La signature électronique

"Archivage électronique - approche technico-légale"
Journée AVA - 1er novembre 2007

Les toujours plus nombreuses applications de commerce électronique ou de cyberadministration accessibles par l'Internet rendent nécessaires de sécuriser les transactions électroniques afin de favoriser une large adoption d'utilisateurs confiants. Confirmer à l'internaute l'identité de la personne qui lui soumet des données informatiques ou encore le rendre attentif lorsque les données obtenues ont été modifiées lors d'une transaction, sont les défis relevés par la signature électronique.

Principe de la signature électronique

Pour créer une signature électronique, le signataire dispose de données informatiques uniques, appelées clés, dont l'une, la clé privée, doit rester secrète, alors que l'autre, la clé publique, peut être largement divulguée.
Ces clés sont liées par une fonction mathématique suffisamment complexe afin qu'il soit impossible de déterminer la clé privée sur la base de la clé publique correspondante. La clé privée (ou clé de signature) sert à signer des données électroniques alors que la clé publique (ou clé de vérification de signature) permet à un tiers de vérifier la signature électronique.
Lors de la signature, l'application informatique du signataire effectue une fonction mathématique utilisant les données à signer et la clé privée du signataire. La signature qui en résulte est ensuite jointe aux données signées. Lors de la vérification de la signature, l'application informatique du vérificateur procède à une fonction mathématique utilisant la clé publique du signataire ainsi que la signature. Cette fonction a pour but d'obtenir les données initialement signées. L'application du vérificateur effectue finalement une comparaison entre les données qui ont fait l'objet de la signature et les données obtenues par la fonction mathématique de vérification.
Si le résultat de cette comparaison est positif, le vérificateur a l'assurance qu'aucune modification des données n'est intervenue suite à leur signature (intégrité des données). Il lui est alors également confirmé que le signataire est bien le titulaire de la clé publique utilisée lors de la vérification.

Les fournisseurs de services de certification

Le principe de la signature électronique précédemment décrit n'est cependant suffisamment sûr que dans le cas où la validité et la diffusion des clés publiques sont assurées. Dans le contexte du commerce électronique ou de la cyberadministration, il est en effet illusoire de s'attendre à ce que les utilisateurs se rencontrent, avant toute transaction électronique, afin d'échanger leur clé publique de manière sûre. Le recours à une tierce partie qui se porte garante de la légitimité des titulaires de clés s'avère par conséquent nécessaire.
Ainsi, les clés sont en principe générées par un tiers de confiance, le fournisseur de services de certification, qui procède par ailleurs à l'émission d'un certificat électronique dans lequel figure la clé de vérification de signature ainsi que l'identité du titulaire de la clé. Le certificat

électronique a donc pour principale fonction de lier la clé publique à son titulaire, identifié lors de l'émission du certificat par la présentation d'une pièce d'identité.
Outre l'intégrité des données, le vérificateur est donc également en mesure, grâce au certificat, de déterminer l'identité du signataire.
Pour assurer l'intégrité des données figurant dans le certificat, ces dernières sont signées électroniquement par le fournisseur de services de certification.
En cas de compromission des clés, leurs titulaires peuvent avoir recours au service de révocation de certificats mis à disposition par le fournisseur de services de certification. Dans un tel cas, ce dernier publiera le certificat révoqué dans une liste accessible à tout vérificateur.

Reconnaissance des fournisseurs de services de certification

La loi fédérale sur les services de certification dans le domaine de la signature électronique (loi sur la signature électronique, SCSE), qui est entrée en vigueur au 1er janvier 2005, définit les conditions auxquelles les fournisseurs de services de certification peuvent être reconnus sur une base volontaire et règle leurs activités dans le domaine des certificats électroniques.
Les dispositions de la SCSE sont compatibles avec la réglementation en vigueur dans l'Union européenne.
La reconnaissance signifie que le fournisseur qui l'a obtenue satisfait aux exigences légales posées, notamment en ce qui concerne l'identification des personnes titulaires de certificats électroniques ainsi que les procédures de gestion des clés et certificats électroniques. Elle se base sur le système général de l'accréditation valable en Suisse pour les organismes de certification et d'inspection et autres laboratoires d'essais et d'étalonnage. Il appartient ainsi au Service d'accréditation suisse (SAS) du Secrétariat d'Etat à l'économie (SECO) d'accréditer les organismes chargés de reconnaître les fournisseurs de services de certification. A l'heure actuelle, seule la société KPMG Klynveld Peat Marwick Goerdeler SA a obtenu l'accréditation du SAS dans le domaine des services de certification électronique.
Jusqu'à la mi-2008, Swisscom SA, QuoVadis Trustlink Schweiz AG, SwissSign SA et l'Office fédéral de l'informatique et de la télécommunication (OFIT) ont été reconnus par KPMG SA pour la fourniture de services de certification selon les dispositions de la loi sur la signature électronique. A l'exception de l'OFIT qui ne fournit que des services à l'administration, ces fournisseurs, présents ou représentés dans plusieurs villes de Suisse, émettent des certificats qualifiés au sens de la SCSE à l'attention d'une clientèle commerciale ou privée.

Valeur juridique de la signature électronique

La loi sur la signature électronique a également réglé la question de la validité de la signature électronique. Ainsi, l'art. 14, al. 2bis, du code des obligations (CO) reconnaît à un certain type de signature électronique, la signature électronique qualifiée, la même valeur que celle qui est conférée à la signature manuscrite à condition qu'elle soit basée sur un certificat qualifié délivré par un fournisseur reconnu au sens de la SCSE. Il est donc possible de conclure, par la voie électronique également, les contrats qui jusqu'ici devaient être passés en la forme écrite traditionnelle, comme le contrat de crédit à la consommation par exemple. Toute autre forme de signature électronique ne peut prétendre à un tel statut. Cela ne signifie toutefois pas qu'une signature électronique ne répondant pas aux exigences de l'art. 14, al. 2bis, CO est dénuée de toute valeur juridique. A défaut de meilleure preuve, un juge peut prendre en considération un document muni d'une simple signature électronique.

Applications de la signature électronique

La signature électronique peut être utilisée chaque fois qu'il s'agit d'assurer l'intégrité et l'authenticité de données électroniques. Cela est valable aussi bien dans le cadre du commerce électronique (entre entreprises ou entre entreprises et particuliers) que dans celui de la cyberadministration (entre autorités ou entre autorités et citoyens). La signature électronique est également utilisée pour assurer l'intégrité des données archivées. Dans ce cadre, toute modification des données archivées et signées sera détectée lors de la vérification de signature. Il convient par conséquent de générer une nouvelle signature si, durant la période d'archivage, les données archivées sont volontairement modifiées.
Suite aux reconnaissances des fournisseurs de services de certification, une faible croissance du nombre de certificats qualifiés émis peut être observée dans notre pays. Le développement du nombre de certificats dans les pays européens démontre que cette évolution est fortement dépendante de la présence d'applications pour lesquelles il est prévu de les utiliser. Dans certains pays, des projets de cyberadministration mettant en œuvre de nombreux certificats ont été réalisés. On constate que le secteur bancaire est également capable d'influencer de manière conséquente l'évolution du nombre de certificats.
Dans notre pays et pour les besoins de la cyberadministration, certains projets ont toutefois d'ores et déjà mis en œuvre la signature électronique. Il s'agit notamment de la signature électronique des factures de contribuables assujettis à la TVA, des données de la Feuille officielle suisse du commerce (FOSC) publiée en ligne et des documents transmis électroniquement entre les études d'avocats et les tribunaux ainsi qu'entre tribunaux de différentes instances. On a également recours à la signature électronique pour sécuriser les votations électroniques.
La signature électronique peut également être appliquée dans le cadre de la communication électronique en procédure administrative fédérale. Des demandes peuvent en effet être adressées aux autorités administratives fédérales par voie électronique et les décisions de ces dernières être notifiées de la même manière.

Jean-Maurice Geiser et Christian Jenny,
Office fédéral de la communication (OFCOM)