



Dictao accompagne la migration à SHA-2 préconisée par la DCSSI

L'algorithme d'empreinte SHA-1, utilisé par l'éditeur de progiciels de dématérialisation de flux reposant sur la signature électronique Dictao, montre des signes de faiblesse en termes de niveau de sécurité. Bien que considéré comme suffisamment solide pour de nombreux usages, une possible diminution du niveau de sécurité de SHA-1 a été décelée en avril 2009. Samuel Lacas, expert sécurité et responsable de la certification des produits Dictao précise : *« Dans des conditions particulières, la probabilité de trouver deux messages différents ayant la même empreinte SHA-1 est moins faible qu'auparavant, ce qui affaiblit les fondements sécuritaires de cet algorithme cryptographique. La Direction Centrale de la Sécurité des Systèmes d'Informations (DCSSI) préconise donc l'utilisation d'un algorithme de la famille du SHA-2 (SHA-256, SHA-384 et SHA-512), d'un niveau de sécurité plus élevé que le SHA-1 et qui confère une durée de vie plus étendue aux preuves »*. Dans ce cadre, Dictao recommande la migration vers SHA-2 de toutes les applications utilisant SHA-1 avant la fin de l'année 2010. A ce sujet, l'éditeur se conforme aux recommandations de la DCSSI, comme le souligne Samuel Lucas : *« Nos produits de signature et de validation de signature sont certifiés au niveau EAL3+ de la norme internationale sécuritaire des Critères Communs par la DCSSI. Cette certification atteste notamment le support de SHA-2 par nos produits et donne une garantie de sécurité supplémentaire à nos clients »*. Pour Dictao, qui a implémenté SHA-2 sur ses progiciels dès 2004, il s'agit avant tout d'anticiper le remplacement nécessaire des algorithmes de calcul d'empreinte SHA-1 par SHA-2, à partir de mi-2010, pour renforcer la sécurité des opérations de signature électronique. A ce titre, les applications de plusieurs de ses clients dont la Direction des Journaux Officiels, TDF, Air France ou la BCE reposent déjà sur cet algorithme, qui offre des garanties de sécurité supérieures à celle de son prédécesseur SHA-1 et allonge la durée de vie des preuves électroniques. Samuel Lacas affirme que *« les applications pour lesquelles la pérennité de la preuve est particulièrement cruciale, comme par exemple l'archivage à valeur probante sur le long terme de documents s'appuient sur le SHA-2 »*. S'appuyant sur sa longue expérience, Dictao note que l'anticipation est fondamentale pour ces projets de migration. En effet tous les environnements ne sont pas encore en mesure de supporter SHA-2.

La migration du SHA-1 au SHA-2 nécessite l'évolution des formats de signature et l'évolution des Infrastructures de Gestion de Clés, d'où sont issus les certificats de signature et de chiffrement. En effet, pour signer électroniquement, il faut avoir un certificat (pièce d'identité électronique) et un outil de signature. L'adaptation des produits de signature de Dictao au passage de SHA-1 à SHA-2 est, elle, instantanée. Pour Samuel Lacas, qui a piloté de nombreuses migrations, la clé du succès réside dans une approche progressive. Son conseil aux entreprises serait le suivant : *« La migration des systèmes du SHA-1 au SHA-2 est relativement simple et peut se faire progressivement. Ainsi, l'usage du SHA-2 peut commencer par la signature des documents de preuve, puis la signature des certificats porteurs, puis être généralisés à l'ensemble des opérations de signature en particulier de la chaîne de certification de l'IGC »*. Le SHA-2 représente la seule alternative crédible au SHA-1 et cela pour de nombreuses années. En effet, les spécifications de son successeur, le SHA-3, sont attendues pour 2012. Sa mise en œuvre opérationnelle aura lieu probablement vers 2015.

<http://www.dictao.com>