



**Marie Wattez**, directrice marketing, et **Bertrand Aït-touati**, ingénieur commercial chez Cryptolog

# Archiver jusqu'en 2109



PHOTOS: J.R.

**C**rise, développement durable, économie numérique... La dématérialisation des documents représente une tendance forte du marché. Le déploiement ou la migration vers des procédures numériques sécurisées constitue aujourd'hui un enjeu stratégique, dont l'archivage électronique est un élément majeur. Une organisation archive deux types de documents électroniques : ceux dont elle souhaite pouvoir disposer pour son usage propre (procédures internes, documents commerciaux ou techniques) et ceux qu'elle doit être en mesure de récupérer, d'en vérifier l'intégrité et l'authenticité, et d'en fournir des preuves à autrui plusieurs années après leur création. Il peut s'agir de contrats commerciaux, d'actes authentiques, de polices d'assurance, ou de confirmations de transactions, qu'ils soient signés ou non.

## La puissance de l'archivage cryptographique

Dans le dernier cas de figure, l'archivage cryptographique est un des moyens les plus puissants de répondre au besoin de gestion des preuves sur le long terme. Mais il ne se substitue pas à l'archivage traditionnel; il le complète en y ajoutant une composante de confiance, à savoir un module de maintenance cryptographique de maintien de la preuve dans le temps. On parle de « pérennisation ». La valeur de la preuve est indépendante des caractéristiques de stockage, autorisant une possible réversibilité de ses composants. Elle est donc indépendante des solutions de gestion documentaire existantes. In fine, le document

archivé avec ce module cryptographique pourra être récupéré, mais, surtout, le scénario de sa signature pourra être « rejoué », comme au moment de la création de celle-ci... et ce, même en 2109.

Dans le cadre de processus d'échange de documents signés, il est indispensable de déterminer, sans doute possible, qui a signé, ce qui est signé et quand. Sur le plan technologique, la signature

**« Maintenir dans le temps les preuves de dépôt et d'intégrité du document signé électroniquement »**

électronique est la réponse aux besoins d'authentification du signataire et d'intégrité du document signé. Cependant, seule, elle ne suffit pas toujours. Pour qu'un document signé électroniquement ait une valeur probante, cette signature doit être validée avant conservation et conservée en l'état; enfin, il faut garantir une méthode de revalidation pérenne afin que quiconque puisse révérifier la signature à tout moment, et ce même très longtemps après sa création, certains documents devant être conservés ad vitam.

Prenons l'exemple d'un contrat signé mais non revalidé périodiquement : dans vingt ans, il pourrait ne plus être vérifiable, parce que les éléments de sécurisation de dépôt et d'intégrité mis en place à l'origine ne seront plus fiables, au regard des évolutions technologiques. Il ne sera

alors plus possible de garantir que ce document n'a pas été modifié ou falsifié. Dites-vous bien que, dans vingt ans, les téléphones portables seront suffisamment puissants pour faire de fausses signatures, et ce avec les algorithmes d'aujourd'hui !

Si une fois établie, la validité d'une signature ne peut être remise en cause elle peut, en revanche, ne plus être vérifiable si les algorithmes utilisés sont devenus obsolètes. Il s'agit donc bien de conserver la possibilité de s'assurer de la validité d'une signature électronique.

## Le modèle des poupées russes

Le principe de l'archivage cryptographique consiste à maintenir dans le temps les preuves de dépôt et d'intégrité du document signé électroniquement et archivé, donc sa « vérifiabilité ». Dans la pratique, l'archivage, qui a la responsabilité du stockage des documents, effectue, à une fréquence définie, une opération de maintenance cryptographique. Sur le modèle des poupées russes, il crée, à intervalles définis, une nouvelle enveloppe de preuve avec les standards les plus performants du moment. Cette enveloppe entourera la précédente enveloppe de preuve, contournant ainsi le problème de la fiabilité des algorithmes de signature au fil du temps.

Un tiers de confiance horodateur sera sollicité ponctuellement pour ces opérations de maintenance. Il est d'ailleurs possible de faire appel à un tiers de confiance horodateur différent à chaque opération. De fait, l'un des points forts de cette technique est de dissocier les fonctions d'archivage, ou de stockage, de celles de gestion de la preuve. ■