



easy.brussels

SERVICE PUBLIC RÉGIONAL DE BRUXELLES
GEWESTELIJKE OVERHEIDSDIENST BRUSSEL

De elektronische handtekening

Referentieids



BRUXELLES CONNECTIT
BRUSSEL CONNECTIT

SERVICE PUBLIC RÉGIONAL DE BRUXELLES
GEWESTELIJKE OVERHEIDSDIENST BRUSSEL



INHOUDSTAFEL

Voorwoord.....	5
-----------------------	----------

Het concept van een handtekening.....	6
--	----------

Gebruikelijke definitie van de handtekening.....	6
--	---

Juridische definitie van de handtekening	6
--	---

De elektronische handtekening	7
--	----------

Juridische definitie van de elektronische handtekening.....	7
---	---

Rol van een elektronische handtekening	7
--	---

Heeft een elektronische handtekening dezelfde juridische waarde als een handgeschreven handtekening?	8
--	---

Concreet: de onderdelen van een elektronische handtekening.....	11
---	----

Welk type van elektronische handtekening moet ik gebruiken? (Beslisboom)	13
--	----

Alvorens een document te (laten) ondertekenen: enkele aandachtspunten.	14
---	----

De uitdagingen van de elektronische handtekening	15
---	-----------

Welke verantwoordelijkheden brengt de ondertekening met zich mee?	15
---	----

Wat gebeurt er als een document niet (geldig) ondertekendis?	16
--	----

De bewijskracht in rechte.....	17
--------------------------------	----

Nuances en verduidelijkingen van begrippen	18
---	-----------

Validering of handtekening?	18
-----------------------------------	----

Handtekening, visum of medeondertekening?	18
---	----

Handtekening of paraaf?.....	19
------------------------------	----

Login, klik, paraaf?.....	19
---------------------------	----

Gefotokopieerde, gescande of originele handtekening?	19
--	----

Authentieke akte, authenticiteit wat betreft de bewaring en het origineel	20
---	----

Valsheid in geschrifte	21
------------------------------	----

Technologische oplossingen	22
---	-----------

Praktische fiches.....	25
-------------------------------	-----------

1. Moet het document worden ondertekend?	27
--	----

2. De 3 types van elektronische handtekening	28
--	----

3. Welk type handtekening kiezen?	29
---	----

4. Hoe lang is een elektronische handtekening geldig?	30
---	----

5. Hoe archiveer je een elektronisch ondertekend document?	31
--	----

6. Welke technologische tool moet je gebruiken?	32
---	----

7. Verzenden en afdrukken van een elektronisch ondertekend document.....	33
--	----

8. Meerdere handtekeningen	34
----------------------------------	----

9. Bulkondertekening	35
----------------------------	----

10. Kan ik een document na ondertekening wijzigen? (inhoud of tijdstempel)	36
--	----

Woordenlijst	37
---------------------------	-----------

CONTACTEER ONS

Voor alle vragen over de inhoud van deze gids, over administratieve vereenvoudiging of over de gebruikersrelatie kunt u contact opnemen met het agentschap **easy.brussels** :

info@easy.brussels

Om contact op te nemen met Brussel ConnectIT, de administratie die verantwoordelijk is voor de IT-strategie voor de administraties van de Gewestelijke Overheidsdienst Brussel en het regionale SAP-competentiecentrum:

connectit@gob.brussels

Om contact op te nemen met ConnectMemory, de Gewestelijke Archiefdienst:

connectmemory@gob.brussels

Let op: deze gids vervangt het advies en de richtlijnen van je eigen overheidsdienst niet. Informeer je steeds intern, bijvoorbeeld bij je juridische dienst.

In deze gids komen heel wat juridische en technische termen aan bod die op het eerste gezicht ingewikkeld kunnen lijken. Geen paniek! In de woordenlijst op pagina 37 worden al deze begrippen uitgelegd.

COLOFON

Redactiecomité:

Cathy Marcus, Directrice van easy.brussels
Florence Biston • Sarah De Cock • Koen De Pauw • Stéphanie Dheur • Roxana Dragomir • Julie Etienne

Coördinatie: easy.brussels

Opmaak: Florence Biston - easy.brussels

Vertaling: Directie Vertaling, Gewestelijk Overheidsdienst Brussel

Verantwoordelijke uitgever: Baptiste Daveau • Directeur-generaal (ad interim) van Brussel ConnectIT, Gewestelijk Overheidsdienst Brussel
Iris Tower, Sint-Lazarusplein 2, 1035 Brussel

ISBN : 2026/14.404/08

©easy.brussels 2026



VOORWOORD

Tegenwoordig is de digitalisering van overheidsdiensten een noodzaak geworden om de efficiëntie van overheidsinstanties te verbeteren, de transparantie te vergroten en de administratieve procedures te vereenvoudigen.

Deze transformatie beperkt zich echter niet tot het vervangen van papier door digitale hulpmiddelen. Ze biedt de mogelijkheid om de overheidsdiensten opnieuw vorm te geven, zodat ze eenvoudiger en toegankelijker zijn en beter afgestemd op de behoeften van burgers, bedrijven en organisaties.

De regelgeving **Digitaal Brussel**¹, die de digitalisering van administratieve procedures stimuleert en tegelijkertijd de inclusie van alle gebruikers waarborgt, vormt in het Brussels Hoofdstedelijk Gewest het kader voor deze ontwikkeling. Iedereen moet toegang kunnen krijgen tot de overheidsdiensten, rekening houdend met zijn of haar vaardigheden, behoeften en voorkeuren.

Digitalisering moet administratieve stappen vergemakkelijken, nooit een obstakel worden.

In deze context worden de Brusselse overheidsdiensten ertoe aangezet om hun werkwijzen, besluitvormingsprocessen en interacties met de gebruikers verder aan te passen. Ze digitaliseren hun procedures en de daaruit voortvloeiende communicatie geleidelijk, en bieden tegelijk offline ondersteuning aan gebruikers die moeilijkheden ondervinden met digitale hulpmiddelen.

Deze transformatie brengt soms het gebruik van een **elektronische handtekening** met zich mee, wat tal van vragen oproept: moeten alle documenten worden ondertekend? Welk type van elektronische handtekening moet ik gebruiken? Heeft een elektronische handtekening dezelfde juridische waarde als een handgeschreven handtekening? Hoe kan de rechtsgeldigheid gedurende de volledige levenscyclus van een document worden gewaarborgd?

Deze gids is bedoeld om de Brusselse overheidsdiensten te begeleiden bij het begrijpen en invoeren van de elektronische handtekening.

Met deze gids willen we concrete toelichtingen en richtlijnen bieden om de behoeften in kaart te brengen en een weloverwogen keuze te maken bij het gebruik van de elektronische handtekening en de daarvoor geschikte technologische oplossingen.

In het eerste deel van de gids worden de principes en begrippen in verband met de elektronische handtekening uitgelegd. Het tweede deel bestaat uit praktische fiches die bedoeld zijn om een snel en duidelijk antwoord te geven op veelgestelde vragen van overheidsdiensten. Dit deel kan in de loop van de tijd worden aangepast en verder worden uitgewerkt.

Gezamenlijk decreet en gezamenlijke ordonnantie van 25 januari 2024 van de Franse Gemeenschapscommissie, het Brussels Hoofdstedelijk Gewest en de Gemeenschappelijke Gemeenschapscommissie betreffende de digitale transitie van de overheidsinstanties, B.S. 21/02/2024.
Bezoek onze website <https://easy.brussels> om de volledige gids 'Digitaal Brussel' te raadplegen.



Een digitale versie van deze gids is beschikbaar op onze website:
<https://easy.brussels>.

HET CONCEPT VAN EEN HANDTEKENING

GEBRUIKELIJKE DEFINITIE VAN DE HANDTEKENING

“Een teken of een opeenvolging van tekens, aangebracht met de hand, elektronisch of via ieder ander procedé, waarmee een persoon zich identificeert en waaruit zijn wilsuiking blijkt?” (Belgisch Burgerlijk Wetboek)

JURIDISCHE DEFINITIE VAN DE HANDTEKENING

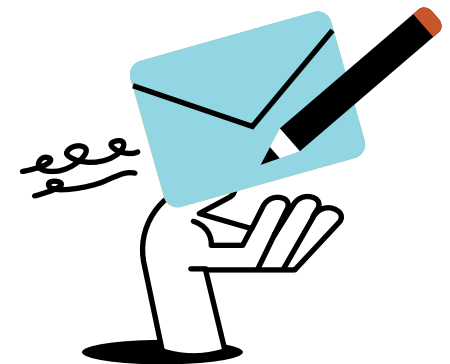
De juridische definitie van de handtekening luidt “naar het opschrift van zijn naam dat een persoon aanbrengt in een kenmerkende en vaste vorm, met als doel de juistheid of authenticiteit van een document te certificeren, en zijn verantwoordelijkheid op te nemen”.

Door deze vrijwillige handeling **bewijst de ondertekenaar zijn identiteit en verklaart hij kennis te hebben genomen** van de inhoud van het document en/of hiermee te hebben ingestemd. De handtekening speelt dus een onmisbare rol in het kader van juridische uitwisselingen: ze maakt het mogelijk om het **bewijs van de instemming** vast te leggen, de relaties tussen de partijen te **beveiligen** en **bewijskracht** te verlenen aan documenten. Tenzij de wet anders bepaalt, is een handtekening vereist op juridische akten. Ze waarborgt de **integriteit** van het document, doordat de ondertekenaar met zekerheid kan worden geïdentificeerd. Daarom neemt ze een centrale plaats in het burgerlijk en handelsrecht in, waar ze bijdraagt aan de geldigheid en de bewijskracht van de akten.



WIST JE DIT AL?

Op papier wordt de integriteit van het document gewaarborgd door de fysieke drager zelf ... Het is onmogelijk om dit te wijzigen zonder dat het opvalt. In digitale vorm wordt deze integriteit verzekerd door een **beveiligingssysteem, namelijk de cryptografie**. Daarmee kan worden gecontroleerd of het document na de ondertekening niet werd gewijzigd.



JURIDISCHE DEFINITIE VAN DE ELEKTRONISCHE HANDTEKENING

In de zin van verordening (EU) nr. 910/2014 (de “eIDAS”-verordening genoemd) wordt een elektronische handtekening gedefinieerd 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”*.

Met andere woorden: een elektronische handtekening is een geheel van digitale gegevens die aan een document zijn “gehecht” om:

- de ondertekenaar te identificeren (of te authenticeren);
- de integriteit van het ondertekende document te waarborgen, dat wil zeggen dat kan worden nagegaan of dit document na de ondertekening niet is gewijzigd.

ROL VAN EEN ELEKTRONISCHE HANDTEKENING

De elektronische handtekening vervult **drie essentiële functies**:

1. de ondertekenaar identificeren (**authenticatie**),
2. zijn akkoord met de inhoud van het document bevestigen (**instemming**),
3. garanderen dat het document na de ondertekening niet is gewijzigd (**integriteit**).

Ze zorgt ook voor **rechtszekerheid** door elektronische documenten dezelfde bewijskracht te verlenen als papieren documenten. Bovendien **stelt** ze de ondertekenaar **aansprakelijk**.

De elektronische handtekening is wettelijk erkend in de hele Europese Unie, en vergemakkelijkt de digitalisering van de procedures terwijl ze tegelijk de veiligheid van en het vertrouwen in de elektronische uitwisselingen waarborgt.

Hoewel de technische evolutie het mogelijk heeft gemaakt de handtekening te digitaliseren, met name via elektronische oplossingen, mogen we niet uit het oog verliezen dat de essentiële functies van de handtekening door de eeuwen heen onveranderd zijn gebleven. Of het nu gaat om een handgeschreven krabbel of om een digitale stempel, de handtekening beoogt altijd de identiteit van de ondertekenaar te authenticeren, hem indien nodig aansprakelijk te stellen en de integriteit van het ondertekende document te garanderen.

Samengevat: de vorm kan veranderen, maar de inhoud blijft hetzelfde: de handtekening geeft de overeenkomst, de beschikking of de verbintenis vorm, terwijl ze ook rechtszekerheid biedt voor uitwisselingen. Deze continuïteit getuigt van het universele belang van de handtekening, ongeacht het gebruikte medium.

***Wat betekent eIDAS?**

Verordening (EU) nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (eIDAS) is het belangrijkste referentiedocument in de Europese Unie op het gebied van elektronische handtekeningen en elektronische archivering. Het biedt een gemeenschappelijk en gestandaardiseerd juridisch kader zodat elektronische handtekeningen in alle lidstaten van de EU juridisch worden erkend en aanvaard.

Deze verordening werd in Belgisch recht omgezet via de wet van 21 juli 2016 (de “Digital Act”).



WIST JE DIT AL?

In 2026 heeft de Federale Overheidsdienst Binnenlandse Zaken **wijzigingen** aangebracht **aan het handtekeningcertificaat van de Belgische elektronische identiteitskaart (eID)**.

Deze wijzigingen maken deel uit van de modernisering van de eID-infrastructuur in België en van de voorbereiding op toekomstige Europese ontwikkelingen. **Sinds 21 mei 2026 kunnen identiteitskaarten die vóór juli 2016 zijn uitgereikt, niet langer worden gebruikt om gekwalificeerde elektronische handtekeningen te plaatsen.** De betrokken gebruikers moeten hun eID vernieuwen of gebruikmaken van andere oplossingen voor gekwalificeerde elektronische handtekeningen die voldoen aan de eIDAS-verordening.

Meer informatie: <https://www.ibz.fgov.be/nl/nieuws/elektronisch-handtekenen-met-je-eid-wijziging-vanaf-21-mei-2026>

Bovendien verleent de wet van 16 juli 2026 betreffende een dienst voor gekwalificeerde elektronische handtekeningen een wettelijke basis aan het door de FOD ingevoerde systeem voor het aanmaken van handtekeningen.

Meer informatie: <https://www.ejustice.just.fgov.be/eli/loi/2026/07/16/2026005829/justel>

HEEFT EEN ELEKTRONISCHE HANDTEKENING DEZELFDE JURIDISCHE WAARDE ALS EEN HANDGESCHREVEN HANDTEKENING?

Dat hangt helemaal af van het wettelijke kader en het beveiligingsniveau dat de gebruikte technologie biedt.

In België geniet de elektronische handtekening dezelfde wettelijke erkenning als de handgeschreven handtekening, op voorwaarde dat aan bepaalde eisen inzake betrouwbaarheid en identificatie van de ondertekenaar wordt voldaan. Bovendien mag een elektronische handtekening, overeenkomstig het **non-discriminatiebeginsel**, niet worden afgewezen of van rechtsgeldigheid worden beroofd louter omdat deze in elektronische vorm is.

De handgeschreven handtekening, die traditioneel als “tastbaarder” wordt beschouwd, is niet noodzakelijk beter of geldiger: een geavanceerde of gekwalificeerde elektronische handtekening **garandeert de integriteit van het document en de identiteit van de ondertekenaar**, en waarborgt tegelijkertijd de **onweerlegbaarheid** (de garantie dat een ondertekenaar niet op geldige wijze kan betwisten dat hij een document heeft ondertekend). In veel gevallen **biedt de elektronische handtekening dus garanties die minstens gelijkwaardig of zelfs beter zijn**, met name op het vlak van traceerbaarheid en veiligheid, op voorwaarde dat het gebruikte procedé voldoet aan de geldende normen.

DE VERSCHILLENDE TYPES ELEKTRONISCHE HANDTEKENINGEN



Volgens de Europese regelgeving (eIDAS) bestaan er **drie types elektronische handtekeningen**, die elk een verschillend niveau van veiligheid en juridische erkenning bieden.

1. EENVOUDIGE ELEKTRONISCHE HANDTEKENING

Dit is het meest elementaire niveau van de elektronische handtekening. Ze is eenvoudig te implementeren, omdat er geen specifieke technologie voor nodig is. Ze wordt vaak gebruikt voor handelingen met een laag risico, maar biedt slechts een beperkte mate van veiligheid.

In de praktijk wordt ze vooral gebruikt wanneer het document weinig of geen juridische gevolgen heeft en het risico op betwisting klein is. **Ze volstaat daarom voor eenvoudige en/of interne handelingen (formulieren, kleine aanvragen)**, maar wordt afgeraden voor belangrijke contracten of verbintenissen, of wanneer de wet een hoger ondertekeningsniveau voorschrijft.

Voorbeelden:

- ✓ gescande afbeelding van een handgeschreven handtekening die op een document wordt geplaatst,
- ✓ aan te vinken vakje in een onlinedocument,
- ✓ handtekening onderaan een e-mail,
- ✓ geheime code van een kredietkaart.



2. GEAVANCEERDE ELEKTRONISCHE HANDTEKENING

Ze is **gebaseerd op de meest strikte identificatie- en authenticatiecriteria en moet voldoen aan de specifieke eIDAS-vereisten**: ze legt het verband tussen de ondertekenaar, zijn handtekening en de ondertekende gegevens. Dit verband moet de integriteit van de gegevens waarborgen (het document werd na de ondertekening niet gewijzigd), de ondertekenaar identificeren en de onweerlegbaarheid garanderen (de mogelijkheid om aan te tonen dat de betrokken persoon niet kan ontkennen dat hij het document heeft ondertekend). Niet alle overheidsinstanties bieden dit ondertekeningsniveau aan.

In de praktijk biedt de geavanceerde elektronische handtekening een **goed evenwicht tussen veiligheid en gebruiksgemak**, zonder dat daarvoor een officieel certificaat nodig is. Het vereist echter het gebruik van een meer specifieke technologie.

Voorbeelden:

- ✓ handtekening met naam en wachtwoord,
- ✓ handtekening via een bankapplicatie,
- ✓ handtekening die wordt gevalideerd met een OTP (one time password): MFA³ (Multi-Factor Authentication), een unieke code via sms, e-mail of een mobiele app,
- ✓ biometrische handtekening (een handgeschreven handtekening die op een tablet of ander apparaat wordt gezet, waarbij de lijnen, de druk en de snelheid van de handtekening worden geregistreerd om de ondertekenaar te identificeren).

3. Een beveiligingsmechanisme waarbij de identiteit van een gebruiker wordt gecontroleerd aan de hand van minstens twee verschillende authenticatiefactoren voordat toegang tot een systeem of dienst wordt verleend. Een gebruiker kan bijvoorbeeld inloggen op een elektronisch ondertekeningsplatform met een wachtwoord (eerste factor) en vervolgens een code invoeren die naar zijn gsm wordt gestuurd (tweede factor). Ook het gebruik van een eID in combinatie met een pincode is hiervan een voorbeeld.



WIST JE DIT AL?

Een gekwalificeerde handtekening plaatst een visuele markering, een stempel, op uw document. Deze markering bevat soms een datum en een tijdstip (**een tijdstempel**), om een bijkomend bewijs toe te voegen dat nadien niet meer kan worden verwijderd of gewijzigd.

Beginnel	eenvoudige handtekening	geavanceerde handtekening	gekwali-ficeerde handtekening
Identificatie van de ondertekenaar	-	✓	✓
Integriteit van het document ¹	-	✓	✓
Non-discriminatie ²	✓	✓	✓
Onweerlegbaarheid ³	-	✓	✓
Certificering ⁴	-	-	✓
Veiligheid en juridische erkenning	+	++	+++

- 1. Integriteit:** garandeert dat het document na de ondertekening niet is gewijzigd.
- 2. Beginnel van non-discriminatie:** een handtekening mag niet worden geweigerd of van rechtsgevolgen worden ontszegd louter omdat ze elektronisch is.
- 3. Beginnel van onweerlegbaarheid:** de ondertekenaar kan niet op geldige wijze weerleggen dat hij het document heeft ondertekend.
- 4. Certificering:** handeling waarbij het verband wordt vastgesteld tussen de identiteit van een persoon en de gegevens die worden gebruikt om een elektronische handtekening aan te maken.

3. GEKWALIFICEERDE ELEKTRONISCHE HANDTEKENING

Dit is het **hoogste niveau van veiligheid en rechtsgeldigheid, en is vergelijkbaar met een handgeschreven handtekening**. De gekwalificeerde elektronische handtekening biedt alle waarborgen van de geavanceerde handtekening, plus een certificering door een **gekwaliificeerde dienstverlener die is erkend door de FOD Economie (of erkend binnen de EU)**. Het certificaat waarmee de ondertekenaar wordt geauthenticeerd, is gebaseerd op strikte procedures. Daardoor is deze handtekening complexer en brengt ze kosten voor de overheidsdienst met zich mee.

In sommige gevallen kan de handtekening worden aangevuld met een **elektronische tijdstempel**. Hiermee kan aan een document een datum - en soms ook een tijdstip - worden toegekend die niet kan worden gewijzigd. Een tijdstempel dient als bewijs dat een document of handeling (zoals een handtekening) op een bepaald moment daadwerkelijk bestond. Deze functie is bijzonder nuttig wanneer de chronologische volgorde van belang is, bijvoorbeeld bij een premieaanvraag of om na te gaan of een procedure vóór een bepaalde deadline werd uitgevoerd.

In de praktijk wordt deze handtekening gebruikt **wanneer dit absoluut noodzakelijk is**, bijvoorbeeld wanneer een onberispelijke authenticatie is vereist of wanneer de regelgeving dit voorschrijft. De handtekening moet worden aangemaakt met behulp van een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen.

Voorbeelden:

- ✓ een handtekening via een eID-kaartlezer en specifieke software (eID),
- ✓ een digitale sleutel online,
- ✓ een methode waarmee burgers zich op een veilige manier kunnen authenticeren, zoals itsme®, myGov.be, enz.,
- ✓ een handtekening via specifieke software of een specifieke oplossing (Adobe Acrobat, Microsoft Word, enz.).



Raadpleeg de praktische fiche
'De 3 types van elektronische handtekening'

CONCREET: DE ONDERDELEN VAN EEN ELEKTRONISCHE HANDTEKENING

Een eenvoudige handtekening kan een afbeelding, een naam of een aan te vinken vakje zijn. Geavanceerde of gekwalificeerde handtekeningen zijn complexer. **Het gaat om een geheel van technische en juridische elementen die de identiteit van de ondertekenaar en de integriteit van het document waarborgen.**

Geavanceerde en gekwalificeerde handtekeningen bestaan doorgaans uit de volgende elementen:

- ✓ **De gegevens van het ondertekende document:** de handtekening is gekoppeld aan het document zelf. Een cryptografisch mechanisme (een wiskundige berekening, ook wel hashing genoemd) creëert een unieke digitale vingerafdruk (hash) voor de inhoud van het document. Tijdens de verificatie wordt een nieuwe vingerafdruk berekend en vergeleken met de oorspronkelijke vingerafdruk, om te garanderen dat het document na de ondertekening niet is gewijzigd.
- ✓ **De gegevens van de handtekening:** het gaat om cryptografische gegevens die tijdens het ondertekenen met behulp van de privésleutel van de ondertekenaar worden gegenereerd. Ze leggen een unieke koppeling tussen de ondertekenaar en het document.
- ✓ **Het elektronische certificaat:** dit kan worden beschouwd als een soort “digitale identiteitskaart”, die onder meer de identiteit van de ondertekenaar, de bijbehorende publieke sleutel, een serienummer (de certificaatcode) en de

geldigheidsperiode bevat, evenals de identiteit van de instantie die het certificaat aflevert. Hiermee wordt aangetoond dat het document niet werd vervalst en wordt de identiteit van de ondertekenaar bevestigd. Het kan online worden getraceerd. **In het geval van een gekwalificeerde elektronische handtekening** is de instantie die het certificaat aflevert speciaal door de Europese Unie erkend en wordt zij regelmatig gecontroleerd, waarbij strengere eisen gelden.

- ✓ **Tijdstempel** (indien van toepassing): bevestigt de exacte datum en het tijdstip van de ondertekening. De tijdstempel mag niet worden gewijzigd, anders worden de handtekening... en het document ongeldig!
- ✓ **Ondertekeningsbewijzen:** afhankelijk van de gebruikte technologische oplossing kunnen aanvullende gegevens worden bewaard, zoals het IP-adres, de authenticatiemethode of het bewijs van validering via sms, eID, itsme®, enz. Dit bewijsmateriaal draagt bij aan de onweerlegbaarheid⁴ en de bewijskracht van het document.



Samengevat werkt een elektronische handtekening als een digitaal “zegel”. Het systeem maakt een digitale vingerafdruk van het document, vergelijkbaar met uw eigen vingerafdruk. Als het document na de ondertekening wordt gewijzigd, zelfs maar heel licht, verandert die vingerafdruk. Zo kan elke wijziging aan het document worden opgespoord, waardoor het document mogelijk ongeldig wordt.



WIST JE DIT AL?

Het elektronisch zegel is vergelijkbaar met een elektronische handtekening, maar dan voor een rechtspersoon. Het is het digitale equivalent van de stempel van een organisatie en stelt een onderneming of administratie in staat een document te authenticeren.

4. Onweerlegbaarheid: het vermogen om betrouwbare bewijzen te leveren dat een elektronische handtekening door een bepaalde persoon werd geplaatst, zodat die persoon redelijkerwijs niet kan betwisten dat hij het document heeft ondertekend.

AANDACHTSPUNT

De afbeelding van een handgeschreven handtekening die op een papieren of digitaal document is aangebracht, vormt op zich geen garantie voor de geldigheid of authenticiteit ervan.

Wat een handtekening rechtsgeldig maakt, zijn de **criteria die tijdens het ondertekeningsproces worden gecontroleerd**: de identificatie van de ondertekenaar, de integriteit van het document en het vermogen om de aanvaarding van de inhoud ervan te bewijzen. Louter de grafische reproductie van een handtekening volstaat dus niet om de wil van de ondertekenaar aan te tonen of om de veiligheid van het document te waarborgen. De controlemechanismen verbonden aan de handtekening (ongeacht of die elektronisch dan wel handgeschreven is) zijn essentieel om de geldigheid en bewijskracht ervan te waarborgen.

AANMAAK VAN DE ELEKTRONISCHE HANDTEKENING



VERIFICATIE VAN DE GELDIGHEID VAN EEN ELEKTRONISCHE HANDTEKENING



Bron: https://fr.wikipedia.org/wiki/Signature_numérique

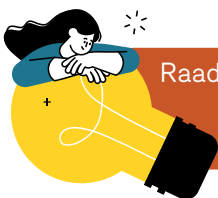
WELK SOORT ELEKTRONISCHE HANDTEKENING MOET JE GEBRUIKEN? (BESLISSINGSBOOM)

De keuze van het ondertekeningsniveau hangt af van het gebruik en het belang van het te ondertekenen document. Bij een geschil geldt: hoe hoger het betrouwbaarheidsniveau van je handtekening, hoe moeilijker het wordt om de geldigheid van het ondertekende document en de verbintenissen die erin zijn opgenomen, te betwisten.

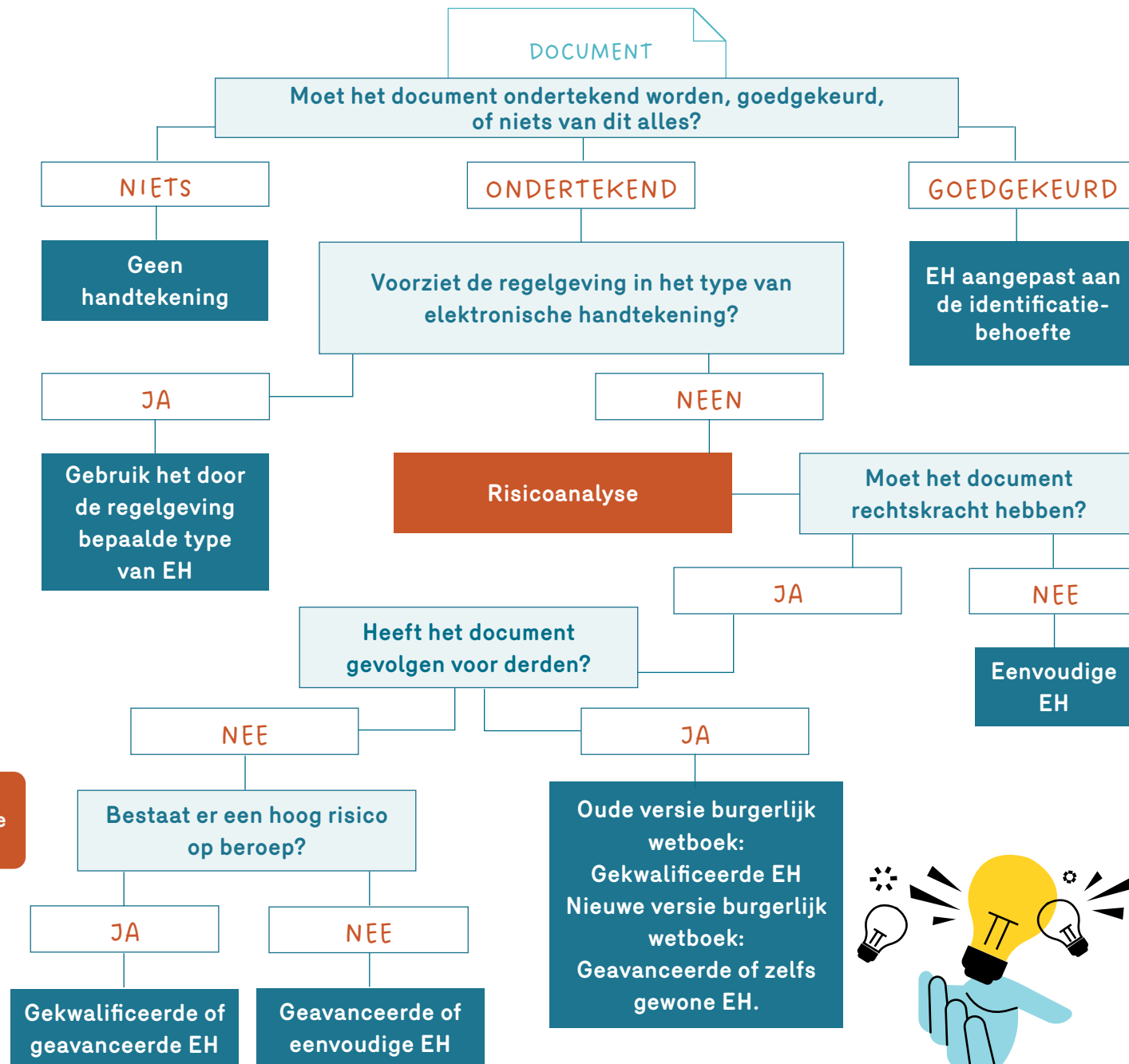
Geef de voorkeur aan geavanceerde (indien beschikbaar) en gekwalificeerde elektronische handtekeningen voor handelscontracten, juridische akten of gevoelige transacties. Gebruik de eenvoudige elektronische handtekening voor administratieve procedures of dagelijkse, minder kritieke uitwisselingen.

Hiernaast vindt u een beslissingsboom die u helpt het geschikte type handtekening te kiezen.

EH = elektronische handtekening

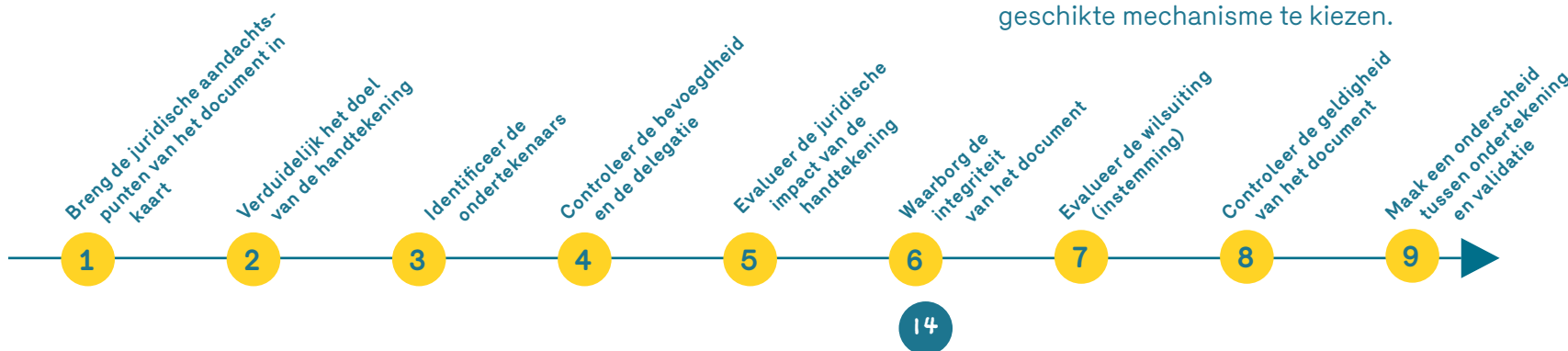


Raadpleeg de praktische fiche
"Welk soort handtekening moet je gebruiken?"



ALVORENS EEN DOCUMENT TE (LATEN) ONDERTEKENEN: ENKELE AANDACHTSPUNTEN.

- 1. Bepaal de aard en het juridische kader (bestuursrecht) van het document.** Gaat het om een eenzijdige beslissing, een kennisgeving, een intern document of iets anders? Wat is het juridische kader? Zo kunt u nagaan aan welke vereisten moet worden voldaan, zowel inhoudelijk (bevoegdheid, rechtsgrond, motivering, procedure) als vormelijk, onder meer wat de handtekening betreft.
- 2. Breng de juridische vragen rond de handtekening in kaart.** Ga na of de handtekening een impact kan hebben op de externe en/of interne regelmatigheid, de bevoegdheid van de auteur, de traceerbaarheid, de bewijskracht, de tegenwerpelijke, de beroepsmogelijkheden, de archivering van het elektronisch origineel, enzovoort.
- 3. Verduidelijk het beoogde doel.** Wordt de handtekening gebruikt om...
 - > de persoon die tussenkomt te identificeren?
 - > aan te geven of men het al dan niet eens is met de inhoud?
 - > de integriteit van het document te waarborgen?
 - > een workflow te organiseren (proeflezen, goedkeuring)?
 - > de geloofwaardigheid van het document te waarborgen?
- 4. Identificeer de ondertekenaar(s).** Wie moet ondertekenen (identiteit) en in welke hoedanigheid (bevoegde overheid, mandataris, gemachtigde medewerker)? Welk niveau van zekerheid over die identiteit is vereist, gelet op het document en de gevolgen ervan?
- 5. Controleer de bevoegdheid en de delegatie van ondertekening.** Heeft de bevoegde overheid daadwerkelijk beslist over het document? Is de delegatie van handtekening (machtiging om "in opdracht" te ondertekenen) geldig, traceerbaar en verenigbaar met de interne organisatie?
- 6. Waarborg de integriteit van het document.** Bepaal wat u moet kunnen aantonen: dat het document na ondertekening niet werd gewijzigd, of dat elke wijziging opspoorbaar is.
- 7. Beoordeel de betekenis.** Moet de handtekening een bereidheid tot verbintenis, instemming, afwijzing van de inhoud of een besluit uitdrukken? Verduidelijk op welk moment deze handtekening is vereist (definitieve ondertekening, medeondertekening, enz.).
- 8. Controleer de geldigheid van de inhoud en de vorm.** Het document moet aan twee soorten voorwaarden voldoen:
 - > *inhoudelijke geldigheid*: bevoegdheid en naleving van de regels,
 - > *vormelijke geldigheid*: formaliteiten, vermelding van de auteur, handtekening, enzovoort. De handtekening maakt deel uit van de vormvereisten, maar volstaat op zichzelf niet om de geldigheid van het document te waarborgen.
- 9. Verwar een handtekening niet met een validering.** Een validering hoeft niet altijd met een handtekening te worden bevestigd, maar kan ook op andere manieren plaatsvinden: een visum in een workflow, een goedkeuringsknop, een login, enz. Een risicoanalyse zal je helpen om het meest geschikte mechanisme te kiezen.



DE UITDAGINGEN VAN DE ELEKTRONISCHE HANDTEKENING

WELKE VERANTWOORDELIJKHEDEN BRENGT DE ONDERTEKENING MET ZICH MEE?

- **Wat de vorm betreft (externe regelmatigheid):** aan de hand van de handtekening kan de ondertekenaar worden geïdentificeerd en kan zijn bevoegdheid worden bevestigd; tevens kan worden nagegaan of er sprake is van een regelmatige delegatie, of de formaliteiten worden nageleefd (vermeldingen, datums, kennisgevingsregels), en kan de integriteit en de traceerbaarheid van het document worden gecontroleerd.
 - › Een tekortkoming op dit vlak kan de betrouwbaarheid van het document in het gedrang brengen, zelfs als de inhoud correct is.
- **Wat de inhoud betreft (interne regelmatigheid):** de handtekening volstaat op zich niet om een document rechtsgeldig of onbetwistbaar te maken. Een geldig ondertekend document kan altijd worden betwist indien het berust op een onregelmatige beslissing, een duidelijke fout, een schending van de wetgeving, een gebrek aan motivering, machtsmisbruik, enz.

Samengevat: in geval van betwisting is niet alleen het type handtekening van belang, maar ook het vermogen om met bewijsmateriaal aan te tonen wie heeft ondertekend, wanneer de handtekening werd geplaatst en onder welke omstandigheden dit is gebeurd.

Waar moet u op letten?

Bij de keuze van het geschikte type handtekening voor een procedure is het ook belangrijk na te gaan welke bewijzen kunnen worden voorgelegd indien de handtekening wordt betwist. Zorg ervoor dat dit bewijsniveau in verhouding staat tot het belang van het document.



Raadpleeg de praktische fiche
"Moet het document worden ondertekend?"



WIST JE DIT AL?

Het recht erkent verschillende vormen van handtekeningen, ongeacht hun visuele vorm, zolang zij toelaten de ondertekenaar te identificeren, zijn akkoord of wil te bevestigen en de integriteit van het document te waarborgen.

Niet alle handtekeningen bieden echter hetzelfde niveau van veiligheid of dezelfde juridische waarde.



WIST JE DIT AL?

De **gekwalficeerde elektronische handtekening** wordt in de hele Europese Unie erkend. In tegenstelling tot andere soorten handtekeningen moet bij een geschil de tegenpartij aantonen dat de handtekening niet geldig is. Voor een eenvoudige of geavanceerde handtekening ligt de bewijslast daarentegen bij de ondertekenaar, die de geldigheid ervan moet aantonen.

WAT GEBEURT ER ALS EEN DOCUMENT NIET (GELDIG) ONDERTEKEND IS?

Het hoofdrisico voor een administratie is niet louter technisch van aard: een document dat niet ondertekend is, ondertekend is door een niet-bevoegde persoon, of via een werkwijze die niet betrouwbaar genoeg is, kan worden aangevochten en kan leiden tot een geschil (nietigverklaring, opschorting, betwisting van bewijs, contractueel geschil enz.).

In de praktijk betekent het ontbreken van een handtekening of een onjuiste handtekening niet automatisch dat het document ongeldig is. De rechter gaat vaak na of het gebruikte mechanisme voldoet aan de functies die van een handtekening worden verwacht: de ondertekenaar identificeren, instemming/wil uitdrukken, de integriteit van het document garanderen, de traceerbaarheid garanderen.

• Wat er in het geding is:

- › de geldigheid van de akte (vorm/inhoud), de tegenwerpbaarheid ervan en de mogelijkheid om er een bewijs van te leveren bij betwisting..

• Wat de rechter zal onderzoeken:

- › de bevoegdheid van de opsteller, de echtheid van de beslissing/instemming, het uitblijven van wijzigingen aan het document en de kwaliteit van de sporen (gebeurtenislogboek, tijdstempel, bewaring)..

Kortom: het gaat niet alleen om de aanwezigheid van een handtekening, maar ook om de mogelijkheid om de identiteit van de ondertekenaar, zijn instemming, de integriteit van het document en de traceerbaarheid ervan aan te tonen.

Hoe blijft het risico beperkt?

Door je analyse te documenteren (kanaalkeuze, niveau van ondertekening/validering, identificatie- en bewaringsmaatregelen) en door de oplossing aan te passen aan de uitdagingen verbonden aan het document.

De gevolgen van het ontbreken van een handtekening (of van een ongeschikt ondertekeningsmechanisme) hangen af van de aard van het document en de rechtbank waar de zaak mogelijk aanhangig wordt gemaakt.

- **Bestuurlijke (met name individuele) akten:** een geschil kan betrekking hebben op de wettigheid (vorm en/of inhoud). Het kan leiden tot een nietigverklaring of opschorting, met concrete gevolgen: heruitgave van documenten, overdoen van een procedure, vertragingen bij de behandeling en bijkomende administratieve kosten.
- **Burgerlijke geschillen:** de handtekening wordt vaak benaderd vanuit het oogpunt van het bewijs. Het kan gaan om het aantonen van het bestaan van een akkoord, de aanvaarding van een verbintenis, een datum of de identiteit van de opsteller. Een ontoereikend ondertekeningsmechanisme kan het aantonen hiervan bemoeilijken en het risico op betwisting vergroten.
- **Strafrechtelijke geschillen:** in bepaalde situaties kunnen er vragen rijzen over de wijziging van documenten, identiteitsfraude of ongeoorloofde toegang. Deze risico's benadrukken het belang van het waarborgen van de traceerbaarheid, de integriteit en de toegangscontroles.

Kortom: de gevolgen van het ontbreken van een handtekening hangen af van de context, maar kunnen van invloed zijn op de geldigheid van een document en de bewijskracht ervan, en kunnen kosten of vertragingen veroorzaken.

Nuttige vragen

Wie kan iets aanvechten? voor welke rechter? welke gevolgen (nietigverklaring, schadevergoeding, sanctie)? welke rechtstreekse/onrechtstreekse kosten?

DE BEWIJSKRACHT IN RECHTE

Naast de geldigheid van het document gaat het er vaak om aan te tonen dat de handtekening betrouwbaar is en dat het document als bewijs kan worden gebruikt (bewijskracht).

In het geval van een betwisting moet de overheidsdienst kunnen aantonen dat:

- ✓ de ondertekenaar inderdaad de persoon is die de handtekening heeft gezet,
- ✓ de ondertekenaar wel degelijk zijn instemming/beslissing kenbaar heeft gemaakt,
- ✓ het voorgelegde document inderdaad het document is dat is ondertekend (integriteit),
- ✓ de omstandigheden van de ondertekening (datum, bewaarketen) kunnen worden aangetoond.

De eIDAS-verordening voorziet in de erkenning van de elektronische handtekeningen en kent aan bepaalde daarvan een vermoeden van betrouwbaarheid toe. De waarde van het bewijs hangt echter af van de kwaliteit van de beschikbare gegevens (sporen): gebeurtenislogboeken, tijdstempel, actielogboek en een certificaat, evenals van de wijze waarop ze worden bewaard.

Kortom: bij een betwisting telt niet alleen het type handtekening, maar ook het vermogen om met bewijsmateriaal aan te tonen wie heeft ondertekend, wanneer en onder welke omstandigheden.

Waarop letten?

Vraag jezelf bij het kiezen van het juiste type handtekening voor de desbetreffende procedure ook af welk bewijsmateriaal kan worden overgelegd als de handtekening wordt betwist, en zorg ervoor dat dit bewijsniveau in verhouding staat tot het belang van het document.

NUANCES EN VERDUIDELIJKINGEN VAN BEGRIPPEN

ONTHOUD VOORAL:



Hanteer de juiste reflex en vraag u af wat u moet kunnen bewijzen: instemming, identiteit, integriteit, datum of iets anders? Als het risico beperkt is, kan een validatie volstaan. Is het risico groter, dan verdient een handtekening (en een versterkte bewaring) de voorkeur.



In de praktijk worden meerdere termen door elkaar gebruikt: ondertekenen, valideren van een visum voorzien, paraferen, medeondertekenen... terwijl ze niet verwijzen naar dezelfde juridische gevolgen noch naar dezelfde bewijsvereisten. De onderscheiden die hieronder worden gemaakt zullen je helpen om de juiste handeling te kiezen (handtekening of gewone validering), te begrijpen wat dit bewijst en de bewaring van het document te organiseren.

VALIDERING OF HANDTEKENING?

Validering: handeling waarmee een persoon bevestigt dat een document “naar de volgende fase kan” (nalezing afgerond, interne goedkeuring, groen licht). Een validering kan de vorm aannemen van een klik, een status in een workflow, een e-mail, een ticket, een login, enz.

Handtekening: handeling waardoor een persoon zich ergens toe verbindt (beslissing, toestemming, instemming met de inhoud) en die het mogelijk maakt het document toe te schrijven aan een geïdentificeerde ondertekenaar, met een sterke verwachting inzake de integriteit van het ondertekende document.

✗ **Veelvoorkomende fout:** een “validering” gebruiken (bv. gewoon een login) terwijl er bij een betwisting moet kunnen worden aangetoond wie de beslissing heeft genomen, op basis van welk document en op welke datum..

HANDTEKENING, VISUM OF MEDEONDERTEKENING?

Visum: merkteken van onderzoek of controle (bv. begrotingsvisum, juridisch visum). Het visum toont over het algemeen aan dat er een controlefase heeft plaatsgevonden, zonder noodzakelijkerwijs de definitieve beslissing uit te drukken.

Medeondertekening: “aanvullende” handtekening bovenop de hoofdhandtekening (bv. als bewijs voor een controle, gedeelde verantwoordelijkheid of de tussenkomst van een andere overheidsinstantie). Naargelang het geval kan de medeondertekening een specifieke juridische betekenis hebben.

Handtekening: handeling waardoor de bevoegde overheid de beslissing neemt of de verbintenis uitdrukt in naam van de administratie.

✗ **Veelvoorkomende fout:** een visum behandelen als een handtekening (of omgekeerd), terwijl de verantwoordelijkheden en verwachte bevoegdheid niet dezelfde zijn.

HANDTEKENING OF PARAAF?

Paraaf: kort merkteken (vaak initialen) aangebracht op een pagina, over het algemeen om aan te geven dat ze is gelezen/gevalideerd, of om het risico te beperken dat pagina's verwisseld worden in een dossier.

Handtekening: (handgeschreven of elektronisch) merkteken dat de ondertekenaar identificeert en zijn verbintenis/instemming met de inhoud concretiseert.

LOGIN, KLIK, PARAAF?

Login/gebruikersaccount: kan aantonen dat een account een handeling heeft verricht, maar niet altijd welke persoon achter het scherm zat (gedeeld account, gestolen inloggegevens, geen tweestapsverificatie).

Goedkeuringsklik: nuttig in een intern proces, op voorwaarde dat het systeem sporen (wie, wat, wanneer) bewaart en dat de toegangsrechten goed worden beheerd.

Paraaf: nuttig om een papieren dossier pagina per pagina "vast te leggen", maar garandeert de identiteit niet met dezelfde bewijskracht als een handtekening.

GEFOTOKOPIEERDE, GESCANDE OF ORIGINELE HANDTEKENING?

Originele handgeschreven handtekening: handtekening die fysiek is aangebracht door de persoon op het papieren document.

Gescande of gekopieerde handtekening: de afbeelding van de handtekening bewijst op zichzelf niet dat de persoon daadwerkelijk heeft ondertekend of dat het document niet is gewijzigd.

Niet te verwarren met een (geavanceerde of gekwalificeerde) elektronische handtekening: een geavanceerde of gekwalificeerde elektronische handtekening berust op een proces dat beoogt een ondertekenaar te koppelen aan het document en de integriteit te garanderen, wat bij een afbeelding niet het geval is. Een afbeelding die op een document is aangebracht, vormt een eenvoudige elektronische handtekening, ze bindt de ondertekenaar niet op een veilige manier aan het document en garandeert evenmin de integriteit van het document.

✗ **Veelvoorkomende fout:** geloven dat een pdf met een afbeelding van een handtekening "geldt als een handtekening". Bij een betwisting zijn aanvullende bewijsmiddelen nodig (processen, e-mails, sporen, enz.), die vaak zwakker zijn dan een systeem voor elektronische handtekeningen.



ONTHOUD VOORAL:

Een paraaf vervangt de handtekening niet wanneer die is vereist. Een paraaf heeft een praktisch nut, maar de juridische betekenis en bewijskracht ervan zijn beperkter.



ONTHOUD VOORAL:

Als er wordt gekozen voor een validering in plaats van een handtekening, is het nuttig de risicoanalyse te documenteren en indien nodig de identificatie (bv. sterke authenticatie), traceerbaarheid (auditlogboek) en bewaring op te krieken.



ONTHOUD VOORAL:

De afbeelding van een handtekening koppelt de ondertekenaar niet op een betrouwbare manier aan het document



ONTHOUD VOORAL:

Goede reflex: ga voor je procedure na welke versie rechtsgeldig is (wat is het origineel) en hoe de overheid dit op lange termijn kan aantonen.

AUTHENTIEKE AKTE, AUTHENTICITEIT WAT BETREFT DE BEWARING EN HET ORIGINEEL

WAT IS EEN "AUTHENTIEK" AKTE?

In juridische zin is een authentieke akte een document dat door een bevoegde openbare ambtenaar⁵ (bv. een notaris) is ontvangen (of opgesteld), volgens nauwkeurige door de wet bepaalde regels. Het gaat dus om een specifiek juridisch begrip en niet zomaar om een document dat als "betrouwbaar" wordt beschouwd.

In de zin van de bewaring (documentbeheer/archivering) spreken we veeleer over **authenticiteit**.

Dit betekent dat het document wel degelijk is wat het beweert te zijn, dat het van de juiste bron afkomstig is en dat het bewaard is zonder onopspoorbare wijzigingen (traceerbaarheid, integriteit, bewaarketen).

WAT IS EEN "ORIGINEEL"?

Papieren origineel: papieren document dat de originele versie vormt, eventueel met de hand ondertekend.

Elektronisch origineel: digitale versie waarvan de integriteit en herkomst gewaarborgd zijn (handtekening, tijdstempel, bewaring). Het is deze versie die "rechtsgeldig" is.

Hybride origineel: dossier dat papier en digitale elementen combineert (bv. een document dat op papier is ondertekend en vervolgens is ingescand). In dat geval is het moeilijk om duidelijk vast te stellen welke versie als het origineel wordt beschouwd.

X Veelgemaakte fout: denken dat documenten die door ambtenaren zijn opgesteld, authentieke akten zijn. In werkelijkheid zijn alleen bepaalde documenten die zijn opgesteld door aangewezen openbare ambtenaren (notarissen, gerechtsdeurwaarders, enz.) authentieke akten (bijvoorbeeld koop- en verkoopakten of akten van de burgerlijke stand (geboorteakte, huwelijksakte, enz.)). Overheidsambtenaren kunnen bestuurlijke akten opstellen, waarvoor een eigen regeling geldt. Wij raden je aan om contact op te nemen met je juridische diensten om de juridische status van elk opgesteld document te bepalen en te achterhalen welke wettelijke regeling van toepassing is.

5. Een openbaar ambtenaar is een overheidsfunctionaris, maar niet elke overheidsfunctionaris is een openbaar ambtenaar. Deze verantwoordelijkheid is bij wet vastgelegd

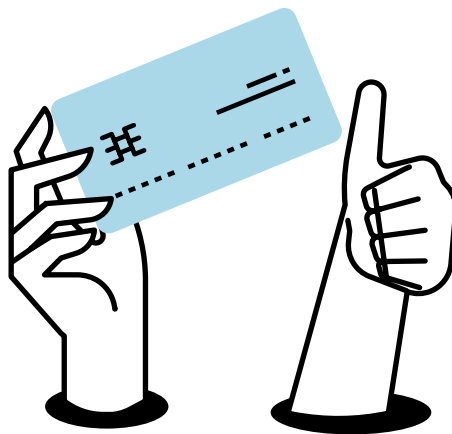
VALSHEID IN GESCHRIFTE

Een valsheid in geschrifte is een strafbaar feit dat met name slaat op de frauduleuze aanmaak, wijziging of aanwending van een schriftelijk document met de bedoeling te misleiden.

Enkele voorbeelden zijn: wijziging van de inhoud, een valse handtekening, identiteitsfraude, vervanging van pagina's, antidatering, enz.

Wat heeft dit met de handtekening te maken?

- › Hoe gevoeliger het document is, hoe groter de behoefte is aan een mechanisme dat elke wijziging opspoorbaar maakt. Het maakt het ook mogelijk om het document aan de ondertekenaar te koppelen.



ONTHOUD VOORAL:

Denk in termen van een “vertrouwensketen”: wie heeft toegang tot het document? Wie kan het wijzigen, goedkeuren of ondertekenen? Welke bewijsstukken worden bewaard? Waar en hoe wordt het origineel gearhiveerd?

TECHNOLOGISCHE OPLOSSINGEN

VOOR DE BURGERS

Voor een burger betekent elektronisch ondertekenen meestal dat hij een online procedure of document bevestigt. Dit kan met behulp van een digitaal identificatiemiddel (elektronische identiteitskaart, itsme® of iets dergelijks).

Er bestaan meerdere technologische oplossingen, die niet allemaal dezelfde mate van zekerheid bieden (identificatie van de ondertekenaar, detectie van wijzigingen, bewijs in geval van betwisting).

De keuze hangt dus af van verschillende factoren: de aard van het document, de risico's die aan het gebruik ervan zijn verbonden, het vereiste bewijsniveau, maar ook het gebruiksgemak en de toegankelijkheid van de tool.

VOOR OVERHEIDSBESTUREN

Er bestaan talrijke oplossingen om een elektronisch document te ondertekenen (of te valideren). Sommige nemen de vorm aan van ondertekeningsplatformen die in administratieve processen zijn geïntegreerd (goedkeuringstrajecten, seriële ondertekening, opvolging van de dossiers), terwijl andere meer specifieke functies bieden, zoals authenticatie, tijdstempels, elektronische verzegeling of het bewaren van bewijsmateriaal.

De markt verandert snel en de behoeften verschillen van de ene overheidsinstantie tot de andere (documentvolume, gebruikersprofiel, technische beperkingen, beveiligingsbeleid, enz.).

ONTHOUD VOORAL:



Neem de juiste reflex aan: het gebruik van een digitale technologie is soms moeilijk toegankelijk voor personen die met een digitale kloof worden geconfronteerd. Ga daarom na of een gekwalificeerde handtekening echt noodzakelijk is. Is dat het geval, denk dan ook aan een fysiek alternatief.



Raadpleeg de praktische fiche
"Welke technologische tool moet je gebruiken?"

Met het oog op de technologische neutraliteit* geven we geen voorkeur aan een specifieke oplossing. Het gaat er in de eerste plaats om ervoor te zorgen dat de gekozen oplossing voldoet aan de behoeften van de overheid en garanties biedt op het gebied van:

- de identificatie en de authenticatie van de ondertekenaars;
- de integriteit van de documenten;
- de traceerbaarheid van de uitgevoerde acties;
- de bewijskracht in geval van een betwisting;
- de bewaring van documenten en het bijbehorend bewijsmateriaal.



Alvorens een oplossing te kiezen, is het dus belangrijk om je behoeften in kaart te brengen:

- ✓ Welke soorten documenten moet je ondertekenen? En welk ondertekeningsniveau is daarvoor vereist?
- ✓ Wie zijn de personen die moeten ondertekenen, en welke rol zullen zij vervullen?
- ✓ Zijn de kosten van de oplossing duidelijk aangegeven en onder controle?
- ✓ Is de oplossing gebruiksvriendelijk, zowel voor de personeelsleden als voor de gebruikers?
- ✓ Kan ze in de interne tools en processen worden geïntegreerd?
- ➡ Gebruik de beslissingsboom of de praktische fiche om na te gaan welk type handtekening vereist is.

*Principe van technologische neutraliteit: geen voorkeur geven aan een specifieke technologie, product, leverancier of drager, maar de verwachte resultaten of functionaliteiten bepalen en de administraties de meest geschikte oplossing laten kiezen.



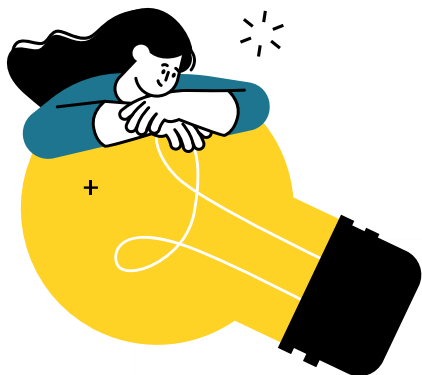
AANDACHTSPUNT

Elke technologie brengt kosten met zich mee: licenties en exploitatie, kosten per handtekening, ondersteuning, opleiding en integratie (connectoren, API's, koppelingen met applicaties of met elektronische archivering). Het gebruik van een gekwalificeerde elektronische handtekening vereist de tussenkomst van een gekwalificeerde dienstverlener, wat de keuzemogelijkheden kan beperken en de kosten kan verhogen. Indien het wettelijke kader of de context geen gekwalificeerde elektronische handtekening oplegt, overweeg dan andere soorten handtekeningen of zelfs een alternatieve vorm van validatie (binnen een proces, akkoord via een interne tool, authenticatiemechanisme/login).



ONTHOUD VOORAL:

Hanteer de juiste reflex: nadat u uw behoeften hebt bepaald, verzamel dan informatie over de oplossingen die andere administraties gebruiken. Ook de gewestelijke administraties voor IT- en technologische ondersteuning kunnen u helpen bij deze keuze.



PRAKTISCHE FICHES



Deze praktische fiches zijn bedoeld om snel antwoord te geven op een aantal specifieke en veelgestelde vragen.

1. **Moet het document worden ondertekend?**
2. **De 3 types van elektronische handtekening**
3. **Welk soort handtekening moet je gebruiken?**
4. **Hoe lang is een elektronische handtekening geldig?**
5. **Hoe archiveer je een elektronisch ondertekend document?**
6. **Welke technologische tool moet je gebruiken?**
7. **Verzenden en afdrukken van een elektronisch ondertekend document**
8. **Meerdere handtekeningen**
9. **Bulkondertekening**
10. **Kan ik een document na de ondertekening wijzigen? (inhoud of tijdstempel)**

1. Moet het document worden ondertekend?

In het kader van de administratieve vereenvoudiging is het zinvol om stil te staan bij het werkelijke nut van de handtekening. Stel jezelf, voordat je een document ondertekent, deze eenvoudige vraag: is de handtekening echt nodig? In veel gevallen is die niet onmisbaar: een validering volstaat.

Handtekening of validering?

- Een **handtekening** verbindt een persoon, bevestigt een instemming of een beslissing en heeft een juridische waarde.
- Een **validering** houdt een goedkeuring in (een "ok"), wordt vaak gebruikt in een intern proces en houdt niet altijd een juridische verbintenis in.

Voorbeelden van een validering: via e-mail "ok" antwoorden, of in een digitale tool op "goedkeuren" klikken.

Veelvoorkomende gevallen waarin een handtekening NIET nodig is

Veel documenten worden "uit gewoonte" ondertekend, terwijl dat niet nodig is: interne nota's, eenvoudige HR-valideringen, uitwisselingen tussen collega's, documenten zonder juridische gevolgen. In die gevallen volstaat een validering.

3 vragen die je jezelf moet stellen

1. Leidt het document tot een recht, een verplichting of een beslissing?

- **Ja:** een handtekening is vereist.
- **Nee:** vaak volstaat een validering.

2. Moet het document als bewijs dienen als er een probleem ontstaat?

- **Ja:** de ondertekening is aanbevolen.
- **Nee:** de validering is mogelijk.

3. Is dit een wettelijke of interne vereiste?

- **Ja:** respecteer het gevraagde type handtekening.
 - **Nee:** pas dit aan in functie van de behoefte; een goedkeuring kan volstaan.
- ✓ *Voor meer informatie over deze keuze, raadpleeg de beslissingsboom op pagina 13 van de referentiegids.*

Praktische fiche

De elektronische handtekening



TE ONTHOUDEN

- ✓ De ondertekening gebeurt niet automatisch.
- ✓ De handtekening mag alleen worden gebruikt wanneer dat nodig is.
- ✓ Vaak volstaat een validering al, wat de procedures vereenvoudigt.

DE JUISTE REFLEX

Stel jezelf altijd de vraag: wat moet ik kunnen aantonen?

- ✓ een formeel akkoord = **een handtekening**
- ✓ een gewoon groen licht of een kennisneming = **een validering**

2. De 3 types van elektronische handtekening (EH)

Niet alle handtekeningen bieden hetzelfde beveiligingsniveau. Er bestaan 3 types, die moeten worden gebruikt afhankelijk van het risico en het belang van het te ondertekenen document.

Eenvoudige EH

Een gebruiksvriendelijke manier van ondertekenen, waarvoor geen speciale technologie nodig is en die weinig juridische uitdagingen met zich meebrengt.

Voorbeelden: online aan te vinken vakje, ondertekening van een e-mail, afbeelding van een gescande handtekening.

- ✓ **Het wordt gebruikt voor** het ondertekenen van interne documenten, eenvoudige aanvragen, zonder dat er echte juridische uitdagingen aan verbonden zijn.

💡 **Goed om te weten:** het beveiligingsniveau ervan is beperkt en het risico op betwisting is groter.

Geavanceerde EH

Hiermee kan de ondertekenaar duidelijk worden geïdentificeerd en wordt gewaarborgd dat het document na de ondertekening niet is gewijzigd.

Voorbeelden: ondertekening via een sms-code (OTP), via een app of op bepaalde onlineplatformen.

- ✓ **Dit wordt gebruikt voor** het ondertekenen van belangrijke documenten of administratieve procedures met een matig risico.

💡 **Goed om te weten:** geavanceerde handtekeningen bieden een goed evenwicht tussen veiligheid en gebruiksgemak. Deze handtekening vereist een specifiek hulpmiddel en wordt niet systematisch aangeboden binnen de overheidsinstanties.

Gekwalificeerde EH

Het hoogste beveiligingsniveau, dat volgens het Europese recht gelijkstaat aan een handgeschreven handtekening. **Ze wordt gevalideerd door een certificaat dat de integriteit van het document en de identiteit van de ondertekenaar garandeert.**

Voorbeelden: ondertekenen met een elektronische identiteitskaart, itsme® of een ander soort van gekwalificeerd certificaat.

- ✓ **Dit wordt gebruikt voor** gevoelige documenten en officiële beslissingen te ondertekenen, in situaties met een hoog juridisch risico, of gewoon wanneer de wet dit voorschrijft.

💡 **Goed om te weten:** dit niveau is complexer om te implementeren en kan kosten met zich meebrengen en het gebruik van een specifieke tool vereisen.

Praktische fiche

De elektronische handtekening

Beginsel	Eenvoud.	Geavanc.	Gekwali.
Identificatie	-	✓	✓
Integriteit	-	✓	✓
Non-discriminatie	✓	✓	✓
Onweerlegbaarheid	-	✓	✓
Certificering	-	-	✓



TE ONTHOUDEN

- ✓ Hoe hoger het beveiligingsniveau, hoe betrouwbaarder de handtekening... maar ook hoe veeleisender en duurder.
- ✓ De keuze van het ondertekenningsniveau moet worden afgestemd op de context en het risiconiveau van je document.

DE JUISTE REFLEX

Gebruik de fiche 'Welk type handtekening kiezen?' als hulpmiddel, evenals de beslissingsboom op pagina 13 van de referentiegids.

3. Welk soort handtekening moet je gebruiken?

De keuze van het handtekeningniveau (eenvoudig, geavanceerd of gekwalificeerd) hangt af van het risiconiveau en het belang van het document. Hoe hoger het risico, hoe hoger het handtekeningniveau ook moet zijn.

Om het risico of de risico's te beoordelen, moet je de volgende vragen analyseren:

Heeft het document rechtsgevolgen?

Leidt dit tot rechten of verplichtingen?

Nee ► een **eenvoudige** handtekening volstaat.

Ja ▼

Heeft het document betrekking op of zijn er derden bij betrokken?

Heeft het gevolgen buiten je organisatie, is er een andere partij (persoon, organisatie, enz.) bij betrokken?

Nee ► kies voor een **eenvoudige** of **geavanceerde** handtekening.

Ja ▼

Bestaat er een risico dat er beroep wordt aangetekend of op een betwisting?

Zou het document in twijfel kunnen worden getrokken?

Nee ► kies voor een geavanceerde handtekening (indien beschikbaar).

Ja ► kies voor een **gekwalificeerde** handtekening.



Praktische fiche

De elektronische handtekening

	Wanneer gebruiken?
eenvoudige	Interne documenten, beperkt belang
geavanceerde	Belangrijke documenten, matig risico.
gekwalificeerde	Gevoelige documenten, hoog risico, wettelijke verplichting. = identiteit en integriteit kunnen aantonen.



TE ONTHOUDEN

- ✓ Als het type van handtekening door een reglementering wordt opgelegd, leef dit dan na.
- ✓ Een sterkere handtekening garandeert meer veiligheid, maar houdt ook meer beperkingen in (kosten, complexiteit).
- ✓ Een gekwalificeerde handtekening is niet altijd de beste keuze, ze mag alleen worden gebruikt als dat nodig is.

DE JUISTE REFLEX

Vraag jezelf af wat de risico's zijn als dit document wordt betwist, want dat bepaalt welk ondertekeningsniveau geschikt is.

4. Hoe lang is een elektronische handtekening geldig?

Kan een document dat moet worden ondertekend en gedurende meerdere jaren moet worden bewaard, elektronisch worden ondertekend? Heeft de elektronische handtekening een beperkte geldigheidsduur?

De geldigheidsduur van een elektronische handtekening hangt niet af van de handtekening zelf, maar wel van die van de elementen waarmee die kan worden gecontroleerd:

- het certificaat dat aan de handtekening is gekoppeld en dat op het moment van ondertekening geldig moet zijn;
- het bewijs of de bewijzen van de integriteit van het document: een betrouwbare tijdstempel, een verzegeling, enz.

Een handtekening vervalt niet automatisch, ze blijft geldig zolang de bewijsstukken waarmee ze kan worden gevalideerd, worden bewaard!

Een elektronisch ondertekeningscertificaat heeft een beperkte geldigheidsduur. Zodra het certificaat is verlopen, is het niet meer mogelijk om nieuwe handtekeningen met datzelfde certificaat aan te brengen, maar de reeds aangebrachte handtekeningen blijven geldig zolang je kan aantonen dat:

- ✓ ze zijn aangemaakt tijdens de geldigheidsduur van het certificaat,
- ✓ het document niet werd aangepast.

Het belangrijkste is dus dat het certificaat geldig is op het moment van ondertekening.

Hoe kan ik de geldigheidsduur van een handtekening verlengen?

Om de geldigheid over meerdere jaren of decennia te waarborgen, wordt vaak gebruikgemaakt van:

- de gekwalificeerde tijdstempel;
- de wettelijk conforme elektronische archivering (zoals vastgelegd in de Belgische wet van 21 juli 2016).

Dankzij deze mechanismen blijft de bewijskracht behouden, zelfs nadat het certificaat is verlopen.

Praktische fiche

De elektronische handtekening



TE ONTHOUDEN

- ✓ Een elektronische handtekening heeft geen vaste geldigheidsduur. Het certificaat verloopt, niet de aangebrachte handtekening.
- ✓ Je handtekening blijft geldig zolang je de authenticiteit ervan en de integriteit van het document kunt aantonen.

DE JUISTE REFLEX

Bewaar alle bewijsstukken waarmee je kunt aantonen dat je handtekening geldig was op het moment dat deze werd gezet. Raadpleeg de fiche "Hoe archiveer je een elektronisch ondertekend document?" voor meer informatie!

5. Hoe archiveer je een elektronisch ondertekend document?

Om ervoor te zorgen dat een elektronisch ondertekend document, in het bijzonder met een gekwalificeerde elektronische handtekening, zijn geldigheid op lange termijn behoudt, moet het onder goede omstandigheden worden bewaard om elke wijziging te voorkomen.

De juiste reflexen:

1. Bewaar het origineel (digitaal of op papier) en voorkom dat er ongecontroleerde kopieën in omloop raken:

- Het afdrukken van een digitaal origineel is een kopie, net als het scannen van een origineel op papier. (tenzij er gebruik wordt gemaakt van een gekwalificeerde archiveringsdienst.)
- Bij een hybride document moeten beide formaten worden bewaard.

2. Bewaar de bewijsstukken die de controle mogelijk maken: het ondertekende document, de handtekening en de bijbehorende technische bewijsstukken (tijdstempel, certificaat, enz.).

3. "Verbreek" de handtekening niet: bepaalde verrichtingen (opnieuw opslaan, opnieuw omvormen, "afdrukken als pdf") kunnen de handtekenemechanismen ongeldig maken of nuttige bewijsgegevens verloren doen gaan.

4. Houd rekening met de duur: de door de meeste aanbieders van elektronische handtekeningen aangeboden bewaartermijnen zijn beperkt. Als deze bewaartermijn niet volstaat, archiveer de documenten dan in je eigen elektronische archiefsysteem.

5. Om een gekwalificeerde elektronische handtekening te bewaren, moet je gebruikmaken van een gekwalificeerde archiveringsdienst om de rechtsgeldigheid van de handtekening te behouden.

Als je de geldigheidsduur van een gekwalificeerde elektronische handtekening wilt verlengen:

- **Elektronische archivering met bewijskracht:** een opslagsysteem waarmee een digitaal document op lange termijn als betrouwbaar bewijs kan worden bewaard, als een gecertificeerde digitale "kluis".
- **De opvolgende ondertekening:** door een nieuwe handtekening of een nieuw tijdstempel toe te voegen, blijft het bewijs in de loop van de tijd behouden.

Praktische fiche

De elektronische handtekening

Gewestelijke dienstverleners

Twee dienstverleners zijn belast met het bewaren van zowel de papieren als de elektronische documenten van de Brusselse overheidsdiensten.

Op gewestelijk niveau:

ConnectMemory, de Gewestelijke Archiefdienst
✉ connectmemory@gob.brussels

Op lokaal/gemeetelijk niveau:

Algemeen Rijksarchief
✉ algemeen.rijksarchief@arch.be



TE ONTHOUDEN

- ✓ Een elektronisch ondertekend document bestaat uit: het document + de handtekening + de bewijzen van de handtekening.
- ✓ Een goede archivering is onontbeerlijk om de juridische geldigheid van je document te behouden.

DE JUISTE REFLEX

Stel jezelf altijd de vraag: zal ik over 5 of 10 jaar nog kunnen aantonen dat het document geldig is?

6. Welke technologische tool moet je gebruiken?

Er bestaan talrijke tools voor elektronische handtekeningen. Met het oog op de technologische neutraliteit en omdat de behoeften per overheidsdienst verschillen, wordt in deze fiche geen voorkeur uitgesproken voor een welbepaald hulpmiddel. De keuze hangt af van je behoeften, die je met behulp van deze checklist kunt vaststellen.

Behoeften

- ☐ Welke soorten van documenten moet je ondertekenen?
- ☐ Wie moet er (intern of extern) ondertekenen?
- ☐ Welke ondertekeningsniveaus zijn vereist voor de verschillende soorten van documenten?

Functionaliteiten

- ☐ Ondersteunt de oplossing de verschillende ondertekeningsniveaus die door de eIDAS-verordening worden vereist?
- ☐ Is ze compatibel met je interne tools?
- ☐ Is ze compatibel met andere digitale ID-aanbieders (bv. itsme®)?
- ☐ Maakt ze het mogelijk om documenten in bulk te ondertekenen en/of te uploaden?
- ☐ Moet je alle pagina's of alle documenten doorlezen voordat je tekent?
- ☐ Biedt ze de mogelijkheid om een ondertekeningsstroom te beheren (volgorde van ondertekenaars, wijziging bij afwezigheid, enz.)?
- ☐ Kan ze op een gsm worden gebruikt?
- ☐ Is integratie met andere systemen (API) mogelijk?
- ☐ Kan ze worden gepersonaliseerd?

Gebruikerservaring

- ☐ Is de oplossing eenvoudig in gebruik?
- ☐ Kunnen externe personen hiermee gemakkelijk ondertekenen?
- ☐ Heeft ze een helpdesk?

Beveiliging en conformiteit

- ☐ Voldoet ze aan de vereisten van de AVG¹?
- ☐ Garandeert ze de identificatie, de integriteit en de traceerbaarheid?

Archivering

- ☐ Voorziet ze in een passende archivering?
- ☐ Hoe lang worden de documenten bewaard?
- ☐ Maakt ze het mogelijk om API te gebruiken in combinatie met je interne archiveringssystemen?

Organisatie en kosten

- ☐ Zijn de kosten duidelijk geïdentificeerd?
- ☐ Moet het personeel een opleiding krijgen over de oplossing?

1 - Algemene Verordening Gegevensbescherming: Europese regelgeving die het kader vormt voor de verwerking en het vrije verkeer van persoonsgegevens.

Praktische fiche

De elektronische handtekening



TE ONTHOUDEN

- ✓ De gekozen oplossing moet aansluiten bij je interne behoeften, die eerst in kaart moeten worden gebracht.
- ✓ De juiste tool moet zowel het bewijs van de handtekening als de veiligheid van je documenten garanderen.
- ✓ Voordat je een bestaande procedure digitaliseert, moet je ervoor zorgen dat deze zo goed mogelijk aansluit bij de verwachtingen en behoeften van de gebruikers. easy.brussels kan je daarbij helpen.

DE JUISTE REFLEX

Bepaal eerst wat je behoeften zijn voordat je een geschikt hulpmiddel kiest. Informeer bij instellingen die vergelijkbaar zijn met die van jou om te horen wat hun ervaringen zijn.

7. Verzenden en afdrukken van een elektronisch ondertekend document

Wanneer een document met een gekwalificeerde elektronische handtekening wordt ondertekend, wordt er automatisch een certificaat aan gekoppeld. Afhankelijk van de gebruikte software verschijnt er een visuele vermelding op het document (bijvoorbeeld: een afbeelding of de tekst "Ondertekend (eID) op xx-xx-xx door Xavier Dupont"). Deze vermelding heeft op zich geen juridische waarde, maar biedt met één muisklik toegang tot het certificaat.

Kan een elektronisch ondertekend document via e-mail, eBox of een ander digitaal kanaal worden verzonden?

Ja. Zolang het document in elektronische vorm blijft bestaan, blijft de gekwalificeerde handtekening eraan gekoppeld. De wettelijke waarde ervan blijft ongewijzigd, aangezien het certificaat nog steeds ter verificatie kan worden gedownload.

Kan een elektronisch ondertekend document worden afgedrukt?

Als je elektronisch ondertekend document moet worden afgedrukt (bijvoorbeeld als de ontvanger geen toestemming heeft gegeven om e-mails via eBox te ontvangen), blijft de vermelding "Ondertekend op xx door xx" zichtbaar, maar verliest deze haar juridische geldigheid, aangezien er niet op kan worden geklikt. Het zal niet langer mogelijk zijn om het bijbehorende certificaat te downloaden, de handtekening online te traceren om de geldigheid ervan te controleren (wie heeft het ondertekend en wanneer?), of aan te tonen dat het document niet is gewijzigd.

Een document dat elektronisch is ondertekend en vervolgens is afgedrukt, wordt juridisch als een "kopie" beschouwd. Het origineel blijft het elektronische bestand.

Om ervoor te zorgen dat je handtekening geldig blijft, kan je het volgende doen:

- ✓ **Voeg onderaan de pagina een downloadlink** voor het document toe (controleregel) en geef aan hoe lang het beschikbaar blijft. Deze "controleregel" wordt doorgaans voorzien door speciale applicaties of platformen. Zorg ervoor dat er voldoende tijd is zodat de ontvanger het document kan bekijken of downloaden (minimaal enkele maanden).
- ✓ Geef de ontvanger de mogelijkheid om contact op te nemen met de overheidsdienst om **een kopie van het originele document** te verkrijgen of te raadplegen.
- ✓ Indien je technologische oplossing niet de mogelijkheid biedt om het document online te controleren of te downloaden, voeg dan een meer **algemene vermelding** toe, zoals: "De handtekening op dit document is door onze administratie gecertificeerd via een door de FOD BOSA erkend systeem"



TE ONTHOUDEN

- ✓ Een elektronische handtekening moet online kunnen worden getraceerd om geldig te blijven.

DE JUISTE REFLEX

Zorg er altijd voor dat er een link is om het originele document te raadplegen en/of te downloaden, of vermeld dat het origineel op verzoek beschikbaar is.

8. Meerdere handtekeningen

Het begrip “meervoudige ondertekening” houdt in dat één ondertekenaar meerdere pagina’s ondertekent, of dat één document door meerdere personen wordt ondertekend.

Moeten alle pagina’s van een document worden ondertekend of geparafeerd?

Nee. Eén enkele handtekening, ongeacht het niveau ervan, volstaat om de ondertekenaar te binden aan het gehele document, ongeacht de lengte ervan. Het is dus niet nodig om elke pagina te paraferen!

Kan één en hetzelfde document door meerdere personen worden ondertekend?

Ja. Om de geldigheid van alle handtekeningen te waarborgen, wordt aanbevolen om alle ondertekenaars in één en hetzelfde ondertekeningsproces te betrekken. Met oplossingen voor elektronische handtekeningen is het doorgaans mogelijk om meerdere ondertekenaars toe te voegen, de ondertekeningsvolgorde vast te leggen, de voortgang van het proces op te volgen en de juridische geldigheid van elke handtekening te waarborgen.

Voordat het document wordt verzonden, is het handig om het volgende vast te stellen:

- ✓ de ondertekenaars: achternaam, voornaam, e-mailadres, rol (ondertekenaar, goedkeurder, waarnemer);
- ✓ de ondertekeningsvolgorde:
 - ➡ sequentieel: eerst A, dan B, dan C... ideaal voor bijvoorbeeld contracten,
 - ➡ tegelijkertijd: iedereen kan het document ondertekenen na ontvangst... ideaal voor interne documenten;
- ✓ de velden die moeten worden ingevuld (velden waar elke persoon moet ondertekenen);
- ✓ de authenticatiemethodes.

Opgelet: elke wijziging aan of of herintroductie van een reeds ondertekend document maakt de bestaande handtekeningen ongeldig.

Wanneer meerdere personen niet binnen hetzelfde ondertekeningsproces kunnen tekenen, ondertekent elke persoon zijn of haar eigen versie. Al deze versies moeten samen worden bewaard.

De handtekeningsvermeldingen zijn louter indicatief! Alleen het handtekeningscertificaat heeft juridische waarde.



TE ONTHOUDEN

- ✓ Eén handtekening volstaat om de ondertekenaar aan het gehele document te binden.
- ✓ Het is heel goed mogelijk om één en hetzelfde document door meerdere personen te laten ondertekenen.

DE JUISTE REFLEX

Stel jezelf de juiste vragen: wie moet je document ondertekenen? Is de volgorde van de handtekeningen belangrijk?

9. Bulkondertekening

Om tijd te besparen, is het mogelijk om meerdere documenten tegelijk elektronisch te ondertekenen. Afhankelijk van de gebruikte oplossing voor elektronische handtekeningen is het mogelijk om:

Meerdere documenten in één keer te ondertekenen (bulkondertekening)

Met bepaalde softwareprogramma's kun je automatisch een gecertificeerde elektronische handtekening op meerdere documenten tegelijk aanbrengen. De ondertekenaar zal de transactie slechts één keer bevestigen via zijn certificaat, zijn eID-kaart of zijn token.

Ook al ondertekent de gebruiker maar één keer, toch genereert het systeem evenveel digitale handtekeningen als er documenten zijn:

- ✓ elk document krijgt een unieke digitale vingerafdruk (hash) toegewezen die de integriteit van het document waarborgt;
- ✓ elke afdruk bevat het certificaat van de ondertekenaar (identificatie van de ondertekenaar);
- ✓ elk bestand kan afzonderlijk worden geverifieerd (onweerlegbaarheid).

Elk document wordt afzonderlijk ondertekend met een rechtsgeldige handtekening.

✗ Je mag nooit een .zip-bestand ondertekenen!

Het ondertekenen van een .zip-bestand geeft de documenten die het bevat geen enkele juridische waarde. Een .zip-bestand kan worden vergeleken met een envelop die meerdere documenten bevat: het ondertekenen van de envelop betekent niet dat men de documenten die erin zitten ook heeft ondertekend.

Meerdere documenten achtereenvolgens ondertekenen tijdens één sessie.

Met bepaalde softwareprogramma's kun je meerdere documenten achter elkaar ondertekenen: nadat je een eerste document hebt ondertekend, biedt het platform automatisch het volgende document aan

Meerdere documenten bundelen in één ondertekeningverzoek.

Er bestaan oplossingen waarmee je één verzoek kunt versturen dat meerdere documenten bevat die moeten worden ondertekend. De ondertekenaars kunnen vervolgens alle documenten in één werkstroom doorlopen en ondertekenen.



TE ONTHOUDEN

- ✓ Via bulkondertekening kan de ondertekenaar in één enkele handeling een handtekening automatisch op meerdere documenten aanbrengen. Alles hangt af van de gebruikte technologische oplossing.
- ✓ Tijdens een bulkondertekening wordt elk document afzonderlijk ondertekend en kan het afzonderlijk worden gecontroleerd.
- ✓ Onderteken nooit een .zip-bestand: het is een drager, niet het uiteindelijke document.

DE JUISTE REFLEX

Elke oplossing voor elektronische handtekeningen heeft zijn eigen kenmerken. Ga na wat je huidige oplossing te bieden heeft.

10. Kan ik een document na ondertekening wijzigen? (inhoud of tijdstempel)

Kan ik de inhoud van een document na ondertekening wijzigen?

Nee. Ook al is het technisch mogelijk om de inhoud te wijzigen, **toch zou dit de (geavanceerde of gekwalificeerde) handtekening ongeldig maken**, omdat:

- ✓ de cryptografische koppeling tussen de handtekening en het document is verbroken;
- ✓ de controletools zullen aangeven dat het document na ondertekening is gewijzigd.

Een van de functies van de elektronische handtekening is het waarborgen van de integriteit van het document, oftewel het aantonen dat het na ondertekening niet is gewijzigd.

Als er na de ondertekening een wijziging nodig is, is het bij bepaalde bestandsformaten (met name pdf's) mogelijk om een nieuwe elektronische handtekening, een tijdstempel of aantekeningen toe te voegen zonder dat dit invloed heeft op de eerdere handtekeningen. Controleer dus of het formaat en de ondertekeningsprocedure deze wijziging toestaan.

Kan ik de tijdstempel van de elektronische handtekening aanpassen?

Nee. In een correct geïmplementeerd systeem voor elektronische handtekeningen kan de tijdstempel niet worden gewijzigd zonder dat dit wordt opgemerkt.

De tijdstempel is in de handtekening geïntegreerd en is gekoppeld aan een hash van het document op een bepaald moment.

Als we dit zouden wijzigen, zouden we de ondertekende gegevens moeten aanpassen en zouden we dus de integriteit van het document niet meer kunnen garanderen.

De handtekening zou dan ongeldig worden.

Als er een nieuwe tijdstempel nodig is (bijvoorbeeld om de bewijskracht van een handtekening te verlengen of bij elektronische archivering), wordt deze aan het document toegevoegd zonder de oorspronkelijke tijdstempel te vervangen. De oorspronkelijke tijdstempel wordt niet gewijzigd; er wordt een extra tijdstempel toegevoegd en er wordt een spoor van deze bewerking bewaard.

Praktische fiche

De elektronische handtekening



TE ONTHOUDEN

- ✓ Als de inhoud van een elektronisch ondertekend document wordt gewijzigd, wordt de handtekening ongeldig.
- ✓ Elke wijziging van het tijdstempel maakt ook de elektronische handtekening ongeldig.

DE JUISTE REFLEX

Als de inhoud na de ondertekening moet worden gewijzigd (fout, aanvullende informatie, enz.):

- ➡ maak een nieuwe versie van het document aan
- ➡ laat deze nieuwe versie ondertekenen
- ➡ bewaar de oude, ondertekende versie als bewijs of om te archiveren.



WOORDENLIJST

WOORDENLIJST

Aansprakelijkheid: de verplichting voor een natuurlijke persoon of rechtspersoon om verantwoording af te leggen voor zijn handelingen, beslissingen of verbintenissen, en de juridische, administratieve, civielrechtelijke of strafrechtelijke gevolgen daarvan te dragen.

Antidatering: het toekennen van een datum aan een document, akte of handtekening die vóór de werkelijke datum van opstelling, ondertekening of goedkeuring ligt. Bijvoorbeeld: als iemand op 15 maart een document ondertekent, maar bewust de datum 1 maart vermeldt om de indruk te wekken dat de ondertekening eerder heeft plaatsgevonden.

API (Application Programming Interface): een reeks regels, protocollen en functies waarmee verschillende applicaties of computersystemen met elkaar kunnen communiceren en op geautomatiseerde wijze gegevens kunnen uitwisselen. Een platform voor elektronische handtekeningen kan bijvoorbeeld een API gebruiken om automatisch documenten te ontvangen die vanuit een bedrijfsapplicatie moeten worden ondertekend, of een overheidsinstantie kan via een API een dienst voor elektronische handtekeningen in haar documentbeheersysteem integreren.

Archivering: het bewaren, organiseren en beschermen van documenten of gegevens gedurende een bepaalde periode, om de beschikbaarheid, de integriteit, de leesbaarheid en, indien van toepassing, de bewijskracht ervan op lange termijn te waarborgen.

Auditlogboek: technisch overzicht waarin wordt aangetoond hoe en wanneer de handtekening is geplaatst.

Authenticatie: het proces waarmee wordt gecontroleerd of iemand inderdaad is wie hij of zij beweert te zijn.

Authentieke akte: een document dat is opgesteld of bekrachtigd door een openbaar ambtenaar (notaris, ambtenaar van de burgerlijke stand, ...) in het kader van zijn wettelijke bevoegdheden. Het heeft een grotere bewijskracht: de inhoud ervan is rechtsgeldig, tenzij er sprake is van vervalsing, en de datum ervan staat vast. Wanneer het document elektronisch wordt ondertekend, zijn de specifieke wettelijke vereisten van toepassing.

Authenticiteit wat betreft de bewaring: de garantie dat een bewaard document inderdaad het document is dat oorspronkelijk is opgesteld, ontvangen of ondertekend, en dat het gedurende de gehele bewaartermijn op betrouwbare wijze aan de opsteller of de afzender kan worden toegeschreven.

Batch signing (bulkondertekening): een methode waarmee meerdere documenten in één keer elektronisch kunnen worden ondertekend, zonder dat voor elk document afzonderlijk een ondertekeningshandeling hoeft te worden uitgevoerd.

Batchondertekening: methode waarmee meerdere elektronische documenten in één ondertekeningstransactie kunnen worden ondertekend.

Belgische identiteitskaart (eID): officiële elektronische identiteitskaart die door de Belgische autoriteiten wordt afgegeven. Hiermee kan de identiteit van de houder worden aangetoond, zowel persoonlijk als online, dankzij een elektronische chip die digitale certificaten bevat.

Beroep: een procedure waarmee iemand kan verzoeken om de herziening of vernietiging van een beslissing waartegen hij bezwaar maakt.

Bestuurlijke akte: een beslissing, document of maatregel die door een administratieve overheid wordt genomen in het kader van de uitoefening van haar opdrachten van openbare dienstverlening en die rechtsgevolgen heeft voor een of meer personen (bijvoorbeeld: vergunning, toestemming, beslissing tot toekenning of weigering van een premie, enz.)

Bewijskracht: het vermogen van een document, een akte of een bewijsstuk om een feit of een situatie aan te tonen en om in een administratieve of gerechtelijke context als betrouwbaar bewijs te worden erkend.

Biometrische handtekening: een vorm van elektronische handtekening die is gebaseerd op het vastleggen en analyseren van gedragskenmerken van de ondertekenaar tijdens het zetten van zijn handtekening, zoals schrijfsnelheid, uitgeoefende druk, versnelling, de hellingshoek van de stylus of het ritme van de beweging.

Bulkondertekening: een proces waarmee een groot aantal documenten op geautomatiseerde of semigeautomatiseerde wijze elektronisch kan worden ondertekend, zonder dat voor elk document afzonderlijk een ondertekeningshandeling hoeft te worden uitgevoerd.

Burgerlijk geschil: alle geschillen die onder het burgerlijk recht vallen en aan de burgerlijke rechtbanken worden voorgelegd. Het heeft voornamelijk betrekking op geschillen tussen natuurlijke personen of rechtspersonen over rechten en verplichtingen van privaatrechtelijke aard, zoals overeenkomsten, burgerlijke aansprakelijkheid of vermogensrechtelijke verhoudingen. Bijvoorbeeld: een partij betwist de authenticiteit van een document dat als bewijsstuk voor de rechtbank is overgelegd.

Certificering: procedure waarbij een bevoegde instantie verklaart dat een persoon, een product, een dienst, een systeem of een proces aan vastgestelde eisen, normen of criteria voldoet.

Cryptografie: het geheel van wiskundige en IT-technieken waarmee informatie kan worden beveiligd door de vertrouwelijkheid, integriteit, authenticiteit en, in bepaalde gevallen, de onweerlegbaarheid ervan te waarborgen. Wanneer een document bijvoorbeeld elektronisch wordt ondertekend, worden cryptografische mechanismen gebruikt om de handtekening aan te maken en te verifiëren.

Delegatie van ondertekening: handeling waarbij een bevoegde autoriteit een andere persoon machtigt om, in haar naam en binnen vastgestelde grenzen, bepaalde documenten, akten of besluiten te ondertekenen die onder haar bevoegdheid vallen.

Digitaal Brussel: het regelgevingskader van het Brussels Hoofdstedelijk Gewest dat tot doel heeft de digitale transitie van de overheidsdiensten te reguleren, digitale overheidsdiensten te ontwikkelen en de toegankelijkheid, inclusiviteit en beschikbaarheid ervan voor alle gebruikers te waarborgen.

Digitale afdruk (hash): een unieke waarde die met behulp van een cryptografisch algoritme op basis van een document wordt gegenereerd. Hiermee kan de integriteit van een document worden gecontroleerd: als het document wordt gewijzigd, verandert ook de digitale afdruk.

Digitale identiteit: een verzameling van gegevens en elektronische middelen waarmee een persoon op betrouwbare wijze in een digitale omgeving kan worden geïdentificeerd.

Digitalisering: het proces waarbij digitale technologieën worden ingezet om activiteiten, processen, diensten of documenten die voorheen op niet-digitale of gedeeltelijk digitale wijze werden beheerd, te transformeren, te vereenvoudigen of te automatiseren. Een overheidsinstantie vervangt bijvoorbeeld een papieren formulier door een onlineformulier.

Downloadlink: adres of hyperlink waarmee een elektronisch bestand kan worden geraadpleegd, gedownload of op een apparaat opgeslagen.

eIDAS: afkorting van 'electronic IDentification, Authentication and Trust Services'. Dit is de Europese verordening die een gemeenschappelijk rechtskader vaststelt voor elektronische identificatie en vertrouwensdiensten binnen de Europese Unie. Het heeft tot doel de veiligheid, de betrouwbaarheid en de grensoverschrijdende erkenning van elektronische transacties te waarborgen.

Eenvoudige elektronische handtekening: een vorm van elektronische handtekening die bestaat uit elektronische gegevens die door een persoon worden gebruikt om zijn instemming met een document of een transactie te betuigen. Ze hoeft niet te voldoen aan de aanvullende eisen die gelden voor geavanceerde of gekwa-

lificeerde elektronische handtekeningen. De eIDAS-verordening erkent deze als het meest elementaire niveau van de elektronische ondertekening.

Elektronisch certificaat: een soort “digitale identiteitskaart” die wordt gebruikt om elektronisch te ondertekenen. Hiermee kan de identiteit van de ondertekenaar worden gecontroleerd en de handtekening worden beveiligd.

Elektronisch zegel: het digitale equivalent van het stempel van een organisatie. Hiermee kan een bedrijf of overheidsinstantie een document authenticeren, net als bij een elektronische handtekening, maar dan voor een rechtspersoon.

Elektronische archivering met bewijskracht: een archiveringstelsel dat is ontworpen om elektronische documenten zodanig te bewaren dat hun juridische geldigheid op lange termijn behouden blijft.

Elektronische handtekening: een procedure waarmee een digitaal document kan worden ondertekend om de ondertekenaar te identificeren, zijn instemming met de inhoud van het document te bevestigen en het document te beveiligen tegen latere wijzigingen.

Geavanceerde elektronische handtekening: een elektronische handtekening die voldoet aan specifieke eisen, waardoor een betrouwbaar verband met de ondertekenaar kan worden gelegd. Ze moet op eenduidige wijze aan de ondertekenaar zijn gekoppeld, diens identificatie mogelijk maken, zijn aangemaakt met behulp van gegevens waarover de ondertekenaar de exclusieve controle heeft, en zodanig aan het document zijn gekoppeld dat elke latere wijziging kan worden opgespoord.

Gekwalificeerd certificaat: een certificaat dat wordt gebruikt voor gekwalificeerde handtekeningen en dat wordt afgegeven door een erkende dienstverlener.

Gekwalificeerde dienstverlener: een officieel erkende instantie die betrouwbare digitale diensten levert, zoals elektronische handtekeningen of tijdstempels, en daarbij aan de vereisten van de eIDAS-verordening voldoet.

Gekwalificeerde elektronische handtekening: een geavanceerde elektronische handtekening die is aangemaakt met behulp van een gekwalificeerde tool voor het aanmaken van elektronische handtekeningen en die is gebaseerd op een gekwalificeerd certificaat dat is afgegeven door een gekwalificeerde vertrouwensdienstverlener. Dit is het niveau van elektronische ondertekening dat de hoogste waarborgen biedt zoals vastgelegd in de eIDAS-verordening.

Gekwalificeerde tijdstempel: een gecertificeerd mechanisme waarmee op betrouwbare wijze kan worden aangetoond op welke datum en op welk tijdstip een elektronisch document bestond of is ondertekend.

Handgeschreven handtekening: een met de hand aangebrachte handtekening op een papieren document om de auteur te identificeren en aan te geven dat hij of zij akkoord gaat met de inhoud ervan.

Handtekening: een teken dat door een persoon op een document wordt aangebracht om zijn identiteit aan te geven, zijn instemming met de inhoud van het document te bevestigen en, indien van toepassing, zijn verbintenis ten aanzien van de daaruit voortvloeiende rechtsgevolgen.

Hashing (of digitale afdruk): een techniek waarmee op basis van een document een unieke digitale afdruk wordt gegenereerd om te controleren of het document niet werd gewijzigd. Bijvoorbeeld: het systeem berekent de afdruk van het te ondertekenen document voordat er een elektronische handtekening wordt aangemaakt. Als er na de ondertekening ook maar één teken in het document wordt gewijzigd, verandert de hashwaarde, waardoor de wijziging kan worden opgespoord.

Identiteit van de ondertekenaar: alle gegevens aan de hand waarvan de natuurlijke persoon of rechtspersoon die een document heeft ondertekend, op betrouwbare wijze kan worden geïdentificeerd.

Inclusie: het beginsel dat ervoor moet zorgen dat iedereen, ongeacht zijn of haar capaciteiten, sociale situatie, leeftijd, vaardigheden of vertrouwdeheid met digitale tools, toegang heeft tot diensten, kan deelnemen aan procedures en zijn of haar rechten onder gelijke voorwaarden kan uitoefenen.

Integriteit: de garantie dat een document sinds het is aangemaakt of ondertekend niet is gewijzigd. Bij elektronische handtekeningen wordt de integriteit van een document gewaarborgd door cryptografische mechanismen die elke wijziging detecteerbaar maken.

IP-adres (Internet Protocol): een numerieke identificatiecode die wordt toegekend aan een apparaat dat is aangesloten op een netwerk dat gebruikmaakt van het internetprotocol. Hiermee kan het apparaat worden geïdentificeerd en kan het worden doorgestuurd bij gegevensuitwisseling via internet of een privénetwerk. Wanneer een gebruiker bijvoorbeeld een document online ondertekent, kan zijn IP-adres worden vastgelegd in de logbestanden die als bewijs van de transactie dienen.

itsme®: een mobiele app waarmee je je identiteit kunt bewijzen, inloggen op onlinediensten en op een veilige manier elektronische documenten kunt ondertekenen.

Juridische akte: een wilsuiting die is bedoeld om rechtsgevolgen teweeg te brengen, zoals het ontstaan, de wijziging, de overdracht of het vervallen van rechten en verplichtingen (bijvoorbeeld: het ondertekenen van een overeenkomst, een volmacht, een bestuurlijke akte van een overheidsinstantie, enz.)

Juridische erkenning: het feit dat een document, akte, handtekening of procedure door de wet wordt erkend als iets dat rechtsgevolgen heeft en op geldige wijze kan worden ingeroepen bij een overheidsinstantie, een autoriteit of een rechtbank.

Klik: een handeling die een gebruiker uitvoert door op een muis-knop te drukken, een element van een digitale interface aan te raken of een opdracht te selecteren om een actie in een computersysteem uit te voeren. Een gebruiker klikt bijvoorbeeld op de knop “Ondertekenen” om het proces van elektronische ondertekening te starten.

Logboek: het geheel van chronologische registraties die automatisch door een computersysteem worden gegenereerd om een overzicht te houden van de gebeurtenissen, acties en bewerkingen die daarin plaatsvinden.

Medeondertekenen: de handeling waarbij een persoon zijn handtekening plaatst op een document dat reeds door een andere persoon is ondertekend, teneinde de akte te bevestigen, goed te keuren, te bekrachtigen of te valideren in het kader van zijn bevoegdheden of verantwoordelijkheden.

Medeondertekening of contrasigneren: Handtekening van een tweede persoon, doorgaans een bevoegde persoon, ter bekrachtiging, bevestiging of authenticatie van de eerste handtekening. Het maakt de medeondertekenaar aansprakelijk en versterkt de juridische waarde van het document.

Meerdere handtekening: het aanbrengen van meerdere handtekeningen op één en hetzelfde document door verschillende personen.

MFA (Multi-Factor Authentication of meervoudige authenticatie): een beveiligingsmechanisme waarbij de identiteit van een gebruiker wordt gecontroleerd aan de hand van minstens twee verschillende authenticatiefactoren voordat toegang tot een systeem of dienst wordt verleend. Een gebruiker kan bijvoorbeeld inloggen op een elektronisch ondertekeningsplatform met een wachtwoord (eerste factor) en vervolgens een code invoeren die naar zijn gsm wordt gestuurd (tweede factor). Ook het gebruik van een eID in combinatie met een pincode is hiervan een voorbeeld. myGov.be: de officiële digitale app en het portaal van de Belgische federale overheid waarmee burgers via een beveiligde identificatie toegang krijgen tot verschillende online overheidsdiensten, hun administratieve documenten, hun eBox en bepaalde persoonsgegevens.

Non-discriminatie: het beginsel dat een document, een handtekening of een handeling niet mag worden geweigerd, onontvankelijk worden verklaard of van rechtsgeldigheid worden beroofd louter op grond van het feit dat het in elektronische vorm bestaat. Een contract mag bijvoorbeeld niet worden afgewezen louter omdat het elektronisch is ondertekend in plaats van met de hand.

Ondertekenaar: een natuurlijke persoon of, in bepaalde gevallen, een vertegenwoordiger van een rechtspersoon, die een document ondertekent om zijn instemming, goedkeuring, verbintenis of betrokkenheid bij de betreffende handeling kenbaar te maken.

Ondertekeningsenvelop: technisch bestand dat het ondertekende document en de bijbehorende bewijsstukken bevat.

Onweerlegbaarheid: vermogen om aan te tonen dat een persoon niet kan ontkennen een handeling te hebben verricht, met name de plaatsing van een elektronische handtekening. Het is gebaseerd op technische en juridische elementen waarmee de handtekening aan een geïdentificeerde ondertekenaar kan worden toegeschreven en de geldigheid ervan kan worden aangetoond.

Opvolgende ondertekening: een nieuwe handtekening of een nieuw tijdstempel waarmee de juridische geldigheid van de vorige handtekening of het vorige tijdstempel wordt verlengd.

Origineel: een document of akte in de rechtsgeldige versie, dat wil zeggen de versie die als authentieke referentie fungeert en waarop de rechten, verplichtingen of rechtsgevolgen die daaruit voortvloeien, zijn gebaseerd.

OTP (one time password): een eenmalige beveiligingscode die wordt gebruikt om de identiteit van een gebruiker te verifiëren en de veiligheid van een elektronische transactie, zoals een elektronische handtekening, te verbeteren.

Paraaf: een handtekening of een reeks initialen die op een document wordt aangebracht om aan te geven dat het in een bepaalde fase is gelezen, gecontroleerd of goedgekeurd.

Privésleutel van de ondertekenaar: vertrouwelijk cryptografisch gegeven dat uitsluitend in het bezit is van de ondertekenaar en wordt gebruikt om een elektronische handtekening aan te maken. Het is gekoppeld aan een bijbehorende openbare sleutel en maakt het mogelijk om een betrouwbare koppeling te leggen tussen de ondertekenaar en het ondertekende document. Wanneer een gebruiker een document elektronisch ondertekent, wordt zijn privésleutel gebruikt om de elektronische handtekening te genereren. De privésleutel kan worden bewaard in een eID, een cryptografisch token, een beveiligd apparaat voor het aanmaken van handtekeningen of een beveiligde infrastructuur voor ondertekening op afstand. Alleen de rechtmatige eigenaar van de privésleutel mag deze gebruiken.

Publieke sleutel: cryptografisch gegeven dat aan een privésleutel is gekoppeld en wordt gebruikt om een elektronische handtekening te verifiëren of om gegevens te versleutelen. Deze informatie kan aan derden worden verstrekt zonder dat dit de veiligheid van het systeem in gevaar brengt.

Raadplegingslink: adres of hyperlink waarmee een bevoegde persoon toegang krijgt tot een elektronisch document om het te bekijken of te raadplegen, zonder dat hij of zij het noodzakelijkerwijs kan wijzigen of downloaden.

Rechtsgeldigheid: de door de wet erkende rechtskracht van een document, een handtekening of een akte, waardoor deze juridische gevolgen kan hebben.

Rechtskracht: het vermogen van een akte, een document of een bewijsstuk om rechtsgevolgen te sorteren, door de rechtsorde te worden erkend en in een administratief, contractueel of gerechtelijk kader te worden ingeroepen.

Risico op geschillen: het risico dat een akte, een document of een beslissing wordt betwist, wat kan leiden tot een administratieve of gerechtelijke procedure.

Risicoanalyse: het proces waarbij risico's die van invloed kunnen zijn op een systeem, een proces of een activiteit worden geïdentificeerd, beoordeeld en geprioriteerd, teneinde passende maatregelen vast te stellen om deze te voorkomen, te beperken of te beheersen. Bijvoorbeeld: een risicoanalyse uitvoeren voordat een oplossing voor elektronische handtekeningen wordt geïmplementeerd, om het risico op betwisting van handtekeningen in te schatten.

Schriftvervalsing: een strafbaar feit dat bestaat uit het verdraaien van de waarheid in een geschrift, document of akte, door het creëren, wijzigen, vervalsen of gebruiken van valse informatie, met de bedoeling rechtsgevolgen teweeg te brengen of anderen te misleiden. Bijvoorbeeld: de inhoud van een contract na ondertekening wijzigen zonder instemming van de partijen.

Strafrechtelijk geschil: alle procedures en geschillen met betrekking tot inbreuken zoals omschreven in het strafrecht en die worden behandeld door de strafrechtbanken. Het doel ervan is vast te stellen of er een overtreding is begaan, de dader te identificeren en, indien van toepassing, een sanctie op te leggen. Een persoon vervalst bijvoorbeeld een elektronisch ondertekend document om een derde te misleiden.

Tegenwerpbaarheid: de periode waarin een document als bewijs kan dienen.

Tijdstempel: een systeem waarbij een datum (en soms een tijdstip) aan een document wordt gekoppeld om aan te tonen dat het op dat exacte moment bestond en dat het sindsdien niet is gewijzigd.

Token: methode waarmee meerdere elektronische documenten in één ondertekeningstransactie kunnen worden ondertekend.

Validering: het controleren en goedkeuren van een document, informatie of een stap in een proces.

Vermoeden van betrouwbaarheid: het beginsel dat een systeem of proces als betrouwbaar wordt beschouwd zolang niet is aangetoond dat het niet betrouwbaar is.

Vertrouwensdienstverlener: een gecertificeerde en gecontroleerde partij die verantwoordelijk is voor het waarborgen van de betrouwbaarheid, de integriteit en de rechtsgeldigheid van de vertrouwensdiensten die bij elektronische procedures worden gebruikt. In België moeten deze dienstverleners de eIDAS-verordening naleven.

Vertrouwensklok: officiële bron die wordt gebruikt om een betrouwbare datum en tijd aan te geven.

Verzegeling: het beveiligen van een elektronisch document door middel van een zegel om de herkomst ervan te waarborgen en eventuele latere wijzigingen op te sporen.

Visum: vermelding op een document waarmee wordt bevestigd dat het door een bevoegde persoon is ingezien, gecontroleerd of geverifieerd. Het visum geldt niet als handtekening: het bevestigt een onderzoek, geen juridische verbintenis.

Zip: een gecomprimeerd bestandsformaat waarmee een of meer bestanden in één archief kunnen worden gebundeld, waarbij de bestandsgrootte wordt verkleind om de opslag, verzending of het downloaden ervan te vergemakkelijken.