La signature électronique (ou numérique)

Par Guy LOMBAERTS, Conseiller général

1. Définitions

Qu'est-ce que la signature électronique ?

La "signature électronique" est un mécanisme informatique, basé sur l'utilisation de fonctions cryptographiques, visant à apporter les mêmes fonctionnalités et garanties que la signature manuscrite. Ce concept est également désigné par les termes de "signature digitale[1]" et/ou de "signature numérique".

D'après la loi fédérale américaine (le *Federal ESIGN Act*), les signatures électroniques se définissent comme suit : *"son, symbole ou processus électronique attaché ou logiquement associé à un contrat ou tout autre enregistrement, qui est appliqué ou adopté par une personne dans l'intention de signer l'enregistrement."*

Aux termes de la loi belge du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (art. 2, 1°), une signature électronique *"est une donnée, sous forme électronique, jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification".*

Cette définition qui date déjà de 2001 est pourtant très proche de celle qui figure dans le *règlement européen n° 910/2014 du 23 juillet 2014* sur l'identification électronique et les services de confiance, à savoir qu'une signature électronique[2] correspond à *"des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer"*.

Ces différentes définitions englobent tous les types de signatures électroniques, comme les signatures manuscrites scannées, les signatures biométriques (reconnaissance vocale, de l'iris de l'œil ou des empreintes digitales), les signatures digitales, ou encore les simples codes des cartes bancaires ou cartes d'identité électroniques (code PIN).

Il existe en effet une grande variété de signatures électroniques qui se distinguent par la technologie utilisée, leur niveau de sécurité et la valeur juridique qui leur est associée.

Au même titre que la signature manuscrite d'un document papier, la signature électronique d'un document permet donc, dans un premier temps, d'établir un lien entre le document et le signataire. Le lien ainsi établi peut avoir plusieurs buts définis par le document lui-même ou par le contexte dans lequel la signature s'applique, par exemple :

- identifier l'auteur d'un document
- marquer l'accord du signataire sur les termes du document
- indiquer que le document a été lu par le signataire
- etc.

1. La notion de "signature digitale" est un anglicisme, l'adjectif "digital" ne se réfère pas aux doigts mais bien aux nombres ("digit" en anglais).
2. Communément appelé "Règlement eIDAS".

Quels types de signatures sont juridiquement contraignantes ?

Suivant la nature du document en cours de signature, une signature électronique sous la forme d'une image numérisée de la signature manuscrite du signataire est considérée juridiquement contraignante dans la plupart des États, malgré des différences en fonction des pays et systèmes juridiques.

De nombreuses réglementations internationales (ex. : le règlement UE eIDAS) et de droit interne[3] (en Belgique, par ce qu'on appelle communément le Digital Act[4] qui transpose le règlement européen), s'orientent désormais vers les signatures numériques, plutôt que des signatures électroniques car une signature numérique qui confirme l'authenticité et l'intégrité[5] peut être acceptée par les tribunaux. Elle dispose en effet d'une force probante supérieure à la simple reproduction scannée de la signature manuscrite.

Le choix du type de signature à mettre en œuvre dépendra du type de documents que l'on doit signer et du niveau d'authenticité que le document doit pouvoir soutenir. Nous y reviendrons plus loin.

2. Contexte général – le droit de la preuve (au sens du Code civil)

Le système probatoire belge est strictement réglementé : sous l'influence du code civil français de 1804, appelé Code Napoléon, l'écrit sur support papier sur lequel est apposée une signature manuscrite a été gravé dans le marbre pendant près de deux siècles. Ce n'est en effet qu'à la fin du 20e siècle que le législateur a abrogé ce quasi monopole de fait, né de la prééminence de l'écrit (papier) dans le domaine de la preuve. Jusque là, étaient seuls admissibles, les moyens de preuve repris aux articles 1341 et suivants du Code civil notamment dès que l'objet de la transaction dépassait un certain montant (375 EUR).

L'existence et le contenu de l'acte juridique devaient être prouvés par un acte sous seing privé, à savoir un écrit original qui s'impose comme acte sous seing privé pour autant que la signature soit reconnue.

Ni l'écrit, ni la signature ne faisant l'objet d'une définition légale, il était difficile de considérer un enregistrement électronique, un fax ou un courrier électronique comme un écrit parfait au sens de l'article 1341 du Code civil.

3. Au Luxembourg, a été adoptée la loi du 14.08.2000 relative au commerce électronique modifiant le Code civil, le nouveau Code de procédure civile, le code de commerce, le Code pénal et transposant la directive 1999/93 relative à un cadre communautaire pour les signatures électroniques ; en France, c'est la loi du 13.03.2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique qui règle la matière.
4. La dénomination 'Digital Act' désigne en fait la loi du 21.07.2016 dont le titre intégral est 'loi mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23.07.2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII "Droit de l'économie électronique" du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique'.
5. Notons à ce propos que la signature numérique dispose d'attributs que n'a pas la signature manuscrite classique car celle-ci ne garantit nullement l'intégrité du document signé.

Vers une réglementation européenne unique

La Belgique n'étant pas le seul État européen à se trouver dans cette situation, la Commission européenne va adopter, à la fin de l'année 1999, une directive 1999/93/CE sur la signature électronique qui sera transposée en droit belge en plusieurs étapes.

La première a consisté à modifier la notion de "signature" reprise à l'article 1322 du Code civil et à introduire dans notre droit de la preuve une définition "fonctionnelle" de la signature, c'est-à-dire définie par rapport aux fonctions qu'elle est supposée remplir, indépendamment de son support (cf. loi du 20.10.2000[6]).

Devenait désormais également une signature "un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte".

Sur le plan de la recevabilité en droit de la preuve, le juge ne pouvait plus dès ce moment écarter une signature électronique comme élément de preuve au seul motif qu'elle revêtait une forme électronique mais il n'était pas encore obligé de lui conférer "force probante". Or, ce n'est qu'à la condition qu'un document électronique ait "force probante" qu'il s'impose au juge.

La seconde étape avait donc comme finalité d'assurer une force probante à certaines signatures électroniques. Elle s'est réalisée par l'adoption de la loi du 9 juillet 2001, loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (M.B. 29.09.2001).

Cette dernière octroyait un statut juridique précis à deux types de signatures électroniques :

- la signature électronique "simple" qui est définie comme "une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification". Ce type de signature se retrouve au quotidien dans différentes technologies (codes secrets, cryptographie symétrique ou asymétrique, signature biométrique, ...)
- la signature électronique "avancée", est définie comme une signature électronique qui satisfait aux exigences suivantes :
  - être liée uniquement au signataire
  - permettre d'identifier le signataire
  - être créée par des moyens que le signataire puisse garder sous son contrôle exclusif
  - être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée.

Cette dernière méthode bénéficiait d'un grand avantage : moyennant le respect de quelques conditions, elle acquiert force probante et peut être purement et simplement assimilée à une signature manuscrite, dont elle devient ainsi l'égal. Quelles étaient ces conditions ? La signature électronique avancée doit reposer sur un certificat qualifié et être créée par un dispositif sécurisé de création de signature tel que décrit à l'annexe III de la loi du 9 juillet 2001.

En matière de "e-gouvernement", les lois du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire et du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification s'appliquent essentiellement aux relations entre citoyens et l'administration, via internet et, en particulier, à la signature électronique produite par la carte d'identité électronique.

6. Loi introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire (M.B. 22.12.2000).

Par la suite, une loi du 24 février 2003 concernant la modernisation de la gestion de la sécurité sociale (M.B. 02.04.2003), étendait l'usage de la signature électronique aux communications électroniques entre des entreprises et l'autorité fédérale en précisant dans son article 4/1 qu' : *"Une signature apposée à l'aide de la carte d'identité électronique (e-ID) est assimilée à une signature manuscrite"*.

Un tournant décisif chez nous : le Digital Act de 2016

On en arrive ainsi au nouveau règlement européen n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, entré en vigueur le 1er juillet 2016 (qui abroge la directive 1999/93/CE) et prévoit à l'article 25 : *"L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée.*

L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite ".

Comme on l'a vu plus haut, ce règlement européen a été mis en œuvre, en droit interne belge, par la loi du 21 juillet 2016 surnommée 'Digital Act' (M.B. 28.09.2016) qui met en place un cadre réglementaire en vue d'encadrer l'économie numérique en plein développement et la numérisation des contacts entre les citoyens et les entreprises d'une part, et avec les pouvoirs publics, d'autre part.

La loi du 21 juillet 2016 insère un titre 2 "Certaines règles relatives au cadre juridique pour les services de confiance" dans le livre XII "Droit de l'économie électronique" du Code de droit économique[7]. Même si techniquement un règlement européen n'exige pas une transposition en droit national comme c'est le cas pour une directive, le chapitre III du règlement eIDAS relatif aux "services de confiance" nécessite une intervention législative au niveau national afin d'assurer sa mise en œuvre. Ainsi, le législateur détermine précisément les sanctions applicables en cas de non-respect des dispositions du règlement et de la loi belge relatives aux services de confiance précités.

Le législateur belge a également consacré un corps de règles complet et cohérent visant à encadrer juridiquement l'offre et l'utilisation des services d'archivage électronique. En effet, lorsqu'on envisage la conclusion, la transmission et la conservation d'un acte juridique dans un processus électronique, il semble important de couvrir juridiquement la totalité des étapes du processus, en ce compris l'étape ultime qui consiste en l'archivage de l'acte, et pas uniquement sa signature, sa datation et son envoi.

Les règles belges s'inscrivent dans les objectifs et la philosophie du règlement eIDAS. Elles reprennent les mêmes principes que ceux édictés par ce règlement pour les autres services de confiance (signature, cachet, horodatage, recommandé électronique). Elles visent à couvrir tant l'archivage électronique de documents originairement électroniques que l'archivage électronique de documents papiers (dans le cadre d'une numérisation-scan).

7. Voir : Le règlement européen n° 910/2014 du 23.07.2014 sur l'identification électronique et les services de confiance, SPF Economie - Décembre 2016.

Au-delà du régime relatif à l'archivage électronique, la loi belge consacre également des dispositions relatives à l'envoi recommandé hybride, à la révocation, la suspension et l'expiration des certificats qualifiés de signature et de cachet électroniques, à la partie utilisatrice d'une signature électronique qualifiée ou d'un cachet électronique qualifié, à l'arrêt des activités d'un prestataire de services de confiance qualifié offrant un ou plusieurs services de confiance qualifiés et à la possibilité d'identifier une personne physique qui se cache derrière un pseudonyme ou un cachet électronique.

Les dispositions envisagées visent manifestement à atteindre un équilibre entre souplesse et sécurité. À l'instar du régime déjà applicable aux autres services de confiance dans le cadre du règlement n° 910/2014, le cadre juridique relatif à l'archivage électronique est envisagé comme une "boite à outils juridiques" permettant aux utilisateurs de recourir à ce service en vue de gérer leurs risques par rapport principalement aux données ou documents présentant une valeur juridique. À cet effet, diverses présomptions sont prévues en faveur des services d'archivage électronique considérés comme "qualifiés" au sens de la loi ainsi qu'en faveur des autres services de confiance qualifiés au sens du règlement.

La loi du 21 juillet 2016 abroge aussi la loi précitée du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ainsi que l'arrêté royal du 6 décembre 2002 organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifiés.

Enfin, dernière évolution en date dans le domaine des actes électroniques, est l'extension de la signature électronique aux actes authentiques, c'est-à-dire ceux émanant d'officiers publics (tel que notaires, officiers de l'état civil, magistrats ou huissiers de justice), qui constituent l'échelon le plus haut en matière de preuve écrite.

L'article 1317 du Code civil prévoit désormais[8] que, pour pouvoir être établis, reçus ou signifiés sous forme dématérialisée par un fonctionnaire public, seule une signature électronique qualifiée, visée à l'article 3.12. du règlement (eIDAS) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, satisfait aux conditions d'une signature.

3. La signature électronique ou numérique, un enjeu de fiabilité dans les projets de dématérialisation

La signature électronique est aujourd'hui un élément clé de la démarche de dématérialisation qui est en cours. Pour un projet de dématérialisation bien réussi, les institutions publiques ne peuvent pas faire l'impasse sur la signature numérique. Contrats de travail et autres, baux actifs, dossiers médicaux… De nombreux documents à forte valeur juridique nécessitent une signature fiable lorsqu'ils sont dématérialisés.

Par rapport à la version papier, les gains en temps ne sont pas négligeables : le traitement d'un document, de sa création à sa signature, passe de plusieurs jours à moins d'une journée. On a pu le constater lors de l'expérience pilote lancée par l'INAMI en 2017 pour la signature numérique des nouveaux contrats de télétravail.

8. Voir art. 315, 1° de la loi du 06.07.2017 portant simplification, harmonisation, informatisation et modernisation de dispositions de droit civil et de procédure civile ainsi que du notariat, et portant diverses mesures en matière de justice (M.B. 24.07.2017).

De plus, la signature électronique apporte une réelle confiance dans les échanges numériques entre l'INAMI et ses partenaires externes (les dispensateurs de soins par ex. qui peuvent introduire des demandes d'intervention à l'aide de formulaires intelligents ou modifier les données dans leur dossier personnel), les autres institutions ou encore les fournisseurs (procédures de marché publics informatisées).

Signature manuscrite versus signature numérique

Depuis de nombreuses années, la signature électronique est considérée comme équivalente à la signature manuscrite. C'est-à-dire qu'elles ont exactement la même valeur légale.

Définie aujourd'hui comme un mécanisme numérique basé sur des techniques de cryptographie, la signature numérique a pour objectif de démontrer à un tiers qu'un document électronique a été approuvé par une personne identifiée.

Comme pour la signature manuscrite, la signature numérique permet alors d'identifier son auteur en toute facilité. De plus, c'est également l'intégrité du document qui est ici assuré. En intégrant une signature numérique, l'institution garantit que le document n'a pas été modifié suite à la signature.

De ce fait, la signature numérique est aujourd'hui considérée comme plus fiable qu'une signature manuscrite car en plus de garantir l'identité du signataire, elle garantit l'intégrité du document.

La signature numérique à l'INAMI

Le processus de dématérialisation en cours à l'INAMI passe par une utilisation de plus en plus poussée de la signature électronique et/ou numérique. Cependant, dans le monde numérique, comme dans les processus métiers non dématérialisés, tous les documents ne nécessitent pas d'être signés en original, loin de là.

En effet, ce n'est que lorsque l'organisation ou une personne appartenant à cette organisation, à l'origine de la production d'une pièce numérique souhaite pouvoir prouver qu'elle est bien l'auteur de cette pièce, et qu'elle est représentative de sa volonté, qu'elle est bien sa création, et qu'elle n'a pas été altérée depuis sa création, qu'elle n'a pas d'autre choix que de produire une signature numérique de cette pièce.

La signature numérique est donc le moyen permettant à cette organisation ou à cette personne qu'elle est bien productrice unique d'un fichier numérique devenu infalsifiable.

Une première étape pour l'intégration de la signature numérique dans nos processus passe donc par la définition d'une politique de signature globale (Signature policy).

Une politique de signature numérique efficace s'accompagne de directives explicites :

- types de documents compatibles avec la signature numérique
- meilleures pratiques à adopter
- informations à inclure dans les différents types de documents.

Au niveau de l'INAMI, les critères principaux permettant de déterminer les types de documents aptes à utiliser une signature numérique sont à lier au "risque métier", c'est-à-dire à l'identification des impacts en termes de responsabilités, en termes financiers, d'image, de préjudices potentiels au regard des destinataires visés.

Pourquoi signer ?	Pour qui signer ?	Quelle valeur a ma signature ?
Signer sert à prouver qui est à l'origine d'une information numérique, et cette signature ne s'impose que si le risque de ne pas disposer de cette preuve peut générer un préjudice.	Signer sert principalement les besoins des "destinataires" qui ont besoin de savoir nominativement qui est à l'origine de la signature numérique ou simplement quelle est l'organisation dont émane cette information numérique.	Signer sert à donner une valeur juridique à mon information numérique dans l'hypothèse d'une contestation ultérieure.

Comme on le voit dans ce tableau, la signature sert essentiellement les besoins des destinataires qui doivent pouvoir identifier avec certitude l'origine du document numérique et/ou à donner une valeur juridique à mon document numérique dans l'hypothèse d'une contestation ultérieure.

Quels sont les types de documents concernés ?

Il s'agit ici essentiellement de tous les documents qui doivent être échangés entre l'INAMI et des tiers (assurés sociaux, O.A., autorités judiciaires,…) présentant un caractère officiel et qui doivent à ce titre être revêtus de la signature de l'autorité.

> Par exemple : en vertu de l'article 181 de la loi SSI, l'administrateur général représente l'Institut dans les actes judiciaires et extrajudiciaires et agit valablement au nom et pour le compte de celui-ci. En cas d'empêchement de l'administrateur général, ses pouvoirs sont exercés par l'administrateur général-adjoint et, en cas d'empêchement de ce dernier, par un fonctionnaire de l'Institut désigné par le Comité général.

Pour ce type de documents officiel, il est nécessaire d'apporter la preuve qu'il émane bien d'une personne identifiée et autorisée (l'administrateur général de l'INAMI ou son remplaçant en cas d'empêchement) et que le contenu n'a pas été modifié lors de sa transmission. Dans ce cas, une signature numérique avancée s'impose.

Par contre, l'immense majorité des courriers envoyés chaque jour sur papier à en-tête de l'INAMI, pour lesquels les destinataires doivent juste savoir qu'ils émanent de notre Institut, pourraient être munis d'une signature numérique de base (signature scannée) ou même d'un cachet électronique[9] tel que défini dans le cadre de la loi du 21 juillet 2016.

Outre que la signature qualifiée n'a d'intérêt que lorsque le courrier est envoyé à son destinataire sous forme électronique, n'oublions pas que ce destinataire doit pouvoir 'lire' (= déchiffrer) la signature électronique (ce qui suppose qu'il dispose de logiciels supportant cette fonction) !

Par ailleurs, rappelons que sauf dispositions légales contraires, et même si les pouvoirs publics tendent à privilégier les échanges électroniques, nul ne peut être contraint de poser un acte juridique par voie électronique. De même, personne ne peut être contraint de poser des actes de procédure ou de recevoir des documents relatifs à ces actes de procédure par voie électronique[10].

9. Remarque : quelle est la différence entre la signature et le cachet électroniques ? Le cachet identifie une personne morale, alors que la signature identifie la personne physique.
10. Art. XII., 25,. § 1er du Code de droit économique et art. 4 de la loi du 10.07.2006 relative à la procédure par voie électronique.

À l'heure actuelle, il est certainement possible de l'envisager dans les échanges entre organismes publics ou coopérants (les O.A. par ex.) et à terme à destination des particuliers : pour des raisons techniques et des motifs d'ordre juridique liés à la protection de la vie privée, il pourrait être risqué d'envoyer une décision à un particulier reprenant des données à caractère personnel, voire médical, vers une boite mail privée non sécurisée. Des solutions sont actuellement à l'étude (notamment utilisation de l'e-Box ou de la e-Healthbox).

Enfin, il n'est pas inutile de signaler que les conditions d'utilisation de la signature 'simple' c'est-à-dire scannée, ont déjà débattues devant les cours et tribunaux. Pour ceux que cela intéresse, ils peuvent consulter une analyse de jurisprudence[11] qui, en conclusion, exprime le conseil donné à nos informaticiens, à savoir : "(…) de veiller à adopter des mécanismes techniques permettant d'identifier de manière certaine le signataire du document et son adhésion au contenu de l'acte, ainsi que d'adopter un dispositif permettant de démontrer le maintien de l'intégrité du document signé. Pour convaincre le juge, ces institutions devront par exemple être en mesure de lui présenter une bonne documentation du processus de numérisation, de conservation et, le cas échéant, de datation électronique des documents électroniques produits ".

En conclusion, le choix d'un type particulier de signature dépend de l'utilisation que l'on compte faire de cette signature numérique :

- la signature électronique "simple" est suffisante pour une application ne demandant pas une sécurité élevée. Ainsi, une signature manuscrite scannée peut très bien être utilisée afin d'être apposée sur tout courrier ordinaire
- la signature numérique "avancée" : elle doit être liée uniquement au signataire, permettre l'identification du signataire, être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée
- la signature numérique "qualifiée" : c'est une signature électronique "avancée" réalisée sur la base d'un certificat qualifié, et conçue au moyen d'un dispositif sécurisé de création de signature électronique tels que définis dans la loi du 21 juillet 2016.

La signature numérique qualifiée présente le niveau de sécurité le plus élevé défini actuellement au niveau européen[12].

Avec E-Signing, la signature numérique sera progressivement intégrée dans les processus de l'INAMI dans le cadre de la nouvelle version de IOC (In and Outbound Communication) qui soutient nos applications de gestion de dossiers.

Sur le plan technique, trois types de signature électronique devraient être disponibles dans IOC V2 à partir de 2018 :

1. la signature électronique qualifiée (QES) qui est considérée comme l´équivalent de la signature manuscrite. L´ICT mettra en place une solution QES qui sera séparée du processus de courrier sortant. De manière globale, pour signer un document avec une signature de type QES, le signataire devra entreprendre les actions suivantes pour chaque document :

- se connecter avec l´application et sélectionner le document à signer
- déclencher le processus de signature électronique à partir de cette application

11. Voir note d'observations : Signature scannée : quand une technologie simple confronte le juriste à des questions complexes, J.-B. Hubin, Revue du droit des technologies de l'information n° 56/2014.
12. Le législateur allemand a également décidé de reconnaître ces trois concepts de signatures électroniques dans la "Signaturgesetz" : la signature électronique simple, la signature électronique avancée et la signature électronique qualifiée.

- choisir les paramètres de visualisation :
  - image-based handwritten signature
  - full name
  - timestamp
  - eID Photo
  - eID Photo watermarked
  - etc.
- s´authentifier avec son eID + Code pin
- recevoir le document signé.

2. le cachet électronique (eSeal) qualifié dont la personne morale titulaire serait l´INAMI, représenté par l´Administrateur général, Jo De Cock. Ce type de signature sera intégré dans le processus de courrier sortant et serait plus adapté pour les signatures de gros volumes. En plus, dans la solution proposée dans le projet IOC V2, il sera possible de combiner la signature simple avec le cachet électronique ou la signature qualifiée (voir les paramètres de visualisation) ;

3. la signature électronique simple (SES) consiste à utiliser l´image de la signature manuscrite pour signer les documents ou courriers sortants. Pour ce type de signature, il n´y a aucune vérification sur l´identité du signataire.

Le type de signature à utiliser pour un document déterminé devra être fixé par le business (pas par IOC). Comme signalé ci-dessus (voir tableau en p. 7), il faudra se demander, pour chaque document à signer, si la signature intervient comme individu (QES) ou comme entité (eSeal) et s´interroger aussi sur les volumes à signer. En fonction du choix du type de la signature électronique, l´utilisateur pourra appeler via son application le service QES (signature électronique qualifiée) ou les solutions eSeal et SES qui sont intégrées au système d´IOC message broker.

Sources et bibliographie

PUBLICATIONS

- Hervé JACQUEMIN, Les services de confiance depuis le règlement eIDAS et la loi du 21 juillet 2016, JTT 2017, p. 197
- Hervé JACQUEMIN, L'identification électronique et les services de confiance depuis le règlement eIDAS, LARCIER - Collection du CRIDS, 2016
- Eric-A. CAPRIOLI, Signature électronique et dématérialisation - Droits et pratiques, LEXIS NEXIS Droit & Professionnels, 2014
- J.-B. HUBIN, Note d'observations : Signature scannée : quand une technologie simple confronte le juriste à des questions complexes, Revue du droit des technologies de l'information, n° 56/2014, p. 122
- Dimitri MOUTON, Sécurité de la dématérialisation - De la signature électronique au coffre-fort numérique, une démarche de mise en œuvre, EYROLLES, 2012.

SOURCES INTERNET

- Le règlement européen n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance, SPF Economie - Décembre 2016
- Murielle CAHEN, La signature électronique et le droit européen, Article juridique posté le 17 avril 2015 sur Legavox.fr
- Eric A. CAPRIOLI & Anne CANTERO, Aspects légaux et réglementaires de la signature électronique, www.caprioli-avocats.com
- Arnaud HULSTAERT, Signature et archivage des documents sortants, posté le 8 novembre 2011 sur SMALS RESEARCH.