La signature électronique

easy.brussels

Guide à l'attention des Autorités publiques bruxelloises

easy.brussels
SERVICE PUBLIC RÉGIONAL DE BRUXELLES
GEWESTELIJKE OVERHEIDSDIENST BRUSSEL
BRUSSELS REGIONAL PUBLIC SERVICE

Guide régional sur la signature électronique

Table des matières

1. Introduction

Depuis le 15 mars 2014, les administrations bruxelloises peuvent communiquer par voie électronique avec les citoyens et les entreprises, en produisant des effets juridiques, même dans le cas où la réglementation ne le prévoit pas explicitement. Cette possibilité leur a été offerte par l'ordonnance du 13 février 2014 relative à la communication par voie électronique dans le cadre des relations avec les autorités publiques de la Région de Bruxelles-Capitale, qui, concrètement, permet aux administrations de dématérialiser leurs procédures. Si cela va dans le sens d'une simplification administrative, cela implique toutefois de se poser certaines questions. L'une d'elles est celle qui va nous intéresser dans ce guide : la question de la signature électronique.

En effet, si une administration décide d'ouvrir la communication électronique, en créant par exemple des formulaires en ligne, ce n'est pas pour imprimer ensuite le formulaire et poursuivre le processus en papier. Dans le cas où une administration fait le choix de dématérialiser une procédure, il convient de le faire du début à la fin : introduction de la demande, réception de celle-ci par l'administration, traitement des autorisations et communication de la décision. Ce document que le demandeur va recevoir, il ne serait pas logique de l'imprimer pour le signer manuellement et le scanner ensuite. Il en va de même pour l'introduction de la demande : si le formulaire est rempli en ligne, comment le demandeur peut-il le signer ? En recourant à une signature électronique.

Avant d'utiliser la signature électronique, il faut se poser certaines questions, qu'il s'agisse du courrier électronique entrant ou du courrier sortant, de l'implémentation de la signature, à son archivage. Ce guide répondra aux deux premières questions qu'il convient de se poser :

1) Peut-on utiliser la signature électronique ?
2) Quelle signature électronique utiliser[1] ?

2. Champs d'application et définition

2.1. Champs d'application

Le présent guide a pour vocation de s'appliquer aux autorité publiques bruxelloises. L'ordonnance du 13 février 2014, qui s'applique aux « autorités publiques » de la Région de Bruxelles-Capitale, définit celles-ci comme comprenant :

a) la Région de Bruxelles-Capitale ;
b) les personnes morales de droit public qui dépendent, directement ou indirectement, de la Région de Bruxelles-Capitale ;
c) les communes et les autres collectivités territoriales situées sur le territoire de la région bilingue de Bruxelles-Capitale ;
d) les entités, quelles que soient leur forme et leur nature, qui :
   - ont été créées pour satisfaire spécifiquement des besoins d'intérêt général ;
   - sont dotées d'une personnalité juridique ;

[1] Pour aller directement à la partie « choix de la signature », vous pouvez vous rendre à la page 8.

- et dont soit l'activité est financée majoritairement par les autorités publiques ou organismes mentionnés au a), b) ou c), soit la gestion est soumise à un contrôle de ces autorités publiques ou organismes, soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par ces autorités ou organismes ;

e) les associations formées par une ou plusieurs autorités publiques visées au a), b), c) ou d).

2.2. Définition et cadre légal

Le règlement eIDAS, transposé en droit belge par la loi du 21 juillet 2016 (« Digital Act »), laquelle a inséré 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, définit la signature électronique comme « *des données sous forme électronique, jointes ou associées à d'autres données électronique que le signataire utilise pour signer* ». Une signature électronique doit permettre de vérifier que le document n'a pas été modifié (intégrité) et en vérifier qui est l'auteur (authentifier).

Concrètement, la signature électronique est un mécanisme permettant de garantir :

- l'**intégrité** d'un document électronique ;
- et d'**authentifier** l'auteur de la signature électronique.

Cette définition très large renvoie à de nombreuses signatures, parfois totalement électroniques comme les signatures électroniques via la carte d'identité, mais également partiellement électroniques, comme les signatures manuscrites scannées. De même, sont considérés comme « signature électronique », sur base de cette définition, les signatures biométriques (par exemple, la reconnaissance vocale, la reconnaissance de l'iris de l'œil, la reconnaissance des empreintes digitales) ou encore les simples codes de cartes (bancaires notamment).

Pour autant, toutes ces signatures ne présentent pas les mêmes avantages ou le même niveau de sécurité. En fonction des exigences auxquelles elle satisfait une signature électronique pourra être « simple », « avancée » ou « qualifiée ».

2.3. Types de signature

2.3.1. Concepts préalables

Avant de présenter les différents types de signature électronique existant, quelques concepts doivent être définis pour bien appréhender les avantages des différentes signatures.

a. Authentification ou identification

Le principe d'authentification (ou d'identification) a pour but de confirmer l'identification d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique. L'idée est donc de lier de manière certaine une signature à une personne.

b. Intégrité

Le principe d'intégrité des données veut que les données ne subissent aucune altération ou destruction volontaire ou accidentelle, lors de leur traitement ou de leur transmission. Garantir l'intégrité des données implique donc d'assurer au destinataire d'un document qu'il n'a pas été modifié après avoir été signé.

c. Non-répudiation

Le principe de non-répudiation (ou non-discrimination) est le fait que la signature électronique ne peut être refusée par un juge en raison de son caractère électronique. Qu'elle soit assimilée à une signature manuscrite ou simple commencement de preuve (voir plus loin), elle ne pourra pas être écartée des débats.

d. Certification

Le service de certification est fourni par un prestataire accrédité[2] (souvent appelé « tiers certificateur » ou « tiers de confiance » en Belgique) et ajoute une assurance de qualité liée, d'une part, à la supervision des moyens et processus mis en œuvre par l'autorité de certification et, d'autre part, à la conformité du dispositif de signature.

Pour comparer cela à la gestion documentaire, le tiers certificateur agit comme le faisait un notaire, désigné comme officier public : son rôle était de vérifier l'identité des parties et si celles-ci consentaient en toute connaissance de cause à l'acte qui était passé devant lui. Le notaire en était le témoin, ainsi que le garant du respect des formes et de la volonté de parties. Tout comme ce rôle rendait l'acte « authentique » en version papier, le tiers certificateur rend la signature « qualifiée » par son implication

[2] L'accréditation des prestataires doit se faire par un organisme de certification belge ou européen. « *Le prestataire qui souhaite offrir un service qualifié est soumis à un régime d'autorisation préalable et doit respecter de nombreuses conditions strictes (notamment en termes de sécurité), consacrées par le règlement eIDAS. Ces conditions font l'objet d'un contrôle approfondi et préalable par un organisme d'audit accrédité ainsi que par l'organe de contrôle. De plus, un audit du prestataire est imposé tous les deux ans.* » (voir https://economie.fgov.be/sites/default/files/Files/Online/FAQ-services-de-confiance.pdf).
La liste des prestataires accrédités en Belgique peut être consultée sur le site internet du SPF Économie et sur le site internet de la Commission européenne :
- https://economie.fgov.be/sites/default/files/Files/Online/Liste-prestataires-qalifies-services-de-confiance-belges.pdf) ;
- https://webgate.ec.europa.eu/tl-browser/#/.

dans le processus de signature en vérifiant l'authentification des parties ainsi que l'intégrité des documents.

2.3.2.Signature électronique « simple »

La signature « simple », « simplifiée » ou encore « ordinaire » est le premier type de signature électronique possible. Elle correspond notamment au fait de cocher une case sur un document en ligne, à la signature apposée manuellement sur un écran ou sur un pad (comme lorsque l'on réceptionne un colis par exemple), ou encore au fait d'apposer une signature manuscrite scannée sur un document.

La signature manuscrite scannée est souvent utilisée dans les administrations. Mais si cette signature est rendue « électronique » dès lors qu'elle est scannée, pour être apposée sur certains documents, elle ne présente **qu'une seule des propriétés susmentionnées**, à la différence des autres types de signature électronique, présentés ci-dessous.

Elle n'est qu'une image apposée sur un document et ne permet pas d'identifier de manière certaine la personne ayant signé le document (puisque toute personne ayant accès au scan de cette signature peut l'utiliser)[3], ni d'assurer que le document n'a pas été modifié ensuite.

X	Identification
X	Intégrité
V	Non-répudiation
X	Certification

2.3.3.Signature électronique « avancée »

La signature électronique « avancée » est une signature électronique pour laquelle des liens techniques sont établis entre les données signées, la signature et le signataire. Ces liens techniques visent à garantir l'intégrité des données, l'identification du signataire et la non-répudiation.

Ce niveau fait nécessairement appel à une signature totalement numérique, impliquant typiquement des moyens de chiffrement qui transforment à l'aide d'un algorithme mathématique tout ou partie d'un message dit « clair » en cryptogramme ou message chiffré.

Pour être avancée, une signature électronique doit répondre aux conditions de l'article 26 du règlement eIDAS, à savoir :

- être liée au signataire de manière univoque ;
- permettre d'identifier le signataire ;
- avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; et

[3] La signature manuscrite scannée a toutefois déjà été acceptée dès lors que seules quelques personnes y avait accès : voir C. trav. Bruxelles, 11 octobre 2013 et C. trav. Bruxelles, 14 février 2014, R.D.T.I., 2014, pp. 115-121 (source : LOSDYCK, B., « L'usage de signatures électroniques dans le cadre du Règlement eIDAS », p.146-147).

- être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

V	Identification
V	Intégrité
V	Non-répudiation
X	Certification

Un exemple de signature électronique avancée est la signature biométrique utilisant une tablette Wacom, une signature utilisant l'identité numérique néerlandaise iDIN, ou encore une signature réalisée après une vérification des papiers d'identité d'une personne par un applicatif dédié (Onfido, IDNow, Ubble,…).

2.3.4.Signature électronique « qualifiée »

La signature électronique « qualifiée » est une signature électronique *avancée* (qui présente donc les avantages repris ci-dessus), basée sur un certificat qualifié et créée au moyen d'un dispositif de signature qualifié.

Si le règlement eIDAS stipule bien qu'une signature électronique ne peut être refusée comme preuve en justice au seul motif qu'elle ne serait qu'« électronique » (y compris une signature manuscrite scannée donc), seule la signature *qualifiée* est assimilée juridiquement à une signature manuscrite, avec tous les effets juridiques qui vont de pair avec la signature manuscrite. Cette assimilation est prévue expressément par le règlement eIDAS, en son article 25.

En justice, une signature électronique, si elle n'est pas qualifiée pourra avec plus de facilité être remise en cause, au contraire de la signature qualifiée, qui aura une valeur juridique plus importante, assimilée à une « vraie signature de la main ».

	V	Identification
	V	Intégrité
	V	Non-répudiation
+	V	**Certification**

L'exemple le plus utilisé de signature électronique qualifiée est la signature au moyen de la carte d'identité, comme lorsque l'on signe un PDF en utilisant Adobe Acrobat, ou encore via Itsme.

Remarque : dans certains cas, la signature électronique qualifiée apporte également une fonction « horodatage », laquelle permet de donner au document une date (voire une heure) certaine. C'est

notamment le cas de la signature électronique par le biais d'Adobe Acrobat. Néanmoins, les deux fonctions ne sont pas forcément liées.

⇨ L'horodatage fait l'objet du point 5.2, ci-dessous.

2.3.5. Conclusion intermédiaire

Plusieurs types de signature électronique s'offrent à l'administration qui fait le choix de dématérialiser ses procédures : signature électronique simple, signature électronique avancée ou signature électronique qualifiée. Comme nous venons de le voir, ces trois types de signature n'apportent pas tous le même niveau de sécurité :

	Signature électronique simple	Signature électronique avancée	Signature électronique qualifiée
Identification	**X**	**V**	**V**
Intégrité	**X**	**V**	**V**
Non-répudiation	**V**	**V**	**V**
Certification	**X**	**X**	**V**

Bien qu'elles n'apportent pas toutes les mêmes garanties, toutes ces signatures peuvent pourtant être utilisées par les administrations, selon le contexte et surtout selon le document à signer.

3. Utilisation de la signature électronique

À présent que nous avons décrit les différentes signatures électroniques existant, il convient de déterminer quelle forme utiliser et dans quel cas.

3.1. Avantages et inconvénients de la signature électronique qualifiée

3.1.1. Avantages

Le Digital Act régit l'utilisation et les conséquences juridiques des services de confiance électroniques, dont la signature électronique, et donne une sécurité quant aux conséquences juridiques liées à l'usage des services de confiance.

Concrètement, le Digital Act et le règlement eIDAS créent une présomption légale de conformité pour les services de confiance électroniques qualifiés : leur utilisation, leur intégrité et leur authenticité ne peuvent pas être remis en question. Les services de confiance qualifiés ont fait l'objet de contrôles approfondis et offrent une garantie de **confiance élevée**, qui est **juridiquement reconnue** dans toute l'Union européenne.

Un autre avantage de la signature électronique qualifiée est qu'elle fait basculer la **charge de la preuve**. Si le document signé avec une signature électronique qualifiée fait l'objet d'un recours, ce sera au demandeur de prouver que la signature n'est pas valide. Dans le cas d'une autre signature électronique, ce sera à la partie ayant signé le document de prouver que la signature est valide, ou encore que le document n'a pas été modifié.

3.1.2. Inconvénients

La signature électronique qualifiée étant la **seule reconnue** juridiquement comme équivalente à la signature manuscrite, et présentant le plus de sécurité, il est tentant de l'utiliser pour signer tous les documents devant l'être. Ce n'est toutefois pas nécessaire, car si cette signature présente de nombreux avantages, elle peut aussi se montrer contraignante.

En effet, pour utiliser la signature électronique qualifiée, il faut faire appel, comme mentionné plus haut, à un prestataire qualifié. Or, seuls les prestataires de services de confiance repris sur la liste officielle du SPF Économie, P.M.E., Classes moyennes et Energie, peuvent proposer ce service. Cela limite donc les solutions techniques pouvant être utilisées par les administrations. Ces solutions seront par ailleurs payantes. Chaque signature apposée aura un coût non négligeable.

D'autre part, imposer la signature électronique qualifiée pourrait mettre certaines personnes en difficulté. Nous pensons ici notamment aux personnes en situation de **fracture numérique**[4], qui ne maitrisent pas les outils numériques, mais également aux personnes ne disposant pas des ressources matérielles pour utiliser la signature électronique qualifiée. En effet, pour signer électroniquement (avec une signature électronique qualifiée), il faudra disposer des outils nécessaires : lecteurs de carte électronique, par exemple, ou encore d'une carte d'identité/de séjour avec puce tout simplement. Or, en pratique, tout le monde ne dispose pas de ces outils. Imposer l'utilisation de la signature électronique qualifiée pourrait mettre en difficulté certaines personnes et les exclure *de facto* de la procédure.

Enfin, un autre inconvénient lié à l'utilisation d'une signature électronique qualifiée est la conservation à long terme de cette signature : les certificats expirent après un certain temps, alors que les documents signés doivent parfois être conservés plus longtemps et doivent donc être validés par la signature pendant une période plus longue. Il serait toutefois possible de prouver que la signature était valide lorsque le document a été signé en archivant le document de manière qualifiée tant que les certificats sont encore valables.

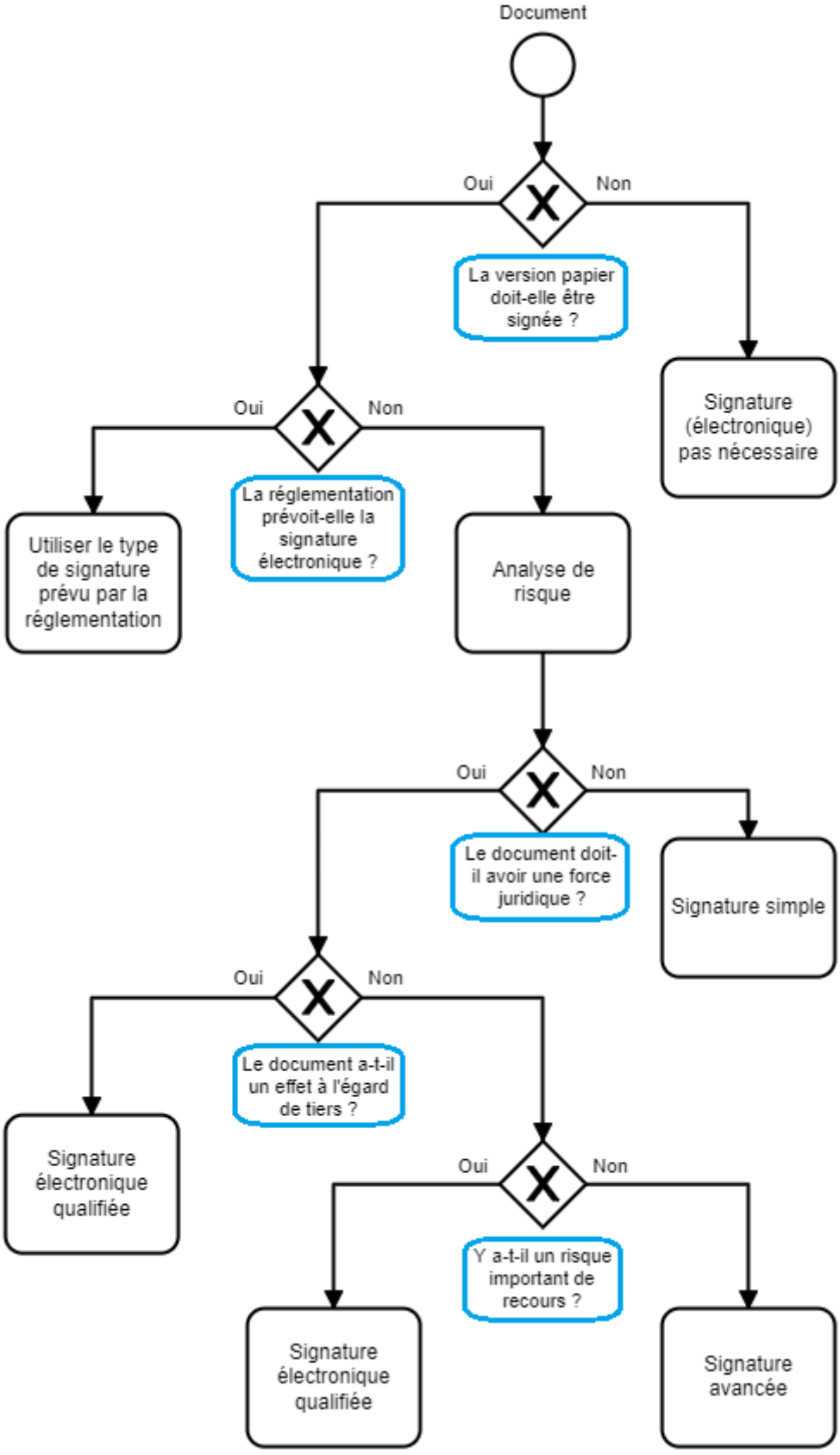
3.2. Choix du type de signature à utiliser

En définitive, la signature électronique qu'il convient d'utiliser va dépendre de la nature (et de l'importance) du document à signer, et diverses questions doivent être envisagées pour choisir le type de signature le plus adapté. Ces questions constituent ce que nous appellerons « l'analyse de risques ».

[4] Des solutions existent pour venir en aide aux personnes en situation de fracture numérique. Outre les moyens dont disposent les différentes administrations, les Espaces Publics Numériques installés dans les différentes communes bruxelloises peuvent être contactés.

L'arbre décisionnel repris ci-après a été développé pour aider les administrations dans le choix de la signature électronique à utiliser. Quant aux questions qui y sont reprises, elles seront développées juste après celui-ci.

3.2.1.Arbre décisionnel



3.2.2. Analyse de risque

1) La signature du document est-elle requise par une loi, une ordonnance ou un autre texte réglementaire ?

Si la signature n'est pas requise par la réglementation applicable, il convient de se demander si la signature est vraiment nécessaire, qu'il s'agisse de signer la version papier ou la version électronique du document. *A fortiori*, si la version papier du document n'est pas signée, il n'y a pas de raison que la version électronique le soit.

Par ailleurs, si le document papier est signé, mais que la signature n'a qu'une valeur symbolique[5], il n'est pas nécessaire de recourir à la signature électronique qualifiée. Une signature électronique « simple » ou « simplifiée » suffit, pour peu que l'étude du processus en confirme le besoin ou l'utilité.

Si la signature est requise par la réglementation applicable[6], par contre, il faut effectivement signer le document et poursuivre l'analyse pour voir quelle signature utiliser :

- Si la réglementation demande l'utilisation d'un type spécifique de signature, il convient d'utiliser le type de signature requis par la réglementation ;
- Si rien n'est mentionné dans la réglementation quant au type de signature à utiliser, nous vous invitons à effectuer une **analyse de risques**, en examinant les questions suivantes.

2) Le document signé doit-il avoir un effet juridique ?

Si le document à signer n'a aucun effet juridique (comme par exemple un courrier d'information), et que le seul but de la signature est de donner une authenticité apparente au document, une signature électronique simple est selon nous être suffisante.

Si le document à signer a un effet juridique, par contre, comme l'octroi d'une prime ou la création d'une obligation, une signature électronique avancée ou qualifiée est à recommander. Elle aura l'avantage d'assurer l'authenticité et l'intégrité du document. Il reste à déterminer laquelle, de la signature avancée ou de la signature qualifiée, utiliser.

3) Le document signé doit-il être opposable aux tiers ?

Si le document doit être opposable à des tiers, il est recommandé d'utiliser une signature électronique qualifiée. Prenons l'exemple d'une décision d'octroi d'un permis à un citoyen, laquelle a des conséquences à l'égard de tiers : dans ce cas, l'utilisation de la signature électronique qualifiée

[5] Dans certains cas, les destinataires des documents préfèrent y voir une signature : par exemple, lorsqu'un citoyen reçoit un courrier informatif de la part du bourgmestre, il s'attend sans doute à y voir la signature de celui-ci. Néanmoins, il n'est pas nécessaire d'utiliser une signature électronique qualifiée pour cela. Une signature électronique simple (notamment la copie scannée de la signature du bourgmestre) suffit.

[6] L'ordonnance du 29 novembre 2018 sur les funérailles et sépultures, par exemple, prévoit en son article 40 que « *La communication et le cas échéant la signature des données relatives aux autorisations d'inhumation et de crémation visées par la présente ordonnance, peuvent être remplacées par une procédure électronique, fixée par le Gouvernement qui garantit de manière démontrable l'authenticité et l'intégrité de ces données* ». Bien que l'ordonnance n'impose pas un type de signature en particulier, elle exclut de facto la signature électronique simple en imposant les garanties d'authenticité et d'intégrité. Quant au choix à faire entre la signature avancée et la signature qualifiée, il convient selon nous d'effectuer une analyse de risques.

permettra d'inverser la charge de la preuve : si un tiers souhaite contester la validité de la signature, ce sera à lui d'apporter les preuves nécessaires.

Si le document ne doit pas être opposable à des tiers, s'il n'a d'effet qu'à l'égard du destinataire du courrier signé, dans ce cas, l'utilisation d'une signature électronique qualifiée ou d'une signature électronique avancée dépendra de la question suivante.

4) Existe-t-il un risque de recours important à l'encontre du document signé ?

En définitive, la question la plus importante à se poser quand il s'agit d'évaluer le type de signature à utiliser est celle des **recours**.

S'il existe un risque de recours important contre la décision, la signature électronique qualifiée est à privilégier.

S'il existe un faible risque de recours contre le document à signer (décision individuelle favorable au destinataire et sans effet à l'égard de tiers, par exemple), par contre, il n'est pas nécessaire d'utiliser une signature électronique qualifiée et une signature électronique avancée suffit.

Comme développé plus haut, une des différences notables entre la signature électronique qualifiée et la signature électronique avancée est que la première entraine une inversion de la charge de la preuve, puisqu'elle est émise via un prestataire qualifié. Si le risque de recours est faible, il nous semble que l'utilisation de la signature électronique avancée peut s'avérer suffisante : si recours il y a, il suffira à l'administration de prouver la véracité du document contesté (par exemple, en cas de décision négative, en apportant les justificatifs de cette décision).

En définitive, la décision de recourir à une signature électronique qualifiée ou avancée appartient à l'administration[7] qui devra mettre en balance les avantages de la signature électronique qualifiée (inversion de la charge de la preuve) et ses inconvénients.

3.3. Cas pratique

Pour illustrer l'analyse de risque que nous venons de présenter, nous proposons d'utiliser un exemple fictif :

- Situation : l'administration A est compétente pour octroyer une prime à tous les citoyens remplissant trois conditions prévues dans une ordonnance : dès que celles-ci sont rencontrées, le citoyen a droit à une prime au montant fixe, sans que cela n'ait aucun effet pour les tiers. Un citoyen a introduit une demande de prime et remplit les conditions d'octroi. Quel type de signature électronique l'administration A va-t-elle utiliser pour signifier au citoyen l'octroi de la prime ?
- Présupposé : pour l'exemple, nous prendrons l'hypothèse que la version papier de la décision d'octroi est signée, et que la réglementation ne prévoit pas explicitement la signature électronique.

[7] Les organes dirigeants de chaque administration devront édicter leurs lignes directrices en la matière.

- Solution : en pratique, dès lors que le courrier notifiant la décision d'octroi produit des effets juridiques (puisqu'il concerne l'octroi d'une prime), qu'il n'a pas d'effet à l'égard de tiers, et que le risque de recours est presque inexistant, une **signature électronique avancée** suffirait.

3.4. Cas particuliers

3.4.1. Acte authentique

L'acte authentique se distingue des autres documents pour plusieurs raisons. L'une d'elle tient au fait que le seul moyen de contester le contenu d'un acte authentique est d'entamer une procédure d'« inscription de faux ». Une autre raison tient en la qualité de la personne attestant des conditions de la signature de l'acte (authenticité, intégrité) et des conditions formelles pour pouvoir passer l'acte. En effet, l'acte authentique doit obligatoirement être passé devant ou établi par un « officier public ». Cette obligation en implique une autre : sur base du Code civil, seule la signature électronique qualifiée peut être utilisée dans ce cas.

Lorsqu'un officier public veut signer un acte authentique de manière électronique, il doit exclusivement avoir recours à la signature électronique qualifiée, telle que présentée ci-dessus.

Les exemples d'actes authentiques sont : les actes de l'état civil, les actes notariés, les actes établis par le juge de paix, les constats d'huissiers, certains actes des comités d'acquisition (SPRBF), etc.

Notons cependant qu'un document qui doit être conservé en original n'est pas toujours un acte authentique. Par exemple, les textes de lois qui sont signés par les ministres ne sont pas considérés comme des actes authentiques. Il n'en reste pas moins que ces documents originaux ont une valeur historique, et ne devraient pas être détruits (voir la partie sur l'archivage).

3.4.2. Signature d'un lot de documents

Certaines solutions techniques de signature électronique permettent de signer plusieurs documents en même temps, ce que l'on appelle également un lot de documents.

Cela ne modifie toutefois pas l'analyse ci-dessus, quant au choix du type de signature à utiliser. En fonction de l'analyse de risques, s'il apparait que le document doit être signé au moyen d'une signature électronique avancée, le fait qu'il fasse partie d'un lot de documents n'aura pas d'impact sur la validité de la signature. Tout au plus, faudra-t-il s'assurer que tous les documents composant le lot nécessitent le même type de signature.

En définitive, l'important est de garantir la validité de la signature pour chaque document individuel.

4. Archivage

Le but de ce guide n'est pas de donner des instructions relatives à l'archivage des divers documents produits ou reçus par les administrations. Deux points, toutefois, doivent être soulevés quant à l'archivage des documents signés électroniquement.

Le premier point tient à la durée de validité des moyens d'identification. En effet, que faire quand le moyen utilisé pour l'identification arrive à son terme ? La carte d'identité électronique, par exemple, a une validité limitée dans le temps. Qu'advient-il des documents signés avec une signature électronique qualifiée et la carte d'identité du signataire, une fois celle-ci « périmée » ? Si la signature a été valablement apposée, à un moment T, le fait que la carte d'identité arrive en fin de validité par la suite ne doit pas remettre en question la signature.

En pratique, les organismes certificateurs (prestataires de services de confiance) ont l'obligation de conserver les certificats ou du moins la preuve du certificat (au moment de la signature), sans limitation de temps. Quand bien même l'organisme cesserait ses activités, l'obligation de conserver l'historique des certificats demeure.

Un autre point concerne l'archivage du document une fois signé, par l'administration. Lors de la signature d'un document, au moyen d'une signature électronique qualifiée, un numéro/code unique va être créé dans les métadonnées du document. Ce code sert à démontrer la validité de la signature au moment T. Lorsque l'administration archive ce document, elle doit s'assurer que le numéro/code unique ne soit pas modifié lors de la migration.

Si l'administration a recours à un archivage électronique qualifié, cette condition est présumée remplie. Dans le cas où l'administration aurait recours à une autre méthode d'archivage, elle devra, par contre, s'assurer que le transfert se fasse correctement, et que le numéro/code unique reste inchangé.

5. À côté de la signature électronique…

5.1. Cachet électronique

Le cachet électronique permet aux personnes morales (aux entreprises notamment) d'avoir l'équivalent d'une signature électronique. Il est défini dans le règlement eIDAS comme « *des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières* ». Il suit donc les mêmes principes que la signature électronique en appuyant davantage sur la garantie de l'origine (la personne morale et non la personne physique qui l'utilise) et de l'intégrité du document.

De la même manière qu'il existe divers types de signature, il en va également pour le cachet électronique. Il sera donc possible d'utiliser : un cachet électronique simple, un cachet électronique avancé ou un cachet électronique qualifié.

Pour être **« avancé »**, le cachet électronique doit répondre aux conditions de l'article 36 du règlement eIDAS, à savoir :

- être lié au créateur du cachet de manière univoque ;
- permettre d'identifier le créateur du cachet ;
- avoir été créé à l'aide de données de création de cachet électronique que le créateur du cachet peut, avec un niveau de confiance élevé, utiliser sous son contrôle pour créer un cachet électronique ;
- et être lié aux données auxquelles il est associé de telle sorte que toute modification ultérieure des données soit détectable.

V	Identification
V	Intégrité
V	Non-répudiation
X	Certification

Pour être **« qualifié »**, le cachet électronique doit répondre aux conditions de l'article 36 (cachet électronique avancé) mais être, en plus, créé à l'aide d'un dispositif de création de cachet électronique qualifié et qui repose sur un certificat qualifié de cachet électronique (art. 3 §27 du règlement eIDAS).

V	Identification
V	Intégrité
V	Non-répudiation
V	Certification

Enfin, de même que pour la signature électronique, si un cachet électronique ne peut être refusé comme preuve en justice sur le seul motif d'être électronique, seul le cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles il est lié (art. 35 du règlement eIDAS).

5.2. Horodatage

Dans certains cas, l'important n'est pas de lier le document avec une personne, mais de lui donner une date (voire une heure) certaine. L'horodatage peut ainsi être important en cas de sanctions, ou encore en cas de demande de prime (pour classer les demandeurs dans l'ordre de demande). Quelle solution utiliser alors ?

L'horodatage électronique est défini dans le règlement eIDAS comme « *des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant* » (art. 3 §33 du règlement eIDAS). Il permet de :

- dater précisément un document ;

- certifier qu'à un moment précis une donnée existait ou qu'une opération a été réalisée par voie électronique (signature électronique, envoi recommandé électronique).

Pour être **« qualifié »**, l'horodatage électronique doit :

- lier la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données ;
- être fondé sur une horloge exacte liée au temps universel coordonné ;
- être signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié, ou par une méthode équivalente (art. 42 du règlement eIDAS).

Enfin, l'horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure (art. 41 du règlement eIDAS). En effet, plutôt que d'être horodaté sur base de l'horloge de la personne émettant le document, laquelle peut être modifiée, il sera horodaté par le prestataire, dont l'horloge est liée « au temps universel coordonné ».

La signature électronique qualifiée et le cachet électronique qualifié offrent une fonction horodatage. Mais comme nous l'avons vu plus haut, cette solution peut se montrer contraignante, voire coûteuse. Il peut dès lors être utile de recourir à une autre solution technique. Le SPF Économie reprend, sur son site internet, les prestataires de services de confiance qualifiés proposant spécifiquement l'horodatage électronique (en-dehors de toute signature).

5.3. Envoi recommandé électronique

Le règlement eIDAS définit le service d'envoi recommandé électronique comme un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée.

Tout comme pour la signature électronique, il existe un service d'envoi recommandé électronique simple et un service d'envoi recommandé électronique qualifié, qui bénéficie des présomptions d'intégrité attachées aux services de confiance qualifiés.

6. Conclusion et recommandations

Le but de ce guide était d'aider les administrations bruxelloises dans la transformation de leurs procédures papier en procédures électroniques, et de leur donner les informations nécessaires pour implémenter la signature électronique dans leurs processus. Nous avons ainsi décrit les différents types de signature électronique existant, et proposé un arbre décisionnel permettant de guider le choix de l'administration quant au type de signature à utiliser.

Il appartient à présent aux administrations de poursuivre le travail entamé ici. Pour ce faire, nous aimerions donner aux administrations quelques recommandations.

Concernant la décision d'utiliser la signature électronique :

Une première recommandation est de réserver la signature électronique aux cas où elle est réellement utile. Si l'idée est de valider le contenu d'un document, en interne, par exemple, le recours à la signature électronique n'est pas nécessaire. Il existe d'autres moyens de valider un document, comme par exemple un accord par email. De même, dans certains cas, un login peut suffire à garantir de l'identité de la personne approuvant une décision. C'est le cas pour traiter un bon de commande ou approuver un ordre de mandater, par exemple.

En conclusion, la signature électronique devrait être réservée aux cas où elle est expressément requise par la réglementation, ou aux cas où elle apporte véritablement une plus-value (voir arbre décisionnel).

Concernant la rédaction de la réglementation applicable :

La deuxième recommandation que nous aimerions faire concerne cette fois non pas le choix d'utiliser ou non la signature électronique, en fonction de la réglementation applicable, mais bien la rédaction de cette réglementation.

Les solutions techniques évoluent rapidement. De nouvelles solutions apparaissent régulièrement. Afin d'éviter de figer une réglementation, et d'empêcher le recours aux nouvelles technologies, nous recommandons aux administrations d'utiliser des expressions et termes technologiquement neutres dans la rédaction de leur réglementation. Plutôt que d'imposer une signature, voire même un type de signature électronique, nous conseillons de mentionner les effets de celle-ci (authenticité, intégrité, etc.).

Sur cette base, l'administration pourra remplacer la signature par toute procédure électronique garantissant l'authenticité et l'intégrité des données, sans être limitée aux seules signatures électroniques présentées dans ce guide. Loin de créer une insécurité juridique, cette formulation neutre permet aux administrations d'évoluer et de simplifier leurs procédures, en recourant aux nouveautés technologiques.

Et ces simplifications seront tant au bénéfice des usagers que des administrations elles-mêmes.

7. Bibliographie

Législation

- Règlement (UE) 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 et abrogeant la directive 1999/93/CE (« Règlement eIDAS »)
- Code civil, article 18
- Loi du 21 juillet 2016 mettant en œuvre et complétant le règlement (UE) 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 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 (« Digital Act »)
- Ordonnance du 13 février 2014 relative à la communication par voie électronique dans le cadre des relations avec les autorités publiques de la Région de Bruxelles-Capitale, M.B. du 5 mars 2014
- Ordonnance du 29 novembre 2018 sur les funérailles et sépultures, M.B. du 27 décembre 2018
- Circulaire du 27 mars 2014 relative à la communication par voie électronique dans le cadre des relations avec les autorités publiques de la Région de Bruxelles-Capitale, M.B. du 23 mai 2014

Sites internet intéressants

- Site de la Commission européenne : https://webgate.ec.europa.eu/tl-browser/#/
- Site du SPF économie : https://economie.fgov.be/fr/themes/line/commerce-electronique/signature-electronique-et

8. Contact

easy.brussels
Boulevard du Jardin Botanique 20
1000 Bruxelles
02 800 33 55
info@easy.brussels
easy.brussels