QuantumLock

Preuve cryptographique post-quantique pour l'IA critique et les décisions souveraines

Livre Blanc Institutionnel

SoftQuantus innovative OÜ

Registre des entreprises : 17048927
https://softquantus.com

Version 1.0 Janvier 2026

Table des matières

Résumé exécutif

L'intégration croissante de systèmes d'intelligence artificielle dans les domaines de la défense, de la sécurité et de l'espace impose une exigence nouvelle, juridique et institutionnelle : la capacité à démontrer, dans le temps long, l'intégrité, la traçabilité et la légitimité des décisions algorithmiques critiques.

QuantumLock est un système de preuve cryptographique post-quantique conçu pour transformer les traitements d'IA en objets de preuve vérifiable, exploitables en environnement souverain, classifié ou air-gapped.

Points clés

- **Conformité légale** : Répond aux exigences de l'AI Act européen (Art. 12) concernant la traçabilité et le record-keeping
- **Sécurité post-quantique** : Protection contre la menace ń harvest now, decrypt later ż via les standards NIST/ETSI/ANSSI
- **Souveraineté numérique** : Déploiement on-premise, air-gapped, sans dépendance cloud
- **Preuve juridique robuste** : Artefacts vérifiables indépendamment, exploitables en audit institutionnel

1 Contexte et enjeux souverains

1.1 L'IA dans les domaines critiques de l'État

Les systèmes d'intelligence artificielle sont désormais déployés dans des contextes où les décisions engagent la sécurité nationale, la défense territoriale et la souveraineté technologique de l'État :

— **Défense et opérations militaires** : Analyse de renseignement, aide à la décision tactique, systèmes autonomes

— **Sécurité et surveillance** : Détection de menaces, analyse comportementale, cyberdéfense

— **Spatial et infrastructures critiques** : Contrôle de satellites, gestion d'infrastructures vitales

— **Recherche souveraine** : Projets classifiés, développement de capacités stratégiques

Dans ces contextes, la **responsabilité juridique** et la **légitimité institutionnelle** des décisions automatisées deviennent aussi critiques que leur performance technique.

1.2 La transformation du risque : de la sécurité à la preuve

Traditionnellement, la sécurité des systèmes IA critiques se concentre sur :

— La protection périmétrique (firewalls, isolation réseau)

— Le contrôle d'accès (authentification, autorisation)

— La supervision opérationnelle (logs SIEM, monitoring)

Or, ces mécanismes ne répondent pas à une question fondamentale :

Comment prouver, plusieurs années après les faits, qu'une décision algorithmique a été prise avec intégrité, dans un contexte vérifié, selon une chaîne de responsabilité établie ?

Cette exigence de **preuve pérenne** devient un impératif dans trois situations :

1. **Contrôle juridictionnel** : Recours administratif, contentieux, enquêtes parlementaires
2. **Audit inter-agences** : Vérification de conformité, certification, transfert de responsabilité
3. **Investigation post-incident** : Analyse forensique, reconstitution de la chaîne décisionnelle

2 Base légale et conformité réglementaire

2.1 AI Act européen : l'obligation de traçabilité

Le Règlement européen sur l'intelligence artificielle (AI Act) impose aux systèmes d'IA à haut risque des obligations explicites de **record-keeping** et de traçabilité (Article 12) :

> *ń Les systèmes d'IA à haut risque doivent être conçus de manière à permettre l'enregistrement automatique des événements (logs) pendant leur fonctionnement. Les capacités de journalisation doivent garantir un niveau de traçabilité approprié [...] ż*

Cette obligation vise notamment :

— L'identification des données d'entrée utilisées

— La traçabilité des décisions automatisées

— La possibilité d'audit et de vérification ex post

— La conservation probante des traitements

Problème : Les journaux applicatifs classiques ne constituent pas une preuve juridique robuste, car ils sont :

— Modifiables a posteriori (absence d'immutabilité cryptographique)

— Dépendants du contexte d'exécution (vulnérables aux compromissions système)

— Non vérifiables indépendamment (liés à la plateforme d'origine)

2.2 Cadre juridique de la défense et responsabilité de l'État

Au-delà de l'AI Act, les systèmes d'IA utilisés dans les contextes de défense et de sécurité sont soumis à des exigences spécifiques :

— **Droit administratif** : Obligation de motivation des décisions, principe de précaution

— **Droit de la défense** : Chaîne de commandement, responsabilité opérationnelle

— **Contrôle démocratique** : Enquêtes parlementaires, commissions de vérification

— **Droit international** : Conventions sur l'usage de systèmes autonomes

Ces cadres convergent vers une même exigence : la capacité à **démontrer** la conformité et l'intégrité des traitements, pas seulement à les **affirmer**.

2.3 Souveraineté numérique et maîtrise technologique

La dépendance aux fournisseurs cloud ou aux plateformes propriétaires pour la preuve d'intégrité constitue un risque souverain inacceptable dans les contextes étatiques critiques.

Les organisations telles que l'**AMIAD** (Agence Ministérielle pour l'Intelligence Artificielle de Défense) nécessitent des solutions :

— Déployables en environnement air-gapped

— Vérifiables sans infrastructure externe

— Maîtrisables sur le plan algorithmique et cryptographique

— Pérennes face aux évolutions technologiques (notamment quantiques)

3 Menace post-quantique et horizon cryptographique

3.1 Le risque ń Harvest Now, Decrypt Later ż

Les ordinateurs quantiques à grande échelle, bien que non encore opérationnels, représentent une menace imminente pour la cryptographie actuelle. L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) identifie le risque suivant :

Menace HNDL : Des adversaires peuvent capturer aujourd'hui des données chiffrées avec l'intention de les déchiffrer demain, lorsque les ordinateurs quantiques seront disponibles.

Pour les systèmes d'IA de défense, cette menace est particulièrement critique :

— Les décisions algorithmiques doivent rester confidentielles pendant des décennies

— Les modèles IA constituent des actifs stratégiques de long terme

— La compromission rétrospective des preuves invaliderait toute capacité d'audit

3.2 Standards post-quantiques NIST, ETSI et ANSSI

Face à cette menace, les organismes de normalisation ont finalisé les premiers standards de cryptographie post-quantique :

NIST FIPS 203/204/205 (août 2024) :

— **ML-KEM** (Module-Lattice-Based Key Encapsulation Mechanism) : Établissement de clés

— **ML-DSA** (Module-Lattice-Based Digital Signature Algorithm) : Signatures numériques

— **SLH-DSA** (Stateless Hash-Based Digital Signature Algorithm) : Signatures sans état

Recommandations ANSSI (2024) :

— Migration progressive vers la cryptographie post-quantique

— Approche hybride pendant la phase de transition

— Priorisation des données à longue durée de vie

ETSI TS 103 744 :

— Profils de migration pour systèmes critiques

— Mécanismes de crypto-agilité

— Protocoles de transition sécurisée

3.3 Impératif de migration pour les systèmes IA critiques

Les systèmes d'IA de défense présentent des caractéristiques qui rendent la migration post-quantique urgente :

Caractéristique	Implication PQC
Durée de vie longue	Vulnérabilité HNDL élevée
Valeur stratégique	Cible prioritaire pour capture
Données classifiées	Exigence de confidentialité pérenne
Audit différé	Nécessité de preuve résistante au quantique

TABLE 1 – Caractéristiques des systèmes IA critiques et implications post-quantiques

4 Limites des approches actuelles

4.1 Journaux SIEM : sécurité opérationnelle, pas preuve juridique

Les systèmes de gestion d'événements de sécurité (SIEM) constituent la référence pour la supervision opérationnelle. Cependant, ils présentent des limitations structurelles pour la preuve juridique :

Critère	**SIEM classique**	**Preuve QuantumLock**
Immutabilité	Non garantie	Cryptographiquement scellée
Vérification indépendante	Dépend du système	Vérifiable offline
Intégrité long terme	Vulnérable (crypto classique)	Résistante au quantique
Portabilité	Liée à la plateforme	Artefact autonome
Valeur juridique	Limitée (modifiable)	Probante (inviolable)

TABLE 2 – Comparaison SIEM vs. preuve cryptographique

4.2 Blockchain : décentralisation non nécessaire, performance limitée

Les solutions blockchain sont parfois proposées pour garantir l'immutabilité. Elles présentent toutefois des inconvénients majeurs pour les environnements souverains :

— **Dépendance réseau** : Incompatible avec les environnements air-gapped

— **Décentralisation non souhaitée** : L'État doit garder la maîtrise complète

— **Performance** : Latence élevée, coût computationnel important

— **Confidentialité** : Modèle inadapté aux données classifiées

— **Crypto classique** : Vulnérable à la menace quantique

4.3 Journalisation applicative : insuffisante pour la responsabilité juridique

Les mécanismes de logging intégrés aux frameworks d'IA (TensorFlow, PyTorch) ne constituent pas une preuve :

— Absence de protection cryptographique des logs

— Pas de chaîne de custodie algorithmique

— Vulnérabilité aux modifications a posteriori

— Non conception pour la vérification indépendante

Constat : Il existe un fossé entre les mécanismes de sécurité opérationnelle et les exigences de preuve juridique pérenne.

5 Modèle de preuve QuantumLock

5.1 Principes fondamentaux

QuantumLock repose sur quatre principes architecturaux :

1. **Preuve cryptographique** : Chaque exécution d'IA génère un artefact prouvable mathématiquement
2. **Chaîne de custodie algorithmique** : Traçabilité complète du modèle, des données et du contexte
3. **Vérification indépendante** : Les preuves sont validables sans accès au système d'origine
4. **Résistance post-quantique** : Protection contre les menaces cryptographiques futures

5.2 Anatomie d'un Evidence Bundle

Un Evidence Bundle QuantumLock contient les éléments suivants :

Structure de l'Evidence Bundle

1. **Empreinte du modèle** : Hash cryptographique de l'architecture et des poids
2. **Contexte d'exécution** : Paramètres, environnement runtime, configuration
3. **Métadonnées de gouvernance** : Version, provenance, autorisation de déploiement
4. **Données d'entrée** : Hash des inputs ou représentation sécurisée
5. **Résultat algorithmique** : Output de l'IA ou décision produite
6. **Horodatage qualifié** : Preuve temporelle cryptographique
7. **Chaîne de signatures** : Signatures post-quantiques multi-niveaux
8. **Métadonnées de vérification** : Informations pour validation indépendante

5.3 Propriétés vérifiables

Un Evidence Bundle QuantumLock permet de vérifier cryptographiquement :

— **Intégrité** : Le bundle n'a pas été modifié depuis sa création
— **Authenticité** : Le bundle a été généré par le système autorisé
— **Non-répudiation** : L'émetteur ne peut nier avoir produit le bundle
— **Temporalité** : L'horodatage est fiable et inviolable
— **Conformité** : Le modèle utilisé correspond à la version certifiée
— **Traçabilité** : La chaîne de responsabilité est complète et vérifiable

Ces propriétés sont vérifiables **des années après les faits**, sans dépendance au système d'origine, et résistent à la menace quantique.

5.4 Workflow de génération et vérification

Phase 1 : Génération de la preuve (au moment de l'exécution)

1. Le système QuantumLock capture le contexte d'exécution
2. Calcul des empreintes cryptographiques (modèle, données, environnement)
3. Horodatage qualifié via autorité de certification temporelle
4. Signature post-quantique multi-niveaux
5. Assemblage de l'Evidence Bundle autonome

6. Stockage sécurisé (système de fichiers probant, HSM)

Phase 2 : Vérification indépendante (audit, investigation)

1. Récupération de l'Evidence Bundle
2. Vérification des signatures post-quantiques
3. Validation de l'horodatage
4. Contrôle de l'intégrité des empreintes
5. Reconstitution de la chaîne de custodie
6. Production du rapport de vérification

Caractéristique critique : La vérification peut être effectuée offline, en environnement air-gapped, par une entité tierce (commission d'enquête, auditeur externe, autorité judiciaire).

6 Cryptographie post-quantique et crypto-agilité

6.1 Schémas cryptographiques recommandés

QuantumLock implémente les standards NIST finalisés en août 2024 :
Pour l'établissement de clés :

— **ML-KEM-768** (FIPS 203) : Sécurité équivalente à AES-192, performance optimale

— Utilisation pour le chiffrement de données sensibles dans le bundle

Pour les signatures numériques :

— **ML-DSA-65** (FIPS 204) : Signature principale, équilibre sécurité/performance

— **SLH-DSA-128s** (FIPS 205) : Signature de secours, basée uniquement sur des fonctions de hachage

6.2 Approche hybride pour la transition

Conformément aux recommandations ETSI TS 103 744 et ANSSI, QuantumLock supporte une approche **hybride** pendant la phase de transition :

— **Signatures duales** : Combinaison d'algorithmes classiques (RSA-4096, ECDSA) et post-quantiques (ML-DSA)

— **Protection progressive** : Migration sans rupture des systèmes existants

— **Compatibilité** : Vérification possible avec ou sans capacités PQC

— **Évolution contrôlée** : Transition planifiée vers PQC pur

Cela garantit que :

1. Les preuves actuelles restent vérifiables avec l'infrastructure existante
2. Les nouvelles preuves sont déjà protégées contre la menace quantique
3. La migration est réversible et contrôlable

6.3 Crypto-agilité : anticipation des évolutions futures

QuantumLock est conçu selon les principes de **crypto-agilité** :

> **Crypto-agilité** : Capacité à changer les algorithmes cryptographiques sans refonte architecturale, en réponse à l'évolution des menaces ou des standards.

Mécanismes implémentés :

— **Abstraction algorithmique** : Les primitives cryptographiques sont interchangeables

— **Versioning des schémas** : Chaque bundle indique les algorithmes utilisés

— **Support multi-algorithmes** : Vérification possible avec différentes combinaisons

— **Évolution planifiée** : Roadmap de migration intégrée au système

Cela garantit la pérennité des preuves même si des algorithmes sont ultérieurement déconseillés ou remplacés.

7 Architecture de référence

7.1 Modes de déploiement

QuantumLock supporte trois modes de déploiement adaptés aux contraintes institutionnelles :

Mode 1 : On-premise souverain

— Déploiement complet dans le datacenter de l'organisation
— Maîtrise totale de l'infrastructure cryptographique
— Intégration avec PKI existante
— Stockage sur systèmes de fichiers probants institutionnels

Mode 2 : Air-gapped (environnements classifiés)

— Fonctionnement sans connectivité externe
— Horodatage via source temporelle locale certifiée
— Vérification offline complète
— Transfert des bundles via supports physiques sécurisés

Mode 3 : Hybride (défense en profondeur)

— Génération locale des preuves
— Archivage répliqué (local + coffre-fort numérique externe)
— Double horodatage (TSA interne + TSA qualifiée externe)
— Redondance pour garantir la pérennité

7.2 Composants architecturaux

L'architecture QuantumLock s'articule autour de cinq composants principaux :

1. **Evidence Generator** : Module de capture et de scellement cryptographique
2. **Timestamping Authority** : Service d'horodatage qualifié (interne ou externe)
3. **Signature Engine** : Module de signature post-quantique (HSM-backed)
4. **Evidence Store** : Système de stockage probant et pérenne
5. **Verification Toolkit** : Outils de validation indépendante

7.3 Intégration avec les systèmes IA existants

QuantumLock s'intègre de manière **non-intrusive** dans les pipelines MLOps :

Pour l'entraînement :

— Capture des métadonnées de training (hyperparamètres, datasets, métriques)
— Scellement du modèle final
— Génération d'un certificat de conformité cryptographique

Pour l'inférence :

— Capture du contexte d'exécution
— Enregistrement des inputs/outputs (ou de leurs empreintes)
— Génération du bundle de preuve
— Impact performance minimal (<5% overhead)

Pour la gouvernance :

— Intégration avec les systèmes de gestion des modèles (MLflow, etc.)
— Export des bundles vers systèmes d'archivage institutionnels
— APIs de vérification pour outils d'audit

8 Cas d'usage défense et sécurité

8.1 Audit inter-agences

Contexte : Une commission parlementaire ou une autorité de contrôle souhaite auditer l'utilisation d'un système d'IA de défense plusieurs années après son déploiement.

Exigences :

— Prouver que le modèle utilisé correspond à la version certifiée

— Démontrer l'intégrité des traitements effectués

— Reconstituer la chaîne de responsabilité

— Vérifier la conformité réglementaire

Apport QuantumLock :

— Fourniture des Evidence Bundles pour la période auditée

— Vérification cryptographique indépendante par les auditeurs

— Reconstitution complète de l'historique d'exécution

— Production d'un rapport de conformité vérifiable

8.2 Investigation post-incident

Contexte : Une décision algorithmique a conduit à un incident opérationnel. Une investigation doit établir la chaîne de causalité.

Exigences :

— Identifier le modèle et la version exacte utilisés

— Reconstituer le contexte d'exécution (données, paramètres)

— Vérifier l'absence de compromission du système

— Établir la chronologie précise des événements

Apport QuantumLock :

— Evidence Bundle horodaté de l'exécution incriminée

— Preuve cryptographique de l'intégrité du modèle

— Traçabilité complète des inputs et du contexte

— Base factuelle incontestable pour l'investigation

8.3 Transfert de responsabilité inter-systèmes

Contexte : Un système d'IA développé par une agence A doit être transféré et opéré par une agence B, avec garantie de conformité.

Exigences :

— Certifier l'intégrité du modèle transféré

— Prouver la conformité aux spécifications

— Établir la continuité de la chaîne de confiance

— Permettre l'audit futur par l'agence B

Apport QuantumLock :

— Bundle de certification cryptographique du modèle

— Preuve de conformité vérifiable indépendamment

— Transfert sécurisé de la chaîne de custodie

— Capacité d'audit préservée pour l'agence réceptrice

8.4 Conformité AI Act pour systèmes à haut risque

Contexte : Un système d'IA classé ń haut risque ż selon l'AI Act doit démontrer sa conformité aux obligations de traçabilité (Article 12).

Exigences :

— Enregistrement automatique des événements

— Traçabilité des décisions et de leur contexte

— Conservation probante des logs

— Capacité d'audit par les autorités de supervision

Apport QuantumLock :

— Génération automatique d'Evidence Bundles conformes

— Preuve cryptographique de la traçabilité

— Archive pérenne résistante aux altérations

— Mécanisme de vérification pour autorités compétentes

9 Évaluation et critères d'acceptation

9.1 Propriétés de sécurité vérifiables

Un système QuantumLock conforme doit démontrer les propriétés suivantes :

Propriété	Critère de vérification
Résistance post-quantique	Utilisation de ML-DSA-65 ou SLH-DSA conforme NIST FIPS 204/205
Immutabilité	Impossibilité de modifier un bundle sans invalider les signatures
Vérification indépendante	Validation possible sans accès au système d'origine
Non-répudiation	Preuve cryptographique de l'émetteur
Horodatage fiable	TSA qualifiée ou source temporelle certifiée
Intégrité long terme	Conservation des bundles sur support probant (10+ ans)

Table 3 – Propriétés de sécurité et critères de vérification

9.2 Performance et scalabilité

Les systèmes IA critiques nécessitent des performances compatibles avec les contraintes opérationnelles :

— **Latence de génération** : <100ms par Evidence Bundle

— **Overhead computationnel** : <5% sur l'inférence IA

— **Taille des bundles** : 10-50 KB (métadonnées + signatures)

— **Throughput** : Support de 1000+ inférences/seconde

— **Vérification** : <50ms par bundle en mode offline

9.3 Critères de conformité réglementaire

Matrice de conformité AI Act Article 12 :

Exigence AI Act	Mécanisme QuantumLock
Enregistrement automatique des événements	Capture automatisée du contexte
Traçabilité du fonctionnement	Evidence Bundle avec métadonnées complètes
Identification des données d'entrée	Hash cryptographique des inputs
Horodatage fiable	TSA qualifiée ou horloge certifiée
Capacité d'audit	Vérification indépendante offline
Conservation appropriée	Stockage probant longue durée

Table 4 – Conformité aux exigences de l'AI Act Article 12

10 Feuille de route et intégration

10.1 Phases de déploiement

Phase 1 : Preuve de concept (3 mois)

— Déploiement sur environnement de test avec modèle IA non critique
— Génération et vérification de bundles de preuve
— Validation des performances et de l'intégration
— Audit de sécurité et revue cryptographique

Phase 2 : Pilote opérationnel (6 mois)

— Intégration avec un système IA critique en production
— Déploiement en mode hybride (génération parallèle, pas d'interruption)
— Collecte de retours utilisateurs et optimisation
— Préparation de la documentation de certification

Phase 3 : Généralisation (12 mois)

— Extension à l'ensemble des systèmes IA à haut risque
— Intégration avec les processus de gouvernance IA
— Formation des équipes techniques et juridiques
— Mise en place de l'archivage pérenne

10.2 Intégration technique

Avec les pipelines MLOps :

— API REST pour intégration dans les workflows d'entraînement
— SDK Python pour capture automatique lors de l'inférence
— Plugins pour frameworks populaires (TensorFlow, PyTorch, ONNX)
— Connecteurs pour outils de gouvernance (MLflow, Weights & Biases)

Avec l'infrastructure de sécurité :

— Intégration avec PKI existante
— Export vers SIEM pour corrélation (métadonnées uniquement)
— Stockage sur systèmes de fichiers probants (WORM)
— Support HSM pour clés de signature critiques

Avec les systèmes d'archivage :

— Export automatique vers coffres-forts numériques
— Rétention configurable selon classification
— Mécanismes de réplication et de sauvegarde
— Compatibilité avec standards d'archivage électronique (NF Z42-013)

10.3 Formation et accompagnement

Le déploiement de QuantumLock nécessite l'accompagnement de trois populations :
Équipes techniques :

— Formation à l'intégration et à la configuration
— Guide de troubleshooting et de maintenance
— Documentation API et SDK

Responsables sécurité et gouvernance :

— Sensibilisation aux enjeux de preuve cryptographique

— Processus d'audit et de vérification

— Cadre juridique et conformité réglementaire

Auditeurs et autorités de contrôle :

— Formation à la vérification indépendante

— Utilisation du Verification Toolkit

— Interprétation des rapports de conformité

11 Conclusion : de la sécurité à la preuve

11.1 Synthèse des apports

QuantumLock répond à une exigence fondamentale des systèmes d'IA critiques de défense :

Apport différenciant

Transformer la capacité technique d'un système d'IA en **légitimité juridique démontrable**, grâce à des preuves cryptographiques pérennes, vérifiables indépendamment, et résistantes à la menace post-quantique.

Les bénéfices opérationnels et institutionnels :

— **Conformité réglementaire** : Réponse directe aux obligations AI Act Article 12
— **Responsabilité juridique** : Base probante pour contrôle juridictionnel et audit
— **Souveraineté numérique** : Déploiement maîtrisé, sans dépendance externe
— **Pérennité cryptographique** : Protection contre la menace quantique (HNDL)
— **Confiance institutionnelle** : Preuve objective face aux parties prenantes

11.2 Positionnement par rapport aux alternatives

Critère	SIEM	Blockchain	Logging applicatif	QuantumLock
Preuve juridique	Non	Partiel	Non	Oui
Air-gapped	Oui	Non	Oui	Oui
Post-quantique	Non	Non	Non	Oui
Vérification indépendante	Non	Oui	Non	Oui
Souveraineté	Oui	Non	Oui	Oui
Performance IA	Neutre	Impact fort	Neutre	Impact minimal

TABLE 5 – Comparaison des approches de traçabilité pour IA critique

11.3 Vision : l'IA souveraine vérifiable

L'utilisation de l'IA dans les contextes de défense et de sécurité ne peut reposer uniquement sur la confiance technique. Elle nécessite une **architecture de preuve** permettant à l'État de :

1. Démontrer la conformité et la légitimité de ses systèmes
2. Répondre aux exigences de contrôle démocratique
3. Maintenir la maîtrise technologique à long terme
4. Anticiper les menaces cryptographiques futures

QuantumLock constitue une brique fondamentale de cette architecture, en transformant chaque exécution d'IA critique en un **objet de preuve cryptographique vérifiable**.

Principe directeur :
ń Sécuriser un système est nécessaire.
Prouver son intégrité est indispensable. ż

QuantumLock répond à cette exigence fondamentale, en fournissant aux organisations telles que l'AMIAD les moyens de garantir que l'IA de défense reste juridiquement défendable, technologiquement vérifiable et souverainement maîtrisée y compris à l'ère post-quantique.

À propos de SoftQuantus innovative OÜ

SoftQuantus innovative OÜ est une entreprise spécialisée dans les solutions de preuve cryptographique et de sécurité post-quantique pour systèmes critiques.

— **Registre des entreprises** : 17048927 (Estonie)

— **Site web** : https://softquantus.com

— **Domaines d'expertise** :

  — Cryptographie post-quantique (NIST, ETSI, ANSSI)

  — Preuve cryptographique pour systèmes d'IA

  — Architectures souveraines et air-gapped

  — Conformité réglementaire (AI Act, RGPD, eIDAS)

Contact

Pour toute information complémentaire sur QuantumLock ou pour discuter d'un projet de déploiement :

— Email : contact@softquantus.com

— Site : https://softquantus.com

Ce document est une publication institutionnelle de SoftQuantus innovative OÜ.
Version 1.0 Janvier 2026