Communiqué de presse
Paris, le 2 février 2023

Docaposte lance la première solution d'archivage électronique résistante aux attaques quantiques

Docaposte, filiale numérique du groupe La Poste et référent français des solutions de confiance numérique, annonce la mise en œuvre, au sein de son système d'archivage électronique Arkhineo, d'un mécanisme de scellement d'archives et d'attestations de conservation capable de résister aux attaques d'ordinateurs quantiques.

Si l'ordinateur quantique paraissait inconcevable il y a encore quelques années, l'accélération de la recherche a fait émerger des premiers prototypes fonctionnels. Au-delà des bénéfices incontestables qu'il apportera dans de nombreux domaines tels que la santé, l'énergie, les sciences environnementales et la finance, l'ordinateur quantique représente également une menace pour les services reposant sur la cryptographie actuelle. La technologie quantique pourrait par exemple fabriquer des signatures électroniques, corrompre des transactions chiffrées et permettre l'usurpation de l'identité de serveurs ou d'autres entités impliquées dans des échanges électroniques.

En tant qu'opérateur de services de confiance, Docaposte est pleinement concerné par les recherches dans ce domaine et a déjà anticipé le virage post-quantique en termes d'archivage électronique à vocation probatoire. Tous les aspects fonctionnels du Système d'Archivage Électronique d'Arkhineo ne sont pas concernés au même niveau par d'éventuelles attaques quantiques. Si le chaînage des empreintes des documents peut résister sous certaines conditions, le cachet électronique utilisé pour sceller l'archive serait lui particulièrement vulnérable.

Ainsi, dans la nouvelle version conçue et réalisée par Docaposte, la solution Arkhineo peut à présent fournir des preuves d'archivage de type hybrides, c'est-à-dire comprenant à la fois une preuve « pré-quantique » classique interprétable par les logiciels actuels, et intégrant également une preuve « post-quantique ». Cette dernière ne perturbera pas les outils de validation existants, mais viendra garantir la robustesse de la preuve lorsque les ordinateurs quantiques deviendront accessibles.
La démonstration d'intégrité, d'antériorité et de traçabilité d'un document, de même que sa confidentialité, ne pourront ainsi pas être remises en cause.

Ce modèle hybride est celui préconisé par l'ANSSI en première phase de transition pour fournir une défense en profondeur post-quantique supplémentaire à l'assurance de sécurité pré-quantique[1]. La solution mise en œuvre par Docaposte se base également sur les dernières avancées en la matière réalisées par le NIST (National Institute of Standards and Technology)[2], en employant l'un des trois algorithmes de signatures préconisés.

Arkhineo, la solution leader de l'archivage électronique en France
Arkhineo est une solution de Docaposte spécialisée dans l'archivage à valeur probante des données numériques (factures, bulletins de salaire, contrats commerciaux, contrats de prêt, contrats de travail, souscriptions de produits d'épargne, états comptables etc.). Elle représente plus de 4 milliards de documents archivés, 200 collaborateurs spécialisés et près de 40 millions d'euros de chiffre d'affaires.
Pour plus d'informations : https://arkhineo.com

A propos de Docaposte

Référent de la confiance numérique en France et filiale du groupe La Poste, Docaposte accompagne toutes les entreprises et institutions publiques dans leur transformation et leur permet de l'accélérer, en confiance.
Expert dans le traitement de données sensibles et Tiers de confiance, Docaposte bénéficie d'un positionnement unique sur le marché qui lui permet de répondre de bout en bout à l'intégralité d'un besoin client, dans le respect des réglementations et avec l'assurance d'une donnée hautement sécurisée. Leader des solutions numériques de confiance (vote électronique, lettre recommandée électronique, signature électronique, archivage numérique) et premier opérateur de données de santé en France avec plus de 45 millions de dossiers médicaux, Docaposte apporte son expertise dans la conception et la gestion de plateformes numériques sur mesure. Ses savoir-faire industriels et de délégation de gestion lui permettent de répondre à tous les besoins de ses clients. Docaposte compte plus de 40 000 entreprises et administrations clientes, 7500 collaborateurs répartis sur près de 86 sites en France et à l'international. Docaposte a réalisé 826 M€ de chiffre d'affaires en 2022. Plus d'information sur www.docaposte.com

---

Contact presse :
Patrice Lemonnier
01 55 44 25 35 / patrice.lemonnier@laposte.fr

BPR France
Madly Pulval-Dady, Judith Martin-Tardivat, Sophie Decaudin
madly@bprfrance.com - judith@bprfrance.com – sophie@bprfrance.com
Tél : +33 1 83 62 88 16 / 88 12 / 88 11

[1] *En phase 2 (après 2025) : hybridation pour fournir une assurance de sécurité post-quantique tout en évitant toute régression de sécurité pré-quantique. En phase 3 (après 2030) : hybridation optionnelle.*

[2] *Organisme de standardisation américain qui réalise depuis 2016 un concours international en vue de la standardisation d'algorithmes cryptographiques post-quantiques. En juillet 2022 a été publiée une liste de quatre premiers algorithmes (un algorithme d'établissement de clés et trois algorithmes de signatures) qui seront utilisés comme base de rédaction pour les normes fédérales américaines mais aussi pour les standards internationaux.*