

Plateforme mutualisée de signature électronique

Emmanuelle Prévost

Chef de projet maîtrise d'ouvrage en systèmes d'information,
Responsable du domaine décisionnel et du domaine de la dématérialisation

Secrétariat général - Service des Technologies et des Systèmes d'Information (SG / STSI-SDITE / A1)
Ministère de l'Éducation Nationale - Ministère de l'Enseignement Supérieur et de la Recherche
61-65, rue Dutot 75732 Paris Cedex 15

Résumé

La dématérialisation des procédures, documents, échanges..., est une démarche généralisée dans le fonctionnement interne de l'administration du ministère comme dans le cadre des télé-procédures mises à disposition des enseignants, élèves, parents d'élèves... Toutefois, les objectifs de simplification, accessibilité, interopérabilité, ou encore transparence et sécurisation, ne seront pleinement atteints que si le document électronique a la même valeur juridique que le document papier.

Dans ce cadre, le Service des technologies et des Systèmes d'Information des ministères de l'éducation nationale, enseignement supérieur et recherche souhaite se doter d'une plateforme mutualisée de signature électronique. En mutualisant les opérations d'apposition et de vérification de signature de documents soumis à la demande ou dans le cadre d'application de gestion de processus électronique, le ministère se donne les moyens de garantir :

- *l'intégrité d'un document («certifié conforme») ;*
- *l'authenticité d'un document ;*
- *la provenance d'un document (équivalent au tampon de la société ou structure administrative émettrice) ;*
- *la non répudiation d'un document pour l'usager comme pour le ministère ;*
- *le caractère d'opposabilité juridique pour les deux parties.*

Sur la base d'une première application de dématérialisation cliente de cette plateforme, seront présentés les résultats d'une étude juridico-technique à savoir :

- *qu'entend-on par signature électronique ?*
- *quelle signature pour quelle nature de document ?*
- *comment maîtriser les problématiques d'authentification et offrir des services de certifications graduées tenant compte ou non de l'identité de la personne en limitant la logistique nécessaire ?*
- *quelles préconisations techniques peut-on envisager ?*

Mots-clefs

Confiance numérique, Certificat, Signature électronique

1 Introduction

Dans un contexte de recherche d'économies d'échelle et de simplifications, l'État cherche à dématérialiser au maximum tout ce qui repose sur des échanges papier. Certains circuits comportent des documents internes (notes, circulaires, etc.). D'autres impliquent plusieurs structures administratives relevant de statut juridique et de tutelles différentes (actes, rapports...). Enfin des échanges sont à prévoir entre administration et particuliers, agents (chercheurs), ou relevant du grand public (élèves, parents d'élèves...)

Pour parvenir à l'objectif visé, plus accessible, moins onéreux, il est nécessaire, outre le fait de ne pas exclure de citoyens par les effets d'une fracture numérique subie ou par quelque handicap, de susciter suffisamment d'adhésion des différentes parties prenantes d'un tel système. La confiance nécessaire pourra être gagnée en travaillant sur les aspects de transparence et de sécurisation. Elle ne pourra être envisageable que si le document électronique a la même valeur

juridique que le document papier, et s'il est offert des garanties suffisantes pour que soit peu probable un détournement ou une falsification lors de l'élaboration ou de l'utilisation d'un document numérique. Cela semble envisageable en mutualisant des techniques de pointe et de savoir-faire associés pour signer des documents soumis à la demande ou via des applications. Pour s'en assurer, cette étude propose d'identifier les risques juridiques techniques en s'appuyant sur l'exemple de l'application Dem'Act : pionnière du domaine, il s'agit de gestion électronique des processus et de documents, visant à dématérialiser des actes émis en Établissement Public Locaux d'Enseignement (EPLÉ) et visant à simplifier les circuits d'informations et de validation entre EPLÉ, rectorat, Collectivité territoriale...

Dem'Act a permis d'identifier les principales contraintes pour la mise en place d'une plateforme mutualisée de signature électronique, à savoir la conformité juridique des documents signés, la sécurité de l'accès à la fonctionnalité de signature électronique (afin d'éviter tout risque de "vraie fausse" signature) et la gestion de différentes formes de signatures et de certificats. Les exigences en termes d'architecture et de circuit d'informations sont :

1. Les dispositifs de sécurité et de contrôles doivent être placés côté serveur (sauf application sensible) ;
2. Les ressources demandées à l'agent, utilisateur d'application, doivent être larges et compatibles avec tout matériel professionnel (parc sous contrôle ou conseillé par le ministère, ou parcs d'autres ministères) ;
3. Les ressources demandées à l'utilisateur grand public doivent être compatibles avec des matériels divers récents ou âgés, sans contraintes de constructeurs ou de systèmes d'exploitation... ;
4. Les sollicitations des services de la plateforme mutualisée de signature électronique peuvent se faire :
 - a. via une application cliente, qui devra se conformer à un cahier des charges-cadre précisant les modalités de raccordement des applications clientes ;
 - b. via un formulaire de soumission de demandes récurrentes ;
 - c. via un formulaire de soumission de demandes "à la volée" ou jetables.

La Plateforme de signature électronique doit permettre l'apposition de signature électronique, avec différents niveaux de sécurité, représentant l'établissement ou une personne, externe ou intégrée au document. Lorsque la signature électronique sera intégrée au document, elle pourra prendre une apparence « officielle », ce qui aura pour effet de renforcer la confiance en l'acte produit. La plate-forme doit offrir les moyens de vérifier la validité et le contenu d'une signature via l'application cliente d'origine et/ou hors application. Dans le cas où la nature d'un document engage l'administration, la plateforme doit permettre d'apporter la preuve de l'authenticité et de la régularité du document. Sinon l'administration se bornera à apporter la preuve de conformité entre le document et ce qui lui a été soumis lorsqu'elle l'a « sertie » en y apposant l'équivalent de son tampon. Étant universelle cette plateforme sera amenée à apposer des signatures de différentes natures (portée, valeur...) selon le type de document soumis (ouvrant des droits, acte, note, information, livret scolaire numérique...) et le niveau de risque encouru (recours, contentieux et impacts). Il est illusoire de pouvoir couvrir a priori la définition juridique de toute situation, toute dématérialisation quelque soient les futures applications à mettre en place. Toutefois, il s'agit ici de présenter une clarification des concepts, d'initier des classifications et démarches qui pourront servir d'exemple.

2 Acte administratif / Juridique

Pour répondre à la question "les actes administratifs peuvent-ils être dématérialisés et signés électroniquement, et avec quel niveau de signature électronique", il est nécessaire d'étudier le cadre¹ légal des actes administratifs dans lequel s'inscrit l'application, celui de la signature électronique, etc.

2.1 Caractéristiques d'un acte

Les documents gérés au sein de l'application Dem'Act sont principalement des actes administratifs. Ils produisent des effets de droit, c'est-à-dire que soit ils imposent des obligations, soit ils confèrent des droits à l'égard des tiers sans le consentement de ceux-ci (on parle de décision exécutoire). Sont à distinguer les actes réglementaires, normatifs à portée générale et impersonnelle, des actes individuels à portée limitée aux destinataires nominativement désignés.

Certains actes émanant des personnes publiques sont des actes de droit privé liés à l'exercice de la gestion privée pour lesquels la compétence de la juridiction administrative est exclue. Il s'agira de décisions non réglementaires relatives à

¹ Articles 1316-1 et 1316-4 du Code civil, instituant l'écrit électronique et la signature électronique, de la loi n° 2004-1343 du 9 décembre 2004 de simplification du droit, Ordonnance n° 200 : Le Référentiel Général de Sécurité (RGS), est établi dans le but de fixer, selon le niveau de sécurité requis, déterminé retenu par l'autorité administrative, les règles que doivent respecter certaines fonctions contribuant à la sécurité des informations. 5-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

la gestion du domaine privé, ou relatives à la gestion des services publics industriels et commerciaux. D'autres actes de personnes privées peuvent être administratifs lorsqu'ils interviennent dans le cadre d'une mission de service public (par exemple lorsqu'ils traduisent la mise en œuvre d'un service public).

L'acte administratif est une mesure prise par une autorité ayant pour effet de modifier ou d'affecter la situation de ses destinataires ou l'ordre juridique. Il comporte un caractère exécutoire, décisive et faisant grief². Certains documents relèvent des « mesures d'ordre intérieur » et ne peuvent être qualifiés d'actes administratifs. Par ailleurs, tant qu'un acte ne correspond pas à une décision, il ne risque pas de recours devant le juge administratif, sauf si l'illégalité l'entachant peut constituer un élément de recours formé contre une décision. Parmi les actes non décisifs et non exécutoires, on retiendra entre autres les avis (dès lors qu'ils n'emportent aucun caractère obligatoire et opposable), les mises en demeure, les directives, les circulaires (à l'exception de circulaires à caractère réglementaire modifiant l'ordonnement juridique), etc.

Ainsi, ne sont pas considérés comme actes administratifs d'établissements publics locaux d'enseignement (EPL) : la motion ne donnant pas lieu à délibération, le rapport, la note de service, etc. En revanche, les délibérations du conseil d'administration formalisées, les décisions du chef d'établissement répondant aux critères des actes administratifs ci-dessus, ou encore les délibérations de la commission permanente sur délégation du conseil d'administration sont des actes administratifs d'EPL.

2.2 La signature de l'acte administratif, condition de forme et de fond

2.2.1 Mentions :

La date d'édition n'est obligatoire que dans le cas où elle est le départ d'un délai. Son absence n'entraîne pas l'irrégularité de l'acte. La date de signature en revanche est nécessaire : un acte administratif existe juridiquement à la date de sa signature³. Si l'acte n'est pas signé, même s'il est publié ou notifié, il n'existe pas et est donc sans effet juridique⁴. La légalité d'un acte administratif s'apprécie à la date à laquelle il a été signé⁵. Les décisions des autorités administratives doivent comporter obligatoirement⁶ : la signature de l'auteur de l'acte, son nom et prénom; sa qualité.

2.2.2 Délégations de signature :

Il est possible de prévoir deux types de délégation : la délégation de signature du chef d'établissement, et la délégation du conseil d'administration à la commission permanente.

2.3 Transmission et publication

Pour être exécutoires, les actes administratifs doivent être publiés (collectifs) ou notifiés (individuels). Le chef d'établissement d'un EPL doit effectuer la publication par voie d'affichage ou par notification individuelle. Dans certains cas, il doit certifier leur caractère exécutoire.

Les actes non transmissibles sont exécutoires dès publication ou notification individuelle. Les actes transmissibles ne deviennent exécutoires qu'après leur transmission à l'Autorité de Contrôle (AC). Seuls certains actes transmissibles font l'objet d'un accusé de réception du destinataire. Pour tout acte transmissible, la date de transmission est importante, car elle fait courir les délais. Le représentant de l'Etat, l'autorité académique et la collectivité territoriale de rattachement peuvent demander à avoir accès⁷ à l'ensemble des actes et documents relatifs au fonctionnement de l'établissement.

3 Qu'entend-t-on par signature ?

3.1 Signature électronique

« Lorsqu'elle est électronique [i.e. la signature], elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache... »⁸

² Une décision fait grief si elle modifie la situation juridique d'une personne. Dans ce cas, elle peut faire l'objet d'une contestation devant le juge.

³ "La date de l'acte est celle du jour où son auteur l'adopte et plus particulièrement le signe" P. Delvolvé, l'acte administratif, Sirey n°441 p. 186

⁴ CE 26 01 1951, Galy, S 1951 3 p. 52.

⁵ CE sect. 14 11 1969, Houdebert, rec. 502.

⁶ "Toute décision prise par l'une des autorités administratives mentionnées à l'article 1er comporte, outre la signature de son auteur, la mention en caractères lisibles, du prénom, du nom et de la qualité de celui-ci." article 4, chapitre II de la Loi n°2000-321 du 12 04 2000 relative aux droits des citoyens dans leurs relations avec les administrations, relative à la transparence administrative

⁷ Article R.421-56 du Code de l'Éducation (Droit d'accès)

⁸ Article 1316-4 alinéa 2 du Code civil

La signature électronique est un code obtenu à partir d'une fonction de cryptographie qui va sceller le document avec l'identité du signataire. Elle repose sur l'utilisation d'un certificat électronique délivré par un prestataire de services de certification électronique (PSCE). Deux niveaux de fiabilité de signature électronique existent : la signature électronique simple et la signature électronique sécurisée. Quelle qu'elle soit, pour être juridiquement recevable, elle doit apporter des garanties :

- d'identification de son signataire ;
- d'intégrité, c'est à dire la possibilité de détecter une altération de l'acte ;
- d'un lien logique entre le signataire et l'acte.

3.1.1 Signature électronique simple

*« Une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil ».*⁹

La signature électronique simple répond à la définition de la signature électronique et doit reposer sur :

- un procédé fiable d'identification ;
- être attachée à l'acte sur lequel elle est apposée, qui par conséquent doit rester intègre.

3.1.2 Signature électronique sécurisée

Une « signature électronique sécurisée »¹⁰ répond à la définition de la signature électronique simple et aux exigences :

- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.

3.1.3 Présomption de fiabilité

*« La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié »*¹¹

La présomption de fiabilité¹² du procédé permet de renverser la charge de la preuve de fiabilité sur le signataire, car elle repose sur un mécanisme permettant d'identifier le signataire. Le « certificat électronique qualifié »¹³ doit comporter certains éléments et être délivré par un PSCE qui satisfait lui-même à certaines exigences fortement contraignantes.

Pour bénéficier de la présomption de fiabilité, il est nécessaire de recourir à un dispositif sécurisé de signature électronique¹⁴. Si la signature n'est pas présumée fiable, il appartient au signataire de démontrer la fiabilité du procédé de signature électronique, qui dépend essentiellement de l'identification du signataire, c'est-à-dire des conditions dans lesquelles intervient la délivrance du certificat électronique. En cas de contestation, le juge devra déterminer si telle ou telle signature doit être considérée comme étant fiable ou non, quelle que soit l'application considérée et même si le procédé bénéficie de la présomption de fiabilité.

3.1.4 Reconnaissance juridictionnelle de la signature électronique

La première décision significative reconnaissant la validité de la signature électronique date de 2013 et elle se fonde sur l'examen du « fichier de preuve » de l'acte signé électroniquement.¹⁵ Il s'agissait de signature à la volée, non envisagée dans Dém'Act.

3.2 Signature numérique

*« La signature numérique consiste en une signature manuscrite conservée sous forme numérique après avoir été apposée sur un écran tactile, au moyen d'un appareil sécurisé garantissant l'intégrité de l'acte dès que la signature a été enregistrée. »*¹⁶

⁹ Décret du 30 mars 2001 (Décr. 2001-272 du 30-3-2001, art. 1)

¹⁰ Décret 2001-272 du 30 mars 2001 fixant les conditions de création de signature électronique pour qu'elle soit reconnue comme étant sécurisée (Art. 3 § II)

¹¹ Décret 2001-272 du 30 mars 2001 (Décr. 2001-272 du 30-3-2001, art. 2.)

¹² C. civ., art. 1316-4, 2nd alinéa 2nde phrase

¹³ Annexe : certificat électronique qualifié.

¹⁴ Annexe : dispositif de création de signature électronique sécurisé.

¹⁵ Cour d'appel de Nancy 14-2-2013, RG 12/01383, Pôle 01 Ch.3. (Examen de la signature électronique de l'autorisation de découvert, à partir d'éléments techniques dont « le fichier de preuve de la transaction » ; La présomption de fiabilité de la signature électronique du document est en l'espèce rapportée par le fichier de preuve technique, consacrant ainsi la signature électronique présumée fiable d'un document dématérialisé)

L'utilisation d'une signature numérique ne requiert pas l'intervention d'un prestataire de confiance. Son utilisation impose la maîtrise du matériel permettant d'apposer sa signature. Il est nécessaire de pouvoir démontrer le lien entre le document et la signature pour garantir sa recevabilité.

La signature numérique n'est utilisée que par les différents acteurs intervenant dans le cadre d'une procédure pénale.

3.3 Signature digitale ou image numérique d'une signature manuscrite

Il n'existe aucune définition légale de la signature digitale, même si elle constitue une signature au sens des dispositions de l'article 1316-4, alinéa 1^{er} du Code civil¹⁷.

La signature digitale consiste à signer de manière manuscrite un écran tactile ou une tablette numérique. Elle n'exige pas de lien avec le document signé. Toutefois l'absence de scellement entre la signature et le document fait obstacle à sa reconnaissance en tant que signature numérique.

3.4 Signature scannée

Il n'existe aucune définition légale de la signature scannée, même si elle constitue une signature au sens des dispositions de l'article 1316-4, alinéa 1^{er} du Code civil

Il s'agit de l'image scannée d'une signature manuscrite. Il peut s'agir de tout document papier sur lequel a été apposée une signature manuscrite. Ce procédé nécessite de conserver l'original du document signé à la main ou à défaut de conserver une copie fidèle et durable conformément aux dispositions de l'article 1348 du Code civil. L'utilisation d'une signature scannée ne permet pas d'identifier le signataire puisqu'elle ne permet pas de démontrer, à elle seule, que le titulaire de la signature a sous son contrôle exclusif la maîtrise de son apposition ou qu'il en est personnellement l'auteur (jurisprudence).

3.5 Traduction pour la plateforme de signature électronique

Les signatures numériques, digitales ou scannées n'ont pas lieu d'être traduites par la mise en œuvre de service au sein de l'offre de la plateforme de signature électronique. Les signatures électroniques simples et sécurisées feront l'objet de mise en œuvre de services au sein de cette plateforme avec différents niveaux de sécurité possible (cf. § 4.3)

4 Usage dans le cadre de la dématérialisation des actes administratifs

4.1 Autorité administrative, qui est concerné ?

*« Les actes des autorités administratives peuvent faire l'objet d'une signature électronique. Celle-ci n'est valablement apposée que par l'usage d'un procédé, conforme aux règles du référentiel général de sécurité mentionné au I de l'article 9, qui permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte ».*¹⁸

Les autorités administratives sont notamment les établissements publics à caractère administratifs et les autres organismes chargés de la gestion d'un service public administratif. Les EPLE sont des autorités administratives.

*« Lorsqu'une autorité administrative met en place un système d'information, elle détermine les fonctions de sécurité nécessaires pour protéger ce système. Pour les fonctions de sécurité traitées par le référentiel général de sécurité, elle fixe le niveau de sécurité requis parmi les niveaux prévus et respecte les règles correspondantes. »*¹⁹

4.2 Validité de signature électronique des actes des Autorités Administratives (AA)

Un procédé qui fixe les modalités des échanges électroniques conformes au RGS (fonctions d'identification, de signature électronique, de confidentialité et d'horodatage)²⁰ doit :

- permettre l'identification du signataire de l'acte ;
- garantir le lien de la signature avec l'acte auquel elle s'attache ;
- assurer l'intégrité de l'acte.

¹⁶ Article R249-11 du Code de procédure pénale

¹⁷ « La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. »

¹⁸ Article 8 de l'Ordonnance n°2005-1516 du 8 12 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre autorités administratives ; Décret n°2010-112 du 2 février 2010 pris pour application des articles 9, 10 et 12 de l'ordonnance du 8 12 2005 précitée.

¹⁹ Article 9 – II de Ordonnance n°2005-1516 du 8 12 2005 Chapitre IV : Dispositions relatives à la sécurité des informations échangées par voie électronique entre les usagers et les autorités administratives et entre les autorités administratives

²⁰ Article 9 – I de Ordonnance n°2005-1516 du 8 12 2005 Chapitre IV : Dispositions relatives à la sécurité des informations échangées par voie électronique entre les usagers et les autorités administratives et entre les autorités administratives

Les conditions de délivrance des certificats électroniques²¹ aux autorités administratives et à leurs agents doivent faire l'objet d'une validation par l'Agence nationale de la sécurité des systèmes d'information (Anssi).

4.3 La signature électronique selon le RGS

« La signature électronique est l'une des fonctions de sécurité apportant de la confiance dans les échanges dématérialisés entre usagers et AA ou entre AA. »²²

4.3.1 Périmètre :

Le RGS couvre :

- la signature électronique par un usager, et sa vérification par un téléservice d'une autorité administrative,
- la signature électronique par un usager, puis vérification par un agent d'une autorité administrative,
- la signature électronique par un agent d'une autorité administrative, puis vérification par un usager,
- la signature électronique par un agent d'un acte administratif puis vérification par un autre agent (sont visés là, les actes des EPLE, transmissibles à une autorité de contrôle, gérés au sein de Dem'Act).

Le RGS détermine aussi les règles applicables à :

- l'authentification,
- la confidentialité,
- l'horodatage,
- l'accusé d'enregistrement et aux accusés de réception.

4.3.2 Niveaux de signature électronique (de personne).

Le niveau de sécurité requis pour l'usage de la signature électronique de l'acte administratif doit être fixé par l'autorité administrative²³ afin de "répondre de manière proportionnée au besoin de protection du système et des informations face aux risques identifiés". Cette analyse doit être faite par l'autorité administrative, acte par acte. Une fois déterminé le niveau de sécurité souhaité de la fonction de sécurité "signature", les exigences correspondantes à ce niveau doivent être respectées pour chacun des composants suivants :

- la bi-clé du certificat électronique permettant la création et la vérification de signature électronique ;
- le dispositif de création de signature électronique ;
- le module de vérification de signature électronique ;
- l'application de création de signature électronique ;
- le certificat électronique : contenu du certificat, conditions d'émission par le PSCE, dispositif de stockage de la clé privée.

La génération et le référencement des certificats s'effectuent en fonction du niveau de risque de leurs applications. Suivant ce niveau, les différentes autorités publiques (et privées), définissent le certificat requis pour leurs applications pour lesquels le RGS propose trois niveaux de sécurité croissants : une étoile *, deux étoiles **, trois étoiles***.

REFERENTIEL GENERAL DE SECURITE ²⁴		
	Risque d'usurpation	Modalités de délivrance
1 étoile (*)	Moyen	Vérification de l'identité par l'envoi d'un dossier papier ou électronique
2 étoiles (**)	Fort	Vérification des pièces d'identité originales, en face à face avec le porteur ou sous forme dématérialisée avec signature électronique de niveau 2 étoiles et sous condition de vérification.
3 étoiles (***)	Très fort	Vérification des pièces d'identité originales, en face à face avec le porteur C'est à ce niveau qu'une signature électronique est présumée fiable, au sens de l'article 1316-4 du code civil, à condition que ladite signature électronique soit sécurisée.
La différence entre le 2 étoiles (**) et le 3 étoiles (***) ne tient pas aux modalités de délivrance mais à la qualification du dispositif d'authentification.		

²¹ Article 10 de l'ordonnance du 8 décembre 2005 et son décret d'application dans sa version consolidée au 04 11 2012 : n° 2010-112 du 2 02 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 12 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

²² Article II de l'annexe 3 "fonction de sécurité Signature" du RGS

²³ Article 3, alinéa 2° du décret n°2010-112 du 2 février 2010 (Décret n°2010-112 du 2 02 2010).

²⁴ Annexe A8 version 2.3 PCT « Signature » du RGS.

Les règles communes à tous les mécanismes cryptographiques doivent être respectées dès lors que la **cryptographie** est mise en œuvre au sein des fonctions de signature électroniques ²⁵

4.3.3 « Cachet » et téléservice.

La fonction de « cachet » concerne les échanges dématérialisés faisant intervenir des serveurs (applicatifs), téléservices automatisés (machine à machine). Elle est l'équivalent pour une machine ou pour une personne morale de ce qu'est la signature pour une personne physique. La mise en œuvre de la fonction de sécurité « cachet » peut se faire également selon les trois niveaux de sécurité définis au RGS. C'est l'autorité administrative qui doit déterminer le niveau de sécurité souhaité de la fonction "cachet" après une analyse de risque.

4.4 Application et pistes d'analyses

Dem'Act vise la dématérialisation d'une cinquantaine d'actes, lesquels ont fait l'objet d'une étude documentaire approfondie et ont donné lieu à une classification par niveau de risque.

4.4.1 La signature électronique des actes d'EPLÉ et l'application Dem'Act : recommandations

Le signataire : au sein d'un EPLE, tous les actes étudiés sont généralement signés de la même personne, le chef d'établissement, ou par son délégataire désigné. Il signera soit en sa qualité de président du conseil d'administration, soit de président de la commission permanente, soit de chef d'établissement pour ce qui relève de sa compétence exclusive.

Le matériel et le système d'information : Le Ministère n'a le contrôle ni du parc déployé (matériel), ni des systèmes d'information des EPLE, collectivité, etc. Le SI de l'EPLÉ reste sous la responsabilité du chef d'établissement.

Caractéristiques des actes gérés au sein de Dem'Act :

- les actes doivent être signés ;
- les actes signés peuvent faire l'objet de recours (ou contestations) comme tout acte administratif ;
- les actes relèvent du domaine de l'action éducatrice ou du domaine du fonctionnement de l'EPLÉ ;
- une majorité de ces actes résulte d'une décision collective ou d'avis consultatif préalable ;
- un grand nombre d'actes est soumis à transmission à l'autorité de contrôle faisant l'objet d'un récépissé de dépôt; cette autorité peut présenter des observations ;
- certains actes transmissibles font l'objet d'un accusé de réception signé de la part du destinataire ;
- ces actes ont une portée limitée dans l'espace (un EPLE), dans le temps (majoritairement la durée de vie est une année scolaire. Les exceptions concerneront, par exemple, des décisions de recourir à un marché public, des acquisitions et aliénations des biens, dons et legs, action en justice...).

Synthèse : il résulte de cette analyse documentaire effectuée et des entretiens avec les Maîtrises d'Ouvrages de Dem'Act, que le risque lié à la dématérialisation et au recours à la signature électronique n'est pas plus élevé que celui pour la signature de documents papier. Il y aurait peu d'intérêt pour une personne d'usurper l'identité du signataire de ces actes, à savoir celle du chef d'établissement. Ceci ne signifie pas qu'il n'y aurait pas du tout d'intérêt à le faire (par exemple le recrutement ou le licenciement de personnel, l'attribution de contrats à incidences financières...).

Sous réserve d'une analyse plus approfondie des risques métiers, le niveau de risque selon le RGS pourrait être qualifié de « moyen ». Ainsi, le niveau de certificat 1 étoile RGS semble suffisant pour la signer les actes d'EPLÉ étudiés dans le cadre de Dem'Act. Toutefois, d'autres actes administratifs des EPLE signés par le Chef d'établissement pourraient exiger un niveau de sécurité plus élevé. Dans d'autres circonstances, dans d'autres contextes, il existe des applications de dématérialisation d'actes administratifs exigeant un niveau de sécurité de deux étoiles. C'est le cas de l'application ACTES²⁶ du ministère de l'Intérieur. Il est probable que dans le cas de la dématérialisation du livret scolaire numérique dont l'étude documentaire est à lancer, compte tenu des risques de contentieux, il soit conclu à une nécessité de sécurisation RGS de niveau deux étoiles. Dans le même ordre d'idées, il est intéressant de noter que le Ministère de la Justice et des Libertés obtient la qualification RGS de niveau trois étoiles pour les services de signature électronique et d'authentification²⁷.

²⁵ Référentiels communs aux mécanismes cryptographiques : chapitre 3.3.1 du RGS -> [RGS_B_1] et [RGS_B_2]

²⁶ Annexe : ACTES et le Référentiel Général de Sécurité (RGS); <http://www.collectivites-locales.gouv.fr/actes-et-referentiel-general-securite-rgs>

²⁷ <http://www.lsti-certification.fr/index.php/actualites.html>

4.4.2 Pistes d'analyse applicables aux autres actes administratifs et non administratifs des EPLE

Tout acte est soumis à son propre référentiel légal. Ce dernier permet, entre autres éléments, de déterminer un niveau de signature approprié. En effet, tout acte ou document n'est pas nécessairement « signable ». En outre, un même niveau de signature n'est pas applicable à tous les actes. Enfin, les actes ne sont toujours signés par le même signataire ou le même type de personnes.

Ainsi, pour d'autres populations de signataires que des chefs d'établissement, la problématique de l'authentification pourra être essentielle, voire cruciale, car cette population pourra se trouver hors des murs de l'EPLE ou être mineure. Sont visées les populations des enseignants et celles des représentants légaux des élèves mineurs et des élèves majeurs.

Rappelons que le RGS s'impose dans le cadre des relations entre les autorités administratives, dont les EPLE, et les usagers, dont les représentants légaux des élèves.

4.4.2.1 Les actes dématérialisés de la population enseignante

Le recours aux annuaires gérés par le rectorat contenant l'identifiant unique (NUMEN) pourrait être envisagé pour la mise en place de procédés d'identification.

Les actes ou documents que les enseignants seront amenés à signer sont divers et disparates : cahier de textes, cahier de correspondance, documents de notation d'élèves, corrections de copies d'examens, convocation de parents d'élèves, thèses, etc. Pour chacun d'entre eux, il est nécessaire de déterminer s'il s'agit ou non d'acte administratif, et s'il peut être nativement électronique, le risque lié à l'impact d'une usurpation d'identité et le contexte lié au métier qui aura des impacts sur les modalités techniques de mise en œuvre (situation de mobilité, matériel informatique fourni par l'établissement ou pas ...). Tous ces éléments entrant entre autres dans la qualification du type de signature attendue.

4.4.2.2 Les actes dématérialisés de la population des représentants légaux d'élèves

On considérera que les représentants légaux des élèves ne peuvent être identifiés qu'à chaque nouvelle année scolaire au sein des EPLE. A noter toutefois que les élèves sont identifiables par un numéro unique au sein des annuaires des rectorats et que ce numéro unique est réputé les suivre durant toute leur scolarité.

Les actes ou documents à signer par les représentants légaux sont tout aussi disparates et ne sont pas tous qualifiables d'actes administratifs. Il conviendra pour chaque acte ou document de s'interroger sur la raison d'être de la signature du représentant légal de l'élève et ce qu'elle apporte. Il est probable que pour la très grande majorité d'entre eux il ne s'agit que d'une reconnaissance de prise d'information. Il peut aussi s'agir de signature requise pour matérialiser une autorisation ou un consentement. Auquel cas, le niveau de sécurité de signature pourra s'avérer de plus grande importance, l'établissement devant être garanti du consentement du signataire à l'acte et de son identité. Dans le cas de mise en place d'un téléservice pour les usagers, les conditions imposées par l'ordonnance de 2005 seront applicables.

5 Comment choisir la "bonne" solution ?

Le ministère se propose de profiter du chantier de refonte de son infrastructure de gestion des clefs (IGC) en vue de son homologation RGS à un niveau élevé, d'élargir son offre de service pour établir la confiance numérique. On parlera « d'Infrastructure de Gestion de la Confiance ». Les nouvelles fonctionnalités²⁸ sont à étudier tant sous l'angle de la sécurité que sous l'angle juridique. Cette offre ne doit pas faire perdre de vue l'obligation de pouvoir répondre aux besoins de sécurisation équivalents au RGS de niveau une étoile à trois étoiles.

Les postes de travail des agents présents en établissement, en collectivité locale, ou ailleurs, ne sont pas sous contrôle du ministère. Ils ne peuvent pas être sécurisés de manière industrielle, du fait d'une grande hétérogénéité matérielle et logicielle, et du fait de l'impossibilité de mise en place d'un support centralisé pour ce parc dont il n'a pas la gestion. C'est pourquoi l'IGC est conçue de manière à centraliser le plus possible les fonctions de sécurité nécessaires à la réalisation des infrastructures dans un environnement technique robuste, procéduré, documenté, maîtrisé.

5.1 Certificats

La fonction de signature électronique repose en premier lieu sur l'usage d'un certificat, découlant d'une bi-clef : clef privée pour réaliser une signature électronique, et clef publique, pour la vérifier. Avant d'émettre un certificat, l'Autorité d'enregistrement doit fournir à l'autorité de certification (IGC) les informations relatives à l'identité d'une personne enregistrée.

²⁸ Fonctions de signature électronique, horodatage, coffre-fort électronique, gestion de preuves...

Cet enregistrement peut prendre trois formes et correspond à la notion de classes de certificats :

- classe 1 : Enregistrement déclaratif ou soumis à une vérification élémentaire (ex possession d'une adresse mail) ;
- classe 2 : Enregistrement réalisé à distance sur la base de l'envoi de copies de papiers d'identité ;
- classe 3 : Enregistrement réalisé en face à face avec présentation à l'Autorité d'enregistrement des papiers d'identité originaux.

La clef privée doit être conservée sur un support qui peut être :

- **physique ou personnel** (carte à puce ou clef USB). La clef privée embarquée sur ce support n'en sort jamais. Un support qualifié permet la mise en œuvre des niveaux deux à trois étoiles du RGS. Il permet un usage sous le contrôle exclusif du signataire. Ce dispositif nécessite de lourdes contraintes logistiques ;
- **logiciel** (magasin de certificats). Même protégé par un mot de passe, il est aisément "crackable", et les clefs privées peuvent être détournées. En théorie ce support est à bannir, même si certaines applications reposant sur un stockage dans le magasin Windows sont homologuées RGS une étoile ;
- **physique centralisé ou carte à puce virtuelle**²⁹ : la clef privée se trouve sur un support matériel sous contrôle d'une autorité dédiée, appelé HSM (Hardware Security Module). La réalisation d'une signature avec cette clef privée doit être conditionnée à une demande authentifiée d'un utilisateur. Ce support est très sécurisé s'il est possible de placer la réalisation d'une signature sous le contrôle exclusif du signataire. Toutefois, l'établissement d'un canal fiable depuis le poste du signataire jusqu'au HSM pour la présentation directe du code de déblocage fait aussi courir le risque d'attaques sur le HSM. À l'inverse, si c'est l'IGC qui dispose de la possibilité de réaliser les signatures après contrôle de l'identité du signataire, la sécurité offerte n'est plus technique, mais seulement organisationnelle. Toute demande de signature doit faire l'objet d'une traçabilité qui doit constituer une piste d'audit fiable.

La fonction de révocation³⁰ est à prévoir dans tous les cas et nécessite d'en définir le processus et les acteurs : qui peut / doit demander la révocation, dans quels cas, avec quelle authentification...? Le renouvellement des certificats doit être prévu dans la Politique de Certification. Les impacts techniques et organisationnels du renouvellement découlent des choix qui seront effectués sur la nature des certificats et de leur support.

5.2 Mise en œuvre des signatures

Deux types de signatures pourront être mises en œuvre :

- **signature électronique individuelle** : marquant l'engagement de signataire en son nom propre. Elle pourra reposer sur un certificat dont la clef privée sera sur le poste client (magasins éventuellement sécurisés), sur support physique qualifié ou au sein d'une carte à puce virtuelle (HSM) ;
- **cachet électronique** : garantissant l'intégrité et la provenance d'un document. Le cachet électronique, s'il a une existence au sein du RGS, n'a pas véritablement d'existence juridique. Cependant, il n'y a pas de jurisprudence à ce sujet. Il s'agit d'un dérivé de signature électronique qui comporte l'identité d'une machine représentant une institution. L'analogie la plus proche dans le monde du papier serait le sceau (cachet de cire apposé avec une bague). Ce type de signature pourra être utilisé dans le cas des accusés de réception.

Le principe mis en avant par le RGS est le contrôle direct de la clef privée par le porteur, de telle manière que la signature ne puisse effectivement être déclenchée que du fait de sa volonté délibérée. Si un mécanisme centralisé, par exemple carte à puce virtuelle, devait être mis en place, il conviendrait d'envisager la mise en œuvre d'une dérogation sur la base d'un dossier d'étude de risques et de sécurité.

²⁹ Ce support n'est pas conforme à [RGS A8] III.3. En effet, toute nouvelle demande de certificat peut être considérée comme un renouvellement, et le renouvellement nécessite de réaliser à nouveau la procédure d'enregistrement. Il n'est pas conforme à [RGS A8] IV.3.1 et VI.1.2 qui précisent que "la clef privée doit être transmise de façon sécurisée au porteur".

³⁰ La liste de certificats révoqués (CRL) doit être disponible sans interruption de service pour les applications de vérification de signature. Du point de vue de la disponibilité, la fonction de révocation est plus sensible que celle d'émission de certificats ou celle de signature. ([RGS A8] V.1.8)

6 Conclusion

6.1 Carte à puce virtuelle et problème de mise en œuvre, l'exemple de Dem'Act

L'application de dématérialisation des actes en EPLE, Dem'Act, ne nécessite qu'un besoin d'homologation de niveau une étoile RGS maximum. Pour des raisons de sécurité et de maîtrise des circuits d'informations, il est souhaité ne recourir ni aux magasins logiciels de certificats, ni à leur stockage sur le poste client du chef d'établissement. Il s'agit donc de stocker les certificats de personnes nécessaires, dans des espaces appropriés, réputés forts, composants (parmi d'autres) de la plate-forme de signature électronique. Cet espace ne devant pas être sur support logiciel, par essence « crackable », mais sur un module de sécurité matériel qualifié : un HSM. En effet, tout doit se faire entre l'application Dem'Act (serveur) et l'IGC (serveur) via des flux entre serveurs parfaitement maîtrisés, sous contrôle du signataire en mode connecté, depuis son poste, dûment authentifié (forte ou renforcée). Cette étude montre le caractère non homologable RGS une étoile, car il est interdit à l'autorité de contrôle de conserver ou dupliquer la clef privée (RGS A8 VI 1.2). Revenir sur ce choix d'architecture reviendrait à sortir les certificats et/ou documents non signés des serveurs et des flux entre serveurs pour les faire transiter par le poste client durant une procédure d'apposition de signature. C'est une faille de sécurité. Un transit par le poste client revient à une dégradation de « garantie » en termes de sécurité effective, car ce changement d'architecture consiste à stocker le certificat du signataire sur le poste client dans un magasin logiciel facilement détournable, même par des non-spécialistes. Pourtant cette architecture serait homologable au niveau une étoile du RGS.

L'architecture initialement retenue revient à la mise en œuvre de cartes à puces virtuelles. Elle nécessiterait une dérogation qu'il faudrait faire entériner par la commission d'homologation, assortie éventuellement d'une demande d'évolution du RGS à l'ANSSI. Pour ce faire, la proposition serait de recourir à deux entités différentes :

- l'autorité de contrôle IGC qui utilisera son HSM pour émettre les certificats et les retourner à l'autorité d'enregistrement en charge de le remettre au destinataire ;
- l'autorité X (appelons la « gestion des cartes à puces virtuelles » ou « plate-forme de signature électronique »), elle aussi détentrice d'un HSM, faisant office de magasin de certificats, dont le seul et unique rôle sera de fournir les services d'utilisation des ces certificats, tels que l'apposition de signature sur un document. Ces services seraient pilotés par le détenteur de ces certificats : leur utilisation serait placée sous sa responsabilité exclusive, à distance.

Pour être viable en termes d'homologation RGS une étoile, il est nécessaire qu'il n'y ait aucun lien direct entre ces deux autorités. Le chemin d'alimentation du magasin de l'autorité de gestion des cartes à puces virtuelles suivra le même chemin que celui actuellement emprunté pour l'alimentation de magasin de certificats sur le poste de travail du signataire. Dès lors, on pourra considérer que le poste du signataire est déporté (hébergé à distance).

À noter, cette architecture ne saurait convenir aux besoins deux et trois étoiles RGS (en l'état) car ces niveaux reposent sur la remise en main propre du support physique (le face à face), et le HSM ne peut être remis en main propre.

Par ailleurs, en ce qui concerne la conservation d'éléments à des fins de preuve, il conviendra de s'assurer que la mise sous séquestre afférente soit sans aucun lien avec l'autorité de gestion des cartes à puces virtuelles. En respectant cette étanchéité, il pourra être envisagé une mise sous séquestre via un coffre-fort.

6.2 Enjeux et risque de contentieux

Lorsque le risque de contentieux apparaît élevé, voir très élevé, dans un domaine traité par une application mettant en œuvre des téléservices, soit en raison du public concerné, soit en raison de la portée des actes manipulés, il est conseillé d'homologuer l'application visée. Aussi elle devra respecter au plus près le RGS, et l'on partira du principe que l'IGC elle-même est homologuée RGS à un niveau élevé. Il est préconisé de recourir, pour ces applications sensibles, à un déploiement de supports physiques qualifiés par le RGS, tel que des cartes à puce de type token gemalto. C'est l'issue la moins risquée d'un point de vue juridique, car chaque maillon de la chaîne sera en totale conformité au RGS. Ce postulat pourra être modifié en fonction des efforts fournis pour faire évoluer le RGS V3.

Doivent être considérés, lors de l'observation du niveau de risque de contentieux, les moyens à mettre en œuvre en termes de logistique et de déploiement, qui peuvent être non négligeables. Ainsi lorsque les risques de contentieux ne sont pas massifs, il est possible de recourir à une homologation interne, avec un traitement du contentieux sans appui du RGS stricto sensu, mais par dérogation. Il revient aux décideurs du ministère de se prononcer pour chaque situation.