Elektronische handtekeningen: juridische waarde en praktisch gebruik

1 Inleiding

Juridische grondslag:
- ⇒ Europese Richtlijn 1999/93/EG;
- ⇒ Wet elektronische handtekening (2003) – aanpassingswet voor Burgerlijk Wetboek en Telecommunicatiewet (civiel recht);
- ⇒ Besluit elektronische handtekeningen (2003);
- ⇒ Wet elektronisch bestuurlijk verkeer (2004) – bestuursrecht.

Verschillende vormen – vorm is afhankelijk van de toepassing:
- ⇒ gewone vorm;
- ⇒ geavanceerde vorm;
- ⇒ gekwalificeerde vorm.

Bij keuze voor bepaalde vorm moeten volgende vragen worden gesteld:
1. kan een bepaalde vorm worden opgevat als elektronische handtekening - voldoet de methode aan de definities van de Europese Richtlijn en de Wet elektronische handtekening?
2. voldoet een bepaalde vorm aan de functionele criteria: kan deze vorm daadwerkelijk de vereiste waarborgen bieden om binnen wettelijk kader als elektronische handtekening te dienen?
3. is een gebruikte methode voldoende betrouwbaar voor het doel en de omstandigheden van het geval?

---

2 Juridisch kader: de Richtlijn en de implementatie

Bij het gebruik van een elektronische handtekening moeten de volgende 2 juridische vragen worden beantwoord:
1. is de gebruikte ondertekening een vorm van elektronische handtekening?
2. kan deze vorm in dit geval worden gelijkgesteld met een conventionele handtekening?

Bij de eerste vraag moet de vorm worden getoetst aan de definitie in art. 3:15a lid 4 BW.
Voor de beoordeling van de tweede vraag moet de vorm functioneren als een conventionele handtekening (dit zijn functionele eisen) en moet de vorm voldoende betrouwbaar zijn voor het doel en de omstandigheden van het geval (dit zijn contextuele factoren).

Definitie elektronische handtekening (art. 3:15a lid 4 BW): Een handtekening die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie.

Deze definitie bestaat uit de componenten:
1. elektronische gegevens
2. die worden gebruikt als middel voor authentificatie
3. die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens.

Toelichting:
1) er is geen nader voorschrift gegeven voor de inhoud van de informatie of het formaat;
2) de term authentificatie is niet uitgewerkt;
3) de elektronische handtekening moet aan het ondertekende zijn verbonden.

De gewone elektronische handtekening
Voor deze vorm zijn vele technische mogelijkheden beschikbaar: een ingescande handtekening, een PIN-code of een naam onder een email.

Vooral in de publieke sector is behoefte aan een laagdrempelige techniek waarover iedere burger eenvoudig en goedkoop kan beschikken voor het indienen van aanvragen, bezwaarschriften en klaagschriften. DigiD kan hierbij zinvol worden toegepast.

Buiten het bestuurlijk verkeer tussen overheid en burgers is ook een bredere toepassing mogelijk in situaties waarin een bestaande relatie tussen de verzender en de ontvanger bestaat. Denk hierbij aan commerciële webdiensten (bol.com), aangifte inkomstenbelasting en bancaire diensten.

De gewone elektronische handtekening leunt meer op de context dan de geavanceerde en de gekwalificeerde vorm waarbij de authentificatie vooral door de ondertekeningtechniek wordt verzorgd.

Hierbij is het risico van fraude een factor. De risico's bij een false positive (een handtekening die onterecht als betrouwbaar wordt gezien) moeten laag zijn om het gebruik van een gewonen elektronische handtekening te kunnen verantwoorden.

Een andere factor bij deze keuze is dat de verificatie van de authentificatie direct kan volgen op ontvangst van het ondertekende. Hierin schuilt het risico van onvoldoende duurzaamheid: omdat de elektronische handtekening meer leunt op contextuele informatie ontstaat het risico dat niet alle informatie nodig voor authentificatie duurzaam bewaard kan worden. Denk hierbij aan een cliëntdossier.

De belangrijkste factor voor het gebruik van deze vorm wordt gevormd door de kosten. In een situatie waarin partijen elkaar kennen en waarin de ontvanger hecht aan laagdrempelige communicatie heeft een goedkope ondertekening een groot voordeel. Een burger zal geen kosten willen maken om digitaal met de overheid te kunnen communiceren.

<u>De geavanceerde elektronische handtekening</u>
Nadelen van de gewone vorm zijn: de gewone elektronische handtekening kan herbruikbaar zijn door de ontvanger (de scan van een handtekening kan in eigen documenten worden gebruikt), er is niet gegarandeerd dat de handtekening uniek is (een e-mailadres kan door meerdere personen worden gebruikt (echtparen, afdelingen) en er kan niet worden getraceerd of het ondertekende document na ondertekening is gewijzigd.

Een geavanceerde elektronische handtekening is een gewone elektronische handtekening aangevuld met de volgende eigenschappen:
1) zij is op unieke wijze aan de ondertekenaar verbonden;
2) zij maakt het mogelijk om de ondertekenaar te identificeren;
3) zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
4) zij is op zodanige wijze aan het elektronische bestand waarop zij betrekking heeft verbonden dat elke wijziging achteraf van de gegevens kan worden opgespoord.

Toelichting:
1) dit houdt in dat uitsluitend de ondertekenaar in verband kan worden gebracht met de gebruikte ondertekening;
2) de ondertekening moet een identificerend karakter hebben: de uniek met de ondertekening verbonden ondertekenaar moet kunnen worden aangewezen. Meestal gebeurt dit indirect doordat op basis van het uitgifteproces kan worden aangetoond aan welke persoon een bepaald certificaat is uitgereikt;
3) onder een middel wordt verstaan: geconfigureerde software of hardware die wordt gebruikt om unieke gegevens, zoals codes of cryptografische privésleutels, die door de ondertekenaar worden gebruikt om een elektronische handtekening mee aan te maken, te implementeren; de ondertekenaar moet dus de enige zijn die de ondertekening kan plaatsen.
4) Er moet kunnen worden gegarandeerd dat het bericht inhoudelijk datgene bevat dat de ondertekenaar heeft ondertekend en dat de ondertekening zelf niet is gewijzigd; de software waarmee elektronisch ondertekende documenten worden getoond aan een eindgebruiker (bv Adobe) moet een controle uitvoeren en de eindgebruiker waarschuwen als blijkt dat de ondertekening niet past bij het ondertekende.

De geavanceerde elektronische handtekening biedt meer garanties dan de gewone vorm. De geavanceerde vorm biedt wel extra waarborgen voor de identificatie, maar niet voor de verificatie van deze identificatie.

<u>De gekwalificeerde elektronische handtekening</u>
De gekwalificeerde elektronische handtekening is een geavanceerde elektronische handtekening, waarbij
1) de ondertekening is gebaseerd op een gekwalificeerd certificaat (zoals bedoeld in de Telecommunicatiewet);
2) de ondertekening is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen.

Een certificaat is een elektronische beveiliging die codes of cryptografische openbare sleutels voor het verifiëren van een handtekening aan een bepaalde persoon verbindt en die de identiteit van die persoon bevestigt.

De identiteit van de eigenaar van het certificaat wordt vastgesteld door degene die het certificaat uitgeeft (een onafhankelijke derde) en geverifieerd door degene die het certificaat gebruikt. Het certificaat is geen legitimatiemiddel (vaststelling van identiteit), maar het bewijs dat een legitimatiemiddel ooit is gecontroleerd (bevestiging van identiteit).

De certificatiedienstverlener ('certification service provider' of CSP) is de partij die verantwoordelijk is voor de uitgifte van certificaten. Een CSP is een onafhankelijke derde en vervult een rol die vergelijkbaar is met die van een notaris.

De voornaamste functie van de CSP is om betrouwbare certificaten en betrouwbare en actuele informatie over de geldigheid van certificaten te vertrekken. Bij de verificatie van een certificaat wordt niet alleen gecontroleerd of het certificaat geldig is (ondertekend door het CSP en binnen de geldigheidstermijn), maar ook of het is ingetrokken.

Een tweede belangrijke functie is het aanbieden van een directory service als een soort telefoonboek van certificaten waaruit een ontvanger van een ondertekend bericht het certificaat van de ondertekenaar kan opvragen.

De eisen waaraan een certificaat en een gekwalificeerde CSP moeten voldoen zijn opgenomen in art. 3 van het Besluit elektronische handtekeningen.

De gekwalificeerde elektronische handtekening voegt ten aanzien van de geavanceerde elektronische handtekening de mogelijkheid toe de authentificatie te verifiëren.

In de Wet elektronisch bestuurlijk verkeer (2004) is geregeld dat het verkeer tussen burger en bestuursorgaan onder voorwaarden elektronisch plaats kan vinden. In de uitbreiding van de Awb (afdeling 2.3) wordt het kader afgebakend waarbinnen elektronisch verkeer plaats moet vinden.

Een aanvraag, bezwaarschrift, beroepschrift of klaagschrift kent als vormvereiste dat deze schriftelijk moet zijn net zoals het antwoord. Bovendien moeten aanvragen, bezwaarschriften, beroepschriften en klaagschriften ondertekend zijn.
Volgens de toelichting kan een schriftelijk stuk in de zin van deze wet op papier staan, maar ook een elektronisch document zijn.

Een bericht kan alleen elektronisch worden verzonden als de ontvangende partij kenbaar heeft gemaakt dat hij langs elektronische weg bereikbaar is. Het bestuursorgaan kan voorwaarden aan het gebruik van de elektronische weg stellen, maar de burger kan dit niet.

Beide partijen moeten op een voldoende betrouwbare en vertrouwelijke manier communiceren gelet op aard en inhoud van het bericht.
De eisen betrouwbaar en vertrouwelijk zij open normen, waarvoor voor nadere invulling wordt verwezen naar de beginselen van behoorlijk IT-gebruik:

1. beschikbaarheid - toegang en ongestoord gebruik van informatie;
2. vertrouwelijkheid- toegang tot informatie moet beperkt zijn tot diegenen die geautoriseerd zijn om kennis te nemen van de informatie;
3. integriteit - gegevens zijn volledig, ongewijzigd, correct en actueel;
4. authenticiteit - bewijs van identiteit van ondertekenaar in relatie tot het document;
5. flexibiliteit - het moet in de toekomst mogelijk zijn om zonder gegevensverlies over te gaan naar andere hardware en software en naar andere procedures en werkwijzen;
6. transparantie - de werking van een toepassing moet voor een gebruiker begrijpelijk kunnen zijn;
7. onweerlegbaarheid.

3 Technisch kader: methoden voor authentificatie

Een elektronische handtekening is een collectie elektronische gegevens met 2 bindingen: een binding met de persoon van de ondertekenaar en een binding met het ondertekende.

Voor de gewone elektronische handtekening zijn geen aanvullende eisen beschreven voor de binding aan de ondertekenaar of het ondertekende, waardoor deze vereisen niet meer omvatten dan elektronische gegevens die worden gebruikt voor authentificatie die zijn logisch geassocieerd of vastgehecht zijn aan het ondertekende.

De gewone elektronische handtekening is vooral bruikbaar in situaties waarin een bestaande relatie tussen verzender en ontvanger bestaat.

Concrete toepassingen:
1. een scan van een conventionele handtekening;
2. een digitale foto;
3. een e-mailadres en een signature in een e-mailbericht - de kwalificatie is afhankelijk van het gebruikte e-mailadres;
4. een naam/wachtwoord als toegang van een webdienst;
5. DigiD;
6. PIN-codes;
7. hardwaretokens.

De meest gebruikte techniek voor de geavanceerde elektronische handtekening is de digitale handtekening. Bij deze techniek wordt versleuteling toegepast op basis van 2 complementaire sleutels: een bericht dat is versleuteld met een van beide sleutels kan met de andere sleutel worden ontsleuteld.

Hierbij is het sleutelbeheer als procedure de zwakke plek.

De gekwalificeerde elektronische handtekening voorziet in voorschriften rond het sleutelbeheer. Deze handtekening is gebaseerd op een gekwalificeerd certificaat. Een certificaat is een soort legitimatie waarin een aantal gegevens over de ondertekenaar zijn vastgelegd.

De ontvanger van een ondertekend document heeft het certificaat van een verzender nodig om de handtekening te kunnen valideren. Het certificaat bevat naast persoonsgegevens van de ondertekenaar ook zijn publieke sleutel die binnen het cryptosysteem nodig is voor het ontsleutelen van de message digest.

Als aan de uitgever van een certificaat wordt getwijfeld ontstaat de behoefte aan een gekwalificeerd certificaat van een betrouwbare uitgever in de vorm van een vertrouwde derde (de Trusted Third Party).

De driehoeksverhouding die zo ontstaat en alle logistiek rond sleutelbeheer daarbinnen wordt in technische zin aangeduid als PKI: een Public Key Infrastructure.

De certificatiedienstverlener(CSP) is de onafhankelijke derde die verantwoordelijk is voor de uitgifte van de private sleutels en de publicatie van de publieke sleutels.

Een CSP vervult meestal de functie van Certificate Authority (CA) voor de uitgifte en de functie van Registration Authority (RA).

Voor de gekwalificeerde elektronische handtekening gelden 2 aanvullende eisen in vergelijk met de geavanceerde elektronische handtekening:
1. de ondertekening is gebaseerd op een gekwalificeerd certificaat;
2. de ondertekening is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen.

In de eerste bijlage van de Richtlijn zijn de eisen opgenomen waaraan het certificaat moet voldoen voor kwalificatie afgegeven door een gekwalificeerde CSP, waarvoor de eisen zijn opgenomen in de tweede bijlage. In Nederland zijn deze eisen ondergebracht in art. 3 van het Besluit elektronische handtekeningen.

De eisen waaraan een veilig middel met voldoen in Bijlage III van de Richtlijn en art 5 van het Besluit elektronische handtekeningen.

Een middel is geconfigureerde software of hardware die wordt gebruikt om de gegevens voor het aanmaken van handtekeningen te implementeren.

Voor de gekwalificeerde elektronische handtekening is een certificatiedienstverlener vereist die aan specifieke eisen moet voldoen. In het gekozen model wordt het vertrouwen op een certificaat gebaseerd op een keten (chain of trust) die uiteindelijk uitkomt bij het bovenste certificaat in de hiërarchie: het root certificate.

De authentificatie kan alleen plaatsvinden op basis van gegevens uit de ondertekening zelf en contextuele gegevens. Als de authentificatie niet (alleen) vlak na ontvangst van het document maar (ook) op een later tijdstip, moet dus worden voorzien in duurzaamheid van zowel de ondertekening als van de contextuele informatie.

In een elektronische omgeving zijn er 2 duurzaamheidproblemen:
1. de duurzaamheid van de elektronische drager - iedere vorm van een elektronische drager gaat slechts een paar jaar mee, omdat ofwel de drager zelf vergaat, ofwel de apparatuur om de drager te kunnen uitlezen niet meer wordt gefabriceerd en onderhouden.
2. de duurzaamheid van de informatie zelf - dit probleem duidt op het bestandsformaat waarin de informatie is gecodeerd; voor ieder bestandsformaat is een specifieke toepassing nodig om het bestand te interpreteren en de informatie in het bestand te presenteren.

Voor de ondertekening spelen 3 aanvullende problemen:
1. de techniek die voor ondertekening werd gebruikt is technologieafhankelijk;
2. het integriteitvereiste staat op gespannen voet met conversie voor duurzame toegang;
3. de contextuele informatie moet mede bewaard blijven.

Een elektronisch document dat is ondertekend omvat 2 componenten: de handtekening en het document zelf. Zoals voor het document geldt dat specifieke programmatuur is vereist om het te interpreteren en te presenteren, is ook voor de validatie en zelfs presentatie van de handtekening programmatuur vereist. Dit geldt zowel voor de gewone elektronische handtekening als de geavanceerde elektronische handtekening en de gekwalificeerde elektronische handtekening.
Zonder speciale voorzieningen, zowel technisch als procedureel, is er geen garantie dat specifieke programmatuur en benodigde kennis op termijn nog bestaat.

De Richtlijn en ook de Nederlandse implementatie vereisen voor de geavanceerde elektronische handtekening dat bij wijziging van de gegevens (zowel de ondertekening als de gegevens) de wijziging wordt gedetecteerd. Dit vereist dat er een unieke message digest wordt gemaakt, gebaseerd op de bitreeks van het te ondertekenen bestand.

Als voor het behoud van de opgeslagen informatie het document wordt geconverteerd naar een moderner bestandsformaat, zal de bitreeks van het nieuwe bestand volledig anders zijn dan die van het originele. En dus vervalt de digitale handtekening omdat deze was gebaseerd op de message digest van het bestand voorafgaand aan conversie. De betekenis van de inhoud van het document (de juridische inhoud) hoeft net te zijn gewijzigd; het is zelfs uitdrukkelijk de bedoeling dat exact dezelfde tekst in het nieuwe formaat is ondergebracht. De digitale handtekening overleeft de conversie echter niet.

Hiervoor zijn 4 oplossingen:
1. het hertekenen van documenten door een vertrouwde derde - een onafhankelijke derde (bv een archivaris) verklaart dat het conversieresultaat inhoudelijk overeenkomt met het oorspronkelijke document, dat dit document ondertekend was en dat de validatie van die ondertekening succesvol heeft plaatsgevonden
2. registratie van de validatie - in de administratie wordt vastgelegd dat bij ontvangst van het document validatie succesvol was;
3. certificering van de migratie - een onafhankelijke derde waarborgt de kwaliteit van de conversie door een controle en de afgifte van een certificaat;
4. het bewaren van het originele bestand inclusief alle gegevens, software en certificaten om de validatie te kunnen blijven uitvoeren - deze oplossing is technisch het meest complex en duur.

De centrale vraag die uit de duurzaamheidproblematiek voorkomt, is in hoeverre het noodzakelijk is om een ondertekening op de langere termijn te valideren.

Als de authentificatie succesvol was, staat voor de ontvanger vast dat het document naar behoren is ondertekend. Als het voor de bewijswaarde van het document voldoende zou zijn om slechts dit feit duurzaam te bewaren is registratie van het validatieproces noodzakelijk.

4 Functioneel kader: functies van de ondertekening

De elektronische handtekening vertoont functioneel op 2 fronten verschillen met de traditionele handtekening. Deze verschillen moeten worden overbrugd om een elektronische handtekening functioneel gelijk te kunnen stellen aan een handgeschreven handtekening.

Ten eerste is er bij elektronische ondertekening meer onzekerheid over de identiteit van de ondertekenaar. Het locatieonafhankelijke karakter van elektronisch handelen introduceert bij gebrek aan een fysieke ontmoeting een grotere noodzaak om de identiteit van de wederpartij betrouwbaar vast te leggen.

Ten tweede bestaat een elektronische handtekening uit digitale informatie die niet aan een fysieke drager is gebonden.

Hoewel de functie van de ondertekening zal afhangen van de functie van het document zelf, worden in de literatuur verschillende basisfuncties onderkend.

Zo worden bewijsfuncties (wilsuiting), een cautiefunctie (erkenning van het document als formeel stuk), een beschermingsfunctie (ontvanger kan vertrouwen op het belang van het stuk), een formaliseringfunctie (door ondertekening krijgt het document een formele lading) en een archiveringsfunctie (het document blijft voor externen een duurzame vastlegging van formeel handelen) benoemd.

De ondertekenaar wordt als identificeerbare natuurlijke persoon gezien. Als namens een rechtspersoon wordt ondertekend handelt de ondertekenaar in de hoedanigheid van vertegenwoordiger.

Voor de functies identificatie en authentificatie moet de ondertekening zijn terug te voeren op een bepaald persoon. De identiteit van de persoon moet worden vastgesteld en de ondertekening moet het document kunnen autoriseren.

De ondertekening moet dus een bepaalde persoon uniek kunnen aanwijzen en met betrekking tot het document kunnen getuigen dat diegene inderdaad met de juiste bevoegdheid het document heeft ondertekend.

De elektronische handtekening heeft betrekking op het document dat wordt ondertekend. De binding van de handtekening met deze data wordt niet omschreven. Zowel de Richtlijn als de Nederlandse implementatie vereist vasthechting of logische associatie. Daarmee heeft de wetgever schijnbaar willen benadrukken dat het geen vereiste is dat het document en de ondertekening in hetzelfde object zijn opgenomen en dat zij als afzonderlijke bestanden kunnen bestaan.

Dat betekent dat de ondertekening en het bericht afzonderlijk kunnen worden bewaard, beheerd en verzonden. De mogelijkheid de ondertekening van het document te scheiden laat niet alleen toe dat de handtekening eerder bestaat dan het document, maar ook dat de handtekening eerder wordt vernietigd dan het document.

In de Nederlandse wetgeving wordt niet gesproken over parafering. In de jurisprudentie wordt er vanuit gegaan dat parafering niet alleen gezien inhoudt, maar ook een uiting van instemming betekent.

Bij de procedurele benadering gaat het om het hertekenen van documenten door een vertrouwde derde, registratie van de validatie of certificering van de ondertekening. Hierbij wordt de validatie vervangen door andere waarborgen.

Functioneel gezien is de vraag hoelang de elektronische handtekening zijn functie moet kunnen vervullen, hoelang moet de associatie blijven bestaan.

Omdat authentificatie draait om het aanwijzen van de ondertekenaar en het document zijn functie kan vervullen nadat dit bewijs in voldoende mate is geleverd is het aannemelijk dat authentificatie slechts voor een afzienbare periode mogelijk moet zijn.

Het belang van de duurzaamheid van de binding tussen ondertekening en het document is groter dan dat van de duurzaamheid van de binding met de persoon.

In de Archiefregeling (art 24 sub c) wordt expliciet gesteld dat de ondertekening zelf niet hoeft te worden gearchiveerd en dat de authentificatie na validatie zijn rol verliest.

De Nederlandse norm voor software waarin archiefbescheiden worden beheerd, de NEN 2082, schrijft voor dat op het moment van opname van het archiefstuk de waarde en status van de digitale handtekening behoort te kunnen worden gecontroleerd, waarna het verificatieproces wordt geregistreerd.
Als de digitale handtekening zelf wordt opgeslagen, moet ook het certificaat worden bewaard zodat de handtekening op een later moment kan worden gevalideerd.

5 Gelijkstelling: contextuele factoren

Als een ondertekening in juridische vorm voldoet aan de definitie van een elektronische handtekening, deze in technische zin aan de gestelde eisen voldoet en het de functionele eisen van ondertekening kan vervullen, zou de elektronische handtekening gelijkgesteld kunnen worden aan een conventionele handtekening.

Daarbij moet de toepassing in het concrete geval nog worden getoetst op betrouwbaarheid. Deze beoordeling moet plaatsvinden binnen de context van het doel van het ondertekende en de situatie waarin de ondertekening heeft plaatsgevonden. Dit is een subjectieve beoordeling die sterk afhangt van de specifieke casus.

De methode moet voldoende betrouwbaar zijn, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval. Het doel waarvoor een elektronische handtekening wordt gebruikt is daarmee de bepalende factor in de keuze voor een gewone, geavanceerde of gekwalificeerde elektronische handtekening.

Bij het gebruik van een elektronische handtekening zal de ondertekenaar de kosten van een methode afwegen tegen het belang van het bericht.

Voor de publieke sector kan het bestuursorgaan bekendmaken welke methode voor welke diensten als voldoende betrouwbaar worden aangemerkt.

De functies van de handtekening vallen uiteen in de functionele criteria (identificatie, authentificatie, integriteit en onweerlegbaarheid) en contextuele criteria (wilsuiting, kennisname van inhoud, originaliteit en borging tegen overijling).

Het eerste deel van deze betrouwbaarheidstoets heeft betrekking op de ondertekeningvorm; het tweede deel heeft betrekking op de situatie waarin is ondertekend en het proces van ondertekenen.

6 Toepassingen

In het civiele recht gelden geen algemene regels voor de vorm waarin wordt gecommuniceerd en dis ook niet voor verplichte ondertekening. Als een ondertekening is vereist blijkt dit expliciet uit de overeenkomst of een wettelijke bepaling. Bij een akte (= ondertekend geschrift dat dient als bewijs) wordt door de definitie indirect een ondertekening verplicht gesteld.

Overeenkomsten hoeven niet te worden ondertekend. Elektronische overeenkomsten hoeven in het algemeen niet ondertekend te zijn, maar het is in die gevallen waarin schriftelijkheid vereist is, raadzaam om een geavanceerde of gekwalificeerde elektronische handtekening te gebruiken.

Bij onderhandse akten hangt de vorm van ondertekening sterk van de omstandigheden af. In gevallen waarin de gekwalificeerde elektronische handtekening te duur of te zwaar is en er voor een lichtere vorm wordt gekozen wordt de akte meer afhankelijk van contextinformatie.

Voor verzekeringspolissen (onderhandse akten) eist de wetgever een gekwalificeerde elektronische handtekening.

Facturen mogen elektronisch worden verzonden onder voorbehoud van acceptatie door de aannemer. Voorafgaand aan de elektronische verzending moet de ontvanger instemmen met de elektronische vorm. De aanvaarding kan stilzwijgend plaatsvinden doordat de afnemer de factuur zonder commentaar verwerkt en betaalt.
De Belastingdienst legt de eisen van de Wet op de omzetbelasting uit dat de factuur authentiek moet zijn: de afnemer moet er zeker van kunnen zijn dat de factuur werkelijk van de leverancier afkomstig is.

De regels voor de publieke sector zijn in de Algemene wet bestuursrecht opgenomen.

Voor inkomende e-mail en faxberichten moet het bestuursorgaan aangeven dat zij elektronisch bereikbaar is. Het bestuursorgaan kan dit per proces bepalen. Ook kunnen hierbij eisen worden gesteld aan het gebruik van de elektronische weg en kan elektronische berichten weigeren voor zover deze praktisch onbruikbaar zijn. Zo kan als voorbeeld een algemeen e-mailadres worden voorgeschreven en bepaalde bestandsformaten. Het bestuursorgaan moet deze elektronische bereikbaarheid en de gehanteerde regels wel daadwerkelijk communiceren.

Voor uitgaande e-mail en faxberichten geldt dat dit alleen is toegestaan als de wederpartij elektronisch bereikbaar is. De burger moet dus ook aangeven elektronisch bereikbaar te zijn. Het bestuursorgaan moet dus een administratie aanleggen van elektronisch bereikbare burgers.

In juridisch opzicht kan een handeling in een workflowsysteem als een gewone elektronische handtekening worden gezien. De gebruiksgegevens van de gebruiker worden in de audit-trail opgeslagen.