Nos données de santé (mal) protégées par l'indésirable SHA-1

C'est un des constats préoccupants du rapport de la Cour des comptes sur les données de santé. Un dispositif cryptologique appelé FOIN (fonction d'occultation des identifiants nominatifs) protège l'anonymat des assurés en *« hachant »* leurs données dans le système national d'information inter régimes de l'assurance maladie (Sniiram). Mais cette fonction repose encore sur SHA-1.

L'algorithme permet, en croisant le numéro d'inscription au répertoire des personnes physiques (NIR), la date de naissance et le sexe de l'ayant droit, d'attribuer un nouveau numéro, non identifiable, à chaque bénéficiaire de soins, explique la Cour des comptes (les données étant enregistrées avec le NIR de l'ayant droit par les centres de traitement informatique des différents régimes). Les numéros non identifiables issus de ce processus (dit-FOIN-1) sont retraités à nouveau, cette fois par la Caisse nationale d'assurance maladie (CNAMTS), selon le même processus (FOIN-2), *« pour éviter l'existence d'une table de correspondance entre le NIR et les identifiants présents dans le Sniiram »*.

Une obsolescence soulignée dès 2008

Ce processus *« irréversible »* est censé garantir l'anonymat des données recueillies. Or FOIN repose sur SHA-1, un algorithme de hachage dont l'obsolescence avait été soulignée dès 2008 par l'Agence nationale de la sécurité des systèmes d'information (Anssi), puis rappelée en 2014 dans le cadre d'une expertise confiée par la CNAMTS à un prestataire tiers. L'expertise concluait que cette protection ne resterait fiable que *« durant une période limitée (quelques années au plus) »*.

Or, *« fin 2015, le ministère n'avait pas encore demandé, ni la CNAMTS engagé, l'élaboration de plan, de calendrier et d'estimations financières en vue d'un changement d'algorithme, inéluctable »*, souligne la Cour des comptes. L'Anssi lui a indiqué que *« le RGS (référentiel général de sécurité) proscrit l'utilisation de SHA-1 en tant que fonction de hachage cryptographique, mais en déconseille seulement l'utilisation, sans la proscrire, lorsqu'il sert de base à des mécanismes [tels que] FOIN »*. Une attaque réussie par ce biais ne serait pas d'actualité. Malgré tout, l'Anssi considère qu'un *« remplacement à moyen terme (5 à 10 ans) par un algorithme à l'état de l'art serait conforme aux recommandations énoncées dans le RGS »*. Il ne reste plus qu'à attendre…

Lire aussi :

Chiffrement : Microsoft va bannir le SHA-1 dans Windows 10 Anniversary Update
Firefox peine à se débarrasser de l'indésirable SHA-1
SHA-1 : Google, Microsoft et Firefox font le ménage dans le HTTPS

crédit photo © wk1003mike / shutterstock.com