Les signatures numériques pour mettre l'individu au centre de son patrimoine de compétences

Sylvain Lagrue *David Markowski*

Les auteurs

Sylvain Lagrue est Maître de Conférence à l'Université d'Artois, dont il est correspondant C2i2 métiers de l'ingénieur.
David Markowski est chargé de mission Université Numérique à l'Université d'Artois et Membre du Groupe de Travail C2i au MESR.

Mots clés : patrimoine de compétences, signature numérique, authenticité, autonomie et responsabilité, transférabilité des données

1. Introduction et problématique

Dans un contexte de formation tout au long de la vie, pour reprendre des cycles d'apprentissage comme pour intégrer des organisations professionnelles, la problématique de la preuve est posée quant à la véracité des témoignages de compétence. Deux voies sont possibles. Une première, pouvant sembler irréaliste, consisterait en un hébergement institutionnel national voire supranational des traces d'activités et des validations des compétences. Ces dernières prenant souvent la forme de fichiers numériques de plus en plus volumineux, il semble illusoire de prétendre tous les stocker de manière centralisée.
A contrario d'une certaine fuite en avant vers une concentration de stockage de données toujours plus volumineuse et problématiques sur le plan de la conservation des données personnelles[1], nous proposons une réponse décentralisée par laquelle chaque individu pourra justifier de l'authenticité de ses traces en interpellant le réseau de confiance, garant des preuves d'acquis de la formation comme de ceux de l'expérience professionnelle. Par le passage de « serveurs de stockage » à des « serveurs de signature », les volumes de données sont réduits à l'extrême. Ce dispositif global peut être offert à chacun et se situe au coeur d'un réseau d'acteurs responsables.

En outre, dès lors qu'une organisation détient des documents, résultats de productions individuelles ou de groupes, elle est doit prendre en compte les problématiques liés aux données personnelles. Sur les plateformes pédagogiques, des suppressions de données, généralement annuelles sur la plupart des espaces de cours sont réalisées, exception faite de données à conserver sur plusieurs années dans le cas notable des certifications débutant en première année de cursus et s'achevant deux ou trois semestres plus tard. Mais au-delà, l'institution universitaire est-elle en droit de conserver des données aussi personnelles que : qui a accompli quoi avec qui en quel lieu et à quelle date et a émis tel ou tel avis sur telle thèse ou idée si on considère tacite la reconduction de détention des données ? Aussi, quelle est la garantie offerte par l'institution quant à la pérennité dans la conservation et l'accès aux données personnelles ?

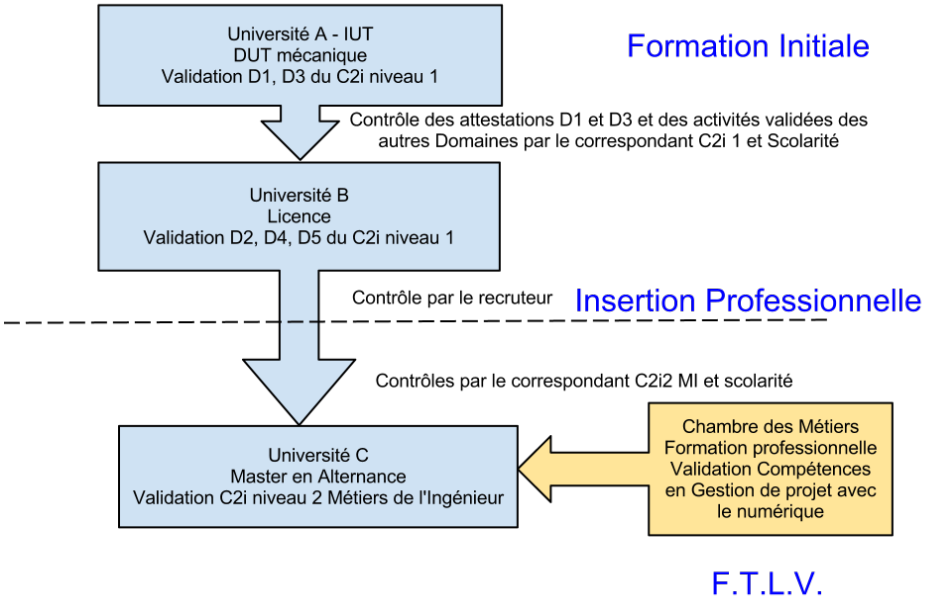
[1] "Les données ne peuvent être conservées dans les fichiers au delà de la durée nécessaire à la finalité poursuivie qu'à des fins historiques, statistiques ou scientifiques ;", loi dite "informatique et libertés" du 6 janvier 1978.

Enfin comment rendre accessible un faisceau de preuves à un tiers tel qu'un autre établissement de formation ou d'un recruteur dans le contexte de validation des dossiers de candidature à tel formation ou à tel poste exigeant des compétences, dès lors qu'il sont exclusivement intégrés dans un système d'information évidemment sécurisé ?

Une approche diamétralement différente peut être envisagée : egocentrée, plus conforme à la réalité et certainement plus pérenne qui relève de la constitution et la diffusion libre par chaque individu d'un ensemble de compétences et des « objets » associés sur des sites institutionnels, communautaires ou personnels. Elle pose en revanche le problème des preuves de la validation de ces compétences. Il s'agit donc de trouver une solution par laquelle, tout en préservant la flexibilité correspondant à l'usage libre de ses données personnelles, celles-ci puissent être « garanties » vis à vis par exemple d'une direction des études à distance, d'un organisme de formation continue exigeant des prérequis ou encore un employeur potentiel face à un document qu'il souhaite voir attesté.

2. Scénario d'utilisation

Formation initiale ou tout au long de la vie, emplois successifs sont jalonnés de moment d'acquisition de compétences délivrées par des instances universitaires ou professionnelles. À travers un exemple nous pouvons illustrer une succession de situations au cours desquelles il est nécessaire de justifier de l'acquisition de compétences et rendre de fait utile la mise en oeuvre d'un dispositif permettant de justifier auprès de l'autorité nouvelle, de la preuve de l'authenticité des éléments apportés.



Dans la situation illustrée ci-dessus, nous avons un individu qui va devoir justifier de l'acquisition de compétences auprès d'instances universitaires en changeant d'université tant en formation initiale que continue, ainsi qu'auprès d'un recruteur. Dans cet exemple, des compétences du C2i attestées en contexte universitaire et des compétences délivrées par des organismes de formation professionnelle peuvent coexister et constituer un patrimoine de compétences dont le porteur pourra justifier en présentant ses réalisations sur base de son e-portfolio dont chaque élément sera reconnu comme étant un original pédagogiquement approuvé.

3. Une solution basée sur les signatures numériques

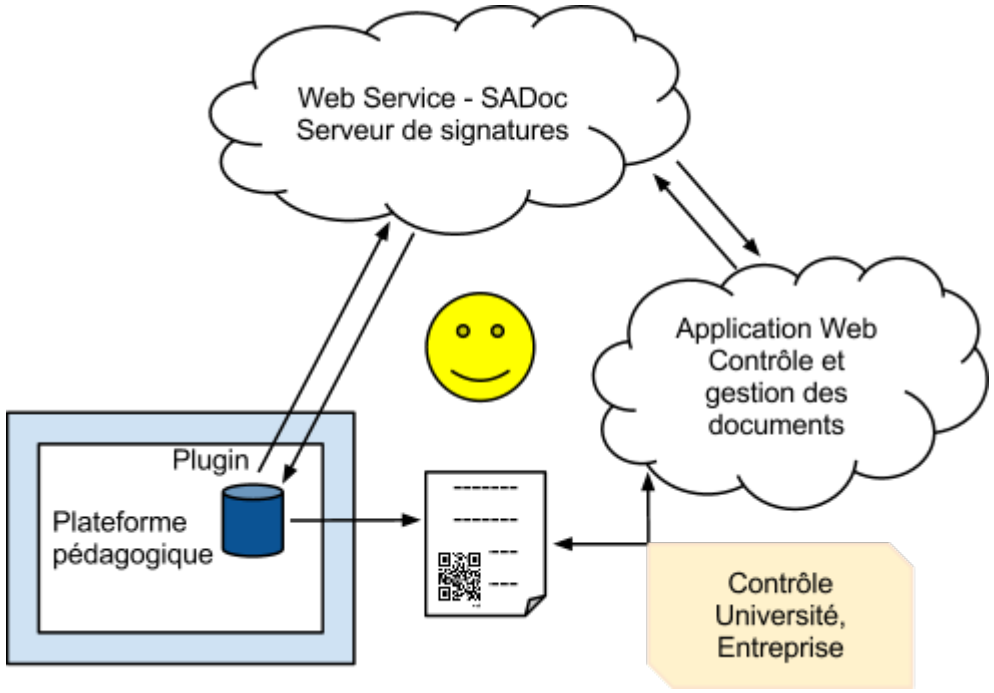
Les signatures numériques

Les signatures numériques de document sont des mécanismes basés sur des méthodes de chiffrement asymétriques permettant à la fois **d'authentifier** l'auteur d'un document numérique, mais également d'en assurer son **intégrité** [1]. En France, et en conformité avec les directives européennes, ces signatures numériques ont légalement même valeur qu'une signature manuscrite [2]. Elles sont basées sur la cryptographie asymétrique et les fonctions de hachage. Une fonction de hachage permet de calculer une empreinte du document. Cette empreinte sera ensuite chiffrée à l'aide de la clé *privée*. Afin de vérifier l'intégrité du document, il suffit de déchiffrer l'empreinte à l'aide de la clé *publique* et de vérifier que celle-ci est bien la même que celle calculée à l'aide de la même méthode. Toute modification du document modifiant systématiquement l'empreinte, seul le possesseur de la clé privée pourra à nouveau signer ce document.

Nous nous appuyons ici sur la norme de cryptographie pour les infrastructures à clés publiques (PKI) de l'Union internationale des télécommunications : X.509. Dans ce cadre, la signature numérique est basée sur des certificats contenant les clés privées et publiques ainsi que l'identité du possesseur des documents.

Architecture proposée

L'architecture que nous proposons ici repose sur un service web pouvant être appelé par 2 entités : la plateforme de type e-portfolio lors de l'export des fichiers et une application web permettant aux possesseurs de documents de les gérer et aux personnes, souhaitant les vérifier, de le faire également.



Le service web, qui est le cœur de l'architecture, possède les fonctionnalités suivantes :

- stockage des certificats des propriétaires et des empreintes des fichiers ainsi que l'URL facultative du fichier ;
- lors d'un export, de signer numériquement le fichier en le modifiant (ajout d'un flashcode pour les pdf par exemple) ;
- il permet également de vérifier l'authenticité d'un fichier, soit en envoyant un fichier de type .p7s contenant le certificat public ainsi que l'emprunte du document, soit par téléchargement direct du fichier.

L'*autorité de certification pédagogique* délègue donc le stockage de l'empreinte et de l'identité

du propriétaire du fichier au web service. Charge à l'utilisateur de stocker ses fichiers afin de les rendre disponible.

Processus

Grâce à un plugin greffé à un applicatif de dépôt et de validation d'activité ou e-portfolio d'évaluation des compétences, l'individu peut, dès lors que l'activité a été pédagogiquement validée, lancer par simple clic le chiffrement de son document via un service web. Ce service web chiffre le document et d'une part conserve les seules informations utiles à son authentification future par un tiers et, d'autre part, retourne le document numériquement greffé d'une marque de codes-barres en deux dimensions (flashcode) comportant une simple adresse web (URL). Ce document pourra en l'état numérique ou publié sur papier être présenté à un tiers qui, dans le premier cas cliquera sur l'objet flashcode, et dans le second cas "flashera" le code à l'aide de son équipement mobile tel un smartphone. Dès lors l'application web est mobilisée. En première utilisation, le contrôleur, obtient, à partir du code inclus dans le document l'identification de l'auteur, le nom du document, l'URL à laquelle est téléchargeable le document et enfin les compétences validées. Une autre démarche possible consiste en un "upload" du document présenté sous forme numérique en vue de recalculer l'empreinte afin de la comparer à celle stockée sur le service web (SADoc). L'application affiche le résultat de la comparaison et donc, dans le cas positif, atteste de l'authenticité de celui qui est présenté.

On le constate, c'est au prix infime de 3 à 5 kilo-octets que des documents sont identifiables et authentifiables alors qu'ils peuvent être eux-mêmes, avec la généralisation de contenus mlultimédia avoir un poids parfois exprimés en centaines de méga-octets L'auteur reste le seul dépositaire de ses publications, qu'il peut conserver sur un espace institutionnel ou dans un e-portfolio individuel, sur un site web, un espace partgé du cloud, dans son blog ou encore sur son espace de réseau social ou enfin, simplement être conservé en version imprimée par choix personnel ou en réponse à des consignes de confidentialité. De plus, rien n'est figé, le jour ou l'individu décide de changer de site de dépôt, il lui suffira ensuite de renseigner la nouvelle URL dans l'application web pour interroger de nouveau l'authentiticé du document. La mobilité devient donc une réalité compatible avec la sécurité.

Une implémentation : SADoc

Un prototype, SADoc (pour Service d'Authenfification de Documents) a été développé dans le but de valider la méthode proposée. Les sources sont d'ores et déjà disponibles [3]. Ce prototype est basé sur des technologies professionnelles OpenSource en utilisant la technologie JEE, le *framework* Spring et la bibliothèque Buncycastle pour ne citer que les principales. Un plugin, étendant le module référentiel réalisé par Jean Fruitet pour Moodle [4], a été développé pour la plateforme moodle 1.9, cette plateforme faisant office de e-portfolio.

5. Conclusion

Nous proposons une solution pratique, en cours de mise en œuvre dans une application open source, basée sur des normes reconnues, ouvertes et interopérables, à vocation d'usage inter-établissement, notamment portée par les Université Numériques en Région (UNR), mais aussi transposable à toute structure de certification. Celle-ci offrant de signer numériquement les traces des compétences validées par l'institution en conservant leur validation pédagogique et institutionnelle et au besoin tous documents de type attestations (certificats de compétences, attestations partielles, brevets, diplômes suite au plan Licence). Elle permet également de générer au profit de son auteur les preuves authentifiés à usage flexible et d'offrir les services web permettant à des tiers de vérifier l'adéquation entre les preuves physiques ou numériques transmises ou hébergées en ligne (espaces de stockages institutionnels ou individuels « dans les nuages » isolés ou intégrés dans un e-Portfolio). Les bénéfices directs sont les suivants :

- gain de stockage ;
- transférabilité de la validation ;
- mobilité et accès préservé des données personnelles ;
- indépendance à la plateforme e-portfolio (au plugin près).

En conclusion, ce dispositif est conçu pour des individus de plus en plus mobiles désirant prouver leurs acquis universitaires, professionnels ou citoyens, et pour, face à eux, les acteurs de la formation et de l'emploi à la recherche d'une garantie préalable quant aux compétences de leurs candidats.

Références

[1] Infrastructure à Clés Publiques: Signature numérique, Cryptographie, Chiffrement, Certificat électronique, Authentification forte, Identité numérique, Hardware Security Module, de Frederic P. Miller, Agnes F. Vandome, John McBrewster (Alphascript Publishing edt.).

[2] loi n° 2000-230 du 13 mars 2000 et le décret 2001-272 du 30 Mars 2001 (Référence NOR : JUSC0120141D), pris en application de la loi de Février 2000 modifiant l'article 1316-4 du Code Civil

[3] https://code.google.com/p/sadoc/

[4] Récentes évolutions du module Référentiel pour la certification des compétences. J. Fruitet. Moodle Moot 2009