Authentification et Certification

L'authentification

Souvent confondu car associé à la certification, ces termes nouveaux pour la plupart de nos confrères, doivent être précisés si l'on veut une compréhension claire de leur introduction dans le monde des échanges informatiques.

S'il est assez coutumier de considérer qu'un courriel reçu à titre individuel, de la part d'un auteur connu du receveur, sans intervention de tierce personne (secrétaire ou autre) présente suffisamment de garanties pour considérer le message comme fiable, la situation est nettement moins claire lorsque interviennent des intermédiaires ou si le message est le fait d'auteurs multiples.

L'apposition simple d'un nom au bas d'un message devient alors insuffisante pour pouvoir attribuer de manière non équivoque le contenu du message à l'auteur présumé, à fortiori s'il est inconnu du receveur.

Cette nécessité à pouvoir s'authentifier de manière sûre par voie informatique a été perçue très tôt par les Communautés Européennes. Elles ont établi des recommandations coulées par la Belgique sous forme de loi dite « de la signature électronique » et publiée au moniteur du 29 septembre 2001. Cette loi précise entre autre toutes les conditions que doit réunir cette « signature virtuelle » pour pouvoir être assimilée à une signature manuscrite, non réfutable par un magistrat (signature dite « avancée »).

Cette loi introduit la notion de certification (attribution d'un certificat) et définit les conditions d'attribution de ces certificats et par qui.

Prenons l'exemple de la Carte d'Identité électronique, actuellement en cours de distribution et dont le mode de délivrance est hautement sécurisé : le sujet doit se présenter en personne à son administration communale, muni de son ancienne carté d'identité et de son code d'accès à sa nouvelle carte d'identité. La ou le préposé enregistre les données nécessaires puis demande au sujet d'introduire le code initial, puis celui qui lui sera propre. C'est de ce degré de sécurité (de contact) que dépend la valeur de l'authentification. Il eût été beaucoup plus simple, pour le Ministère de l'Intérieur, d'ouvrir un site Web et de nous suggérer de s'y inscrire, mais quelle serait alors la valeur de cette signature et de ce mode d'authentification ?

En procédant de cette manière stricte, l'état belge « transfère » en quelque sorte la responsabilité de l'utilisation ultérieure de la carte à son possesseur tout en restant garant de cette authentification qu'il a accordée. L'autorité qui certifie est ainsi une donnée fondamentale car c'est elle, finalement, qui permet d'apprécier le degré de confiance à accorder à la signature elle-même. Outre la délivrance des signatures, cette autorité de certification doit maintenir à jour les renouvellements, les révocations … .

Cette carte dispose de clés d'authentification et de signature. L'authentification se fait par sa simple introduction dans un lecteur approprié, manœuvre qui autorise la lecture du « certificat », c'est-à-dire grosso-modo ce qui est écrit sur la carte, ainsi que le responsable (l'auteur) de cette authentification, en l'occurrence ici l'état belge, la durée de validité de ce certificat et d'autres données précisées par la loi. La signature fait appel à la clé de signature également contenue dans la puce de la carte, obligatoirement associée au code propre attribué par le sujet. L'effet de cette signature, associée à un document quelconque, est de rendre celui-ci non modifiable (mais lisible) et d'y associer une copie du certificat de son auteur.

Le receveur du message dispose ainsi d'un document non modifié depuis sa signature, également non modifiable par lui sous peine de « casser » la signature et associé à un certificat garantissant l'identité de l'auteur.

Le certificat qui accompagne le document signé se présente alors sous forme d'un petit fichier annexé au document signé et donne au receveur du message les informations concernant le type de certificat (essentiellement son mode de distribution), quelle est l'autorité de certification qui l'a délivré, sa validité, sa non révocation, son objet ainsi que des données plus techniques concernant sa composition.

La Certification

Comme on vient de le voir plus haut, l'authentification d'une personne, en tant que telle, fait appel à un certificat.

Cette authentification première reste toutefois insuffisante si l'on veut isoler un groupe parmi l'ensemble des certifiés.

Prenons l'exemple de la population médicale belge. Tous les médecins vont recevoir une carte d'identité, mais celle-ci s'avère insuffisante pour déterminer le titre de Docteur en Médecine. Cette reconnaissance à pouvoir exercer la médecine ne relève en outre ni du ministère de l'Intérieur ni de l'administration communale.

Deux orientations techniques sont possibles pour isoler ce sous-groupe : soit en attachant un « certificat d'attribut » à la carte d'identité, ce qui obligera à l'utiliser en permanence et augmentera ses désagréments en cas de perte ou de vol, soit en procédant comme le ministère de l'intérieur, en délivrant une propre carte professionnelle.

Le certificat d'attribut présente l'avantage du support existant (la carte d'identité) et fonctionne sur le mode du référencement à un site qui fait le lien entre le possesseur de la carte et son statut (de médecin en l'occurrence).

Cette possibilité est à l'étude à l'heure actuelle.

L'autorisation d'exercer la médecine en Belgique nécessite d'une part un visa décerné par la Commission médicale Provinciale et d'autre part l'inscription obligatoire au Tableau de l'Ordre des Médecins.

La Commission Médicale Provinciale a vocation, en grande partie, à vérifier la capacité à cet exercice. Si cette capacité « va de soi » pour les jeunes promus des universités belges qui vont y présenter leur diplôme tout neuf, imaginons les difficultés à l'évaluer pour des ressortissants de pays étrangers dont les programmes d'études sont parfois fort différents et variés. Cette capacité comprend aussi, et ce n'est pas toujours su par le plus grand nombre, y compris médecin, la capacité physique à l'exercice de l'art de guérir. Prenons l'exemple d'un médecin toxicomane ou présentant des problèmes psychiatriques sévères : c'est la Commission Médicale Provinciale qui a le pouvoir de réunir les experts nécessaires à l'évaluation de la situation et éventuellement retirer son visa.

L'Ordre des Médecins n'intervient qu'en cas de comportement non déontologique (non conforme au Code de Déontologie) d'un membre inscrit à son Tableau. Il a aussi pour mission d'élaborer ce Tableau, c'est-à-dire de procéder au recensement et à la reconnaissance par ses pairs, de tous ses membres. Ne peuvent être inscrits que ceux qui disposent du visa délivré par la Commission Médicale Provinciale.

C'est sur base de cette inscription obligatoire et légale que le Conseil National a proposé, dès 2001, d'assurer la certification des médecins inscrits à son tableau. Le seul but est de certifier que le possesseur d'un certificat délivré par le Conseil National est bien médecin, autorisé à exercer en Belgique.

Les avantages de cette certification nationale repose sur l'uniformisation du certificat, sur la garantie offerte (la qualité d'un signataire éloigné), et sur la prise en charge de cette procédure lourde que représente la reconnaissance des médecins. Notons ici que la loi oblige au secret des sentences juridiques, disciplinaires ou administratives prononcées vis-à-vis d'un médecin mais oblige au transfert des décisions lourdes qui ont ou pourraient avoir des conséquences dans les compétences autres. L'Ordre est ainsi bien positionné pour assurer le maintien à jour d'éventuelles révocations ou suspensions.

Les inconvénients sont liés au degré de haute sécurité que souhaite donner le Conseil à ses certificats, donc au contact direct nécessaire avec le médecin, à la forme actuelle de ces certificats, nécessitant des compétences trop élevées en informatique pour le commun des médecins. D'autres formes de support (type carte bancaire) devraient être étudiées mais entraînent l'obligation de s'équiper d'un lecteur de carte à puce.

Dr ROBINET Philippe