

Une chaîne de haute sécurité pour les données sensibles

Dans les prochaines années, la progression de la demande pour le traitement et le stockage sécurisés de données électroniques sera quatre fois plus élevée que celle pour les services de private banking. La Suisse occupe une position clé dans le développement et l'exécution de services de haute confidentialité pour lesquels elle bénéficie d'une excellente réputation au niveau international. Ce sont les conclusions d'une étude récente effectuée par une entreprise spécialisée en conseils IT pour les services financiers.

Raoul Oliver WUERGLER

*Secrétaire général adjoint,
Association des banques étrangères en Suisse*

La révision de l'article 957 du Code des obligations assimile les documents électroniques à des titres. De nouvelles solutions doivent désormais être identifiées pour l'entreposage, l'archivage et la récupération des milliers de documents électroniques – les factures transmises par internet sont concernées de la même façon que les e-mails rédigés par n'importe quel employé – produits chaque année par les entreprises. Désormais, la composition d'une chaîne de valeur intégrée pour le traitement des données sensibles s'impose. Quels en sont les éléments? Comment fonctionne-t-elle et quelle valeur ajoutée crée-t-elle?

Plusieurs éléments interdépendants

Le premier élément de la chaîne de haute sécurité consiste en le cryptage des données; il détermine le degré de protection dont celles-ci bénéficieront. Les modes de cryptage actuellement utilisés reposent sur des algorithmes prédéfinis et connus par l'émetteur et le récepteur, comme par exemple le cryptage 128 bit utilisé pour l'e-banking. La sécurité d'un tel type de cryptage est fonction de la longueur, voire complexité, de la clé utilisée: plus celle-ci est grande, plus le décryptage par des tiers sera difficile. Même si la clé peut être protégée par des astuces comme son remplace-

ment fréquent, il reste que sa définition repose sur un algorithme prédéfini et fixe pour toute sa durée de validité. Aussi, la clé doit être échangée entre émetteur et récepteur, ce qui constitue une étape délicate parce que le risque d'interception est élevé: une fois l'algorithme de la clé intercepté, le cryptage perd toute sa valeur. Afin de parer à ce danger, la recherche propose le recours

«La Suisse accueille un nombre élevé d'entreprises multinationales de plus en plus gourmandes en solutions pour l'archivage sécurisé de leurs données»

à la physique quantique où les objets changent sous chaque observation, ce qui permet aux utilisateurs autorisés de contrôler si leurs messages ont été interceptés. Le degré de sécurité dans l'échange de clés et de messages cryptés est dès lors nettement plus élevé. La physique quantique permet aussi de générer de véritables nombres aléatoires qui permettent d'éviter le recours aux algorithmes dans la définition des clés de cryptage et accroissent ainsi sa sécurité. La chaîne se prolonge par la transmission des données. Même si le courriel traditionnel est comparé à des cartes postales quant à son degré de confidentialité, plusieurs solutions complétant les clés de cryptage

sophistiquées permettent d'assurer la protection des données échangées. Il est ainsi possible de couper le message initial en blocs transmis par différents réseaux de télécommunication (la répartition peut se faire entre différentes générations ou différents fournisseurs de réseaux mobiles ou fixes). Avant de passer au décryptage, l'intercepteur sera obligé d'assembler correctement les différentes parties du message initial.

Recyclage des bunkers militaires

Le troisième élément de la chaîne de haute sécurité se situe au niveau du stockage des données dans un lieu répondant, lui aussi, aux exigences de protection les plus élevées. Les documents électroniques devront respecter les délais de conservation légaux de dix, quinze voire cinquante ans, ce qui pose au moins trois défis de taille. Premièrement, une stratégie devra être définie pour assurer l'accès aux données produites avec des hardwares ou softwares anciens. Soit un parc de machines de toutes les générations devra être conservé soit des logiciels de transcription devront être rédigés à la sortie de chaque nouvelle application informatique. Deuxièmement, il faudra résoudre le problème de la détérioration rapide des supports électroniques: pendant que l'écrit sur papier a prouvé sa longévité, le disk des années 70 a été remplacé par le floppy des années 80, le CD-Rom des années 90 et le stick USB susceptible, à son tour, d'être détrôné sous peu. La microfiche présente une alternative: en photo couleur elle arrive à stocker une quantité de données élevée tout en assurant l'accessibilité nécessaire, sa durée de vie s'élevant à plusieurs siècles et le

procédé de lecture inventé par les frères Lumière étant des plus simples. Troisièmement, des lieux d'entreposage offrant la protection physique – et contre les aléas de la nature comme inondations ou tremblements de terre et contre l'accès par des tiers non-autorisés – doivent être identifiés. Les lieux sécurisés sont à portée de main sous forme de nombreux bunkers devenus disponibles dans le cadre de la restructuration de l'Armée suisse et vendus à des sociétés spécialisées dans l'archivage et le stockage en milieu sécurisé. Ces bunkers se trouvent près des principaux axes de transport Nord-Sud où passent aussi les réseaux de télécommunication internationaux. Ils offrent une protection physique élevée qui peut être complétée par des systèmes modernes comme des contrôles d'accès de nouvelle génération. Ceux-ci font recours à des identifiants liés de façon inaliénable à la personne de droit comme le scanning de l'iris ou la lecture de l'empreinte digitale remplaçant ainsi les mots de passe – souvent notés par les utilisateurs.

Le maillon final de la chaîne de haute sécurité couvre la récupération des données qui est assistée par des procédures informatiques sophistiquées reposant sur des algorithmes comparables à ceux utilisés par Google. La nécessité d'un appareil de recherche informatique s'impose si l'on tient compte de la quantité de données produites quotidiennement, ne serait-ce que dans une PME, et du Code des obligations qui exige la conservation de tout document, électronique ou physique, qui peut être mis en relation avec les activités de l'entreprise d'une manière ou d'une autre. En cas de litige, l'entreprise pourra être amenée à produire les documents relatifs à un cas de figure très précis. C'est à ce moment-là qu'il lui sera indispensable de pouvoir distinguer l'email confirmant le rendez-vous du déjeuner de celui qui confirme l'ordre d'achat.

Le défi qui devient opportunité

La Suisse compte sur son territoire de nombreuses sociétés indigènes et étrangères ainsi que plusieurs instituts universitaires s'activant dans l'un ou l'autre des nombreux domaines de la haute sécurité. Ainsi, Wisekey propose une multitude de certificats d'authenticité pendant que Kudelski joue à la pointe mondiale dans le domaine des systèmes de contrôle d'accès et que Swiss Data Safe AG est en train de dévelop-

per une gamme de services dans le stockage et l'archivage sécurisé des données. En même temps, la recherche des hautes écoles s'intéresse à la physique quantique pour l'échange des données ou à l'imagerie pour leur entreposage à long terme. D'autre part, la Suisse accueille un nombre élevé d'entreprises multinationales de plus en plus gourmandes en solutions pour l'archivage sécurisé de leurs données – les banques sont loin d'être les seules à manipuler des données sensibles méritant un degré de protection élevé, les secteurs chimique et pharmaceutique ou la micromé-

canique sont deux exemples de domaines dans lesquels une importante recherche de pointe méritant protection adéquate est faite en Suisse.

Il devient impératif que ce cluster composé de prestataires, dont certains services viennent d'être présentés, et d'utilisateurs prenne une forme plus concrète. La Suisse dispose d'une longue expérience dans le traitement de données sensibles et elle a tout intérêt à développer une chaîne intégrée de haute sécurité dans un monde où l'exigence de transparence et sa satisfaction deviendront toujours plus importants. ■

R.O.W.

L'ART DANS B&F



F.-O. Brunet, *Identités nomades*, acrylique et pastel sur papier (26 x 20 cm)