De elektronische handtekening

easy.brussels

Gids voor de Brusselse overheden

easy.brussels

Gewestelijke gids over de elektronische handtekening

Inhoudsopgave

1. Inleiding

Sinds 15 maart 2014 mogen Brusselse besturen via elektronische weg met burgers en ondernemingen communiceren. Deze communicatie is rechtsgeldig, zelfs in gevallen waar de regelgeving dit niet uitdrukkelijk bepaalt. Deze mogelijkheid werd hen geboden door de ordonnantie van 13 februari 2014 met betrekking tot de communicatie via elektronische weg in het kader van de relaties met de overheidsinstanties van het Brussels Hoofdstedelijk Gewest, die besturen toelaat hun procedures te dematerialiseren. Dit sluit aan bij het bredere proces van administratieve vereenvoudiging. Het brengt wel bepaalde vragen met zich mee. In deze gids zullen we ons echter beperken tot de specifieke kwestie van de elektronische handtekening.

Als een bestuur beslist over te stappen naar elektronische communicatie door bijvoorbeeld online formulieren aan te maken, is het niet de bedoeling dit formulier vervolgens af te drukken en het proces via papieren weg voort te zetten. Integendeel, als een bestuur de keuze maakt om een procedure te dematerialiseren, moet dit consequent worden doorgevoerd, van de indiening van de aanvraag, de ontvangst door het bestuur, de verwerking van de vergunningen tot de mededeling van de beslissing. Het zou niet logisch zijn dat een aanvrager een document ontvangt, dat vervolgens afdrukt, met de hand ondertekent en weer scant. Hetzelfde geldt voor het indienen van de aanvraag. Hoe kan de aanvrager het formulier ondertekenen nadat het online werd ingevuld? Door gebruik te maken van de elektronische handtekening.

Alvorens de elektronische handtekening te gebruiken, moeten er evenwel enkele vragen worden beantwoord, of het nu gaat om binnenkomende elektronische post of uitgaande post, de implementatie van de handtekening of de archivering. Deze gids zal trachten een antwoord te bieden op de eerste twee vragen die men zich moet stellen:

1) Mag ik de elektronische handtekening gebruiken?
2) Welke elektronische handtekening moet ik gebruiken[1]?

2. Toepassingsgebied en definitie

2.1. Toepassingsgebied

Deze gids is bedoeld voor de Brusselse overheden. De ordonnantie van 13 februari 2014, van toepassing op de overheden van het Brussels Hoofdstedelijk Gewest, definieert deze overheden als volgt:

a) het Brussels Hoofdstedelijk Gewest;
b) de publiekrechtelijke rechtspersonen die rechtstreeks of onrechtstreeks afhangen van het Brussels Hoofdstedelijk Gewest;
c) de gemeenten en de overige territoriale collectiviteiten, gesitueerd op het grondgebied van het tweetalig Brussels Hoofdstedelijk Gewest;
d) de entiteiten die, ongeacht hun vorm of aard:

[1] Ga rechtstreeks naar pagina 8 voor het gedeelte 'keuze van de handtekening'.

- zijn opgericht met het specifieke doel te voorzien in behoeften van algemeen belang;
- rechtspersoonlijkheid bezitten;
- en waarvan hetzij de activiteit in hoofdzaak wordt gefinancierd door de overheden of instellingen vermeld in a), b) of c), hetzij het beheer is onderworpen aan toezicht door deze overheden of instellingen, hetzij de leden van het bestuursorgaan, het leidinggevend orgaan of het toezichthoudend orgaan voor meer dan de helft door die overheden of instellingen zijn aangewezen;

e) de verenigingen opgericht door één of verschillende overheden bedoeld in a), b), c) of d).

2.2. Definitie en wettelijk kader

De eIDAS-verordening die in Belgisch recht werd omgezet door de wet van 21 juli 2016 (Digital Act), welke in boek XII "Recht van de elektronische economie" van het Wetboek van economisch recht een titel 2 heeft ingevoegd, luidende "Bepaalde regels in verband met het juridisch kader voor vertrouwensdiensten", definieert de elektronische handtekening als "*gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen* ". Een elektronische handtekening maakt het mogelijk na te gaan of een document werd gewijzigd (integriteit) en wie er de auteur van is (authenticatie).

Concreet is de elektronische handtekening een mechanisme dat:

- de **integriteit** van een elektronisch document garandeert;
- en de **authenticatie** van de auteur van de elektronische handtekening garandeert.

Deze zeer brede definitie verwijst naar meerdere handtekeningen, soms volledig elektronisch zoals elektronische handtekeningen via de identiteitskaart, maar ook gedeeltelijk elektronisch, zoals de gescande handgeschreven handtekeningen. Zo worden op basis van deze definitie ook biometrische (bijvoorbeeld stemherkenning, irisscans, vingerafdrukken) handtekeningen als elektronische handtekening beschouwd, net als eenvoudige kaartcodes (voornamelijk bankkaarten).

Deze handtekening bieden evenwel niet allemaal dezelfde voordelen of dezelfde mate van bescherming. Afhankelijk van de eisen waaraan ze voldoet, kan een elektronische handtekening als 'eenvoudig', 'geavanceerd' of 'gekwalificeerd' worden aangeduid.

2.3. Soorten handtekeningen

2.3.1. Enkele basisbegrippen

Alvorens de soorten elektronische handtekeningen te beschrijven, moeten enkele begrippen worden omschreven om de voordelen van de verschillende handtekeningen goed te kunnen begrijpen.

a. Authenticatie of identificatie

De bedoeling van authenticatie (of identificatie) is het bevestigen van de identificatie van een natuurlijke persoon of rechtspersoon, of van de oorsprong en integriteit van gegevens in elektronische vorm. Zo kan men een handtekening aan een welbepaalde persoon koppelen.

b. Integriteit

De integriteit van gegevens verwijst naar het feit dat gegevens tijdens de verwerking of overdracht ervan op geen enkele manier opzettelijk of per ongeluk gewijzigd of vernietigd worden. Het garanderen van de integriteit van gegevens veronderstelt dus dat men de bestemmeling verzekert dat een document niet werd gewijzigd nadat het werd ondertekend.

c. Onweerlegbaarheid

Het principe van onweerlegbaarheid (of non-discriminatie) houdt in dat de elektronische handtekening niet kan worden geweigerd door een rechter wegens het elektronische karakter ervan. Of ze nu gelijkgesteld is aan een handgeschreven handtekening of een eenvoudig begin van bewijs (zie verderop in de tekst), ze kan niet worden geweigerd.

d. Certificering

De certificering wordt geleverd door een geaccrediteerde dienstverlener[2] (In België vaak "certificerende derde" of "vertrouwensderde" genoemd) en voegt een kwaliteitsgarantie toe die enerzijds verband houdt met het toezicht op de middelen en processen die worden toegepast door de certificeringsautoriteit en anderzijds met de conformiteit van het middel voor het aanmaken van handtekeningen.

[2] De accreditatie van de dienstverleners moet gebeuren door een Belgische of Europese certificeringsorgaan. "*De dienstverlener die een gekwalificeerde dienst wenst aan te bieden is onderworpen aan een systeem van voorafgaande toestemming, en moet talrijke strikte voorwaarden in acht nemen (onder meer qua beveiliging), die in de eIDAS-Verordening worden gesteld. Die voorwaarden worden diepgaand en vooraf gecontroleerd door een geaccrediteerd auditorgaan, alsook door het toezichthoudende orgaan. Bovendien moet de dienstverlener om de twee jaar aan een audit worden onderworpen.*" (zie https://economie.fgov.be/sites/default/files/Files/Online/FAQ-vertrouwensdiensten.pdf).
De lijst van de in België geaccrediteerde dienstverleners kan worden geraadpleegd op de website van de FOD Economie en op de website van de Europese Commissie:
- https://economie.fgov.be/sites/default/files/Files/Online/Lijst-gekwalificeerde-dienstverlenersprestataires-vertrouwensdiensten-in-Belgie.pdf)
- https://webgate.ec.europa.eu/tl-browser/#/.

Als we dit vergelijken met het documentbeheer, dan handelt de certificerende derde als een notaris, die wordt aangesteld als openbaar ambtenaar. De rol van de notaris bestaat eruit de identiteit van de partijen na te gaan en of die met volledige kennis van zaken instemmen met de akte die voor hem verleden werd. De notaris is daarbij de getuige en staat garant voor de naleving van de vormen en de wil van de partijen. Net zoals deze rol de papieren akte authenticiteit verleent, maakt de certificerende derde de handtekening gekwalificeerd op basis van haar betrokkenheid in het ondertekeningsproces en door het controleren van de authenticatie van de partijen en van de integriteit van de documenten.

2.3.2. Eenvoudige elektronische handtekening

De eenvoudige, vereenvoudigde of gewone handtekening is de eerste soort elektronische handtekening die mogelijk is. Het kan gaan om het aankruisen van een vakje op een online document, de handtekening die handmatig wordt aangebracht op een scherm of een tablet (zoals wanneer men een pakje ontvangt bijvoorbeeld), of het aanbrengen van een gescande handgeschreven handtekening op een document.

De gescande handgeschreven handtekening wordt vaak bij administraties gebruikt. Maar hoewel deze handtekening zogenaamd elektronisch is omdat ze werd gescand, om vervolgens te worden aangebracht op een bepaald document, **beschikt ze slechts over één van de bovengenoemde eigenschappen**, in tegenstelling tot de andere soorten elektronische handtekeningen die hieronder aan bod komen.

De handgeschreven handtekening betreft slechts een afbeelding die wordt aangebracht op een document, en men kan aan de hand van deze eenvoudige handtekening niet op sluitende wijze de persoon identificeren die het document heeft ondertekend (aangezien iedereen die toegang heeft tot de scan deze handtekening kan gebruiken)[3], noch kan men zich ervan vergewissen of het document naderhand werd aangepast.

X	Identificatie
X	Integriteit
V	Onweerlegbaarheid
X	Certificering

2.3.3. Geavanceerde elektronische handtekening

De geavanceerde elektronische handtekening is er een waarbij technische verbanden worden aangebracht tussen de ondertekende gegevens, de handtekening en de ondertekenaar. Deze

[3] De gescande handgeschreven handtekening werd niettemin aanvaard, aangezien slechts een beperkt aantal personen er toegang toe had: zie C. trav. Brussel, 11 oktober 2013 en C. trav. Brussel, 14 februari 2014, R.D.T.I., 2014, pp. 115-121 (bron: LOSDYCK, B., "L'usage de signatures électroniques dans le cadre du Règlement eIDAS", pp.146-147).

technische verbanden moeten de integriteit van de gegevens garanderen, alsook de identificatie van de ondertekenaar en de onweerlegbaarheid.

Deze handtekening is volledig digitaal, wat inhoudt dat een "leesbare" boodschap met behulp van een wiskundig algoritme geheel of gedeeltelijk wordt omgevormd tot een versleutelde tekst.

Een elektronische handtekening is geavanceerd als ze voldoet aan de voorwaarden van artikel 26 van de eIDAS-verordening, te weten:

- zij is op unieke wijze aan de ondertekenaar verbonden;
- zij maakt het mogelijk de ondertekenaar te identificeren;
- zij komt tot stand met gegevens voor het aanmaken van elektronische handtekeningen die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitende controle kan gebruiken;
- zij is op zodanige wijze aan de daarmee ondertekende gegevens verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.

V	Identificatie
V	Integriteit
V	Onweerlegbaarheid
X	Certificering

Voorbeelden van geavanceerde elektronische handtekeningen zijn de biometrische handtekening gemaakt met een Wacom-tablet, een handtekening die gebruik maakt van de Nederlandse digitale identiteit iDIN, of een handtekening op basis van een verificatie van de identiteitspapieren van een persoon met behulp van een speciale app (Onfido, IDNow, Ubble, ...).

2.3.4. Gekwalificeerde elektronische handtekening

De gekwalificeerde elektronische handtekening is een *geavanceerde* elektronische handtekening (dus met de hierboven uiteengezette eigenschappen), gebaseerd op een gekwalificeerd certificaat en aangemaakt met behulp van een gekwalificeerd middel voor het aanmaken van handtekeningen.

Hoewel de eIDAS-verordening bepaalt dat een elektronische handtekening niet mag worden ontkend als een bewijsmiddel in gerechtelijke procedures louter op grond van het feit dat de handtekening elektronisch is (met inbegrip van een gescande handgeschreven handtekening dus), wordt enkel de *gekwalificeerde* handtekening juridisch gelijkgesteld aan een handgeschreven handtekening, met alle rechtsgevolgen die samenhangen met de handgeschreven handtekening. Deze gelijkstelling wordt uitdrukkelijk bepaald in het artikel 25 van de eIDAS-verordening.

Voor het gerecht kan een niet-gekwalificeerde elektronische handtekening makkelijker in vraag worden gesteld dan een gekwalificeerde elektronische handtekening, die een grotere - bijna onbetwistbare - juridische waarde zal hebben en gelijkgesteld wordt aan een "echte geschreven handtekening".

	V	Identificatie
	V	Integriteit
	V	Onweerlegbaarheid
+	V	**Certificering**

Het meest voorkomende voorbeeld van een gekwalificeerde elektronische handtekening is de handtekening met behulp van de identiteitskaart, net als een ondertekening van een pdf-document met Adobe Acrobat, of ook wel een handtekening via *Itsme*.

Opmerking: in sommige gevallen biedt de gekwalificeerde elektronische handtekening ook de functie van 'tijdstempel', waarbij aan een document een zekere datum (en zelfs een tijdstip) wordt toegekend. Dat is met name het geval voor de elektronische handtekening via Adobe Acrobat. Niettemin zijn de twee functies niet noodzakelijkerwijs met elkaar verbonden.

⇨ Het tijdstempel komt in punt 5.2 hieronder aan bod.

2.3.5. Tussentijdse conclusie

Er staan het bestuur dat zijn procedures wil dematerialiseren meerdere soorten elektronische handtekeningen ter beschikking, namelijk de eenvoudige elektronische handtekening, de geavanceerde elektronische handtekening of de gekwalificeerde elektronische handtekening. Zoals we net hebben gezien, bieden deze drie soorten handtekeningen niet allemaal hetzelfde beveiligingsniveau:

	Eenvoudige elektronische handtekening	Geavanceerde elektronische handtekening	Gekwalificeerde elektronische handtekening
Identificatie	**X**	**V**	**V**
Integriteit	**X**	**V**	**V**
Onweerlegbaarheid	**V**	**V**	**V**
Certificering	**X**	**X**	**V**

Hoewel ze niet allemaal dezelfde garanties bieden, kunnen al deze handtekeningen nochtans door de besturen worden gebruikt, afhankelijk van de context en vooral van de te ondertekenen documenten.

3. Gebruik van de elektronische handtekening

Nu we de verschillende soorten elektronische handtekeningen hebben beschreven, kunnen we bepalen welke soort in welk geval te gebruiken.

3.1. Voor- en nadelen van de gekwalificeerde elektronische handtekening

3.1.1. Voordelen

De Digital Act regelt het gebruik en de juridische gevolgen van de verleners van elektronische vertrouwensdiensten, waaronder de elektronische handtekening, en biedt een zekerheid met betrekking tot de juridische gevolgen die verband houden met het gebruik van de verleners van vertrouwensdiensten.

Concreet scheppen de Digital Act en de eIDAS-verordening een wettelijk vermoeden van conformiteit voor de gekwalificeerde elektronische vertrouwensdiensten, wat inhoudt dat hun gebruik, integriteit en authenticiteit niet in vraag kunnen worden gesteld. De gekwalificeerde vertrouwensdiensten werden grondig gecontroleerd en bieden een garantie op een **verhoogd vertrouwen** dat in de hele Europese Unie **juridisch wordt erkend**.

Een bijkomend voordeel van de gekwalificeerde elektronische handtekening is het feit dat ze de **bewijslast** verschuift. Als tegen een document dat werd ondertekend met een gekwalificeerde elektronische handtekening bezwaar wordt aangetekend, moet de indiener van dat bezwaar aantonen dat de handtekening niet geldig is. In het geval van een andersoortige elektronische handtekening moet de partij die het document heeft ondertekend aantonen dat de handtekening geldig is of dat het document niet werd gewijzigd.

3.1.2. Nadelen

De gekwalificeerde elektronische handtekening is de **enige handtekening** die wordt erkend als juridisch gelijkwaardig aan de handgeschreven handtekening, en biedt bovendien de grootste beveiliging, wat maakt dat men in de verleiding kan komen om deze te gebruiken voor alle te ondertekenen documenten. Dat is nochtans niet noodzakelijk, want hoewel deze soort handtekening vele voordelen biedt, brengt ze ook heel wat verplichtingen met zich mee.

Zoals hoger vermeld moet men, om een gekwalificeerde elektronische handtekening te gebruiken, immers een beroep doen op een gekwalificeerde dienstverlener. Maar uitsluitend de vertrouwensdienstverleners die zijn opgenomen in de officiële lijst van de FOD Economie, K.M.O., Middenstand en Energie, kunnen deze dienst verlenen. Dat beperkt dus de technische oplossingen die de besturen kunnen gebruiken. Deze oplossingen zullen bovendien betalend zijn. Elke aangebracht handtekening zal een niet-verwaarloosbare kostprijs met zich meebrengen.

Anderzijds kan de verplichting van de gekwalificeerde elektronische handtekening bepaalde personen in de problemen brengen. Denken we bijvoorbeeld aan personen die **zich aan de andere kant van de**

digitale kloof bevinden[4], die niet met digitale tools overweg kunnen, maar ook aan personen die niet over de materiële middelen beschikken om gebruik te maken van de gekwalificeerde elektronische handtekening. Om elektronisch te ondertekenen (met een gekwalificeerde elektronische handtekening) moet men immers beschikken over de nodige instrumenten, zoals een digitale kaartlezer of een identiteits-/verblijfskaart met chip. Maar niet iedereen beschikt over zulke instrumenten. Het verplichte gebruik van de gekwalificeerde elektronische handtekening zou bijgevolg moeilijkheden kunnen opleveren voor bepaalde personen en hen *de facto* van de procedure uitsluiten.

Nog een nadeel van het gebruik van een gekwalificeerde elektronische handtekening is de bewaring op lange termijn van deze handtekening, want certificaten verlopen immers na een bepaalde tijd, terwijl de ondertekende documenten soms langer moeten worden bewaard en de erop aangebrachte handtekening dus langer geldig moet zijn. Het zou nochtans mogelijk zijn aan te tonen dat de handtekening geldig was toen het document werd ondertekend door het document op gekwalificeerde wijze te archiveren zolang de certificaten nog geldig zijn.

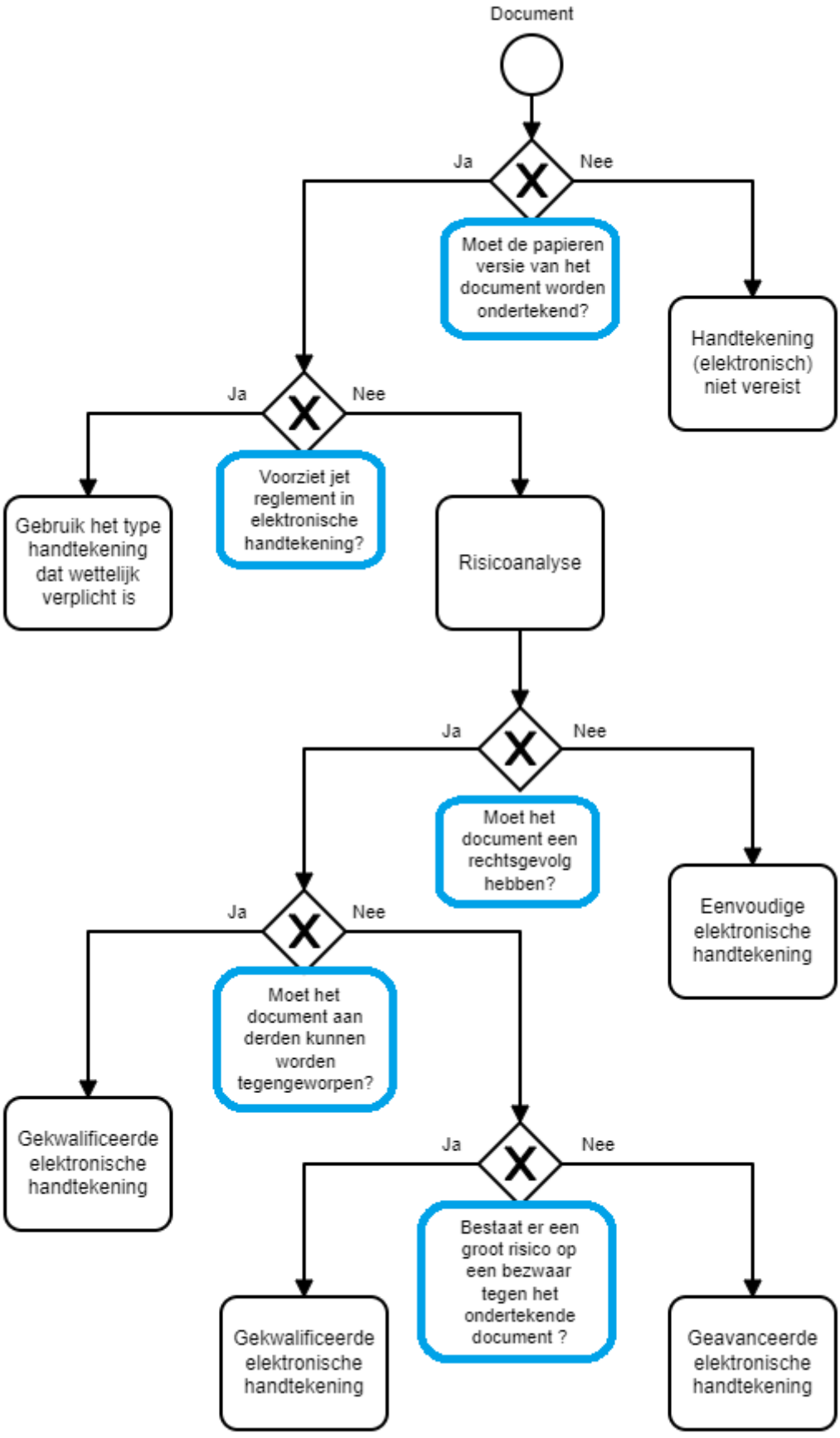
3.2. Keuze van het soort handtekening

Uiteindelijk zal de keuze van de aangewezen elektronische handtekening afhangen van de aard (en het belang) van het te ondertekenen document, en van een reeks vragen die moeten worden beantwoord. Deze vragen vormen wat we een risicoanalyse zullen noemen.

De beslisboom hieronder werd ontwikkeld om besturen te helpen bij hun keuze van de te gebruiken elektronische handtekening. De erin opgenomen vragen zullen onder de beslisboom in detail worden besproken.

[4] Er bestaan manieren om deze personen te helpen. Naast de middelen waarover de verschillende besturen beschikken kunnen de Openbare Computerruimten in meerdere Brusselse gemeenten worden gecontacteerd.

3.2.1. Beslisboom



3.2.2. Risicoanalyse

1) Is de ondertekening van het document vereist door een wet, een ordonnantie of een andere regelgevende tekst?

Als de ondertekening niet vereist is door de toepasselijke regelgeving, moet men zich afvragen of de ondertekening echt noodzakelijk is, of men de papieren dan wel de elektronische versie van het document moet ondertekenen. *Als* de papieren versie van het document niet wordt ondertekend, is er alvast helemaal geen reden om dat met de elektronische versie te doen.

Als daarentegen het papieren document wordt ondertekend, maar de handtekening slechts een symbolische waarde heeft[5], is het niet noodzakelijk een beroep te doen op de gekwalificeerde elektronische handtekening. Een eenvoudige of vereenvoudigde elektronische handtekening volstaat, zodra het onderzoek van het proces de noodzaak of het nut ervan bevestigt.

Als de ondertekening daarentegen wel vereist is door de toepasselijke regelgeving[6], moet men het document effectief ondertekenen en de analyse voortzetten om te bekijken welke handtekening moet worden gebruikt:

- Als de regelgeving het gebruik van een welbepaalde soort handtekening vereist, moet men dit soort handtekening bijgevolg gebruiken.
- Als de regelgeving niets vermeldt over het te gebruiken soort handtekening, verzoeken we u om een **risicoanalyse** uit te voeren en daarbij de volgende vragen te stellen.

2) Moet het ondertekende document een rechtsgevolg hebben?

Als het te ondertekenen document geen enkel rechtsgevolg heeft (bijvoorbeeld een informatieve brief) en het enige doel van de handtekening erin bestaat een duidelijke authenticiteit te verlenen aan het document, volstaat volgens ons een eenvoudige elektronische handtekening.

Als het te ondertekenen document daarentegen een rechtsgevolg heeft, zoals de toekenning van een premie of de creatie van een obligatie, bevelen wij een geavanceerde of gekwalificeerde elektronische handtekening aan. Dit heeft als voordeel dat de authenticiteit en integriteit van het document worden gewaarborgd. Er moet dan wel nog worden bepaald welke handtekening - geavanceerd of gekwalificeerd - moet worden gebruikt.

[5] In sommige gevallen verkiezen de bestemmelingen van de documenten een handtekening op het document, bijvoorbeeld wanneer een burger een informatieve brief ontvangt van een burgemeester, verwacht deze zonder twijfel de handtekening van de burgervader op de brief. Nochtans is het niet nodig daarvoor een gekwalificeerde elektronische handtekening te gebruiken. Een eenvoudige elektronische handtekening (met name de gescande kopie van de handtekening van de burgemeester) volstaat.

[6] De ordonnantie van 29 november 2018 op de begraafplaatsen en de lijkbezorging bijvoorbeeld bepaalt in artikel 40 dat "*De communicatie en waar nodig de betekening van de gegevens betreffende de verloven tot begraving en crematie voorzien door deze ordonnantie, kunnen vervangen worden door een door de Regering vastgestelde elektronische procedure die op een aantoonbare wijze de authenticiteit en de integriteit van de gegevens waarborgt*". Hoewel de ordonnantie geen soort handtekening in het bijzonder oplegt, sluit ze de facto de eenvoudige elektronische handtekening uit door waarborgen inzake authenticiteit en de integriteit op te leggen. Het is volgens ons aangewezen om een risicoanalyse uit te voeren om te bepalen of men gebruik moet maken van de geavanceerde dan wel de gekwalificeerde handtekening.

3) Moet het ondertekende document aan derden kunnen worden tegengeworpen?

Als het document aan derden moet kunnen worden tegengeworpen, raden wij het gebruik van een gekwalificeerde elektronische handtekening aan. Nemen we het voorbeeld van een besluit voor de toekenning van een vergunning aan een burger, die gevolgen heeft voor derden. In dat geval maakt het gebruik van de gekwalificeerde elektronische handtekening het mogelijk de bewijslast om te keren, want als een derde de geldigheid van de handtekening wenst te betwisten, moet die laatste daarvoor de nodige bewijzen aandragen.

Als het document niet aan derden moet kunnen worden tegengeworpen, en als het ondertekende document slechts een gevolg heeft voor de bestemmeling, dan zal de keuze inzake het gebruik van de gekwalificeerde dan wel de geavanceerde elektronische handtekening afhangen van het antwoord op de volgende vraag.

4) Bestaat er een groot risico op een bezwaar tegen het ondertekende document?

Uiteindelijk moet men bij de keuze van het soort handtekening in de eerste plaats rekening houden met de mogelijkheid van een **bezwaar**.

Als er een groot risico op een bezwaar tegen het besluit bestaat, moet de voorkeur naar de gekwalificeerde elektronische handtekening uitgaan.

Als er daarentegen een gering risico op bezwaar tegen het te ondertekenen document bestaat (een individueel gunstig besluit voor de bestemmeling en zonder gevolg voor derden bijvoorbeeld), is het niet vereist gebruik te maken van een gekwalificeerde elektronische handtekening - een geavanceerde elektronische handtekening volstaat.

Zoals hoger aangehaald is een van de belangrijkste verschillen tussen de gekwalificeerde en de geavanceerde elektronische handtekening dat de eerste een omkering van de bewijslast met zich meebrengt, omdat deze via een gekwalificeerde dienstverlener wordt geleverd. Als het risico op bezwaren gering is, lijkt de geavanceerde elektronische handtekening ons voldoende, maar als er toch sprake is van een bezwaar, volstaat het dat het bestuur de waarachtigheid van het betwiste document aantoont (bijvoorbeeld in het geval van een negatieve beslissing, door de verantwoordingsstukken voor de beslissing aan te dragen).

Uiteindelijk moet het bestuur beslissen om een beroep te doen op een gekwalificeerde of een geavanceerde elektronische handtekening[7], en daarbij de voordelen van de gekwalificeerde elektronische handtekening afwegen (omkering van de bewijslast) tegen de nadelen.

3.3. Voorbeeld uit de praktijk

We zullen een fictief voorbeeld bespreken, om de risicoanalyse die we net hebben gepresenteerd te illustreren

- Situatie: bestuur A is bevoegd voor het toekennen van een premie aan alle burgers die voldoen aan drie voorwaarden die in een ordonnantie worden bepaald. Zodra aan de voorwaarden werd

[7] De leidende instanties van elk bestuur zullen hun richtsnoeren ter zake moeten uitvaardigen.

voldaan, heeft de burger recht op een premie met een vast bedrag, zonder dat dit een gevolg heeft voor derden Een burger heeft een premieaanvraag ingediend en voldoet aan de toekenningsvoorwaarden. Welk soort elektronische handtekening gaat bestuur A gebruiken om de burger de toekenning van de premie mee te delen?

- Hypothese: voor het voorbeeld gaan we ervan uit dat de papieren versie van de toekenningsbeslissing werd ondertekend en dat de regelgeving niet uitdrukkelijk voorziet in een elektronische handtekening
- Oplossing: in de praktijk, aangezien de brief die kennis geeft van het toekenningsbesluit rechtsgevolgen heeft (de toekenning van een premie), en aangezien de brief geen gevolgen heeft voor derden, en aangezien het risico op bezwaren zo goed als onbestaande is, volstaat een **geavanceerde elektronische handtekening**.

3.4. Bijzondere gevallen

3.4.1. Authentieke akte

De authentieke akte onderscheidt zich om meerdere redenen van andere documenten. Een van die redenen is dat het instellen van een procedure wegens 'valsheid in geschrifte' de enige manier is om de inhoud van een authentieke akte te betwisten. Een tweede reden heeft te maken met de hoedanigheid van de persoon die voldoet aan de voorwaarden voor het ondertekenen van de akte (authenticiteit, integriteit) en de formele voorwaarden om de akte te passeren. De authentieke akte moet immers verplicht worden gepasseerd ten overstaan van of worden opgesteld door een 'openbaar ambtenaar'. Deze verplichting brengt een andere verplichting met zich mee: op basis van het Burgerlijk Wetboek mag in dit geval enkel de gekwalificeerde elektronische handtekening worden gebruikt.

Als een openbaar ambtenaar een authentieke akte op elektronische wijze wil ondertekenen, dient hij uitsluitende gebruik te maken van de gekwalificeerde elektronische handtekening, zoals hierboven werd uiteengezet.

Voorbeelden van authentieke akten zijn akten van de burgerlijke stand, notariële akten, akten opgesteld door een vrederechter, vaststellingen van deurwaarders, bepaalde akten van aankoopcomités (GOBF), enz.

Hierbij moet evenwel worden opgemerkt dat een document dat in originele versie moet bewaard worden, niet altijd een authentieke akte is. Bijvoorbeeld wetteksten die door ministers werden ondertekend, worden niet beschouwd als authentieke aktes. Dat neemt niet weg dat deze originele documenten een historische waarde hebben en niet zouden mogen worden vernietigd (zie het gedeelte over archivering).

3.4.2. Ondertekening van een reeks documenten

Met sommige technische oplossingen voor de elektronische handtekening kunnen meerdere documenten tegelijk worden ondertekend, wat ook wel een reeks documenten wordt genoemd.

Dat verandert evenwel niets aan de uiteenzetting hierboven over de keuze van het soort handtekening. Als na de risicoanalyse blijkt dat het document moet worden ondertekend met een geavanceerde elektronische handtekening, heeft het feit dat het deel uitmaakt van een reeks

documenten geen enkel gevolg voor de geldigheid van de handtekening. Hooguit zal men moeten nagaan of alle documenten van de reeks dezelfde soort handtekening vereisen.

Uiteindelijk is het belangrijk de geldigheid van de handtekening te garanderen voor elk individueel document.

4. Archivering

Het is niet de bedoeling van deze gids om richtlijnen te bieden over de archivering van de uiteenlopende door het bestuur opgemaakte of ontvangen documenten. Twee punten moeten nochtans worden aangestipt als het gaat om de archivering van elektronisch ondertekende documenten.

Het eerste heeft te maken met de geldigheidsduur van de identificatiemiddelen. Wat te doen als het gebruikte identificatiemiddel verloopt? De elektronische identiteitskaart is bijvoorbeeld beperkt geldig. Wat gebeurt er met documenten die werden ondertekend met een gekwalificeerde elektronische handtekening en de identiteitskaart van de ondertekenaar eens deze verlopen zijn? Als de handtekening geldig werd aangebracht op een tijdstip T, mag het feit dat de geldigheid van de identiteitskaart naderhand verstrijkt de handtekening niet in twijfel trekken.

In de praktijk zijn de certificerende instanties (vertrouwensdienstverleners) verplicht de certificaten of ten minste het bewijs van het certificaat (op het moment van de ondertekening) zonder beperking in de tijd te bewaren. Zelfs als de instantie haar activiteiten zou stopzetten, blijft de verplichting om de historiek van de certificaten te bewaren.

Een ander punt heeft betrekking op de archivering van het document zodra het werd ondertekend, door het bestuur. Bij de ondertekening van een document door een gekwalificeerde elektronische handtekening wordt er een unieke code aangemaakt in de metagegevens van het document. Deze code dient om de geldigheid van de handtekening op tijdstip T aan te tonen. Als het bestuur dit document archiveert, moet het zich ervan vergewissen dat deze unieke code tijdens de migratie niet wordt gewijzigd.

Als het bestuur gebruik maakt van een gekwalificeerde elektronische archivering, wordt verondersteld dat aan deze voorwaarde is voldaan. In het geval het bestuur een beroep zou doen op een andere archiveringsmethode, moet het er daarentegen voor zorgen dat de overdracht correct verloopt en dat de unieke code onveranderd blijft.

5. Naast de elektronische handtekening...

5.1. Elektronisch zegel

Het elektronische zegel biedt rechtspersonen (in het bijzonder ondernemingen) de mogelijkheid te beschikken over het equivalent van een elektronische handtekening. In de eIDAS-verordening wordt het elektronisch zegel gedefinieerd als volgt: "*gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die worden gebruikt om de oorsprong en integriteit daarvan te waarborgen*". Het gehoorzaamt dus aan dezelfde principes als de elektronische handtekening door nog meer te steunen op de waarborg inzake de oorsprong (de

rechtspersoon en niet de natuurlijke persoon die er gebruik van maakt) en de integriteit van het document.

Net als bij de handtekeningen bestaan er verschillende soorten elektronische zegels. Zo kan men gebruik maken van een eenvoudig, een geavanceerd of een gekwalificeerd elektronisch zegel.

Een elektronisch zegel is **geavanceerd** als het voldoet aan de voorwaarden van het artikel 36 van de eIDAS-verordening, te weten:

- het is op unieke wijze aan de aanmaker van het zegel verbonden;
- het maakt het mogelijk de aanmaker van het zegel te identificeren;
- het komt tot stand met gebruikmaking van gegevens voor het aanmaken van elektronische zegels die de aanmaker van het zegel met een hoog vertrouwensniveau onder zijn controle kan gebruiken voor het aanmaken van elektronische zegels;
- het is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.

V	Identificatie
V	Integriteit
V	Onweerlegbaarheid
X	Certificering

Een elektronisch zegel is **gekwalificeerd** als het voldoet aan de voorwaarden van artikel 36 (Eisen voor geavanceerde elektronische zegels), maar bovendien moet het aangemaakt zijn door een gekwalificeerd middel voor het aanmaken van elektronische zegels, dat gebaseerd is op een gekwalificeerd certificaat voor elektronische zegels (art. 3§27 van de eIDAS-verordening).

V	Identificatie
V	Integriteit
V	Onweerlegbaarheid
V	Certificering

Net als bij de elektronische handtekening is het zo dat een elektronisch zegel niet kan worden ontkend louter op grond van het feit dat het zegel elektronisch is, maar enkel voor het gekwalificeerde elektronische zegel geldt het vermoeden van integriteit van de gegevens en van juistheid van de oorsprong van de gegevens waaraan het gekwalificeerde elektronische zegel is verbonden (art. 35 van de eIDAS-verordening).

5.2. Tijdstempel

In sommige gevallen is het in de eerste plaats belangrijk om het document aan een bepaalde datum (en zelfs tijdstip) te koppelen in plaats van aan een persoon. Het tijdstempel kan van belang zijn in het geval van sancties, of bij een premieaanvraag (om aanvragers volgens volgorde van aanvraag te rangschikken). Welke oplossing krijgt nu de voorkeur?

In de eIDAS-verordening wordt het elektronische tijdstempel gedefinieerd als volgt: "*gegevens in elektronische vorm die andere gegevens in elektronische vorm verbinden aan een bepaald tijdstip en die bewijzen dat die laatstgenoemde gegevens op dat tijdstip bestonden*" (art. 3§33 van de eIDAS-verordening). Het elektronische tijdstempel maakt het mogelijk om:

- een document op precieze wijze te dateren;
- te certificeren dat op een precies ogenblik een gegeven bestond of dat een verrichting langs elektronische weg werd uitgevoerd (elektronische handtekening, elektronische aangetekende zending).

Een elektronische tijdstempel wordt **gekwalificeerd** genoemd indien het voldoet aan volgende eisen:

- het koppelt de datum en het tijdstip op zodanige wijze aan gegevens dat onmerkbare wijziging van de gegevens redelijkerwijs kan worden uitgesloten;
- het is gebaseerd op een nauwkeurige tijdsbron die aan de gecoördineerde universele tijd is gekoppeld;
- en het wordt ondertekend met behulp van een geavanceerde elektronische handtekening of verzegeld met een geavanceerd elektronisch zegel van de gekwalificeerde verlener van vertrouwensdiensten, of met behulp van een andere gelijkwaardige methode (art. 42 van de eIDAS-verordening).

Ten slotte geldt voor een gekwalificeerde elektronische tijdstempel het vermoeden van de juistheid van de aangegeven datum en het aangegeven tijdstip, en van de integriteit van de gegevens waaraan de datum en het tijdstip zijn gekoppeld (art. 41 van de eIDAS-verordening). Het document zal immers niet worden voorzien van een tijdsaanduiding op basis van de tijdsbron van de persoon die het document uitgeeft, want die kan worden gewijzigd, maar wel op basis van de tijdsbron van de verlener van vertrouwensdiensten, die aan de 'gecoördineerde universele tijd' gekoppeld is.

De gekwalificeerde elektronische handtekening en het gekwalificeerde elektronisch zegel bieden een tijdstempelfunctie. Maar zoals we hogerop in de tekst hebben gezien, kan deze oplossing heel wat verplichtingen met zich meebrengen, en zelfs kostelijk zijn. Het kan dus nuttig zijn om een beroep te doen op een andere technische oplossing. De website van de FOD Economie vermeldt de gekwalificeerde verleners van vertrouwensdiensten die specifiek het elektronische tijdstempel aanbieden (buiten gelijk welke ondertekening).

5.3. De elektronische aangetekende bezorging

De eIDAS-verordening omschrijft de dienst voor elektronisch aangetekende bezorging als een dienst die het mogelijk maakt gegevens via elektronische middelen tussen derden te verzenden en die bewijs verschaft ten aanzien van het hanteren van de verzonden gegevens, met inbegrip van bewijs van het

verzenden en ontvangen van de gegevens, en die de verzonden gegevens beschermt tegen het risico van verlies, diefstal, beschadiging of onbevoegde wijzigingen.

Net als bij de elektronische handtekening bestaat er een eenvoudige elektronische aangetekende bezorging en een gekwalificeerde elektronische aangetekende bezorging, waarvoor het vermoeden van integriteit geldt verbonden aan de gekwalificeerde verleners van vertrouwensdiensten.

6. Conclusie en aanbevelingen

Het is de bedoeling van deze gids de Brusselse besturen te helpen bij de overstap van papieren procedures naar elektronische procedures, en hen de nodige informatie aan te reiken voor het implementeren van de elektronische handtekening in hun processen. Zo hebben we de verschillende soorten elektronische handtekeningen beschreven en een beslisboom opgesteld die het bestuur kan gebruiken om te bepalen welke handtekening het moet gebruiken.

Nu is het aan de besturen om dit werk voort te zetten. Daartoe zouden we enkele aanbevelingen willen doen.

M.b.t. de keuze voor de elektronische handtekening:

Gebruik de elektronische handtekening alleen als ze echt nut heeft. Als het bijvoorbeeld de bedoeling is de inhoud van een document intern te valideren, is het gebruik van de elektronische handtekening niet noodzakelijk. Er bestaan andere manieren om een document te valideren, zoals een akkoord per e-mail. In bepaalde gevallen kan zo ook een login volstaan om de identiteit te bevestigen van de persoon die een beslissing goedkeurt. Dit is bijvoorbeeld het geval bij de verwerking van een bestelbon of de goedkeuring van een bevel tot mandateren.

Kortom, de elektronische handtekening zou moeten worden voorbehouden voor de gevallen waarbij ze uitdrukkelijk vereist wordt door de verordening, in het geval ze een echte meerwaarde biedt (zie de beslisboom).

M.b.t. het opstellen van de toepasselijke regelgeving:

De tweede aanbeveling die we zouden willen formuleren betreft niet het al dan niet opteren voor de elektronische handtekening op grond van de toepasselijke regelgeving, maar wel het opstellen van die regelgeving.

De technische oplossingen evolueren snel en relmatig zien nieuwe oplossingen het licht. Om een te starre regelgeving en een te grote afhankelijkheid van nieuwe technologieën te vermijden, raden we de besturen aan gebruik te maken van technologisch neutrale uitdrukkingen en termen bij het opstellen van hun regelgeving. Eerder dan het voorschrijven van een handtekening of zelfs een soort elektronische handtekening, raden we aan de gevolgen ervan (authenticiteit, integriteit, enz.) te vermelden.

Op die gronden kan het bestuur de handtekening vervangen door gelijk welke elektronische procedure die de authenticiteit en de integriteit van de gegevens waarborgt, zonder zich louter te moeten beperken tot de in deze gids besproken elektronische handtekeningen. Deze neutrale formulering zou

geen rechtsonzekerheid veroorzaken, maar de besturen de kans bieden hun procedures te doen evolueren en vereenvoudigen, met een beroep op de technologische vernieuwingen.

Deze vereenvoudiging zullen bovendien zowel de gebruikers als de besturen zelf ten goede komen.

7. Bibliografie

Wetgeving

- de EU-verordening nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (e-IDAS-verordening)
- Burgerlijk Wetboek, artikel 18
- de wet van 21 juli 2016 tot uitvoering en aanvulling van de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, houdende invoeging van titel 2 in boek XII "Recht van de elektronische economie" van het Wetboek van economisch recht, en houdende invoeging van de definities eigen aan titel 2 van boek XII en van de rechtshandhavingsbepalingen eigen aan titel 2 van boek XII, in de boeken I, XV en XVII van het Wetboek van economisch recht (Digital Act)
- Ordonnantie van 13 februari 2014 met betrekking tot de communicatie via elektronische weg in het kader van de relaties met de overheidsinstanties van het Brussels Hoofdstedelijk Gewest, B.S. van 5 maart 2014
- Ordonnantie van 29 november 2018 op de op de begraafplaatsen en de lijkbezorging, B.S. van 27 december 2018
- Rondzendbrief van 27 maart 2014 met betrekking tot de communicatie via elektronische weg in het kader van de relaties met de overheidsinstanties van het Brussels Hoofdstedelijk Gewest, B.S. van 5 23 mei 2014

Interessante websites

- Website van de Europese Commissie: https://webgate.ec.europa.eu/tl-browser/#/
- Website van de FOD Economie: https://economie.fgov.be/nl/themas/online/elektronische-handel/elektronische-handtekening-en

8. Contact

easy.brussels
Kruidtuinlaan 20
1000 Brussel
02 800 33 55
info@easy.brussels
easy.brussels