Le 18 octobre 2004

Le chef du département de l'innovation technologique et de l'innovation

aux directeurs et responsables des services d'archives nationales, départementales, régionales et communales

Note d'information DITN/RES/2004/004. Résumé du rapport de Jean-François Blanchette sur « *La conservation de la signature électronique : Perspectives archivistiques* », septembre 2004

J'ai le plaisir de vous annoncer la parution d'un rapport, que vous trouverez à l'adresse suivante (adresse de la direction des Archives de France), sur la signature électronique et sa conservation : « *La conservation de la signature électronique : Perspectives archivistiques* ».

Contexte

Ce rapport a été réalisé par un chercheur canadien, Jean-François Blanchette, qui aujourd'hui travaille en tant que professeur au Department of Information Studies, University of California, Los Angeles (UCLA), Mél: blanc@ucla.edu, Web : polaris.gseis.ucla.edu/blanchette.

Ce chercheur, qui a fait sa thèse sur la signature électronique, a travaillé plusieurs années en France et a notamment participé à la rédaction du projet de décret d'application relatif aux actes authentiques de la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

C'est la direction des archives de France qui, en 2003, a commandé ce rapport, étant donné les conséquences importantes de cette loi et de son premier décret d'application n° 2001-272 du 30 mars 2001 sur la signature électronique.

En effet, désormais, un document électronique a même valeur probante qu'un document sur support papier, à condition que son auteur puisse être précisément identifié et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité (article 1316-1 du Code civil). Dès lors, la signature électronique se trouve introduite et notamment, dans le cadre de la Directive Européenne du 13 décembre 1999, la signature fondée sur la cryptographie a-symétrique, qui bénéficie, dans certains conditions, d'une présomption de fiabilité.

Or, ne sont nullement précisées les modalités de conservation de cette sorte de signature dans le temps ou plutôt, on se retrouve face à une contradiction : cette technique permet précisément de déceler toute modification d'un document (toute l'économie repose sur le principe du respect de l'intégrité du document) ; or, les archivistes savent que pour préserver la lisibilité d'un document dans le temps, il est parfois nécessaire de procéder à des migrations de formats qui font échouer la procédure de vérification de ce document.

On se retrouvait par conséquent devant une absurdité : avoir un document intègre mais qui n'était plus lisible ; ou bien avoir privilégié la lisibilité au détriment de l'intégrité.

En outre, la mise en place de ces technologies implique des infrastructures extrêmement lourdes, et d'autant plus lourdes que le temps passe et qu'on peut se demander dans quelle mesure les services publics d'archives, voire les administrations pour les documents à longue durée d'utilité administrative, pourraient prendre en charge ces infrastructures.

Il a par conséquent été demandé à Jean-François Blanchette d'étudier comment les grandes institutions d'archives internationales (canadiennes, australiennes, américaines) abordaient la question et quelles étaient leurs recommandations aux producteurs en la matière.

Contenu du rapport

Le rapport se découpe en 4 grandes parties.

Une première partie décrit les technologies de signature numérique : leur contexte (science des cryptologues, découverte du système cryptographique à clé publique (double clé), application de ces technologies pour la signature d'un document, ce qui permet à coup sûr de déterminer son origine et le fait qu'il n'a pas pu être modifié) ; le principe de la certification permettant, par le biais d'un certificat, de relier une clé publique à son propriétaire ; ce que recouvre une infrastructure à clé publique (ou PKI en anglais). L'auteur montre que c'est l'explosion des technologies de l'internet qui fera tout le succès de ces techniques.

La deuxième partie concerne le cadre juridique de la signature électronique : directive européenne du 13 décembre 1999 qui pose déjà les grands principes et annonce une signature avancée (en fait celle reposant sur les technologies cryptographiques) qui se voit attribuer une force probante supérieure (statut préférentiel) ; émergence et adoption de la loi du 13 mars 2000 qui reconnaît une force probante équivalente aux documents papier et électronique sous certaines conditions, avec l'introduction d'une définition de l'écrit et de la signature et celle d'une présomption de fiabilité « *lorsque la signature est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie* ».

De même, la loi permet la dématérialisation des actes authentiques, et pas seulement celle des actes sous seing privé, comme le prévoyait le projet de loi, sommet de la hiérarchie probatoire dans le système français. Par ailleurs, l'importance de la signature est accentuée par rapport au passé : c'est elle à présent qui confère l'authenticité, alors que jusqu'alors elle ne constituait qu'un des éléments.

J.F. Blanchette relève deux faiblesses à ces dispositifs : le processus de vérification n'est pas régulé et le problème de la conservation à long terme des signatures cryptographiques n'est pas abordé.

La troisième partie présente plusieurs stratégies techniques pour la conservation de la signature électronique. L'auteur distingue bien ce qui relève, dans le cas des signatures cryptographiques, de la vérification immédiate par le destinataire, de celle qui peut intervenir des années plus tard, par exemple devant un juge dans le cadre d'un contentieux. On se heurte alors au problème de l'obsolescence des équipements matériels, logiciels et des formats. Or, on doit pouvoir d'une part disposer d'équipements permettant d'accéder aux informations binaires du document sur son support physique, de les décoder et de les rendre manifestes sur écran ou papier ; et d'autre part, disposer d'équipements permettant d'accéder à la signature électronique sur son support physique, de la décoder et d'exécuter l'algorithme de vérification qui permet de déterminer la validité de la signature.

Les solutions techniques actuellement proposées pour la conservation des signatures sur le long terme sont de trois ordres :

- la re-signature, dès lors que les tailles des clés de signature ne semblent plus suffisantes pour assurer la sécurité : le rapport explicite toutes les étapes du processus de vérification et nous permet de mieux comprendre tous les éléments dont il convient de disposer si on veut « re-jouer » la signature sur le long terme ;
- l'émulation dont on sait qu'elle reste largement expérimentale ;
- la canonicalisation qui a pour principe de migrer le document vers un format plus pérenne (format XML canonique) avant de le signer, afin d'éviter de devoir opérer des migrations futures.

Aucune de ces approches ne permet de résoudre le problème : la première ne pose pas la question de la *conservation simultanée* du document et de la signature ; la seconde reste expérimentale ; la troisième ne permet que de repousser le problème dans le temps.

La dernière partie aborde les réponses apportées à cette question par de grandes institutions d'archives étrangères.

Les archives nationales américaines ont publié dès 2000, des recommandations pour les diverses administrations : si une administration veut conserver outre son contenu et son contexte, la structure d'un document, la préservation de celle-ci implique de respecter l'intégrité logique et physique du document et, par conséquent, de conserver les **équipements matériels et logiciels ayant servi à la création de la signature afin que le document puisse être validé a posteriori.**

Si l'administration ne juge pas indispensable de conserver la structure du document (ce que recommande la NARA pour les documents qui ont une longue durée d'utilité administrative), dans ce cas, la NARA prescrit la conservation des informations contextuelles permettant de documenter l'existence et la validité de la signature électronique ainsi que les mécanismes en place au moment de la signature.

Enfin, la NARA recommande **que, dans tous les cas, soient enregistrés en clair dans le document, le nom du signataire en toutes lettres, ainsi que la date de la signature.**

Les archives nationales australiennes ont, elles, établi des recommandations en 2004. Il est recommandé, si le risque juridique est nul ou faible, de se contenter de conserver des métadonnées sur la signature (identifiant du certificat à clé publique et de l'organisation qui l'a émis, informations relatives à la signature proprement dite comme l'algorithme, la date et heure où la signature a été apposée, vérifiée).

A l'inverse, si le risque est élevé, c'est aux administrations d'implanter un plan de gestion de clés, ce qui implique pour celles-ci la conservation de tous les certificats successifs, jetons d'horodatage, listes de révocation, audits du système. Lors de leur transfert aux archives nationales, celles-ci déclarent de pas pouvoir assurer la conservation de l'ensemble de ces éléments (elles ne pourront pas re-jouer les signatures a posteriori) mais s'assurent par contre de la conservation de toutes les informations contextuelles.

Les archives nationales du Canada abondent dans ce sens et précisent que dès le transfert des documents électroniques, la signature cessera d'être utile en tant que moyen de preuve mais que l' « authenticité » des documents reposera plutôt sur leur histoire, leur positionnement au sein de leur système d'information dans le cadre des activités de l'organisation, sur les éléments de contexte et de traçabilité accompagnant le document tout au long de son cycle de vie (respect de la chaîne de préservation).

Ces recommandations sont le reflet de principes et pratiques archivistiques qui font reposer l'évaluation de l'authenticité d'un document, sur un faisceau de critères dont la signature n'est qu'un élément : contexte de création, d'établissement, description et structuration, conservation de l'ensemble des événements tant organisationnels que physiques ou techniques qui ont pu affecter le document tout au long de son cycle de vie.

Conclusion

On retiendra par conséquent de ce rapport quelques éléments de réponses quant au positionnement que pourraient avoir les institutions publiques d'archives quant à l'archivage des documents électroniques signés avec des mécanismes basés sur la cryptographie :

- recommander aux administrations de bien déterminer quelles sont les catégories de documents méritant, au regard des risques de contentieux, une conservation de leur contenu, contexte et structure (intégrité physique et logique à maintenir dans le temps) au-delà de 1 à 3 ans (3 ans étant actuellement la durée de vie généralement admise d'un jeton d'horodatage);
- s'ils en existent, les enjoindre à mettre en place le temps qu'ils jugeront nécessaires, un plan de gestion des clés
- recommander aux administrations de ne pas exiger une telle préservation totale pour les documents à longue DUA
- dans tous les cas, demander à ce que soient enregistrés et figurent dans le document l'identification en clair du signataire ainsi que la date et heure de la signature
- dans tous les cas, conserver les informations contextuelles concernant la signature (voir les recommandations des archives australiennes)
- à partir du moment où le transfert dans les services d'archives s'opèrent, ne pas assurer la prise en charge de ces mécanismes, en considérant qu'on ne pourra plus « re-jouer » les signatures. Cette position est d'autant plus rationnelle qu'il y a très peu de chances qu'on ait encore à vérifier une signature apposée des années auparavant, et que le risque encouru ne vaut pas les coûts induit ; d'autant que les institutions d'archives ont toute une palette d'autres moyens, fondés sur les grands principes archivistiques, de jauger, à la lumière d'un faisceau d'indices, l'authenticité d'un document.

Françoise Banat-Berger