De elektronische (of numerieke) handtekening

Door Guy LOMBAERTS, Adviseur-generaal

1. Definities

Wat is de elektronische handtekening ?

De “elektronische handtekening” is een elektronisch mechanisme, gebaseerd op het gebruik van cryptografische functies, met als doel dezelfde functionaliteiten en garanties dan de handgeschreven handtekening te verschaffen. Dit concept wordt ook aangeduid door de term “digitale handtekening”[1] en/of “numerieke handtekening”.

In de Amerikaanse federale wet (de *Federal ESIGN Act*) worden (de) elektronische handtekeningen als volgt gedefinieerd: *“Een elektronisch geluid, symbool of proces dat verbonden is met of logisch gekoppeld is aan een contract of ander document, dat gebruikt wordt door een persoon met de intentie dat document te ondertekenen.”*

Volgens de tekst van de Belgische wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten (art. 2, 1°), is een elektronische handtekening *“een gegeven in elektronische vorm, vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authentificatie”*.

Die definitie die al van 2001 dateert, leunt nochtans zeer dicht aan bij de definitie die vermeld is in *de Verordening (EU) nr. 910/2014 van 23 juli 2014* over de elektronische identificatie en de vertrouwensdiensten, namelijk een elektronische handtekening[2] stemt overeen met *“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 ”*.

Die verschillende definities omvatten alle types van elektronische handtekening, zoals handgeschreven gescande handtekeningen, biometrische handtekeningen (stemherkenning, irisherkenning of herkenning van vingerafdrukken), digitale handtekeningen of nog de eenvoudige codes van elektronische bankkaarten of identiteitskaarten (PINcode).

Er bestaat inderdaad een grote verscheidenheid aan elektronische handtekeningen die zich van elkaar onderscheiden door de gebruikte technologie, hun veiligheidsniveau en hun juridische waarde.

Net als een handgeschreven handtekening voor een papieren document creëert het elektronisch ondertekenen van een elektronisch document dus in een eerste fase een verbintenis tussen het document en de ondertekenaar. Deze (zo) vastgestelde link kan verschillende doelen hebben, bepaald door het document zelf of door de context waarin de handtekening zich voordoet, bijvoorbeeld:

- identificeren van de auteur van een document
- aantonen dat de ondertekenaar instemt met de voorwaarden van het document
- aangeven dat het document is gelezen door de ondertekenaar
- enz.

1. Het begrip “digitale handtekening” is een anglicisme, het adjectief “digitaal” verwijst niet naar de vingers of de tenen, maar naar de getallen (“digit” in het Engels).
2. Gewoonlijk “Verordening eIDAS” genoemd.

Welke types van handtekening zijn juridisch bindend?

Afhankelijk van de aard van het document dat ondertekend wordt, wordt een elektronische handtekening in de vorm van een numeriek beeld van de handgeschreven handtekening van de ondertekenaar in de meeste landen als juridisch bindend beschouwd, ondanks de verschillen van land tot land en van rechtssysteem tot rechtssysteem.

Voor talrijke internationale reglementeringen (bv. de Europese eIDAS-verordening) en reglementeringen van intern recht[3] (in België, gewoonlijk Digital Act genoemd[4] waarin de Europese verordening wordt omgezet) worden voortaan eerder numerieke dan elektronische handtekeningen gebruikt, want een numerieke handtekening die de authenticiteit en de integriteit bevestigt[5], kan door de rechtbanken worden aanvaard. Ze heeft inderdaad een grotere bewijskracht dan de gewone gescande reproductie van de handgeschreven handtekening.

De keuze van het type van handtekening dat moet worden aangebracht, zal afhangen van het type document dat moet worden ondertekend en van het vereiste authenticiteitsniveau van het document. We komen hierop later terug.

2. Algemene context – het bewijsrecht (in de zin van het Burgerlijk Wetboek)

Het Belgisch bewijssysteem is strikt gereglementeerd: onder invloed van de Franse “Code civil” van 1804, de code Napoléon genoemd, was het geschrift op papieren drager waarop een handgeschreven handtekening werd aangebracht, gedurende bijna twee eeuwen de norm. Het is immers slechts op het einde van de 20e eeuw dat de wetgever dat bijna feitelijke monopolie heeft opgeheven, dat ontstaan was uit de voorrang van het geschrift (op papier) op bewijsvlak. Tot dan waren alleen de bewijsmiddelen die vermeld zijn in de artikelen 1341 en volgende van het Burgerlijk Wetboek toegelaten, meer bepaald zodra het voorwerp van de transactie een bepaald bedrag overschreed (375 EUR).

Het bestaan en de inhoud van de juridische akte moesten worden bewezen met een onderhandse akte, namelijk een origineel geschrift dat dient als onderhandse akte op voorwaarde dat de handtekening is erkend.

Omdat er noch voor het geschrift, noch voor de handtekening een wettelijke definitie bestond, was het moeilijk om een elektronisch document, een elektronische fax of brief als een correct geschrift te beschouwen in de zin van artikel 1341 van het Burgerlijk Wetboek.

3. In Luxemburg werd de wet van 14.08.2000 goedgekeurd “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”; in Frankrijk gaat het om de wet van 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. De benaming ‘Digital Act’ verwijst in feite naar de wet van 21.07.2016 waarvan de volledige titel luidt als volgt: ‘Wet tot uitvoering en aanvulling van de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23.07.2014 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’.
5. We merken in dit verband op dat de numerieke handtekening eigenschappen heeft die de klassieke handgeschreven handtekening niet bezit, omdat die laatste de integriteit van het ondertekende geenszins verzekert.

Naar een eengemaakte Europese regelgeving

Omdat België niet de enige Europese staat was die zich in die situatie bevond, heeft de Europese Commissie eind 1999 een Richtlijn 1999/93/EG aangenomen over de elektronische handtekening, die in verschillende fasen in het Belgisch recht is omgezet.

De eerste fase bestond uit een wijziging van het begrip "handtekening" dat is opgenomen in artikel 1322 van het Burgerlijk Wetboek en uit de invoering in ons bewijsrecht van een "functionele" definitie van de handtekening, dat wil zeggen een definitie met betrekking tot de functies die de handtekening moet vervullen, ongeacht de drager ervan (cf. wet van 20.10.2000[6]).

Vanaf toen werd een handtekening ook "een geheel van elektronische gegevens dat aan een bepaalde persoon kan worden toegerekend en het behoud van de integriteit van de inhoud van de akte aantoont".

Wat de toelaatbaarheid in het bewijsrecht betreft, kon de rechter een elektronische handtekening vanaf dan niet meer verwerpen louter op grond van het feit dat de handtekening elektronisch was, maar hij was nog niet verplicht om daaraan "bewijskracht" te verlenen. Het is echter zo dat de rechter een elektronisch document slechts in aanmerking kan nemen als het "bewijskracht" heeft.

De tweede fase was dus bedoeld om aan bepaalde elektronische handtekeningen bewijskracht te geven. Dat gebeurde door de goedkeuring van de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten (B.S. 29.09.2001).

Die wet kende een duidelijk juridisch statuut toe aan twee types van elektronische handtekening:

- de "gewone" elektronische handtekening die gedefinieerd wordt als "een gegeven in elektronische vorm, vastgehecht aan of logisch geassocieerd met andere elektronische gegevens en die wordt gebruikt als middel voor authentificatie". Dat type van handtekening treft men dagelijks aan in allerlei technologieën (geheime codes, symmetrische of asymmetrische cryptografie, biometrische handtekening, ...)

- de "geavanceerde" elektronische handtekening die gedefinieerd wordt als een elektronische handtekening die voldoet aan de volgende eisen:

    - zij is op unieke wijze aan de ondertekenaar verbonden
    - zij maakt het mogelijk de ondertekenaar te identificeren
    - zij wordt aangemaakt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden
    - zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft, verbonden dat elke latere wijziging van de gegevens kan worden opgespoord.

Die laatste methode had een groot voordeel: mits enkele voorwaarden worden nageleefd, verwerft ze bewijskracht en kan ze zonder meer helemaal worden gelijkgesteld met een handgeschreven handtekening. Wat waren die voorwaarden? De geavanceerde elektronische handtekening moet gebaseerd zijn op een gekwalificeerd certificaat en moet worden aangemaakt met een veilig middel voor het aanmaken van elektronische handtekeningen, zoals beschreven wordt in bijlage III van de wet van 9 juli 2001.

Wat "e-government" betreft, zijn de wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure en de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten hoofdzakelijk van toepassing op de relaties tussen de burgers en de overheid, via Internet, en in het bijzonder op de elektronische handtekening aangebracht met behulp van de elektronische identiteitskaart.

6. Wet tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure (B.S. 22.12.2000).

Vervolgens werd bij wet van 24 februari 2003 betreffende de modernisering van het beheer van de sociale zekerheid (BS 02.04.2003) het gebruik van de elektronische handtekening uitgebreid tot de elektronische communicatie tussen ondernemingen en de federale overheid; in artikel 4/1 van deze wet wordt gepreciseerd: *"Een handtekening aangebracht met behulp van een elektronische identiteitskaart (e-ID) wordt gelijkgesteld met een handgeschreven handtekening "*.

De Digital Act van 2016 heeft bij ons voor een beslissende ommekeer gezorgd.

Zo komt men bij de nieuwe Verordening (EU) nr. 910/2014 van 23 juli 2014 over de elektronische identificatie en de vertrouwensdiensten voor elektronische transacties in de interne markt (en tot intrekking van Richtlijn 1999/93/EG) die in werking is getreden op 1 juli 2016. Artikel 25 van de verordening stelt: *"Het rechtsgevolg van een elektronische handtekening en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures mogen niet worden ontkend louter op grond van het feit dat de handtekening elektronisch is of niet aan de eisen voor gekwalificeerde elektronische handtekeningen voldoet."*

Een gekwalificeerde elektronische handtekening heeft hetzelfde rechtsgevolg als een handgeschreven handtekening ".

Zoals hierboven is gezegd, werd die Europese verordening omgezet in Belgisch intern recht bij de wet van 21 juli 2016, de zogenaamde 'Digital Act' (BS 28.09.2016) die een reglementair kader schept voor de digitale economie die in volle ontwikkeling is, en voor de digitalisering van de contacten tussen burgers en ondernemingen aan de ene kant en de overheid aan de andere kant.

Bij de wet van 21 juli 2016 wordt een titel 2 "Bepaalde regels in verband met het juridisch kader voor vertrouwensdiensten" ingevoegd in het boek XII "Recht van de elektronische economie" van het Wetboek van economisch recht[7]. Hoewel een Europese verordening technisch gezien geen omzetting in nationaal recht vereist, wat wel het geval is bij een richtlijn, is het toch zo dat hoofdstuk III van de eIDAS-verordening over de "vertrouwensdiensten" een wetgevende tussenkomst op nationaal niveau noodzakelijk maakt om te zorgen voor de uitvoering ervan. Zo bepaalt de wetgever op precieze wijze de toepasselijke sancties in geval van niet-naleving van de bepalingen van de verordening en van de Belgische wet in verband met de hiervoor genoemde vertrouwensdiensten.

De Belgische wetgever heeft ook een volledig en samenhangend geheel van regels vastgelegd die als doel hebben het aanbod en het gebruik van elektronische archiveringsdiensten juridisch te omkaderen. Als men voor het sluiten, het overdragen en het bewaren van een juridische akte een elektronische procedure overweegt, lijkt het inderdaad belangrijk om voor al deze procedurefasen in een juridisch kader te voorzien, ook voor de laatste fase, die bestaat uit de archivering van de akte, en niet alleen de handtekening, datering en verzending ervan.

De Belgische regels sluiten aan bij de doelstellingen en de gedachtegang van de eIDAS-verordening. Ze nemen dezelfde principes over als vastgesteld door deze verordening voor de andere vertrouwensdiensten (elektronische handtekening, zegel, datumstempel, aangetekende zending). Zij beogen om zowel de elektronische archivering van origineel elektronische documenten als de elektronische archivering van documenten op papier (in het kader van het digitaliseren/inscannen) te omvatten.

7. Zie de Europese verordening nr. 910/2014 van 23.07.2014 over de elektronische identificatie en de vertrouwensdiensten, FOD Economie December 2016.

Naast het oorspronkelijke stelsel in verband met de elektronische archivering legt de Belgische wet ook bepalingen vast over hybride aangetekende zendingen, de intrekking, schorsing en het verval van gekwalificeerde certificaten van elektronische handtekening en van elektronisch zegel, de vertrouwende partij van een gekwalificeerde elektronische handtekening of een gekwalificeerd elektronisch zegel, de stopzetting van de activiteiten van een gekwalificeerde vertrouwensdienstverlener die een of meer gekwalificeerde vertrouwensdiensten verleent, alsook de mogelijkheid een natuurlijke persoon te identificeren die zich schuilhoudt achter een pseudoniem of een elektronisch zegel.

De beoogde bepalingen streven duidelijk naar een evenwicht tussen soepelheid en veiligheid. Naar het voorbeeld van het stelsel dat al van toepassing is op de andere vertrouwensdiensten in het kader van de verordening 910/2014, wordt het juridisch kader over elektronische archivering gezien als een “juridische gereedschapskist” die de gebruikers toelaat om een beroep te doen op deze dienst om hun risico’s te beheren, voornamelijk voor gegevens of documenten die juridische waarde bezitten. Met het oog hierop wordt in een aantal vermoedens voorzien ten voordele van de diensten van elektronische archivering die in de zin van de wet als “gekwalificeerd” worden beschouwd, alsook voor andere gekwalificeerde vertrouwensdiensten in de zin van de verordening.

Bij de wet van 21 juli 2016 worden ook de voornoemde wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten en het Koninklijk Besluit van 6 december 2002 houdende organisatie van de controle en de accreditatie van de certificatiedienstverleners die gekwalificeerde certificaten afleveren, opgeheven.

Tot slot is de laatste evolutie in het domein van de elektronische akten de uitbreiding van de elektronische handtekening tot de authentieke akten, dat wil zeggen de akten die opgesteld worden door openbare ambtenaren (zoals notarissen, ambtenaren van de burgerlijke stand, magistraten of gerechtsdeurwaarders) die in de hoogste rang staan wat het schriftelijke bewijs betreft.

Artikel 1317 van het Burgerlijk Wetboek stelt[8] dat voor de authentieke akten die door een openbaar ambtenaar in gedematerialiseerde vorm zijn opgemaakt, verleden of betekend, enkel een gekwalificeerde elektronische handtekening, bedoeld in artikel 3.12. van de verordening (eIDAS) 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, voldoet aan de voorwaarden van een handtekening.

3. De elektronische of numerieke handtekening zet in op betrouwbaarheid in de dematerialisatieprojecten

De elektronische handtekening is vandaag het sleutelelement van de lopende dematerialisatiefase. Voor een welgeslaagd dematerialiseringsproces mogen de overheidsinstellingen zich niet afzijdig houden op het vlak van de numerieke handtekening. Arbeidsovereenkomsten en andere, actieve huurcontracten, medische dossiers... Voor talrijke gedematerialiseerde documenten met een grote juridische waarde is een betrouwbare handtekening vereist.

Vergeleken met de papieren versie is de tijdwinst niet onbelangrijk: de verwerking van een document, vanaf de aanmaak tot de ondertekening ervan, neemt in plaats van verscheidene dagen minder dan één dag in beslag. Men heeft dat tijdens het proefproject dat het RIZIV in 2017 heeft gestart voor de numerieke handtekening van de nieuwe telewerkcontracten vastgesteld.

8. Zie art. 315, 1° van de wet van 06.07.2017 houdende vereenvoudiging, harmonisering, informatisering en modernisering van bepalingen van burgerlijkrecht en van burgerlijk procesrecht alsook van het notariaat, en houdende diverse bepalingen inzake justitie (B.S. 24.07.2017).

De elektronische handtekening zorgt bovendien voor een reëel vertrouwen in de numerieke uitwisselingen tussen het RIZIV en zijn externe partners (bv. de zorgverleners die tegemoetkomingsaanvragen kunnen indienen met behulp van intelligente formulieren of de gegevens kunnen wijzigen in hun persoonlijk dossier), de andere instellingen of nog de leveranciers (geïnformatiseerde procedures voor overheidsopdrachten).

Handgeschreven handtekening versus numerieke handtekening

Sinds vele jaren wordt de elektronische handtekening beschouwd als een equivalent van de handgeschreven handtekening. Ze hebben namelijk juist dezelfde wettelijke waarde.

De numerieke handtekening die vandaag wordt gedefinieerd als een numeriek mechanisme dat gebaseerd is op cryptografietechnieken, is bedoeld om aan een derde te bewijzen dat een elektronisch document goedgekeurd werd door een geïdentificeerde persoon.

Zoals dat het geval is voor de handgeschreven handtekening, kan aan de hand van de numerieke handtekening de auteur van het document zeer gemakkelijk worden geïdentificeerd. Bovendien wordt hier ook de integriteit van het document verzekerd. Door het aanbrengen van een numerieke handtekening garandeert de instelling dat het document niet gewijzigd werd na de handtekening.

Daarom wordt de numerieke handtekening vandaag beschouwd als betrouwbaarder dan een handgeschreven handtekening, omdat ze niet alleen de identiteit van de ondertekenaar verzekert, maar ook de integriteit van het document.

De numerieke handtekening bij het RIZIV

Het dematerialiseringsproces dat bij het RIZIV aan de gang is, verloopt via een steeds meer doorgedreven gebruik van de elektronische en/of numerieke handtekening. In de numerieke wereld moeten, zoals dat het geval is in de niet-gedematerialiseerde bedrijfsprocessen, niet alle originele documenten ondertekend worden, verre van.

Alleen wanneer de organisatie of een persoon die tot die organisatie behoort en die een numeriek stuk heeft aangemaakt, (immers) wil bewijzen dat hij/zij wel degelijk de auteur van dat stuk is, dat het representatief is voor zijn /haar wil, dat het stuk wel degelijk door hem/haar gecreëerd is en dat hij/zij sinds de aanmaak ervan daarin niets heeft veranderd, dat heeft hij/zij geen andere keuze dan een numerieke handtekening voor dat stuk te gebruiken.

De numerieke handtekening is dus het middel voor die organisatie of die persoon om te bewijzen dat zij/hij wel degelijk de enige aanmaker is van een numeriek bestand, dat aldus niet kan worden vervalst.

In een eerste fase van de integratie van de numerieke handtekening in onze processen moet dus een globaal ondertekeningsbeleid worden vastgelegd (Signature policy).

Een efficiënt numeriek ondertekeningsbeleid gaat gepaard met expliciete richtlijnen:

- types van documenten die compatibel zijn met de numerieke handtekening
- best practices
- informatie die in de verschillende types van documenten moet worden opgenomen.

Op het niveau van het RIZIV moeten de belangrijkste criteria aan de hand waarvan de verschillende types van documenten kunnen worden bepaald waarvoor een numerieke handtekening kan worden gebruikt, gelinkt worden aan het “bedrijfsrisico”, dat wil zeggen aan de identificatie van de gevolgen op het vlak van verantwoordelijkheden, financiën, imago, potentiële nadelen voor de beoogde geadresseerden.

Waarom ondertekenen?	Voor wie ondertekenen?	Welke waarde heeft mijn handtekening?
Een handtekening dient om te bewijzen wie aan de oorsprong ligt van een numerieke informatie en die handtekening is slechts verplicht wanneer het een risico inhoudt als men niet over dat bewijs beschikt.	Een handtekening dient hoofdzakelijk de behoeften van de "geadresseerden" die de naam moeten kennen van de persoon die de numerieke handtekening heeft aangebracht of eenvoudigweg van de organisatie die de numerieke informatie heeft verstrekt.	Een handtekening dient om een juridische waarde toe te kennen aan mijn numerieke informatie, in geval van een latere betwisting.

Zoals u in deze tabel kunt vaststellen, dient de handtekening hoofdzakelijk om de behoeften van de geadresseerden te vervullen die met zekerheid de herkomst van het numerieke document moeten kunnen achterhalen en/of om een juridische waarde toe te kennen aan het numeriek document in geval van een latere betwisting.

Welke types van documenten zijn daarbij betrokken?

Het gaat hier voornamelijk om alle documenten die tussen het RIZIV en derden (sociaal verzekerden, V.I., gerechtelijke overheden,...) moeten worden uitgewisseld en die als zodanig de handtekening van de overheid vereisen.

> Bijvoorbeeld: krachtens artikel 181 van de GVU-wet vertegenwoordigt de administrateur-generaal het Instituut in de gerechtelijke en buitengerechtelijke handelingen en treedt hij rechtsgeldig op namens en voor rekening van het Instituut. Ingeval de administrateur-generaal verhinderd is, worden zijn bevoegdheden uitgeoefend door de adjunct-administrateur-generaal en ingeval deze verhinderd is door een door het Algemeen comité aangewezen ambtenaar van het Instituut.

Voor dat type van officiële documenten moet het bewijs worden geleverd dat ze wel degelijk afkomstig zijn van een geïdentificeerde en gemachtigde persoon (de administrateur-generaal van het RIZIV of zijn vervanger als hij verhinderd is) en dat de inhoud ervan ongewijzigd werd overgedragen. In dat geval is een geavanceerde numerieke handtekening vereist.

De overgrote meerderheid van de poststukken die elke dag op papier, met hoofding van het RIZIV, worden verzonden en waarvoor de geadresseerden alleen moeten weten dat ze afkomstig zijn van het RIZIV, zou van een numerieke handtekening (gescande handtekening) of zelfs van een elektronisch zegel kunnen worden voorzien[9], zoals dat bepaald is in de wet van 21 juli 2016.

Naast het feit dat de gekwalificeerde handtekening slechts van belang is wanneer de post elektronisch wordt verstuurd naar de geadresseerde, mag men niet vergeten dat die geadresseerde de elektronische handtekening moet kunnen 'lezen' (= ontcijferen) (men gaat ervan uit dat hij over software beschikt die deze functie ondersteunt)!

We herinneren er bovendien aan dat behoudens andersluidende wettelijke bepalingen en ook al zijn de openbare overheden geneigd om de voorkeur te geven aan de elektronische uitwisselingen, niemand verplicht kan worden om een juridische akte langs elektronische weg te stellen. Zo ook kan niemand verplicht worden om procedurele handelingen langs elektronische weg te stellen of documenten betreffende die procedurele handelingen langs elektronische weg te ontvangen[10].

9. Opmerking: wat is het verschil tussen een elektronische handtekening en een elektronisch zegel? Het zegel identificeert een rechtspersoon terwijl de handtekening de natuurlijke persoon identificeert.
10. Art. XII., 25, § 1 van het Wetboek van economisch recht en art. 4 van de wet van 10.07.2006 betreffende de elektronische procesvoering.

Vandaag de dag kan dat zeker overwogen worden voor de uitwisselingen tussen de openbare of samenwerkende instellingen (bv. de V.I.'s) en op termijn voor de privépersonen: om technische en juridische redenen die verband houden met de bescherming van de persoonlijke levenssfeer, zou het riskant zijn om een beslissing met persoonlijke, zelfs medische gegevens naar een privépersoon te sturen via een niet-beveiligde privémailbox. Er worden momenteel oplossingen bestudeerd (onder meer het gebruik van de eBox of de eHealthbox).

Tot slot is het ook nuttig om mee te delen dat de gebruiksvoorwaarden voor de 'gewone', namelijk de gescande handtekening, al voor de hoven en rechtbanken zijn behandeld. Degenen die daarin geïnteresseerd zijn, kunnen een analyse van de rechtspraak raadplegen[11] waarin tot slot de raad die aan onze informatici is gegeven, is opgenomen, namelijk: "(…) *(vertaling) erop toezien dat er technische mechanismen worden gehanteerd aan de hand waarvan de ondertekenaar van het document en zijn toetreding tot de inhoud van de akte met zekerheid kunnen worden geïdentificeerd, alsook een middel waarmee het behoud van de integriteit van het ondertekende document kan worden bewezen. Om de rechter te overtuigen zullen die instellingen hem bijvoorbeeld een goede documentering van het digitaliserings-, bewarings- en eventueel elektronisch dateringsproces van de elektronisch aangemaakte documenten moeten voorleggen"*.

Tot slot hangt de keuze van een bepaald type van handtekening af van het gebruik dat men van die numerieke handtekening wil maken:

- de "gewone" elektronische handtekening volstaat voor een toepassing die geen hoge beveiliging vereist. Zo kan een handgeschreven gescande handtekening zeer goed worden gebruikt voor alle gewone poststukken
- de "geavanceerde" numerieke handtekening zij moet op unieke wijze aan de ondertekenaar verbonden zijn, de identificatie van de ondertekenaar mogelijk maken, worden aangemaakt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden en op zodanige wijze aan de gegevens waarop zij betrekking hebben, zijn verbonden dat elke latere wijziging van de gegevens kan worden opgespoord
- de "gekwalificeerde" numerieke handtekening: dat is een "geavanceerde" elektronische handtekening die gebaseerd is op een gekwalificeerd certificaat en die moet worden aangemaakt met een veilig middel voor het aanmaken van elektronische handtekeningen, zoals bepaald is in de wet van 21 juli 2016.

De gekwalificeerde numerieke handtekening biedt het hoogste veiligheidsniveau dat momenteel op Europees niveau is vastgelegd[12].

Met E-Signing zal de numerieke handtekening geleidelijk worden geïntegreerd in de processen van het RIZIV in het kader van de nieuwe versie van IOC (In and Outbound Communication) die onze toepassingen voor dossierbeheer ondersteunt.

Op technisch vlak zouden drie types van elektronische handtekening in IOC V2 vanaf 2018 beschikbaar moeten zijn:

1. de gekwalificeerde elektronische handtekening (QES) die als het equivalent van de handgeschreven handtekening wordt beschouwd. De IC-dienst zal een QES-oplossing creëren die zal losstaan van het proces van uitgaande post. Om een document met een handtekening van het type QES te ondertekenen, zal de ondertekenaar voor elk document in het algemeen de volgende acties moeten ondernemen:

- zich connecteren met de toepassing en het te ondertekenen document selecteren
- het proces voor elektronische ondertekening vanuit die toepassing starten

11. Zie "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. Ook de Duitse wetgever heeft beslist om die drie concepten van elektronische handtekening te erkennen in de "Signaturgesetz": de gewone elektronische handtekening, de geavanceerde elektronische handtekening en de gekwalificeerde elektronische handtekening.

- de visualiseringsparameters kiezen:
  - image-based handwritten signature
  - full name
  - timestamp
  - eID Photo
  - eID Photo watermarked
  - enz.
- zich aanmelden met zijn eID + pincode
- het ondertekende document ontvangen.

2. het gekwalificeerd elektronisch zegel (eSeal) waarvan het RIZIV dat door de administrateur-generaal, Jo De Cock, wordt vertegenwoordigd, de gerechtigde rechtspersoon zou zijn. Dat type van handtekening zal worden geïntegreerd in het proces van de uitgaande post en zou geschikter zijn voor de ondertekening van grote volumes. Bovendien zal het in de oplossing die voorgesteld wordt in het project IOC V2, mogelijk zijn om de gewone handtekening te combineren met het elektronisch zegel of de gekwalificeerde handtekening (zie de visualiseringsparameters);

3. bij de gewone elektronische handtekening (SES) wordt gebruik gemaakt van het beeld van de handgeschreven handtekening om de uitgaande documenten of post te ondertekenen. Voor dat type van handtekening wordt de identiteit van de ondertekenaar helemaal niet gecontroleerd.

Het type van handtekening dat voor een bepaald document moet worden gebruikt, zal door de business (niet door IOC) moeten worden bepaald. Zoals hierboven is gezegd (zie tabel op p. 7) zal men zich voor elk te ondertekenen document moeten afvragen of de handtekening als individu (QES) of als entiteit (eSeal) wordt aangebracht en hoe groot de te ondertekenen volumes zullen zijn. Afhankelijk van het gekozen type van elektronische handtekening zal de gebruiker via zijn toepassing een beroep doen op de QES-dienst (gekwalificeerde elektronische handtekening) of de eSeal- en SES-oplossingen die geïntegreerd zijn in het systeem IOC message broker.

Bronnen en bibliografie

PUBLICATIES

- 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.

INTERNETBRONNEN

- De Europese verordening nr. 910/2014 van 23 juli 2014 over de elektronische identificatie en de vertrouwensdiensten, FOD Economie - December 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.