Sujet national pour l'ensemble des centres de gestion organisateurs

EXAMEN PROFESSIONNEL DE PROMOTION INTERNE ET EXAMEN PROFESSIONNEL D'AVANCEMENT DE GRADE DE TECHNICIEN PRINCIPAL TERRITORIAL DE 2ème CLASSE

SESSION 2017

ÉPREUVE DE RAPPORT AVEC PROPOSITIONS

ÉPREUVE D'ADMISSIBILITÉ :

Rédaction d'un rapport technique portant sur la spécialité au titre de laquelle le candidat concourt. Ce rapport est assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : INGÉNIERIE, INFORMATIQUE ET SYSTÉMES D'INFORMATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- L'utilisation d'une calculatrice de fonctionnement autonome et sans imprimante est autorisée.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 25 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

Vous êtes technicien principal territorial de 2ème classe, à la Direction des Systèmes d'Information (DSI) dans la commune de Techniville comptant 30 000 habitants.

La commune étant engagée dans un processus de dématérialisation des actes administratifs, le Maire souhaite mettre en place un parapheur électronique.

Dans un premier temps, il vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport technique sur les enjeux du parapheur électronique.

10 points

Dans un deuxième temps, le Maire vous demande d'établir un ensemble de propositions opérationnelles pour mettre en place un parapheur électronique dans la commune.

10 points

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances.

Liste des documents :

Document 1 **« Parapheur électronique par ixBUS ».**
www.srci.fr – Consulté le 16 novembre 2016 - 2 pages.

Document 2 **« DEMAETER – Parapheur électronique & signature électronique ».**
www.demaeter.fr - Consulté le 10 novembre 2016 - 6 pages.

Document 3 **« E-megalis et l'administration électronique : retour d'expérience de la Communauté d'agglomération de Vannes ».**
www.a-brest.net - Février 2014 - 2 pages.

Document 4 **« Les enjeux de la dématérialisation : développement durable, greenwashing ou business ? ».**
Bernard Lombardo - www.journaldunet.com - Avril 2012 - 2 pages.

Document 5 **« Signature électronique - CIG Grande Couronne ».**
CIG Grande Couronne - Service archives - Fiche Pratique n°2 - Mars 2013 - 3 pages.

Document 6 **« Actualités Dématérialisation - La signature électronique "pour les Nuls" ».**
Benoît COLINET - www.sictiam.fr - Février 2016 - 3 pages.

Document 7 **« Manche Numérique – Parapheur électronique ».**
www.manchenumerique.fr - Novembre 2016 - 2 pages.

Document 8 **« La dématérialisation : avantages - inconvénients ».**
« C2i, métiers du droit » de l'Université Lyon III - Octobre 2012 - 2 pages.

Document 9 **« Le parapheur électronique à la ville de Montbéliard ».**
Jean-Pierre BRINGARD - www.teamnet.fr - Septembre 2016 - 1 page.

Certains documents peuvent comporter des renvois à des notes ou à des documents Non fournis car non indispensables à la compréhension du sujet.

DOCUMENT 1

« Parapheur électronique par ixBUS ».

www.srci.fr – Consulté le 16 novembre 2016.

srci
Solutions de dématérialisation

Parapheur électronique par iXBUS®

DÉMATÉRIALISEZ VOS CIRCUITS DE VALIDATION

Dans une organisation, la signature des parapheurs est un processus chronophage, qui peut engendrer des problèmes de sécurité, confidentialité et traçabilité.

Le parapheur électronique permet de **faire circuler virtuellement** des documents pour validation et/ou signature électronique.
En remplaçant le parapheur traditionnel, il constitue une **interface unique** qui **centralise tous les documents** (courriers, factures, notes internes,...) destinés aux personnes signataires (chefs de service, directeurs, élus,...).

Le parapheur électronique **structure et accélère le processus de visa et de signature.**
Ses avantages sont multiples :

- Fluidité,
- Traçabilité,
- Rapidité,
- Souplesse.

Une organisation peut désormais signer, stocker et transmettre d'une manière totalement dématérialisée un document original avec la même valeur légale qu'un original papier.

SRCI est Tiers de télétransmission agréé.

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

MINISTÈRE DE L'INTÉRIEUR ET DE L'OUTRE-MER, DES COLLECTIVITÉS TERRITORIALES ET DE L'IMMIGRATION

Quelles principales fonctions attendre d'un parapheur électronique ?

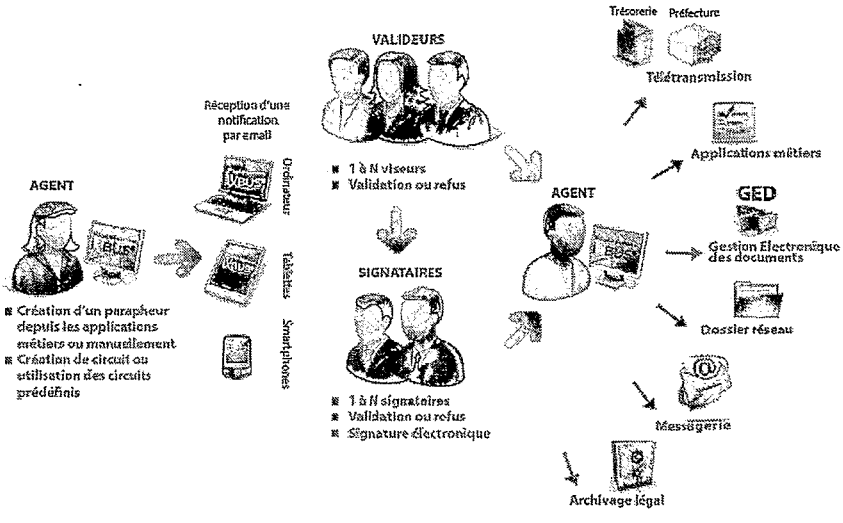
En parfait remplaçant du parapheur carton, le parapheur électronique permet à chaque interlocuteur d'un circuit décisionnel de **récupérer** à tour de rôle les fichiers déposés dans le circuit et de les **valider et/ou signer**, en fonction du profil et du rôle qui lui est assigné.

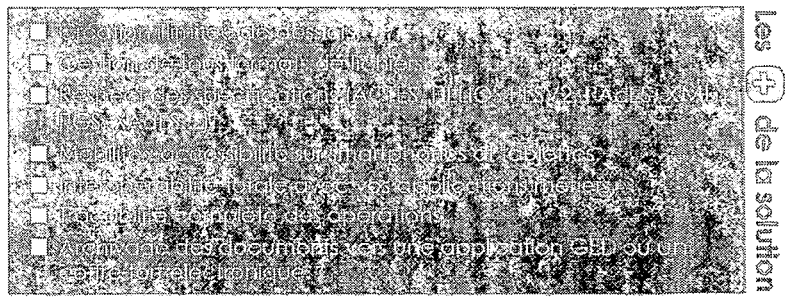
Pour éviter de multiplier les outils informatiques et les workflows, un parapheur électronique doit être **transversal avec les applications existant** dans la collectivité.

Accessible via un simple navigateur web couplé à un certificat électronique, le viseur et/ou signataire peut valider et/ou **signer les documents au bureau ou à distance.**

La solution Parapheur électronique, par iXBus®

Une plateforme décisionnelle complète et sécurisée pour dématérialiser vos circuits de validation et de signature.





Un bouquet de fonctionnalités au service de votre productivité

Le Parapheur électronique vous permet un gain de temps significatif à court, moyen et long terme dans les processus de validation et de signature de tous vos documents.
L'interopérabilité est au cœur des solutions techniques développées par SRCI. Vous avez la garantie de pouvoir gérer dans votre parapheur et avec un seul outil, tous les contenus venant de vos applications métiers.

Une administration simple

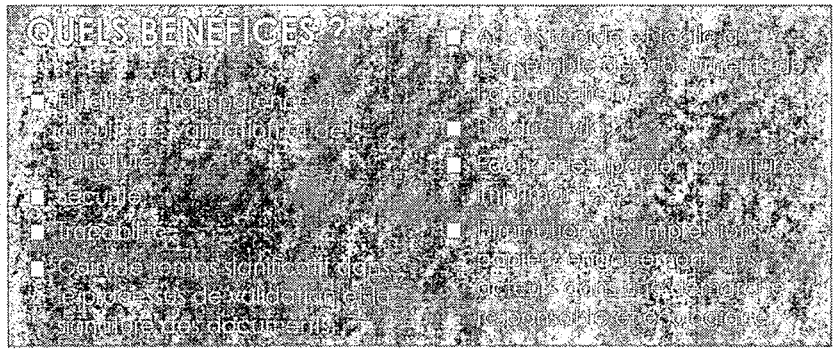
- ☐ Gestion multi-organisations (sites, entités juridiques, ...),
- ☐ Synchronisation avec l'annuaire de l'organisation,
- ☐ Gestion des services, fonctions, personnes et délégataires,
- ☐ Paramétrage du circuit de validation/signature (niveau hiérarchique, délais de traitement,...),
- ☐ Organisation des délégations (permanentes et temporaires).

Une validation optimisée

- ☐ Notifications par mail (visa ou signature)
- ☐ Correction possible des documents à chaque étape (avec historique des modifications),
- ☐ Annotations publiques et privées des documents,
- ☐ Refus de signer (motivation obligatoire),
- ☐ Validation sur smartphones et tablettes,
- ☐ Gestion des signatures électroniques ou manuscrites.

Une gestion intuitive

- ☐ Gestion automatique ou manuelle des circuits de validation et des types de documents,
- ☐ Nombre illimité de pièces jointes,
- ☐ Suivi et traçabilité des actions sur les dossiers/documents,
- ☐ Possibilité de transformer directement les documents en PDF,
- ☐ Signature électronique avec image intégrée,
- ☐ Impression d'un QR-code sur les documents,
- ☐ Possibilité de télétransmettre directement des documents (Préfecture, Trésorerie, partenaires extérieurs, ...),
- ☐ Archivage des dossiers (versement au système de conservation à valeur probante).



Ils ont choisi le Parapheur électronique iXBus®

Une plateforme unique pour toutes vos procédures de dématérialisation

La plateforme iXBus® offre de nombreux outils et fonctionnalités pour dématérialiser l'ensemble de votre système d'information.

SRCI, expert reconnu et pionnier dans ce domaine, est également Tiers de Confiance agréé par l'Etat.

- ☐ Convocation des élus
- ☐ E-administration
- ☐ Coffre-fort électronique
- ☐ Relation fournisseurs
- ☐ Facture électronique
- ☐ Editique
- ☐ Courrier électronique
- ☐ Développements spécifiques

☐ A PROPOS DE SRCI

Créée en 1986, SRCI opère dans le développement de solutions innovantes d'échanges de documents par voie électronique sécurisée, au service des collectivités et des entreprises.
Les solutions déployées permettent la circulation des documents entre partenaires afin d'optimiser, automatiser et sécuriser les échanges documentaires. Approuvé par plus de 8 000 clients, notre savoir-faire en développement, intégration et hébergement de solutions de dématérialisation positionne aujourd'hui SRCI comme l'acteur incontournable du marché de la dématérialisation en France.
Pour en savoir plus : www.srci.fr

DOCUMENT 2

« Parapheur électronique & signature électronique ».

www.demaeter.fr - Consulté le 10 novembre 2016.

Le parapheur électronique

Le développement de la dématérialisation au sein des entreprises et des administrations passe par la mise en œuvre de circuits de validation de documents, qui permettent à chacun des décideurs successifs de valider ou de rejeter le document et, en bout de chaîne de le signer pour le transmettre à l'extérieur.

Ces échanges constituent un complément à la Gestion Électronique de Documents (GED), dont le rôle est la gestion du cycle de vie des documents depuis leur création jusqu'à leur archivage, ce qui inclut la gestion des versions, des droits, l'indexation, le partage.

Lorsque la circulation du document n'a pas pour but sa conception, mais uniquement sa validation et sa signature, on parle de parapheur électronique.

Le parapheur électronique doit respecter plusieurs règles essentielles :

- le parapheur doit permettre au signataire de visualiser le ou les documents à signer ;
- le parapheur doit permettre à plusieurs personnes de signer le même document successivement ;
- dans le cas où une ou plusieurs personnes ont déjà signé le document, le signataire suivant doit pouvoir visualiser et vérifier les signatures précédentes ;
- le parapheur ne doit pas imposer de choix techniques aux utilisateurs (formats de signature, inclusion ou non d'horodatage...), mais être purement fonctionnel ;
- le parapheur doit permettre au signataire d'inclure des mentions (manuscrites ou typographiques) à l'attention du destinataire du document ;
- le parapheur doit pouvoir s'adapter aux différents types de signature électronique existants et proposer à chaque utilisateur uniquement le mode de signature qui lui correspond ;
- à l'issue de la signature, le parapheur doit réintégrer le document signé dans le workflow métier et/ou la GED.

Un parapheur électronique bien conçu peut être un formidable outil d'optimisation des flux internes d'une entreprise.

La signature électronique

Un mot, de multiples réalités

Le terme « signature électronique » désigne à la fois un acte simple que chacun peut réaliser au quotidien, un procédé technique applicable dans de nombreux cas de figure différents, et une définition juridique, qui peut varier selon les contextes.

Cette multitude d'acceptions rend l'usage du terme délicat, et l'implémentation de la fonctionnalité sujette à de nombreuses interrogations.

La signature électronique en pratique

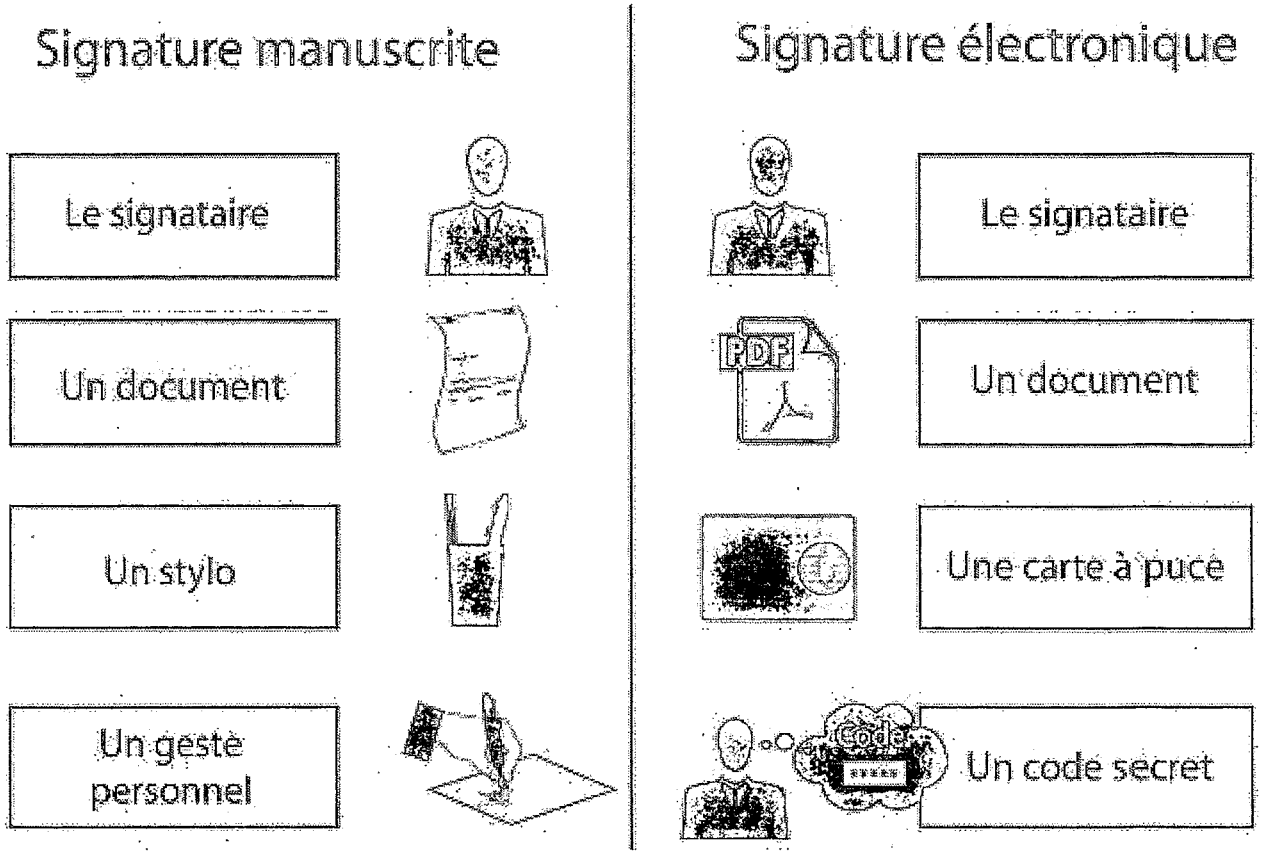
La réalisation d'une signature nécessite quatre éléments :

1. **un individu**, le signataire, qui peut agir en son nom propre ou au nom d'une entité qu'il représente ;
2. **un document à signer**, qui peut être de natures diverses tant pour le fond (contrat, lettre, formulaire...) que pour la forme (papyrus, parchemin, simple papier, papier sécurisé, formulaire CERFA...) ;
3. **un instrument d'écriture** (stylet, plume, stylo...) ;
4. **un geste**, que le signataire est le seul à savoir réaliser avec l'instrument d'écriture : la signature à proprement parler.

La signature électronique est un cas particulier de signature, qui porte sur un document de nature électronique en non de nature physique.

La réalisation de la signature électronique nécessite quatre éléments, dans un parallèle quasiment parfait avec la signature manuscrite :

1. **un individu**, le signataire, qui peut agir en son nom propre ou au nom d'une entité qu'il représente, en général muni d'un terminal informatique pour réaliser l'opération de signature ;
2. **un document à signer**, qui peut être de natures diverses tant pour le fond (contrat, lettre, formulaire...) que pour la forme (document issu d'un traitement de texte, fichier PDF, fichier image, données informatiques au format XML, csv ou autre...) ;
3. **un instrument de signature** (la carte à puce, la clef USB ou le magasin logiciel support du certificat) ;
4. **un secret**, que le signataire est le seul à connaître : le code de déblocage de sa clef privée sur le support du certificat, appelé en général code PIN (Personal Identification Number) : c'est l'équivalent du code de la carte bancaire.



La signature électronique, une définition juridique

La mise en œuvre de la signature électronique dans un projet répond nécessairement à un besoin juridique. Dans le cas inverse, il faudrait, en amont, s'interroger sur l'utilité de la mise en œuvre de la signature !

En France, 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 a défini dans l'article 1316-4 du Code civil le cadre juridique applicable pour la signature électronique.

Le décret du 30 mars 2001 a ensuite approfondi la notion de signature électronique en développant les notions de « signature électronique sécurisée » et de « signature électronique présumée fiable ».

Code civil – Article 1316-4 (1er alinéa)

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. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

Deux choses fondamentales sont à remarquer.

Tout d'abord, cet alinéa ne porte pas sur la signature électronique, mais sur la signature en général, qu'elle soit manuscrite ou électronique. Aucune distinction n'est faite entre les deux cas.

Ensuite, il s'agit de la première définition de la signature dans le droit français. Auparavant, la signature était un usage lié à l'habitude, à la tradition, mais ne faisait pas l'objet d'une description précise.

À quoi sert la signature ?

Elle sert à la perfection d'actes juridiques. À défaut de signature, le document ne sera pas dénué de valeur juridique, mais il ne constituera qu'un commencement de preuve.

En quoi consiste la signature ?

Elle consiste en une identification du signataire. Pour faire le parallèle avec la définition pratique établie plus haut, cette identification certaine du signataire reposera sur l'existence d'un « secret » détenu par le seul signataire : sa capacité à former le signe manuscrit qui constitue sa signature sur papier, ou l'élément cryptographique secret qui lui sert à faire un calcul dans le cas de la signature électronique.

Qu'emporte la signature ?

La signature emporte le consentement du signataire aux termes du document signé.

Code civil – Article 1316-4 (2ème alinéa)

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État.

La signature électronique est... Une signature !

Ce dernier alinéa de la loi du 13 mars 2000 aborde enfin la notion de signature électronique à proprement parler. Il convient de porter une attention toute particulière aux termes choisis. En effet, le législateur n'a pas écrit « la signature électronique est... », mais : « lorsqu'elle est électronique, elle... ».

Par ce choix délibéré est exprimé le fait que la signature électronique n'est qu'un cas particulier de signature. Dans la continuité des articles précédents du code civil, qui établissaient l'équivalence du papier et de l'électronique, la signature électronique n'est qu'un cas particulier de signature, et pas une notion juridique à part.
Une signature électronique n'est rien d'autre qu'une signature, qui porte sur un document de nature électronique. Tout ce qui a été dit sur la signature plus haut s'applique donc à la signature électronique.

En quoi consiste la signature électronique ?

La signature électronique consiste en l'usage d'un procédé fiable d'identification. La fiabilité de ce procédé repose sur la qualité du certificat de signature employé, et en particulier sur le procédé d'enregistrement de l'utilisateur, c'est-à-dire les moyens mis en œuvre pour garantir que le porteur du certificat est bien qui il prétend être et pour protéger sa clef privée.

Ce procédé d'identification doit « garantir son lien avec l'acte auquel il s'attache » : nous verrons dans la définition technique de la signature électronique comment les mécanismes cryptographiques permettent de créer et de maintenir ce lien de manière irréfutable. Cette exigence, qui n'est pas exprimée pour la signature manuscrite, pose le principe équivalent au fait que l'encre marque le papier de manière indélébile et est donc indissociable du document signé.

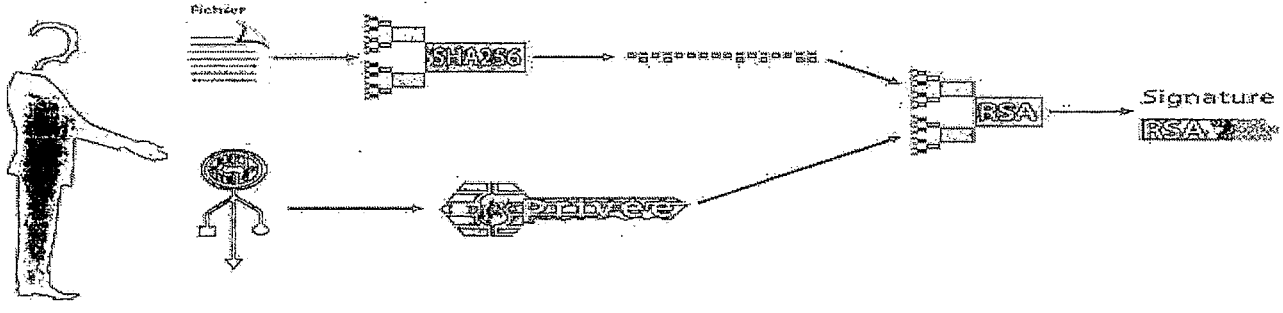
Un élément est fondamental à faire ressortir : inclure dans un document le scan d'une signature manuscrite ne répond absolument pas à la définition. En effet, il suffirait de disposer d'un document signé par un individu et de copier l'image de sa signature (ou la scanner s'il s'agit d'une signature papier) pour constituer un document signé par cette personne ! Cela ne peut en aucun cas constituer « un procédé fiable d'identification », puisque ce travail de faussaire est aujourd'hui à la portée de n'importe quel enfant un peu familier avec l'outil informatique.

La signature électronique, une définition technique

Le déroulement d'une signature électronique, du strict point de vue cryptographique, est le suivant :

- le document est condensé à l'aide d'une fonction de hash, par exemple SHA256 ;
- le hash du document est soumis à un calcul RSA à l'aide de la clef privée du signataire (cette opération nécessite la saisie du code PIN du signataire si le certificat est sur un support physique) ;
- le résultat de ce calcul est, au sens technique, un scellement garantissant l'intégrité du document et réalisé par un acteur identifié, le signataire.

Lorsqu'on est dans le cadre juridique de l'engagement d'une personne sur le contenu d'un document, on appelle ce scellement une « signature électronique », et c'est le terme générique retenu abusivement pour décrire l'opération technique ici décrite. Pourtant, dans certains contextes, cette même procédure peut donner naissance à un cachet, à un jeton d'horodatage, à un certificat...

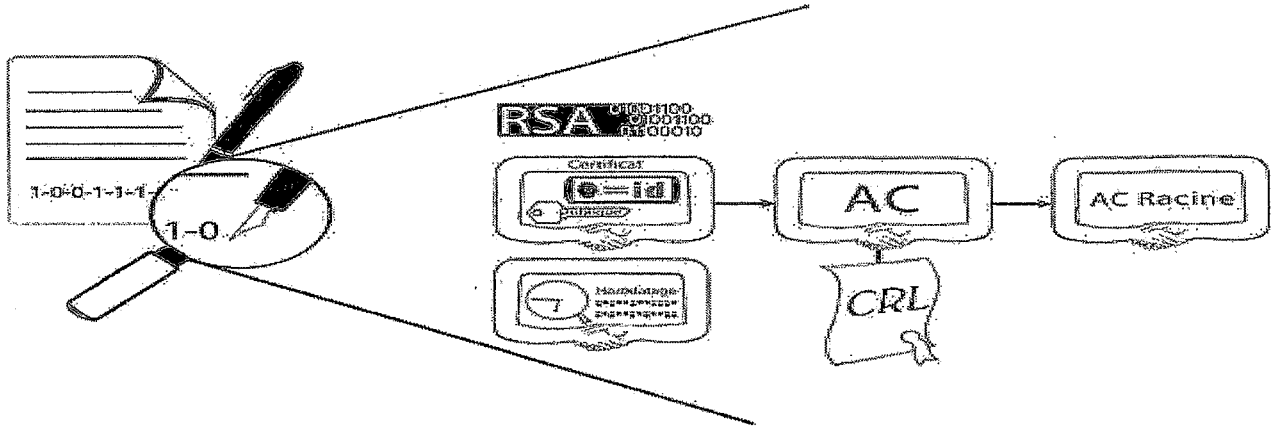


Une fois le calcul décrit ci-dessus réalisé, la signature électronique doit être complétée par les éléments nécessaires à sa vérification par le destinataire, et mise en forme à l'un des formats standards que nous évoquerons plus bas.

Les éléments complémentaires à ajouter dans une signature électronique sont au nombre de trois :

- le certificat du signataire et la chaîne de certification correspondante ;
- un jeton d'horodatage permettant de connaître avec certitude le moment de réalisation de la signature, et ainsi de vérifier la validité du certificat du signataire ;
- une preuve de non révocation du certificat du signataire.

Le contenu d'une signature électronique est alors le suivant :



Les différents formats de signature électronique

Il existe trois formats principaux de signature électronique :

- CAdES (CMS Advanced Electronic Signature) ;
- XAdES (XML Advanced Electronic Signature) ;
- PAdES (PDF Advanced Electronic Signature).

Chacun d'eux permet de nombreuses options (modes englobant, opaque ou détaché, inclusion ou non d'horodatage et de preuve de non-révocation...) et sont applicables préférentiellement à certains types de fichiers ou de processus métier.

Le choix d'un format de signature électronique devra être fait en fonction du contexte applicatif.

Les différents modes de réalisation de signature électronique

Pour réaliser une signature électronique, une personne doit disposer d'une clef privée et du certificat correspondant d'une part, et d'un outil de signature d'autre part.

On peut imaginer que l'utilisateur génère son propre certificat (c'est par exemple le modèle de PGP) ; qu'il l'obtienne gratuitement auprès du service qu'il utilise (c'était le modèle de TéléIR) ; qu'il l'achète auprès d'une Autorité de Certification (par exemple pour la réponse aux marchés publics) ; ou que son certificat soit généré de manière éphémère uniquement pour la durée de l'acte de signature (par exemple pour la signature des demandes d'aide auprès de la Région dans la plate-forme PlaNet Limousin).

De même, l'outil de signature peut être inclus dans les outils bureautiques (Outlook permet de signer électroniquement les mails) ; il peut être un outil autonome (par exemple dans SignExpert, la signature électronique des experts-comptables) ; il peut être inclus dans un service en ligne (par exemple dans achatpublic.com) ; il peut être en mode SaaS (par exemple CertSign) ; il peut être présent uniquement sur un serveur (par exemple K WebSign)...
Les modes de réalisation de signature électronique sont ainsi très nombreux, et il faut veiller à adapter le choix au contexte applicatif et juridique.

Vérifier une signature électronique

La vérification d'une signature électronique comporte trois étapes :

- la vérification technique, qui consiste à vérifier que la signature est bien formée techniquement et correspond bien au document signé ;
- la vérification de la chaîne de confiance, qui consiste à vérifier que le certificat du signataire est bien émis par une Autorité de Certification fiable, et qu'il n'était ni expiré ni révoqué au moment de la réalisation de la signature ;
- la vérification juridique, qui consiste à vérifier que, dans le contexte précis de l'application, la signature est bien recevable.

Les autres formes de « signature électronique »

Le même procédé technique qui permet à un individu de marquer son consentement sur le contenu d'un document peut également être employé dans d'autres contextes fonctionnels et juridiques :

- la « signature électronique » d'une personne morale portera le nom de « cachet » et garantira la provenance et l'intégrité d'un document, par exemple une facture ou une fiche de paie ;
- la « signature électronique » apposée par une Autorité de Certification sur les données d'identité d'un utilisateur et sur sa clef privée constitue le scellement du certificat de l'utilisateur : elle sert alors à reconstituer la chaîne de la confiance et à garantir l'intégrité du certificat ;
- la « signature électronique » apposée par une Autorité d'Horodatage sur le hash d'un document et la date et l'heure émises par une source de temps fiable sert à positionner dans le temps l'existence d'un document, et ainsi à prouver son intégrité mais aussi son existence à un instant donné dans le cadre d'un processus ;

La « signature électronique » apposée par un serveur sur des données de traçabilité en constitue un scellement à des fins de vérification ultérieure d'intégrité…

DOCUMENT 3

« E-megalis et l'administration électronique : Retour d'expérience de la Communauté d'agglomération de Vannes ».

www.a-brest.net - Février 2014.

En 2014, pour faciliter la signature électronique à distance des élus, la Communauté d'Agglomération de Vannes prévoit de déployer la solution i-parapheur sur des tablettes numériques

Entretien avec Alain Cottencin, Responsable Informatique et SIG à la Communauté d'Agglomération de Vannes.

Vous vous apprêtez à mettre en œuvre la solution i-parapheur sur des tablettes numériques à disposition des élus : pourquoi ce projet ?

Le projet que je vais vous présenter s'inscrit dans le cadre à la fois de notre politique de développement durable Agenda 21 et de la dématérialisation de bout en bout (dite à 100%) de nos échanges administratifs.

En juin 2013, nous avons adopté et déployé la solution i-parapheur de Mégalis dans plusieurs services (informatique et finances) de la collectivité pour la signature électronique des bons de commande (inférieur à 15 K euros), des visas de factures, des flux PES V2. La solution est actuellement hébergée sur un espace sécurisé et partagé (serveur interne) et nous prévoyons le mois prochain d'étendre l'accès à d'autres services de l'agglo.

A terme, ce sont les 24 communes de l'Agglomération de Vannes qui pourront disposer, si elles le souhaitent, de leur propre i-parapheur hébergé à Vannes agglo.

Le projet en gestation repose sur l'idée que les élus tireraient avantage de cette solution de signature électronique de documents sur un outil mobile (fonctionnant comme un PC portable) telle une tablette numérique. Ainsi, pourraient-ils signer des documents de n'importe quel endroit, sans délai (dès l'avertissement reçu via l'i-parapheur), de façon simple (quelques minutes suffisent pour signer un document), le tout sans avoir à se déplacer dans les locaux de l'agglomération.

Pour la collectivité, cette solution innovante sur tablettes numériques serait la garantie d'une plus grande interactivité avec nos élus (certaines signatures présentent un caractère urgent), la suppression des documents imprimés (d'où un gain financier substantiel) et une réduction conséquente des délais de signature et de déplacements, puisque celle-ci ne nécessiterait plus la présence de l'élu dans les locaux de la collectivité. Selon nous, ce n'est pas un gadget. Au contraire, c'est un outil véritablement pratique que les élus, nous l'espérons, apprécieront comme tel.

Pouvez-vous nous présenter le montage technique du projet et nous expliquer la première phase de déploiement ?

La problématique a consisté à choisir l'équipement mobile et le système d'exploitation ad hoc pour installer et faire fonctionner les clés du RGS avec la solution d'i-parapheur sur tablette numérique. Très vite nous avons exclu les systèmes androïd et iOS qui s'avéraient trop compliqués d'un point de vue de compatibilité avec l'environnement de notre système. Notre choix s'est donc porté vers des tablettes numériques sous système Windows Pro 8.1 (32 ou 64 bits), totalement compatibles et interopérables avec notre environnement.

Le projet est actuellement dans sa phase de test sur deux tablettes numériques (Microsoft Surface Pro 2 et Dell venue 11 Pro), utilisées pour les besoins du service informatique, afin de signer

des bons de commande et de viser les factures. En quelques minutes je peux signer numériquement une facture qui m'est adressée dans le i-parapheur et cela, quel que soit l'endroit où je me trouve dès lors que ma tablette est connectée à Internet.

A l'heure actuelle, tout fonctionne parfaitement, ce qui m'encourage à étendre l'expérimentation aux élus qui adhéreront à ce service. Reste à valider le projet avec eux, notamment dans ses aspects budgétaires car la solution reste assez onéreuse. En effet, une tablette numérique de ce type coûte 500 à 800 euros auquel il faut ajouter le coût (environ 300 euros) des applications Office pour que l'élu puisse utiliser sa tablette comme un véritable PC portable.

Quel est aujourd'hui l'état d'avancement de votre projet ?

Forts des tests effectués avec les premières tablettes numériques, nous envisageons de mettre des tablettes numériques à disposition des futurs vice-présidents de la Communauté d'Agglomération ayant délégation de signature, qui prendront leurs fonctions à l'issue des Municipales 2014. Cela devrait concerner 4 à 5 élus qui, je l'espère, verront très vite les atouts de cette solution innovante qui pourra leur épargner de nombreux déplacements et apportera une souplesse dans l'utilisation de la signature électronique. De plus, quand ces élus viendront dans les locaux de Vannes agglo ils pourront aussi, facilement, connecter leur tablette numérique à l'i-parapheur via le futur réseau wifi en cours d'installation.

Auriez-vous aujourd'hui un conseil à donner aux collectivités qui souhaitent se lancer dans une démarche similaire ?

Mes conseils portent essentiellement sur les données techniques du projet, pour le reste chaque collectivité adaptera la démarche à ses attentes et spécificités. Donc, je suggère aux collectivités de choisir le système Windows 8.1 Pro compatible avec les drivers et utilitaires des clés du RGS. Pour les tablettes numériques, je suggère des écrans d'au moins 10-11 pouces (un écran plus petit rend difficile la lecture des documents à signer) disposant d'un port USB classique pour connecter la clé cryptographique de certification (du type certificats Chambersign).

Pour information, nos tests sont réalisés sur deux types de tablettes que je considère performantes pour l'usage que nous en avons fait : Microsoft Surface Pro 2 et Dell Venue 11 Pro.

Sur quels points avez-vous été accompagnés dans le cadre de votre démarche ?

Nous n'avons pas eu besoin de suivre une formation poussée à l'utilisation de l'i-parapheur. En revanche les nombreux échanges avec le Pôle promotion et accompagnement de Mégalis ont été très enrichissants et fort utiles. Parallèlement, j'ai pu, au sein du groupe de travail des DSI animé par Mégalis, échanger avec mes homologues d'autres collectivités bretonnes sur la question de l'i-parapheur et cela nous a été tout à fait bénéfique.

Nous pouvons dès aujourd'hui répondre aux demandes de nos communes et peut être d'ici quelques semaines leur permettre d'utiliser à distance la solution i-parapheur installée sur notre serveur web. Sans doute ferons-nous appel à Mégalis pour nous aider à accompagner et former ces communes dans la démarche envisagée.

URL: http://www.e-megalisbretagne.org/
Publié le 6 février 2014

DOCUMENT 4

« Les enjeux de la dématérialisation : développement durable, greenwashing ou business ? ».

Bernard Lombardo - www.journaldunet.com - Avril 2012.

« La dématérialisation est la première étape incontournable de toute stratégie de développement durable » déclarait Eric Boustouller, président de Microsoft France, en octobre 2009.

Dans cette perspective, la gestion responsable des ressources naturelles ainsi que la réduction des émissions de CO^2 débordent le cadre de la stricte production industrielle et concernent également la production et la gestion des flux d'information. **En cause** : la production et l'impression du papier. Est-ce à dire qu'un contenu produit au format numérique (correspondance, facture, ...), c'est autant d'arbres qui ne seront pas abattus ?

Pas si simple !

En effet, la dématérialisation contribue de fait à une augmentation exponentielle de la production et de la circulation de l'information. En outre, à cause de l'effet rebond de la re-matérialisation (Cf. le livre vert du Syntec), **la consommation de papier continue à augmenter en valeur absolue** (+5% en 20 ans).Il faudra sans doute attendre que la génération numérique – née avec internet - affranchie de la « lecture papier » soit majoritaire dans la population active pour voir cette consommation baisser. Sans compter les problèmes écologiques induits par le recyclage et la consommation d'énergie nécessaire à la production, toujours croissante, d'équipements indispensables à la dématérialisation. On pourrait mentionner la diminution des transports physiques comme l'un des bénéfices les plus tangibles de la dématérialisation : **seulement, axer une politique de développement durable sur ces considérations d'économie d'énergie et autres concepts accrocheurs de type « zéro papier » relèverait d'une stratégie de « greenwashing ».**

En réalité, à ses débuts, la dématérialisation visait l'efficacité, la rapidité, la sécurisation des échanges... et surtout les gains de productivité. Concernant la relation collaborateur et le traitement des données à caractère personnel dans l'exploitation des SIRH, le véritable enjeu d'une dématérialisation durable se situe ailleurs.

La confidentialité et la sécurité des données personnelles, un enjeu de responsabilité sociale
La protection des données personnelles occupe une place centrale dans la Responsabilité Sociale d'Entreprise (RSE). L'employeur a un devoir de protection et de préservation de ces données.

Or **la numérisation des données accroît considérablement le risque de perte ou de diffusion non souhaitée** (malveillance, hacking...). Avec l'augmentation des volumes de données, l'employeur doit assumer une charge de plus en plus lourde, d'autant que cette tâche se complexifie avec le progrès technologique : on assiste ainsi à la mise en place de dispositifs particulièrement intrusifs de cyber surveillance. De ce point de vue, dématérialisation ne rime pas forcément avec développement durable.

En cause, les **« traces » informatiques** que produit massivement la société de l'information. Ces « déchets » ne peuvent être éliminés définitivement. Quant au recyclage ou à l'anonymisation, ils n'offrent guère de garanties.

Face à la complexité et à l'importance de cette problématique, l'erreur serait de penser que la dématérialisation puisse être une « réponse simple et rapide » à mettre en œuvre pour « respecter l'environnement ».

La dématérialisation est une chaîne de valeurs technologique, économique, et surtout organisationnelle, dont chaque maillon apporte une valeur à optimiser au travers d'une démarche projet.

L'identification des usages est déterminante : que souhaite-t-on ? Réduire l'utilisation de papier et de frais postaux? Apporter des réponses en termes de gestion documentaire, affranchir les collaborateurs de tâches de classement et de recherches physiques peu valorisantes, favoriser le partage de l'information notamment dans les organisations décentralisées, sécuriser les données, récupérer de l'espace... ?

De l'expression des besoins au choix d'une solution, **la conception est structurante** : quelles activités, quels processus, quelles méthodes vont faire l'objet d'une dématérialisation, avec quel modèle business, avec quel ROI, quelle politique de sécurité ... ?

Le choix technologique est un premier élément de réponse : quelle solution, certifiées, labellisées, quel éditeur ou prestataire pour quel niveau de service, quelles garanties de réversibilité... ?

Enfin, considérant que **la dématérialisation intervient comme un levier de réorganisation fonctionnelle, facilitant notamment le travail collaboratif, il conviendra de considérer avec la même attention les enjeux liés aux gains de productivité attendus que ceux liés à la conduite du changement.** Car il apparaît en effet que les principaux points de résistance soient liés, dans une certaine mesure, à des sujets de sécurité, de pérennité du dispositif et surtout, au sentiment de dépossession induit par un changement d'habitudes.

La productivité est l'enjeu central de la dématérialisation, loin devant les considérations écologiques habituellement évoquées. Un projet de dématérialisation doit faire l'objet d'une approche globale, tenir compte des spécificités métiers légales et organisationnelles, et se concentrer sur les usages.

La dématérialisation est un sujet d'organisateur. A l'instar des projets d'intégration de technologie, le recours au conseil et à l'accompagnement est essentiel, il est la garantie d'un ROI mesurable et satisfaisant.

DOCUMENT 5

« Signature électronique - CIG Grande Couronne ».

CIG Grande Couronne - Service archives - Fiche Pratique n°2 - Mars 2013.

LA SIGNATURE ELECTRONIQUE

Service archives

Fiche pratique 2

Cadre législatif et réglementaire

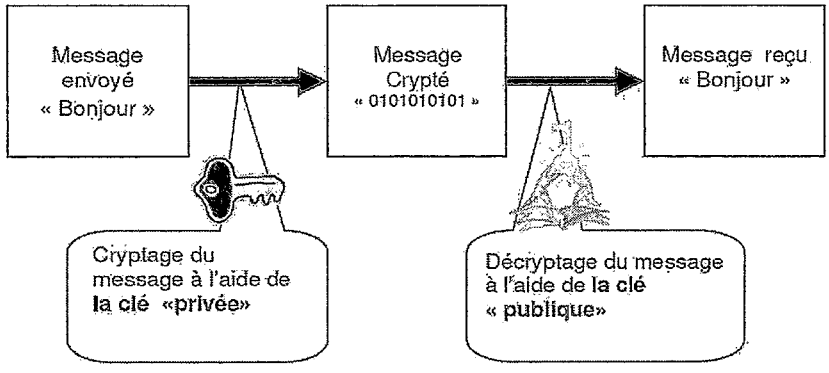
- *Directive européenne 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.*
- *Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.*
- *Décret d'application n° 2001-272 du 30 mars 2001*
- *Décret d'application n° 2002-535 du 18 avril 2002*
- *Loi n° 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique (précisions sur les responsabilités des organismes de certification)*
- *Ordonnance du 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre autorités administratives*
- *Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques*

Qu'est ce que la signature électronique ?

Rappel de la définition de la signature : « 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. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte » (Code Civil, article 1316- 4, premier alinéa).

La signature électronique est un procédé cryptographique retenu pour garantir **l'authenticité** et **l'intégrité** d'un document numérique. C'est un procédé qui met en comparaison l'empreinte du document envoyé avec celle du document transmis et reçu.

Ce mécanisme est fondé sur la séparation d'une clé unique en deux clés distinctes ; la première dite « privée » est utilisée pour la signature (chiffrement) et la seconde dite « publique » est utilisée pour la vérification de la signature (déchiffrement).



Contrairement à la signature électronique, **la signature numérique** est une signature d'origine manuscrite conservée sous forme numérique après avoir été apposée sur un écran tactile, au moyen d'un appareil garantissant l'intégrité de l'acte une fois la signature enregistrée. De la même manière que pour la signature électronique, une homologation de sécurité du système d'information est requise.

D'un autre coté, existe également le **parapheur électronique**. Il s'agit de l'équivalent du parapheur carton dans l'e-administration. Ce parapheur définit le circuit des signatures et visas requis pour la validation des documents. Il circule virtuellement de service en service comme le parapheur carton et fournit les mêmes exigences en termes de confidentialité, sécurité et intégrité des documents. Le parapheur électronique remplace les visas et signatures par des signatures électroniques à valeur probante.

La reconnaissance de l'écrit électronique et sa fiabilité

La loi du 13 mars 2000 reconnait aux documents numériques la même valeur probante que les documents papiers :

« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, ***sous réserve*** *que puisse être dûment* ***identifiée la personne dont il émane*** *et qu'il soit établi et conservé dans des conditions de nature à en garantir l'****intégrité*** *» (Code Civil, article 1316-1)*

La fiabilité du procédé de la signature électronique est établie à l'aide d'un dispositif sécurisé de création de signature électronique :

- La clé doit être unique et strictement confidentielle (être liée uniquement au signataire, permettre l'identification du signataire, être infalsifiable).
- La clé doit être liée aux données auxquelles elle se rapporte et permettre une détection de toute modification.

Les éléments à considérer sont les clés cryptographiques publiques de vérification de signature électronique.

D'autres éléments peuvent être pris en compte, tels que :
- le document en lui même
- le certificat qui contient le nom
- un horodatage du certificat et du document signé
- les listes de certificats révoqués

Dans le cas de la signature électronique présumée fiable, des données supplémentaires peuvent être constituées des éléments suivants :
- le certificat qualifié
- la politique de certification des clés

Pour obtenir une signature électronique, vous devez vous adresser à une autorité de certification. Celle-ci est un tiers de confiance, c'est à dire que c'est sur elle que repose l'ensemble du processus de certification.

Le certificat de signature électronique

La fiabilité du procédé de la signature électronique repose également sur un certificat utilisé pour la vérification de la signature.

Un certificat de signature électronique est un document sous forme électronique qui a pour but d'authentifier l'identité de la personne signataire, l'intégrité des documents échangés (protection contre toute altération) et l'assurance de non-répudiation (impossibilité de renier sa signature).

Cependant, pour que le procédé de signature électronique soit présumé fiable, **le certificat électronique doit être qualifié.**

Les certificats de signature électronique sont commercialisés par des sociétés spécialisées appelées prestataire de services de certification électronique. Un certificat délivré par un prestataire reconnu qualifié sera présumé qualifié.

Ces certificats ont pour la plupart une durée de validité de 3 ans. Il est donc important de prendre en considération leur renouvellement pour permettre de garantir la continuité de l'intégrité des documents signés antérieurement.

Procédure de signature électronique

Etapes	Actions	Descriptions
I. Sélection des documents	Repérer les documents susceptibles d'être transférés par voie électronique.	L'intégrité de certains documents, transmis par voie électronique, doit pouvoir être garantie (exemples : actes administratifs, documents comptables, marchés publics,....)
II. Signature	Signature de l'auteur avec une clé « privée ».	Génération d'une empreinte indissociable du document. Cette empreinte permettra de vérifier que le document n'a pas été modifié au cours de son transfert. La clé privée est utilisée seulement par son signataire et permet de l'identifier.
III. Certification	Certification par un tiers. L'enregistrement de cette garantie est délivré sous la forme d'un certificat électronique. Ce certificat est signé par la clé « privée ».	Un tiers se porte garant que votre clé publique est conforme et créé un lien entre votre clé et votre identité. A ce stade là, l'auteur certifie que le document émane de lui ; on parle alors de non répudiation.
IV. Vérification et décryptage	Réception du document par le destinataire et vérification avec la clé « publique » (= déchiffrement).	La vérification de l'empreinte s'effectue avec la clé « publique » de l'auteur du document. Elle correspond à la clé « privée » et est destinée à être communiquée à ceux qui veulent vérifier la signature. C'est une confrontation entre l'empreinte du document à l'envoi et l'empreinte à sa réception.
V. Archivage	Assurer l'authenticité et la fiabilité du document.	Pour conserver sa fiabilité, doivent être conservés - le document - les métadonnées du document - le certificat de la signature électronique

Les risques encourus

La conservation de la signature électronique sur le long terme est un enjeu archivistique important, puisque sans elle le document perd sa valeur probante.

La vérification de la signature doit donc se faire avant archivage et rapidement après signature du document. Cette vérification et son résultat sont portés dans les métadonnées qui accompagneront le document lors de son archivage.

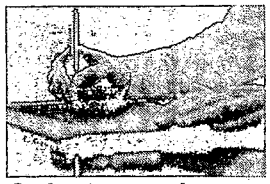
Il convient ici de bien distinguer la différence entre la simple sauvegarde des données électroniques et leur archivage.

Enfin il est également important de se rappeler que la collectivité est responsable de ses archives électroniques au même titre que de ses archives papier.

Le service archives du CIG vous accompagne dans vos démarches d'archivage électronique.

« Actualités Dématérialisation
La signature électronique « pour les Nuls » ».

Benoît COLINET - www.sictiam.fr - Février 2016.



Qu'est-ce qu'un certificat électronique ?

Une signature électronique est produite sur un document par l'intermédiaire d'un certificat électronique.

Ce certificat électronique est **votre carte d'identité numérique** attestant avec certitude l'identité d'une personne. « *Il permet de signer des documents numériques en ayant la garantie que l'identité du signataire est reconnue sans aucune ambiguïté, ni contestation* ».

Le certificat contient des **informations personnelles** (nom, prénom, etc.).

Le certificat RGS : trois niveaux de sécurité disponibles

- RGS * : le certificat 1 étoile est une base de sécurité essentielle, destinée aux entités avec des risques d'usurpation d'identité faibles et sans grande conséquence. Il se présente sous la forme d'un logiciel qu'il suffit d'installer sur votre PC.
- RGS ** : le certificat 2 étoiles, plus complexe, est une base de sécurité forte pour les entités avec des risques élevés d'usurpation d'identité.
- RGS *** : le certificat 3 étoiles est la solution optimale, assurant la sécurité des entités avec le risque le plus élevé en matière d'usurpation d'identité.

Contrairement aux certificats RGS* et **, le RG*** implique l'inversion de la charge de la preuve. C'est-à-dire que juridiquement, en cas d'usurpation d'identité, ce n'est plus à vous de fournir la preuve de votre identité, mais à l'accusation.

Les **certificats électroniques RGS** ** & *** nécessitent une délivrance en main propre sur une clé cryptographique ou une carte à puce au format USB.

A quoi sert la signature électronique ?

La signature électronique est à un document numérique, ce que la signature manuscrite est à un document papier. Une signature électronique a pour objectif de prouver à un tiers la validation d'un document numérique par une personne identifiée.

*Chaque certificat est nominatif et intransmissible, **il ne peut donc être ni prêté, ni échangé.** Le certificat électronique est délivré par une Autorité de Certification qui atteste de la véracité des informations contenues dans le certificat ainsi que le lien entre l'identité de son titulaire et la clé.*

La signature électronique a-t-elle une valeur légale ?

Oui. Aujourd'hui, le document signé électroniquement est admis comme preuve au même titre que l'écrit sur support papier, à condition d'identifier la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. L'article 1316 du code civil définit la signature électronique comme « *l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* ».

Quels sont les avantages de la signature électronique ?

La signature électronique permet notamment de :

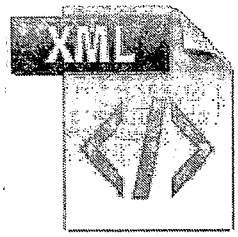
- **s'authentifier** sur des applications (plus de login et de mot de passe),
- **signer un document sans l'imprimer** (économie de papier),
- **transmettre un document par e-mail** (économie d'affranchissement),
- **signer un document à distance via un parapheur électronique** (plus de déplacements),
- **conserver le document au format numérique** (simplification et suppression de l'archivage papier).

Une signature électronique est-elle visible sur un document ?

La signature électronique se différencie de la signature écrite par le fait qu'elle n'est pas visuelle mais correspond à un nombre ou une suite de nombres. En effet, l'action de signer numériquement produit une information binaire appelée communément signature électronique.

Cependant des logiciels comme Adobe Reader vérifient automatiquement la ou les signature(s) à l'ouverture du document et affichent un message de validation, permettant de matérialiser la signature électronique.

Un document peut contenir plusieurs signatures électroniques.



Quels sont les fichiers que vous pouvez signer électroniquement ?

Tous les fichiers de type Word, PDF, JPG, XML, etc. Cependant, le format de fichier le plus usité est le **PDF**, pour sa portabilité et aussi la possibilité d'apposer plusieurs signatures électroniques. Mais également les **fichiers XML** normés pour les échanges entre les entités publiques.

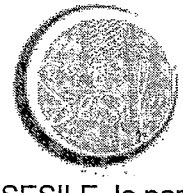
Un document signé électroniquement est-il crypté ?

Non, la signature électronique ne chiffre/crypte pas le document. Le document est toujours lisible en clair.

Que vous garantit la signature électronique ?

La signature électronique permet, pour un document numérique, de garantir :

- **l'identité et l'authenticité** du signataire,
- **la non-répudiation** (preuve fiable prouvant l'envoi des données par l'expéditeur),
- **l'intégrité** du document signé (cohérence entre les données envoyées et celles reçues).



SESILE, le parapheur électronique du SICTIAM

De quoi avez-vous besoin pour signer électroniquement ?

Pour signer électroniquement un document numérique, il vous faut :

- Un document,
- Un parapheur électronique (SESILE) ou des lecteurs de documents (Acrobat, Xémélios),
- Un certificat électronique.

Où pouvez vous vous procurer un certificat électronique ?

Au SICTIAM, via le formulaire en ligne, pour obtenir uncertificat RGS**. Une fois la commande passée, un déplacement physique du demandeur auprès du SICTIAM est nécessaire. Lors de cette étape, le demandeur présente ses papiers d'identité contre remise du certificat.

Quelles sont les grandes étapes de la signature électronique ?

1. Visualiser le document à signer,
2. Cliquer sur un bouton « signer »,
3. Insérer la clé USB certificat et le sélectionner,
4. Taper le code PIN associé au certificat,
5. Valider.

Une signature manuscrite numérisée a-t-elle une valeur juridique ?

Non. Pour les raisons évoquées plus haut cette signature ne présente aucune garantie en termes d'identité du signataire et rend très facile l'usurpation d'identité. Une signature manuscrite scannée peut très facilement être reproduite à l'identique via un bon logiciel de retouche d'image. En justice, **numériser une signature revient à la copier**.

Qu'est-ce que l'horodatage électronique ?

L'horodatage consiste à **apposer à un fichier une date fiable** qui garantit l'existence d'un fichier à une date donnée et qu'il n'a pas été modifié depuis cette date (principe d'intégrité). Tout comme la signature électronique, l'horodatage **garantit l'intégrité du document**.

Il est fortement recommandé d'associer un horodatage à chaque signature électronique.

DOCUMENT 7

« Manche Numérique – Parapheur électronique ».

www.manchenumerique.fr - Novembre 2016.

Parapheur électronique

La dématérialisation est un facteur d'amélioration de la gestion interne des collectivités. Dans cet esprit, le parapheur est, sans aucun doute, un projet socle pour améliorer la célérité, la transparence et la sécurité des traitements et de la gestion des flux au sein de votre organisation.

Objectifs

Une collectivité collecte, traite et produit un nombre considérable d'informations quotidiennement.

Ces nombreuses sollicitations internes et externes conduisent les agents et les élus à gérer et suivre des processus de décisions de plus en plus complexes, à soumettre à validation des documents administratifs dans des formats de plus en plus variés, et le plus souvent numérisés.

Le parapheur permet de mettre en place un processus de gestion complètement dématérialisé, sans rupture de la chaine. Le parapheur permet en outre, d'assurer et gérer le suivi de prises de décisions toujours plus nombreuses, dans un contexte de temps toujours plus contraint.

Lire, vérifier, annoter et signer les courriers à distance constituent les principaux avantages du parapheur électronique.

Présentation

La mise en place d'un parapheur électronique est aujourd'hui possible. En effet, la signature électronique a désormais la même valeur juridique que la signature manuscrite.

Le fonctionnement du parapheur électronique est simple :

- La collectivité émet un courrier
- Elle le dépose sur la plateforme internet
- Ce document suit un circuit de validation interne, identique à la version papier du document
- L'élu peut alors en prendre connaissance puis :
- L'annoter
- Le refuser
- Le signer

Quelques fonctionnalités courantes :

- Viser, mettre en attente, refuser, signer, co-signer…
- Définir les rôles (émetteur, visa, signataire, destinataire)
- Gérer des annotations, remarques
- Diffuser aux différents services
- Délégation de pouvoir…

Recommandations:

- Une réflexion préalable à sa mise en place est nécessaire – il implique une réorganisation dans les modes de travail et d'échanges
- Commencer avec des circuits de validation simples
- Émettre des documents à destination des partenaires déjà impliqués dans les processus de dématérialisation.

Bénéficiez de l'accompagnement de Manche Numérique si vous souhaitez introduire le parapheur électronique dans votre structure.

Témoignages

Christine Saint-Laurent, Manche Numérique

"Nous avons mené au sein de Manche Numérique une expérimentation sur le parapheur électronique.

La réussite d'un tel projet passe par ***l'implication en amont de tous les intervenants*** dans le circuit du document, du rédacteur jusqu'au signataire.

Ne jamais perdre de vue que ***le parapheur a une seule fonction : signer !***

Admettre que la ***gestion électronique des documents est parfois plus contraignante*** que la gestion papier constitue un facteur de réussite. La gestion électronique nécessite une discipline et facilite les recherches ultérieures. Les délais de mise en œuvre parfois longs seront compensés par le gain de temps notable dont pourront bénéficier tous les participants."

Ressources

La signature électronique :

La directive européenne n° 1999/93/CE du 13/12/99 sur les signatures électroniques consacre la reconnaissance légale de la signature électronique. Cette directive est aujourd'hui transposée en droit français :

La signature électronique a **une valeur légale en France depuis la loi du 13 mars 2000**. Cette loi a été complétée par plusieurs décrets et arrêtés qui précisent les conditions d'application :

- Le décret du 30 mars 2001
- Le décret du 18 avril 2002
- L'arrêté du 26 juillet 2004 (en remplacement de l'arrêté du 31 mai 2002 abrogé)
- La loi du 21 juin 2004 pour la confiance dans l'économie numérique
- Ordonnance du 8 décembre 2005

DOCUMENT 8

« La dématérialisation : Avantages - Inconvénients »

« C2i, métiers du droit » de l'Université Lyon III - Octobre 2012.

I- Les avantages de la dématérialisation au sein de l'entreprise

a) La notion d'intelligence économique : L'intelligence économique est l'ensemble des activités coordonnées de collecte, de traitement (d'analyse), de diffusion et de protection de l'information utile aux acteurs économiques, obtenue légalement, dans les meilleures conditions de qualité des délais et des coûts. On peut y ajouter les actions d'influence et de notoriété. Sur cette notion, reportez-vous à l'article du blog sur l'intelligence économique.

b) Productivité, économies : moins de papier, moins de besoin de personnel d'archivage, moins de déplacements, possibilité de travail à la maison…

c) Rapidité, réactivité de l'entreprise, souplesse : on trouve les documents en un clic, transmission instantanée dans le monde entier via les mails… , adaptation en temps réel face aux changements qui peuvent survenir, moins de soumission aux aléas de la Poste, des grèves…

d) Partage des informations facilité, travail collaboratif performant.

e) Possibilité de travail à domicile

f) Rendre son entreprise plus singulière, la faire évoluer, faire ré-émerger un patrimoine qui est dans l'entreprise et qui est source de croissance (les nouvelles formes l'économie ne sont plus dans la production, l'acquisition, mais dans les talents, les services à la personne…)

Exemple : une entreprise d'appareils photos argentiques devenue obsolète avec l'avènement du numérique, a utilisé son « capital mythique » auprès des photographes pour réinvestir les champs de l'économie de la photo numériques via internet.

g) Vers une autre forme d'économie : Economie du don et de la contribution :
on donne gratuitement des connaissances sur internet (exemple : Wikipédia) et les revenus sont différés par l'audience générée, la pub…

h) L'enjeu environnemental de la dématérialisation : D'une part, la dématérialisation permet moins de pollution, avec 15 tonnes de papier économisées. En ce sens, la dématérialisation semble répondre aux enjeux du développement durable. Les entreprises sont aujourd'hui de plus en plus sollicitées au niveau environnemental, en ce qui concerne notamment l'émission de CO^2 dans l'atmosphère.

La dématérialisation permet de réduire considérablement les déchets rejettés par les entreprises (emballages, cartouches d'encre…), mais également la limitation des déplacements, ce qui entraine moins de rejet de gaz à effet de serre.
(L'étude «Smart 2020 : Enabling the low carbon economy in the information age» estime le réduction totale d'émissions de CO^2 liées à la dématérialisation à 500 mille tonnes, en prenant en compte la dématérialisation des documents papier mais aussi celle des autres médias, de la visioconférence et du télétravail.)

Mais la dématérialisation des activités humaines est-elle une si bonne nouvelle ?
En effet, il ne faut pas oublier que clics et recherches sur Internet génèrent d'autres dépenses énergétiques lourdes, à fort impact environnemental.

Cette dernière réflexion nous conduit à nous interroger sur les enjeux négatifs de la dématérialisation des entreprises :

II- Les inconvénients de la dématérialisation au sein de l'entreprise

a) Mauvais maîtrise de l'informatique : il faut organiser des formations spécifiques.

b) Mauvaise maîtrise de sa e-réputation : des informations erronées, compromettantes pour l'entreprise peuvent se glisser très rapidement sur internet et deviennent accessibles à tous.Peut avoir de graves conséquences pour l'entreprise (vous pouvez vous reportez à l'article sur les risques de l'e-reputation des entreprises).

c) Risque de perte de données

d) Coût élevé d'un matériel informatique performant.

e) Consommation électrique accrue (dépenses énergétique, impact sur l'environnement) : Chacun de nos clics a des conséquences directes sur la réalité physique.
Chacune de nos requêtes aboutit à des usines numériques, les centres de données, où des rangées de serveurs consomment de l'énergie et dégagent de la chaleur. Cette consommation d'énergie est même devenue la première difficulté des propriétaires de serveurs et géants du Web.

f) Informations accessibles partout à tous moments : le monde de l'entreprise s'immisce dans la sphère privée. Il faut être disponible à tout moment pour répondre à la dernière information parue.

g) Contribue à augmenter le chômage ? (moins de personnel nécessaire).

Conclusion.

Dématérialiser, oui, mais pas n'importe comment ! En effet, le passage à une dématérialisation massive est rarement pertinent. Une telle démarche sans accompagnement ni prise en compte de certaines contraintes aboutira paradoxalement à la déperdition du résultat.

La résistance au changement et les nouveaux comportements imposés par la dématérialisation comme la lecture à l'écran, la sécurisation des procédures et la culture du papier fortement ancrée dans la société, nécessitent en amont une politique d'accompagnement du changement tant en interne qu'en externe.

Exemple de Carrefour qui avait parfaitement intégré cette problématique : il lui aura fallu deux ans et demi et de nombreuses réunions en interne comme en externe pour piloter le changement et faire en sorte que 70 % de ses factures fournisseurs soient dématérialisées.

Cela peut paraître long mais ce délai était nécessaire pour obtenir l'adhésion des personnes concernées.

DOCUMENT 9

« Le parapheur électronique à la ville de Montbéliard ».

Jean-Pierre BRINGARD - www.teamnet.fr - Septembre 2016.

Retour d'expérience de la ville de Montbéliard, 27 000 habitants, sous-préfecture du Doubs, concernant le parapheur électronique MPI de TEAMNET

La ville de Montbéliard s'est engagée dès 2010 dans une démarche de dématérialisation des flux financiers et des actes. Ce projet s'appuie sur la mise en œuvre du parapheur électronique.

L'enjeu principal pour la ville était de remplacer la centaine de parapheurs carton par un outil logiciel devant assurer la circulation et la signature des documents numérisés de bout en bout de la chaîne de décision aussi bien à l'intérieur de la collectivité qu'avec ses principaux interlocuteurs (les citoyens, les administrations ou organismes connexes, et les entreprises). La ville souhaitait se doter d'un outil unique de validation de l'élu et de l'administration pour tous les documents « à viser ou à signer ».

Le bilan est clairement positif :

- Amélioration de la circulation, de la validation et de la signature des documents
- Augmentation de la mobilité : visa et signature depuis n'importe quel endroit
- Réduction des délais de traitement
- Amélioration du suivi et de la traçabilité
- Optimisation des ressources humaines et des tournées de distribution du courrier
- Diminution progressive des parapheurs carton

Quelques chiffres portant sur les flux financiers :

- Mise en production depuis janvier 2011
- 2 000 flux signés par an (environ 15 000 mandats et 4 000 titres par an)
- 50 % signés le jour même
- 30 % en 1 jour
- 20 % en 3 jours maximum
- 200 000 feuilles économisées par an

Quelques chiffres portant sur actes (arrêtés et décisions) :

- 3 000 actes visés et signés par an
- 65 % des actes signés en 2 jours maximum
- 35 % des actes signés entre 3 et 5 jours
- 15 000 feuilles économisées par an