Politique de sécurité configurable ?	Liste des protocoles analysables (ex : TLS, IKEv2, SSH, etc)	Compatibilité de l'outil : quels formats en entrée et en sortie (tableau, analyse, CBOM…?)	Stockage de ces données générées par l'outil	Où est faite l'analyse ?	Commentaires
Quantum Safe Explorer	IBM	USA	Propriétaire		Oui	Code source		Oui (analyse de code source)	Oui	C, C++, C#, Dart, Go, Java, Python	Entrée : code source. Sortie : CBOM et autres formats	Local	On-prem	
Guardium Quantum Safe	IBM	USA	Propriétaire		Oui	Code source		Oui (analyse de code source)	Oui	au moins : C, C++, C#, Dart, Go, Java, Python	Entrée : code source. Sortie : CBOM (et autres formats ?)	Local	On-prem	Utilise notamment Quantum Safe Explorer
Crypto Analytics Tool (CAT)	IBM	USA	Propriétaire		Oui	Code source, keystores		Oui (analyse de code source, keystores)	Oui		Entrée : code source, keystores.	Local	On-prem	Pour mainframes IBM Z
IBM Z® Crypto Discovery & Inventory (IBM zCDI)	IBM	USA	Propriétaire		Oui	Capteurs de : - Appels crypto des applications - Chiffrement réseau - Système	Non	Non	Oui	Tout protocole ou algorithme cryptographique qui produit un enregistrement SMF sur Z	Entrée : Z/OS subsystems (SMF log streams, ICSF data) Sortie : CBOM	Local, dans une database PostgreSQL	On-prem	Pour IBM Z https://www.ibm.com/fr-fr/products/z-crypto-discovery-inventory
Isara Advance	Isara	Canada	Propriétaire		Oui	4 types de connecteurs agentless (SGDB, Cloud KMS, source code, crypto)		Oui via fichiers pcap et connecteurs externes			Entrée : fichiers SAR, pcap, SGBD, KMS…	Option locale	Option on premise full (no phone home)	Analyse 571 primitives cryptographiques
CBOMkit-action	PQCA (Linux Foundation)	USA	Apache License 2.0		Oui	code source	Non	Oui (analyse de code source)		Java, Python	Entrée : code source. Sortie : CBOM	Local	On-prem	
Sonar-cryptography (Sonarqube)	Post-Quantum Cryptography Alliance	USA	Apache License 2.0		Oui	Code source	Non, à part en developpant son propre capteur	Oui	Non	Java, Python	Entrée : code source (Java, Python) Sortie : CBOM (CycloneDX), SonarQube UI	Local	On-prem	Plugin créé par la PQCA pour SonarQube server.
Qvision	PQStation	Singapore	Propriétaire	PCI DSS, NIST SP 1800, ISO 27000, SOC2 ...		Combinaison de capteurs légers pour endpoints et intégration avec les outils existants. Déploiement de capteurs sur serveurs, instances cloud et appareils, ou intégrer QVision à des outils EDR/de surveillance existants	Oui	Oui		SSL/TLS, SSH; IPsec, E2E	Sortie : CBOM			
CipherInsights	QuantumX-change Acheté par KeyFactor	USA	Propriétaire		Oui	Capteurs passifs de trafic réseau	Non	Oui	Non	Data-in-transit protocols	Entrée : Live network traffic fed via TAP/SPAN Sortie : Web Dashboard, CBOM, JSON, XML	Local	On-prem	https://quantumxc.com/cipherinsights/
QuProtect	QuSecure	USA	Propriétaire		Oui	Capteurs et analyse basés sur le réseau	En fonction des modules de QuSecure	Non	Oui	Data-in-transit protocols	Entrée : Network data streams (via span ports, agents, or gateway integrations) and possibly system APIs Sortie : Unified Dashboard with live inventory and analytics, CBOM, PDF			https://www.qusecure.com/quprotect/
S-CAPE	Samsung SDS	Corée	Propriétaire		Oui	Code source (static), CI/CD integration		Oui (SBOMs, Application Security Testing (SAST) tools)	Oui	Focus sur les algorithmes cryptographiques utilisés plutôt que sur l'analyse des protocoles.	Entrée : SARIF, SBOM Sortie : Dashboard, CBOM, CSV, PDF	Samsung Cloud Platform (SCP)	SaaS	
AqtiveGuard	SandboxAQ	USA	Propriétaire	ISO27001 (Sandbox), SOC2 type 1 (AQG), FedRAMP Moderate (AQG)	Oui	Analyse du code source (dynamique et statique), analyse du système de fichiers, analyse réseau, analyse binaire. Capteurs propriétaires (développés par SAQ).	Oui, (third part sensors)	Oui (si on a le code source)	Oui	TLS (incl. v1.2), SSH, VPNs	Data formats - In: CBOM, PCAP, JSON. Out Dashboard, CSV	Cloud pour les déploiements SaaS	Déploiement SaaS : cloud. Autres déploiements possibles.	Souche Cryptosense française
Tychon ACDI (Automated Cryptographic Discovery & Inventory)	Tychon	USA	Propriétaire	NSM-10 et le mandat fédéral américain PQC (HR 7535).	Oui (via TYCHON Quantum Readiness Module)	endpoint-focused + analyse des fichiers binaires	Oui	Oui		TLS (incl. v1.2), SSH, VPNs	Entrée: Signing Certificates;, Certificate Files, Encryption Libraries, Listening & Web Services, Root & User Certificates	On-prem /self-hosted	Local or Hybride	Ensemble d'outils et modules avec architecture flexible. Configurable au besoin, utilisé par DoD US. https://tychon.io/wp-content/uploads/2025/03/TYCHON_Capabilities_QR_2025_001.pdf https://tychon.io/wp-content/uploads/2025/12/TYCHON_Capabilities_QRUC_2026_001.pdf
CONTINUUM platform (ACDI)	QubitOwl	USA	Propriétaire		Oui (FIPS 203, 204, 205)	Analyse de système via des agents (données au repos / data-at-rest), analyse réseau passive (données en transit / data-in-transit).	Oui	Oui	Oui	TLS, SSH	Scan basé sur le système avec primitives cryptographiques réseau. Import/Export de CBOM CycloneDX (JSON), CSV ou PDF.	Cloud (SaaS), ou Déploiement Self-hosted	Hybride (Analyse hybride entre les capteurs locaux et l'agrégation/hiérarchisation des risques sur la plateforme.)	

< CLM : contient les outils permettant de gérer et monitorer des certificats pendant toute leur durée de vie **>**

	Outil	Produit par	Pays	PQC ready ?	Visualisation des certificats (tableau central ? Personnalisable ?)	Scoring (personnalisable?) des certificats	Types de certificats gérés (uniquement SSL, gère d'autres certificats ?)	Certifications de sécurité	On-Prem / SaaS	Protocoles d'automatisation supportés	Découverte de certificats (scan dns, scan réseau...?)	Commentaire
FR / EU	BerryCert	DigitalBerry	France	Prévu S2 2026	Dashboard personnalisable	Oui	Tous types de certificats	Membre d'hexatrust	On-Prem	SCEP, ACME, CMP, Protocoles propriétaires API REST		
	Horizon	Evertrust	France	Prévu	Dashboard personnalisable	Oui	Tous types de certificats	Solution PKI Stream possède une certification CSPN de l'ANSSI	On-Prem & SaaS	SCEP, ACME, CMP, EST, WCCE, Protocoles propriétaires API REST	Scans réseaux (sondes), services cloud, conteneurs, endpoints, interfacage avec scanner de vulnérabilités existants tels que qualys	Partenariat avec CryptoNext pour l'inventaire
	ZeroSSL	HID Global (filiale)	Autriche	Non	Management Console	Non	Certificats SSL/TLS	NA	SaaS : C'est une AC qui permet le management automatique et centralisé de certificat	ACME et API REST		
	Keytalk PKI management solutions	KeyTalk	Pays-Bas	Oui pour Keytalk CKMS (pas confirmé pour les autres composants)	Dashboard	Non	Tous types de certificats TLS/SSL, S/MIME, document signing, device certs, X.509, VPN	Unknown	On-Prem & SaaS & Hybrid	ACME, SCEP, Protocoles propriétaires API REST	Scans réseaux, importation manuel	
	Nexus – M2Trust	Nexus	France - Allemagne	Oui - Version 8.12 disponible depuis avril 2025 • Support ML-DSA (FIPS 204 / Dilithium) et SLH-DSA (FIPS 205 / SPHINCS+) • Juin 2025 : Support ML-KEM (FIPS 203 / Kyber) pour TLS + PKCS#11 PQC Thales Luna HSM • Q4 2025 : Support format hybride X.509 + PKCS#11 v3.2 standard • H1 2026 : Support FIPS 206 (FN-DSA / Falcon) + clés composites potentielles	Tableau central via Certificate Controller • Filtres de recherche personnalisables (par protocole d'enrollment, statut, dates, etc.) • Interfaces multiples : Web UI, clients Java, API REST • Metrics via InfluxDB et visualisation Grafana	Oui	**Tous types de certificats X.509** • SSL/TLS pour serveurs et communications sécurisées • Certificats utilisateurs (workforce) pour authentification Windows et applications • IoT et équipements réseau (routers, firewalls, machines industrielles) • Véhicules connectés (V2X - Vehicle-to-Everything) • Code signing et signature de documents • Email encryption (S/MIME) • Support multi-CA et multi-tenancy (plusieurs domaines Windows, plusieurs clients)	• Common Criteria EAL4+ pour PKI (Certificate Manager) et OCSP Responder • Organisation conforme ISO 27001 (gestion de la sécurité de l'information) • TISAX (Trusted Information Security Assessment Exchange) pour l'industrie automobile • Principe des 4 yeux obligatoire pour tous les changements de politique critique • Protection PKI de toutes les étapes avec certificats d'officiers dédiés	**Les deux modèles disponibles** • On-Premise : Installation complète sur infrastructure client • SaaS/Service : Offert en tant que service avec SLA garanti et capacité évolutive • Architecture hautement performante et scalable (plusieurs milliards de certificats par an)	**Support complet de tous les protocoles d'enrollment standard** • ACME (RFC 8555) - Automatic Certificate Management Environment • SCEP - Simple Certificate Enrollment Protocol (avec support Microsoft Intune) • EST - Enrollment over Secure Transport • EST-CoAPS - EST over Constrained Application Protocol Secure • CMP - Certificate Management Protocol • CMC - Certificate Management over CMS • REST API complète pour intégration DevOps et automatisation custom **Fonctionnalités avancées :** • Pré-enregistrement des devices pour sécurisation de l'enrollment automatisé • Support Docker, Kubernetes et environnements virtualisés	Scans réseaux	
	AVX One	AppViewX	USA	Oui	Dashboard	Oui	TLS, code signing, SSH, device, PKI	ISO 27001, SOC2,	On-Prem, SaaS, private cloud	ACME, SCEP, EST, CMP, Protocoles propriétaires API REST		
	CertM	Com-SignTrust	Israël	Oui	Dashboard personnalisable Filtres personnalisables Graphs reports	Non	Tous types de certificats	ISO 27001	On-Prem & SaaS	Inconnu	Analyse réseau basée sur des agents périodiques	Utilise des HSM Luna certifiés FIPS 140-2 Israel et non Belgique
	Venafi	CyberArk	Israël	Oui	Dashboard personnalisable	Oui, personnalisable "Indicateurs de risques par certificat (avec paramètres configurables)	Tous types de certificats : SSL/TLS, SSH, code signing, device/client certificates	ISO 27001, SOC2 , Common Criteria	On-Prem & SaaS & Hybrid	ACME, SCEP, EST, Protocoles propriétaires API REST	Scan réseau (ip & DNS), agent-based local scanning, targeted device/cloud inventory integrations	
	Trust Lifecycle Manager	Digicert	USA	ML-DSA (pure PQC, composite), SLH-DSA (pure PQC)	Oui	Oui	X.509	WebTrust, SOC 2, EU QTSP, ISO 27001, ISAE 3402 (company, not a specific product)	On-Prem & SaaS	ACME, EST, SCEP, CMPv2	Certificate discovery	

< Suite >

Outil	Produit par	Pays	PQC ready ?	Visualisation des certificats (tableau central ? Personnalisable ?)	Scoring (personnalisable?) des certificats.	Types de certificats gérés (uniquement SSL, gère d'autres certificats ?)	Certifications de sécurité	On-Prem / SaaS	Protocoles d'automatisation supportés	Découverte de certi-ficats (scan dns, scan réseau...?)	Commentaire
Device Trust Manager	Digicert	USA	ML-DSA, SLH-DSA (pure PQC)	Oui	Non	X.509	WebTrust, SOC 2, EU QTSP, ISO 27001, ISAE 3402 (company, not a specific product)	On-Prem & SaaS	REST, EST, SCEP, CMPv2, ACME		
Certsecure manager	Encryption-Consulting	USA	Inconnu	Dashboard		Tous types de certificats, mais voir rubrique "divers"	ISO 27001, SOC	On-Prem, cloud-based, Saas. Hybrid	REST APIs, SCEP, ACME, EST	Scan réseau	Restreint l'accès aux autorités de certification (publiques et privées) ; impose la conformité FIPS
Entrust Certificate hub	Entrust	USA	Oui (hybride & pure PQC)	Dashboard personnalisable	Non	Tous types de certificats TLS, S/MIME, code signing, document signing, IoT and device certs, X.509	ISO 27001	On-Prem & SaaS	ACME, EST, INTUNE, MDMWS, SCEP, WSTEP, Protocoles propriétaires API REST	Network scanning, CA connectors, Manual Import API, Other sources (F5, KMS...)	
Certification automation manager	GlobalSign	Japon	Prévu	Dashboard personnalisable	Non	Tous types de certificats TLS/SSL, S/MIME, code signing, document signing, IoT and device certs, X.509	ISO 27001	Hybrid	ACME, SCEP, Protocoles propriétaires API REST	Network scanning	
Enterprise SSL	HID Global	USA	Oui	Oui			ISO 27001, SOC2, PCI-DSS, PCI-SLC	On-Prem, hybrid, multi-cloud	ACME, SCET, EST, API REST		
Command	Keyfactor (PrimeKey)	USA	Oui	Dashboard personnalisable	Oui	Tous types de certificats	EJBCA certifié Common Criteria, Keyfactor ISO27001	On-Prem & SaaS	SCEP, ACME, CMP, EST, Protocoles propriétaires API REST		
Key Manager Plus	ManageEngine	USA	Seemingly no	Dashboard customizable	Non	X.509 (+ clés SSH, clés PGP)		On-Prem	ACME	Certificate discovery	
Sectigo	Sectigo	USA	Oui	Dashboard personnalisable		Tous types de certificats TLS, S/MIME, code signing, document signing, device certs, X.509	ISO 27001 PCI DSS	SaaS	SCEP, ACME, EST, Protocoles propriétaires API REST	Agents d'analyse du réseau interne, analyses AD	
Segura Certificate Manager	Segura	Brésil	Inconnu	"Dashboard personnali-sable Filtres personnalisables"	Oui	Tous types de certificats : SSL/TLS, X.509, SSH keys, A1/A3 smartcards certs	FIPS 140-2, ISO 27001/27701	On-Prem & SaaS	ACME, Protocoles propriétaires API REST SCEP, CMP ?	Scan Réseau, DNS, répertoires Périodique/manuel	
TrustAsia - CertCloud (Chine)	TrusAsia	Chine	Inconnu	-	Oui	Multiples types : SSL/TLS, Code Signing (signature de code), Document Signing (signature de documents PDF/Office), S/MIME (certificats email), certificats OV/EV. Gère également des certificats de multiples CA (multi-CA certificate discovery).	WebTrust : Certification Authority, BR-SSL, Extended Validation, Code Signing	On-Prem & SaaS & Hybrid	ACME, REST API (OPENAPI), Command line (ligne de commande), PartnerAPI. Support également de l'intégration avec des serveurs web mainstream et divers dispositifs gateway.	-	

< **HSM** : contient les offres HSM existantes >

	Outil	Produit par	Pays	Détail	Prise en compte des algorithmes PQC	Framework crypto-agile ?	Certifications et visas de sécurité	Informations complémentaires (protocoles pris en charge, hébergement)
FR / EU	Eviden Proteccio HSM (anciennement Trustway)	Eviden	France	Cas d'usages : signature et chiffrement de données sensibles, gestion PKI, authentification et contrôle d'accès, protection des transactions et intégrité applicative, sécurisation des services cloud, conformité réglementaire et souveraineté	Oui, ML-DSA, ML-KEM, SLH-DSA	Oui, via intégration logicielle (CryptoNext, OQS)	Qualification renforcée (QR) ANSSI (pour certains modèles), Common Criteria EAL4+ (produit évalué), EU-R, NATO restricted	
	Eviden Crypt2pay HSM (anciennement Trustway)	Eviden	France	Sécurité des transactions et émission de cartes, paiement mobile, par internet, compteurs intelligents et objets connectés	Non	Non	FIPS 140-2 Level3+, PCI PTS, GIE-CB	
	Protect server	Gemalto (avant fusion avec Thales)	France	Encore utilisé dans certains environnements.	Non	Oui, firmware	"FIPS 140-2 Level 3 FIPS 140-3 en cours"	
	NetHSM	Nitrokey	Allemagne	HSM open source, orienté PME, facile à intégrer.	Non (en roadmap, pas de date publique)	Oui, open source et extensible	Non, en roadmap	
	Primus HSM CyberVault	Securosys	Suisse	Bare metal HSM	Oui, ML-DSA, SLH-DSA, ML-KEM, HSS/LMS, XMS		FIPS140-3 Level 3 ; Common Criteria EAL4+ (in certification): CC EN 419221-5 eIDAS protection profile, CC EN 419241-2 Sole Control (SAM)	
	Thales payShield HSM	Thales	France	(spécifique au secteur bancaire et aux paiements)	Non	Non	PCI HSM, FIPS 140-2 Lvl 3, CC EAL4+	
	Luna PCIe / Luna T-Series (Luna HSM 7 / T-Series PCIe)	Thales	France	Module/firmware PQC (PQC functionality module, ML-KEM / ML-DSA, hybrid PQ schemes, et support ajouté dans firmwares/clients récents). Mise en œuvre via firmware / client (in-field).	Oui	Oui	FIPS 140-2 Level 3 / FIPS 140-3 Level 3 (selon modèle et firmware validé), Common Criteria (selon configuration), conformité eIDAS possible (QSCD selon modèle)	
	U.trust / CryptoServer Se-Series (PCIe cards)	Utimaco	Allemagne	Application package / extension PQC (firmware/app package) pour ajouter algorithmes post-quantiques aux modèles PCIe. Annoncé comme solution de transition PQC	Oui, extension logiciel pour transition PQC	Oui, via logiciel et firmware	FIPS 140-2 Level 3 (et autres variantes selon modèle), Common Criteria (selon configuration), VS-NfD (version approuvée BSI pour usages classifiés), eIDAS / conformité réglementaire selon packaging.	
	u.trust General Purpose HSM	Utimaco	Allemagne	HSM dédié avec fonctionnalité multi-tenant évolutive. Son architecture basée sur des conteneurs prend en charge jusqu'à 31 conteneurs et offre une flexibilité pour divers cas d'usage, notamment la cryptographie post-quantique (PQC), la 5G, la blockchain et les applications personnalisées	Oui	oui	FIPS 140-2 Level 3, NITES (Singapore), PCI PTS HSM v3, Common Criteria ET [FIPS 140-3 (Level 3) - EN COURS]	
	Ultimaco security server	Utimaco	Allemagne	Utimaco SecurityServer / uTrust	Quantum Protect est le package pour les algorithmes PQC: ML-KEM, ML-DSA, LMS/HSS et XMSS/XMSS-MT	Mise à jour sur site		
	CryptoServer SDK	(WIBU-SYSTEMS) / Utimaco IS	Allemagne	HSM pour la protection de la propriété intellectuelle et la gestion de licences logicielles.	Oui, via le package "quantum connect"	Plateforme "crypto server"	FIPS 140-2 niveau 3, d'autres possibles à vérifier	
	Yubi HSM 2	Yubico	Suède - USA	HSM format USB (format compact, usage pour serveurs/applications de taille moyenne)	Non		FIPS 140-2	Algorithmes non PQC (RSA, ECDSA, EdDSA, ECDH) + AES, SHA1, SHA2, HMAC
	NitroX HSM	Cavium (Marvell)	USA	Destiné aux applications réseau, appliances de sécurité, accélération cryptographique.	Non (en roadmap, pas de date publique)	Non	FIPS 140-2 Level 3	
	QXHSM	Crypto4A	Canada	Nouvelle génération de HSM orientés post-quantique, pour clouds hybrides.	Oui	PKCS#11, Microsoft CAPI and CNG, OpenSSL, REST API, gRPC, Java (JCA/JCE); Extensible RESP API for HSM Lifecycle Management	FIPS 140-2 niveau 3+ ; FIPS 140 niveau 2 (MIP) en attente ; NIST SP 800-90A et NIST SP 800-90B ; certificat PQC CAVP du NIST.	Prise en charge de tous les algorithmes standardisés par le NIST :ML-KEM (FIPS-203), ML-DSA (FIPS-204), SLH-DSA (FIPS-205), LMS : toutes les variantes SHA2/SHAKE (RFC 8554), HSS : tous les formats jusqu'à 8 sous-arborescences, XMSS/XMSSMT : toutes les variantes telles que définies dans la RFC 8391, KDF hybrides (SP800-56C), McEliece, futurs algorithmes pris en charge grâce à des mises à jour de micrologiciels sécurisés contre les attaques quantiques,la plupart des algorithmes symétriques/asymétriques classiques, ainsi que les KDF et les RNG. Hébergement : environnements sur site, hybrides, cloud
	ePass2003	Feitian Technologies	Chine	USB-based cryptographic token for secure storage of keys and certificates			FIPS 140-2, Common Criteria EAL 5+	"API PKCS#11 version 2.40, clés RSA 2048, 3072 et 4096 bits (avec e=65537), signature PKCS#1v1.5, OAEP et PSS, SHA-256, SHA-384, SHA-512, SHA-1. Cryptographie à courbe elliptique (ECC) : Courbes : secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, Ed25519 ; Signature ECDSA (toutes sauf Ed25519), EdDSA (Ed25519 uniquement) ; Dérivation de clé ECDH (toutes sauf Ed25519)"
	Servsec	Feitian Technologies	Chine	Utilisé dans l'APAC, pour la sécurité des transactions et l'authentification.				
	Excrypt HSM	Futurex	USA	HSM "tous usages" et paiements	Oui, ML-DSA, ML-KEM, SLH-DSA		PCI DSS, PCI PTS HSM, PCI PIN, PCI P2PE, FIPS 140-2 Level 3, ANSI X9.24 part 1 and 2 – TR-39, et FCC part 15 – class B.	
	RT645	Rambus	USA	Embedded HSM (automotive applications: integration into automotive semiconductors)	Oui (optionnel)		ISO 26262, ISO 21434	LMS, XMSS, ML-KEM, ML-DSA, AES (tous les modes), SHA-1/2/3 (tous les modes), HMAC et CMAC, RSA jusqu'à 4K, ECC jusqu'à 521 bits, ECDSA, EdDSA, RSA, signature/vérification SM2D-SA, générateur de bits aléatoires SP 800-90a/b/c , SM-2-3-4

< Suite >

Outil	Produit par	Pays	Détail	Prise en compte des algorithmes PQC	Framework crypto-agile ?	Certifications et visas de sécurité	Informations complémentaires (protocoles pris en charge, hébergement)
CryptoManager RT-7xx HSM	Rambus	USA	HSM intégrés, conçus pour applications embarquées et industriels (dans le secteur automobile par exemple)	Oui		ISO 26262 (sécurité fonctionnelle automobile) ISO 21434 (cybersécurité automobile)	EVITA, SHE, TPM (spécifique à automobile)
Unbound CORE	Unbound Security (racheté par Coinbase)	Israël	HSM virtuel reposant sur la cryptographie multipartite (MPC), pas d'appliance physique nécessaire. Permet une gestion centralisée des clefs avec une haute vision sur la conformité	La MPC est une technologie résiliente à la menace quantique, mais pas d'autres communications faites		FIPS 140-2 Level 1 et 2	PKCS11, JCE, SunPKCS11, Docker, API REST
Sansec	Sansec	Chine		Oui, Kyber, Dilithium, Falcon, Sphincs+	Oui, via logiciel et firmware	FIPS 140-2 Level 3 FIPS 140-3 en cours	
Fortanix Self-Defending Key Management Service (SDKMS)	Fortanix	USA	HSM logiciel virtualisable pour clouds privés/publics.	Oui, ML-KEM, ML-DSA, en cours	Hybride, avec "PQC Central", inclus la découverte	FIPS 140-2 niveau 3	
nShield 5s (PCIe cards)	Entrust	USA	positionnement « Post-Quantum Ready » — SDK / outils et mises à jour pour intégrer algorithmes PQC standardisés	Oui, via mises à jour	Oui, SDK et firmware	FIPS 140-3 Level 3 (validation obtenue pour la famille nShield 5), Common Criteria EAL4+ (selon modèle), status QSCD / eIDAS pour certains usages	
4770 (PCIe Cryptographic Coprocessor)	IBM	USA	Produit hautement sécurisé et programmable (PCIe). IBM fournit frameworks et firmare évolutifs. L'IBM 4770 est le HSM PCIe le plus récent de la gamme IBM et le premier à intégrer des capacités cryptographiques post quantiques. Il s'agit d'un HSM PCIe programmable, doté d'un FPGA reconfigurable, permettant l'accélération matérielle et l'intégration native d'algorithmes PQC.	Oui, ML-DSA, ML-KEM	Oui, via intégration logicielle	FIPS 140-2 Level 4, Common Criteria selon implémentation	Page officielle IBM – PCIe Cryptographic Coprocessors (incluant le 4770) https://www.ibm.com/products/pcie-cryptographic-co-processor
	AWS		Service HSM managé dans le cloud d'Amazon Web Services (Cavium/Marvell)				
Microchip ATECC608A (IoT / embarqué)							
IBM Cloud HSM	IBM		Fournisseur HSM: Gemalto (Thales)				
IBM 4767 PCIe Cryptographic Coprocessor							
Google Cloud HSM	Google		Service HSM managé dans Google Cloud Platform --> Hardware par Cavium Marvell				
Azure Key Vault Premium	Microsoft		Fournisseur hardware: Marvell LiquidSecurity				
Azure Dedicated HSM	Microsoft		Fournisseur hardware: Thales SafeNet Luna				
Azure Key Vault Managed HSM	Microsoft		Fournisseur hardware: Marvell LiquidSecurity				
Azure Payment HSM	Microsoft		Fournisseur hardware: Thales payShield 10K				
Azure Cloud HSM	Microsoft		Fournisseur hardware: Marvell LiquidSecurity				
Azure integrated HSM	Microsoft		Fournisseur hardware: Microsoft custom chips	Oui, via Adams Bridge, intégré dans Caliptra 2.0 dans le cadre de la stratégie quantum-safe de Microsoft		FIPS 140-3 Level 3	
ATECC608A / ATECC608B	Microchip	USA	HSM embarqués pour objets connectés (IoT), sécurisation de microcontrôleurs.	Non	Non		

< LIBRAIRIES >

< LIBRAIRIES : contient les librairies (open source ou commerciales) existantes offrant des briques cryptographiques **>**

	Outil	Produit par	Pays	SDK / Librairie	Langages	Licence		Usage	Hybridation	Description
	MLDS-B235	BERTEN	Espagne			Propriétaire		FPGA / ASIC		Kyber (hardware)
FR / EU	MLKE-B135	BERTEN	Espagne			Propriétaire		FPGA / ASIC		ML-KEM (hardware)
FR / EU	Quantum-Safe Library	CryptoNext Security	France	Librairie	C, C++ et Assembleur (+ wrappers: Go, Rust, Python et Java)	Propriétaire. Souscription annuelle donnant droit d'utilisation		Provider software, Provider pour l'embarqué (architectures hybrides SW/HW)	Oui	Algorithmes d'échange de clés (ML-KEM, FrodoKEM) et de signature (ML-DSA, SLH-DSA, Falcon, XMSS)
FR / EU	SphereIDEMIA Secure Transactions	IDEMIA	France	Librairie				Secure Transactions		Ensemble d'algorithmes classiques et post-quantiques standardisés. Conçu pour une cryptographie performante en conditions réelles.ML-KEM, ML-DSA, SLH-DSA, LMS.
FR / EU	LibCryptyQ	PortyQ	France	Librairie	C	Propriétaire		SW		
FR / EU	CryptyQ Provider	PortyQ	France			Propriétaire		SW		
	Embedded with LibCryptyQ	PortyQ	France	Lib embarquée	C – Assembleur	Propriétaire		Embarqué		
	PQCryptoLib-Core	PQ Shield	Royaume-Uni	Librairie				SW	Oui	ML-KEM, ML-DSA, Falcon, SPHINCS+
	PQCryptoLib-SDK	PQ Shield	Royaume-Uni	SDK				SW	Oui	Même set PQShield
	Botan	Botan	Australie	Librairie	C++	Open-source, BSD-2		SW		ML-KEM, Dilithium, Falcon (selon compil.)
	CAST	CAST Inc	USA			Propriétaire		FPGA / ASIC		ML-KEM
	BSAF Crypto Module for C	Dell Technologies	USA	SDK		Propriétaire		SW		Crypto Module Quantum-Resistant Plugin 3.0 permet le support de ML-DSA et et la vérification de signatures créé avec LMS
	Dell BSAF Crypto-J	Dell Technologies	USA	SDK		Propriétaire		SW		La version 7.1 inclut ML-DSA, et vérification de la signature HSS/LMS.
	TrustCore SDK	DigiCert	USA	SDK		Propriétaire		SW		Kyber, Dilithium (TLS cert.)

< Suite >

	Outil	Produit par	Pays	SDK / Librairie	Langages	Licence		Usage	Hybridation	Description
	nShield	Entrust Option Pack	USA	SDK + HSM		Propriétaire		HSM		Kit de développement logiciel (SDK) permettant d'accéder à la PQC via les Modules Matériels de Sécurité (HSM) nShield, intégrant la PQC au niveau du firmware.Algorithmes PQC standardisés (via accélération matérielle).
	Bouncy Castle	Keyfactor	USA	Librairie	Java, C#	Open-source, MIT		SW	Oui	Très populaire pour les applications Java et .NET. Le support PQC est ajouté au fil des mises à jour, notamment pour les schémas de signature et d'échange de clés PQC. ML-KEM, Dilithium (beta)
	Liboqs	Open Quantum Safe		Librairie	C	Open-source, MIT		SW	Oui	ML-KEM, ML-DSA, Falcon, SPHINCS+, FrodoKEM...
	OpenSSL	OpenSSL		Librairie	C	Open-source, Apache		SW	Oui	ML-KEM (TLS hybrid), ML-DSA (en cours)
	Libssl	OpenSSL		Librairie	C	Open-source, Apache		SW	Oui	Intégration en cours/avancée. Une des librairies les plus utilisées. Support PQC en cours d'intégration via OpenSSL-PQC ou directement dans les versions récentes pour permettre des connexions TLS/KEM hybrides (par exemple, x25519-kyber).
	PQClean	PQClean		Librairie	C - Assembleur	Open-source, CC0		SW		ML-KEM, ML-DSA, SPHINCS+, Falcon
	PQCP	PQ Code Package (PQC Alliance)		Librairie	C – Assembleur					ML-KEM native
	PQMicroLib-Core	PQ Shield	Royaume-Uni	Librairie microcontrôleurs				Embarqué	Oui	ML-KEM, ML-DSA optimisés embedded
	CryptoComply PQTLS	Safe Logic	USA	SDK		Propriétaire		TLS		ML-KEM
	Secure-IC	Secure-IC	USA		C			Embarqué		ML-KEM embedded acceleration
	TQ42	Terra Quantum		Librairie				SW		ML-KEM, ML-DSA, SLH-DSA, Falcon.Librairie de Terra Quantum. Se positionne comme l'une des librairies open source les plus complètes et est alignée sur les normes FIPS du NIST.
	wolfSSL	wolfSSL	USA	Librairie	C	Open-source, GPLv2/commercial		SW/Embarqué	Oui	Support existant Petite, rapide, conçue pour l'embarqué. Propose un support des algorithmes PQC du NIST (Kyber, Dilithium, Falcon, SPHINCS+) et offre une option de mode hybride (classique + PQC).
	libsodium			Librairie	C	Open-source, ISC		SW		Une librairie axée sur la facilité d'utilisation et la robustesse. Traditionnellement moins à la pointe sur l'intégration rapide des PQC par rapport aux librairies TLS, mais des extensions ou forks peuvent exister.
	NET		USA			Propriétaire		SW	Oui	Intégration native. MLKem, MLDsa, SlhDsa.Les versions récentes de .NET (comme .NET 10) intègrent des types natifs pour les algorithmes PQC, s'appuyant sur les capacités de Windows CNG ou OpenSSL.
						Ci-dessous nous proposons une liste d'outils liés à des usages spécifiques qui seront précisés.				
	BoringSSL	Google	USA	Librairie	C++	Open-source (partiel), Apache		SW	Oui	Intégration avancée Librairie développée par Google, utilisée dans Chrome et Android. A été précurseur dans les tests de KEM hybrides (comme Kyber-based KEM) dans TLS pour une résistance quantique anticipée. BoringSSL est un fork de OpenSSL créé pour les besoins de Google spécifiquement. Il n'est pas recommandé d'en dépendre.

< PKI : contient des offres PKI complètes (i.e. solutions n'offrant pas uniquement des briques cryptographiques - pour ceci, le lecteur est invité à regarder la feuille «librairies», mais aussi la structure d'une PKI (CA, gestion des certificats, etc...) **>**

	Nom de l'outil	Produit par	Pays	Licence	Certifications	Algorithmes PQC	Support d'hybridation (et méthode choisie)	On-Prem / SaaS	Commentaires	
FR / EU	ADSS PKI server	Ascertia	Royaume-Uni	Propriétaire	EAL4+ ALC_FLR.3	RSA & ECDSA, FIPS 204 (CRYSTALS Dillithium), FIPS 203 (Kyber), FIPS 205 (SPHINCS+), Classic McEliece		On-Prem, Private Cloud or hybrid models	Met à disposition un PQC Starter Kit and Proof of Concept (POC) pour exploration, tests et préparation à la transition	
	CZERTAINLY	CZERTAINLY	Tchéquie	Open Source Commercial (MIT License)		ML-DSA, ML-KEM, SLH-DSA	Composite/Catalyst	On-Prem	https://github.com/CZERTAINLY/CZERTAINLY	
	STREAM/HORIZON	Evertrust	France	Propriétaire	CSPN	ML-DSA, ML-KEM, SLH-DSA, Falcon, XMSS/LMS	Support alternative signature (catalyst)	On-Prem & SaaS		
	Eviden PKI (anciennement IDnomic)	Eviden	France	Propriétaire	Common Criteria EAL4+	ML-DSA	Pure PQC + catalyste	On-Prem & SaaS	Outil PQC didactique disponible en ligne: PQC-Explorer	
	Nexus Certificate Manager PKI	Nexus Group / In Groupe	France	Propriétaire	CC EAL4+ certi-fication for PKI + OCSP	supporte les algorithmes PQC standardisés par le NIST à date, FIPS 206 en cours	X.509 alternative signature support. Support: Traditional signature (X.509) + alternative (FIPS-204 / FIPS-205)	On-Prem & SaaS	Supporte les HSM qui fournissent un driver PCKS#11 A savoir, IN groupe proposent des solutions pour compléter la PKI - Nexus IDM Credential Manager - Nexus – M2Trust CLM Certificate Lifecycle Management	
	Cara	MTG	Allemagne	Propriétaire	BSI TR-03145 ISO 27001 Common Criteria EAL4+	ML-DSA,SLH-DSA, Falcon, XMSS, McEliece, SPHINCS+	Non documentée publiquement, a priori ne supporte pas catalyst d'après la matrice du PKI Consortium (hafeda)	Saas	Cara n'est disponible que via l'offre managée avec DARZ qui fournit l'infrastructure, la gestion, la maintenance et le support	
	CLM	MTG	Allemagne	Propriétaire	Aucune mentionnée publiquement	Supporte les algorithmes PQC standardisés par le NIST à date	Support des certificats hybrides et des certificats ML-DSA, avec support SLH-DSA "à venir" Pas d'information publique sur la methode	On-Prem et cloud environments	La prise en main est gratuite avec le forfait GRATUIT. Avec le forfait BUSINESS, vous pouvez évoluer de manière flexible par tranches de 500 certificats jusqu'à 10 000 certificats. Pour les environnements plus importants, le forfait ENTERPRISE propose des tarifs dégressifs attractifs, où le coût par certificat diminue considérablement à mesure que les quantités augmentent. Il existe une offre managée : DARZ Managed PKI & CLM powered by MTG ISO 27001 – Système de Management de la Sécurité de l'Information certifié. BSI C5 Type 2 – Critères de sécurité des services cloud selon l'Agence fédérale allemande de sécurité informatique. EN 50600 CAT III – Norme européenne pour la disponibilité et sécurité des centres de données. BSI TR-03145 – Norme technique allemande pour Trusted Service Systems / eIDAS-like frameworks. "	

< Suite >

Nom de l'outil	Produit par	Pays	Licence	Certifications	Algorithmes PQC	Support d'hybridation (et méthode choisie)	On-Prem / SaaS	Commentaires	
XiPKI	XiPKI	Allemagne	Open Source (Apache 2.0)	Dépend du déploiement	MLDSA, MLKEM	Oui	On-Prem		
EJBCA	Keyfactor	USA	Dual-license (Open Source LGPL & Enterprise)	Common Criteria EAL4+	ML-DSA, ML-KEM, SLH-DSA, Falcon, LMS, XMSS	Support alternative signature (catalyst) et Composite (IETF, ex : RSA + ML-DSA)	On-Prem & SaaS	Keyfactor propose un "PQC Lab" permettant de tester concrètement l'émission de certificats racines ML-DSA et leur déploiement au sein d'architectures TLS complexes.	Keyfactor propose un "PQC Lab" permettant de tester concrètement l'émission de certificats racines ML-DSA et leur déploiement au sein d'architectures TLS complexes.
AVX ONE PKIaaS	AppViewX	USA	Propriétaire	Aucune mentionnée publiquement	FIPS 204 (CRYSTALS-Dilithium), FIPS 205 (SPHINCS+), Falcon.	Pas explicitement	SaaS		
Khatim PKI Server	Codegic	Pakistan	Propriétaire	ISO 27001	ML-DSA ML-KEM, SLH-DSA en roadmap	Support d'hybridation (méthode inconnue)	On-Prem & SaaS	Documentation : https://www.codegic.com/wp-content/uploads/2026/03/Khatim-PKI-Server-datasheet.pdf	Documentation : https://www.codegic.com/wp-content/uploads/2026/03/Khatim-PKI-Server-datasheet.pdf
Private CA	Digicert	USA	propriétaire	ISO 27001 et SOC 2 (Digicert)	ML-DSA, SLH-DSA pour la signature, ML-KEM et FN-DSA en étude	Composite en étude	On-Prem & SaaS	https://dpcs.digicert.com/en/digicert-private-ca.html	
Step-ca	Smallstep	USA	Open Source (Apache 2.0)	Aucune native (dépend HSM)	Support PQC expérimental (GO crypto / ML-KEM en cours)	Oui	On-Prem	voir le github commentaire https://github.com/smallstep/certificates/discussions/1395#discussioncomment-12721491	
ADCS	Microsoft	USA	propriétaire		ML-KEM/ML-DSA à partir de Windows Server 2025 / Windows 11	Prévu pour S1 2026	On-Prem	https://learn.microsoft.com/fr-fr/windows-server/identity/ad-cs/	

< REMERCIEMENTS >

Merci aux contributeurs du Groupe de travail :
Air France KLM, Banque de France, BNP Paribas, CryptoNext Security, ENSTA (Ecole Nationale Supérieure des Techniques Avancées), Eviden, HeadMind Partners, Orange Cyberdefense, Portyq, QuRISK

CAMPUS CYBER

POUR EN SAVOIR PLUS : WIKI.CAMPUSCYBER.FR
ADRESSE MAIL DE CONTACT : COMMUNAUTES@CAMPUSCYBER.FR
5 - 7 RUE BELLINI 92800, PUTEAUX

Ce projet a été financé par le gouvernement dans le cadre du Programme d’investissements d’avenir.