



**Vermijd elektronische
handtekeningen
te verbreken**



eSignFlow
meer dan digitaal tekenen

Elektronische handtekeningen op basis van een certificaat worden door de EU – zelfs wereldwijd – erkend als een juridisch sluitend alternatief voor handgeschreven handtekeningen. Ze worden vaak gebruikt om te bewijzen of te garanderen wie op welk tijdstip een document heeft ondertekend en dat ook de inhoud niet is gewijzigd sinds de ondertekening.

Maar soms maken gebruikers een fout: ze wijzigen een document nadat het al (deels) ondertekend werd.

Denk bijvoorbeeld aan het wijzigen van de tekst of de lay-out, of het verwijderen of toevoegen van een pagina.

Hierdoor worden sowieso eerdere handtekeningen **ongeldig** verklaard door software zoals Adobe Acrobat Reader of de handtekeningvalidatietools van de Belgische overheid (FOD BOSA) of die van de EU-Commissie.

Vermijd een document digitaal te ondertekenen en daarna nog te wijzigen, zelfs als je het document daarna opnieuw zult laten ondertekenen.

Wijzig in zo'n geval altijd het originele document zonder enige handtekening en laat dat document dan (her)ondertekenen door alle ondertekenaars.

Kun je niet anders dan toch een handeling stellen waarbij de eerdere handtekening(en) verbroken wordt (worden), bewaar dan sowieso goed elk ondertekend exemplaar.

Na het lezen van dit document weet je:

- hoe elektronische handtekeningen werken;
- waarom handtekeningen verbroken worden;
- wat je wel en niet mag doen met een ondertekend document;
- en hoe je zelf de geldigheid van een handtekening kunt controleren.

Inhoud

1. Wat is een elektronische handtekening?	4
2. Hoe weet je of een handtekening (nog) geldig is?	5
3. Wat maakt een elektronische handtekening ongeldig?	6
4. Elektronische en geschreven handtekeningen combineren?	8
5. Wat mag wél nog met een ondertekend document gebeuren?	9
6. Goede praktijken bij het werken met elektronische handtekeningen	10
7. eIDAS en de eisen aan elektronische handtekeningen	11
8. Gekwalificeerde handtekeningen in België	12
9. Ondertekencertificaten van een (Q)TSP	13
10. Gekwalificeerde tijdstempels	14
Conclusie	15
Wilt u meer ontdekken?	16

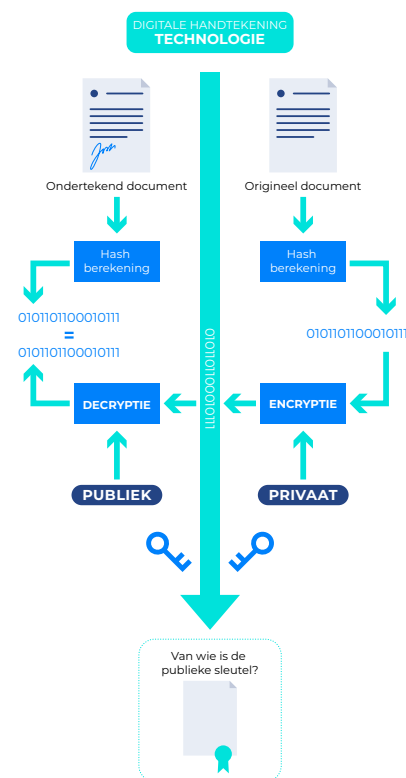


1. Wat is een elektronische handtekening?

Een elektronische handtekening is een soort digitale stempel die aan een document wordt toegevoegd. Ze bewijst wie het document heeft ondertekend en zorgt ervoor dat het document na ondertekening niet ongemerkt kan worden aangepast.

Technisch gezien werkt het als volgt:

- Er wordt een unieke **“vingerafdruk” van het document** gemaakt, een zoge-naamde **hash**. Een hash is een korte reeks cijfers en letters die op een unieke manier berekend wordt uit de volledige inhoud van het document. Zelfs een kleine wijziging in de tekst of lay-out zorgt daarom voor een totaal andere hash.
- Deze *hash* wordt versleuteld met de geheime (“private”) sleutel van de ondertekenaar.
- De versleutelde *hash* en de bijhorende “publieke sleutel” worden aan het document toegevoegd als elektronische handtekening.



Belangrijke eigenschappen van een veilige elektronische handtekening:

- **Identiteitsgarantie:** je weet wie het document heeft ondertekend.
- **Tijdstipgarantie:** je weet wanneer het document werd ondertekend.
- **Integriteitsgarantie:** je weet dat het document niet gewijzigd is na ondertekening.
- **Niet-afwijsbaarheid:** de ondertekenaar kan de handtekening niet ontkennen, want hij/zij plaatste de handtekening met een veilig ondertekenenmiddel dat de identiteit van de ondertekenaar bewijst.
- **Langetermijnvalidatie:** de nodige bewijzen van de identiteiten van de ondertekenaars, de tijdstippen van ondertekening en andere noodzakelijke bewijselementen zitten ingesloten in het document (LTV of “Long Term Validation”).

2. Hoe weet je of een handtekening (nog) geldig is?

Software kan controleren of een elektronische handtekening nog geldig is. De software kijkt na:

- of de documentinhoud nog exact dezelfde is als bij ondertekening (*hash*-controle);
- of het certificaat waarmee is ondertekend nog geldig is (vertrouwensketen);
- of er een geldige tijdstempel aanwezig is.

Je kunt zelf de geldigheid van een handtekening controleren met volgende tools:

- **Adobe Acrobat Reader DC** (gratis)
 - Toont automatisch of een handtekening geldig is wanneer je een PDF-document opent en er 1 of meer elektronische handtekeningen gevonden worden. Adobe herkent automatisch handtekeningen wanneer het gebruikte certificaat opgenomen is in de Adobe Acrobat Trusted List (AATL), maar ook als het opgenomen is in de European Union Trusted List (EUTL).
- **EU DSS Demonstration Tool** (Europese Commissie, gratis)
 - Test of een elektronische handtekening “**gekwalificeerd**” is (zie ook verder), d.w.z. gelijkgesteld met een handgeschreven handtekening.
 - De online validator kan je vinden op: <https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation>.
- **FOD BOSA Validator** (België, gratis)
 - Test of een elektronische handtekening **geplaatst met de Belgische eID** nog geldig is.
 - De online validator kan je vinden op: <https://signing.fts.bosa.belgium.be/validate?language=nl>.

3. Wat maakt een elektronische handtekening ongeldig?

Zodra een document is ondertekend, wordt het als “bevroren” beschouwd. Als je daarna nog iets aanpast — zelfs het kleinste detail — verandert de vingerafdruk (*hash*) van het document. De handtekening komt dan niet meer overeen met de nieuwe inhoud en wordt ongeldig.

Voorbeelden van handelingen die je **niet** mag doen:

- Tekst veranderen of toevoegen (zelfs een spatie toevoegen/weghalen is al een wijziging).
- Lay-out wijzigen (bijv. lettertype aanpassen, kleur aanpassen, ...).
- Pagina's toevoegen, verwijderen of herschikken.
- Formulievelden invullen nadat het document is ondertekend.
- Een reeds ondertekend document nog eens heropladen ter verdere ondertekening, waarbij je ondertekensoftware daarbij iets aan de tekst van het document wijzigt.

In geval van **eSignFlow** betreft het dan deze mogelijke aanpassingen van het document:

- **eSignFlow** plaatst (al dan niet opnieuw) een **verificatiereg**el op het document.
- **eSignFlow** voegt achteraan een **handtekeningenpagina** toe aan het document.
- **eSignFlow** plaatst handtekeningen op “**signmarkers**” (afgesproken tekstaanduidingen waar de handtekenvakken mogen komen). eSignFlow neemt daarbij eerst de *signmarkers* weg, en dat is een tekstwijziging ...

GEVOLG » validatiesoftware zal de handtekening als “verbroken” of “ongeldig” aanduiden.

Belangrijke tip met voorbeeld van foute handelingen:

Indiener X laadt (al dan niet via een andere software) een document **A** op ter ondertekening van ondertekenaar Y. Ondertekenaar Y ondertekent. Indiener X downloadt het door ondertekenaar Y ondertekende document en wijzigt dat document. Die wijziging verbreekt de handtekening van Y. Dan laadt indiener X het gewijzigde document **A'** terug op ter ondertekening van ondertekenaar Z. Ondertekenaar Z ondertekent. Het document **A'** is nu geldig ondertekend door Z, maar bevat ook nog de verbroken handtekening van ondertekenaar Y!

→ **Validatietools zullen het document als ongeldig ondertekend beschouwen...**

NB: stel dat indiener X de versie **A'** van het document opnieuw aanbiedt aan dezelfde ondertekenaar Y. Dan zal document **A'** tweemaal de handtekening bevatten van Y, waarvan 1 verbroken handtekening en 1 geldige handtekening.

→ **Validatietools zullen ook d t document als ongeldig ondertekend beschouwen...**

NOOT » we zien soms ook verbroken handtekeningen in opgeladen documenten, die al eerder met bv. Adobe Acrobat Reader werden ondertekend, om ze nadien nog bijkomend met eSignFlow te ondertekenen. Let dus ook op gelijkaardige foutieve handelingen in Adobe.

4. Elektronische en geschreven handtekeningen combineren?

Algemeen raden we af om eenzelfde document zowel handgeschreven als digitaal te ondertekenen (doorgaans is dat omdat 1 van de ondertekenaars niet in staat zou zijn tot digitaal ondertekenen). Probeer best altijd eenzelfde document ofwel volledig digitaal of volledig op papier te (laten) ondertekenen.

Waarom? Omdat een elektronische handtekening alleen digitaal kan bewezen worden, terwijl een analoge handtekening enkel op papier kan bewezen worden. Welke van de 2 documenten zul je dan bewaren als bewijsstuk?

Aanvaardbare oplossing: bewaar beide documenten zorgvuldig, zodat ze bij discussie voor een rechtbank tezamen kunnen voorgelegd worden aan de rechter.

LET OP » Pas deze combinatiemethodiek alleen toe als het echt niet anders kan.



5. Wat mag wél nog met een ondertekend document gebeuren?

Zolang je de inhoud van het ondertekende document niet aanpast, mag je wel nog het volgende doen, althans als de ondertekensoftware die mogelijkheden voorziet/toelaat:

- **Extra handtekeningen toevoegen:** bijvoorbeeld door een tweede persoon te laten ondertekenen, op voorwaarde dat de oorspronkelijke inhoud niet verandert.
- **Een tijdstempel toevoegen:** via een officiële dienst (een zogenaamde “*timestamp authority*”) om aan te tonen wanneer het document is ondertekend.
- **Vooraf voorziene velden invullen.**
- **Visuele markeringen en annotaties (tekstopmerkingen) toevoegen.**

LET OP » Dit moet gebeuren met software die werkt met het principe van “enkel toevoegen” (*append-only*): nieuwe info wordt als extra laag toegevoegd zonder het originele document te wijzigen.

6. Goede praktijken bij het werken met elektronische handtekeningen

- Onderteken pas wanneer het document volledig afgewerkt is.
- Zorg voor een duidelijke werkwijze waarin bewerken en ondertekenen strikt gescheiden blijven.
- Vermijd een document digitaal te ondertekenen en daarna nog te wijzigen, zelfs als je het document daarna opnieuw zult laten ondertekenen.
- Wijzig desgevallend altijd het originele document (zonder enige handtekening) en laat dat document dan (her)ondertekenen.
- Gebruik betrouwbare software voor PDF's en elektronische handtekeningen.
- De documenten worden best opgeslagen als PDF/A. PDF/A biedt stabiele archivering van ondertekende documenten en garandeert dat ze integraal en authentiek blijven, wat essentieel is voor juridische en administratieve doeleinden van elektronische ondertekening.
- Licht medewerkers in over het belang van ongewijzigde ondertekende documenten.
- Bewaar ondertekende documenten ergens waar ze niet meer gewijzigd kunnen worden.
- Heb je alsnog meer dan 1 versie van een document met telkens andere handtekeningen, bewaar dan sowieso elk ondertekende versie!

7. eIDAS en de eisen aan elektronische handtekeningen

Definitie eIDAS: electronic IDentification, Authentication and trust Services. Dit is een EU-verordening (nr. 910/2014) die een juridisch kader biedt voor elektronische identificatie- en vertrouwensdiensten binnen de EU-lidstatenmarkt. Het doel is veilige en grensoverschrijdende digitale transacties mogelijk te maken, met rechtsgeldige elektronische handtekeningen, zegels, tijdstempels, documenten en meer.

De eIDAS-verordening onderscheidt drie soorten elektronische handtekeningen:

1. **Gewone elektronische handtekening:** elke vorm van elektronische handtekening, zoals een naam onder een e-mail of een handtekenscan.
2. **Geavanceerde elektronische handtekening:** deze handtekening is op unieke wijze verbonden met de ondertekenaar, gebruikt een certificaat en maakt het mogelijk om achteraf wijzigingen in het document op te sporen.
3. **Gekwalificeerde elektronische handtekening:** voldoet aan alle eisen van een geavanceerde handtekening én is gezet met een gekwalificeerd ondertekenmiddel.

Een gekwalificeerde elektronische handtekening heeft in alle EU-lidstaten dezelfde juridische waarde als een handgeschreven handtekening.

Verschillen tussen geavanceerd en gekwalificeerd:

Kenmerk	Geavanceerd	Gekwalificeerd
Certificaat vereist	Ja	Ja
Unieke link met ondertekenaar	Ja	Ja
Detecteert wijzigingen	Ja	Ja
Uitgegeven door	TSP ^(*)	QTSP ^(*)
Juridische waarde	Sterk bewijs	Gelijk aan handgeschreven

(*) (Q)TSP: (Qualified) Trust Service Provider, zie ook verder.

8. Gekwalificeerde handtekeningen in België

In België kun je gebruikmaken van diverse betrouwbare middelen om een gekwalificeerde handtekening te zetten:

- De **Belgische eID-kaart**: deze bevat een gekwalificeerd certificaat, uitgegeven door de overheid (via FOD Binnenlandse Zaken). Wanneer je met de eID ondertekent, wordt de ondertekening bevestigd met je pincode en een beveiligde kaartlezer. De eVK of elektronische vreemdelingenkaart is functioneel identiek aan de eID en kan dus ook gebruikt worden voor gekwalificeerde handtekeningen.
Opmerking: handtekeningen geplaatst met een “oude” Belgische eID worden door de validatietool van de EU-Commissie niet meer als gekwalificeerd beschouwd, omdat ze gebaseerd zijn op een verouderde encryptie (SHA1).
Dit is enkel oplosbaar door de betreffende ondertekenaar te verzoeken een nieuwe eID aan te vragen bij de bevolkingsdienst van zijn/haar woonplaats. Zowel Adobe als de validatietool van de FOD BOSA (h)erkennen deze handtekeningen (voorlopig) wel nog.
- De **Itsme-app**: deze app werd in 2020 erkend als gekwalificeerde ondertekenmethode. De gebruiker ondertekent met een combinatie van smartphone, app-verificatie en pincode of biometrie (zoals gezichtsherkenning). Achterliggend gebruikt Itsme om te ondertekenen een gekwalificeerd persoonlijk certificaat van een QTSP (zie hierna).
- Een **gekwalificeerd persoonlijk certificaat** of een **gekwalificeerde organisatiezegel**: als mandataris of medewerker van een organisatie kun je een certificaat aanschaffen dat je voor een bepaalde tijd (doorgaans 3 jaar) kunt gebruiken via een ondertekensoftware die dat certificaat dan aanwendt. Meestal moet je een mobiele app installeren om handtekeningen met dat certificaat veilig te bevestigen. Zie hoofdstuk 9 voor meer toelichting.

Deze 3 methodes voldoen volledig aan de vereisten voor een gekwalificeerde elektronische handtekening volgens eIDAS en hebben daardoor dezelfde rechtskracht als een klassieke handtekening, in alle EU-lidstaten. Let wel op de **opmerking** betreffende “oude” Belgische eID's.

9. Ondertekencertificaten van een (Q)TSP

Handtekencertificaten, zowel persoonlijke certificaten als elektronische (organisatie)zegels (eseals), kunnen aan de eIDAS-verordening voldoen als ze aan bepaalde technische en organisatorische eisen voldoen.

Voor een **geavanceerde elektronische handtekening** moet het certificaat uniek verbonden zijn met de ondertekenaar, onder diens exclusieve controle blijven, en wijzigingen aan het ondertekende document detecteerbaar maken. Deze certificaten worden in principe uitgegeven door een TSP (Trust Service Provider) of door een QTSP (Qualified TSP).

ESEAL » Een *eseal* of elektronisch zegel wordt gekoppeld aan een (deel van een) **organisatie** in plaats aan van een natuurlijke persoon.

Een **gekwalificeerde elektronische handtekening** vereist daarnaast het gebruik van een **gekwalificeerd certificaat**, uitgegeven door een gekwalificeerde vertrouwensdienstverlener (**QTSP**: *qualified trust service provider*), en moet worden aangemaakt met een gekwalificeerd middel voor elektronische handtekeningen (**QSCD**: *qualified signature creation device*).

Bedrijven als Digicert, SK ID Solutions, GlobalSign e.a. zijn QTSP's en hebben systemen die als QSCD dienen. Zij worden dus erkend als leveranciers van certificaten en ondertekensystemen die juridisch 100% evenwaardig zijn aan een handgeschreven handtekening.

Hun certificaten en ondertekensystemen zijn vaak "**HSM's**" (*Hardware Security Modules*). Die HSM is doorgaans een server(park) en bijhorende software die digitale sleutels uiterst veilig opslaat en gebruikt om documenten veilig digitaal te ondertekenen. De HSM zorgt ervoor dat de ondertekensleutel nooit buiten de HSM komt, waardoor de HSM bestand is tegen misbruik. Dit maakt het een veilige manier om elektronische handtekeningen te zetten, omdat het voorkomt dat iemand jouw sleutel gebruikt, steelt of vervalst.

Ondertekenplatformen zoals **eSignFlow** kunnen gebruik maken van diensten van QTSP's om jezelf of je organisatie toe te laten documenten geavanceerd of gekwalificeerd te ondertekenen (met persoonlijk certificaat) of om documenten te "certificeren" (met *eseal*).

10. Gekwalificeerde tijdstempels

Een **gekwaltificeerde tijdstempel** bij een elektronische handtekening is een elektronisch bewijs dat vastlegt wanneer een elektronische handtekening ontstond, met een hoge mate van betrouwbaarheid. Deze tijdstempel wordt ook uitgegeven door een gekwalificeerde vertrouwensdienstverlener (QTSP) en voldoet aan de eisen van de **eIDAS-verordening**.

De tijdstempel zorgt voor volgende veiligheden:

1. **Bewijs van tijdstip:** het bevestigt het exacte tijdstip waarop de elektronische handtekening is geplaatst.
2. **Integriteit:** de tijdstempel is cryptografisch gekoppeld aan het document en maakt het duidelijk of het document sinds dat moment al dan niet is gewijzigd.
3. **Langdurige geldigheid:** in combinatie met archiveringsstandaarden zorgt een gekwalificeerde tijdstempel ervoor dat de handtekening ook na jaren nog als juridisch geldig erkend wordt, zelfs als het onderliggende certificaat intussen vervalst of wordt ingetrokken.
4. **Rechtszekerheid:** in juridische procedures geeft een gekwalificeerde tijdstempel extra zekerheid over de authenticiteit en het moment van ondertekening.

Betrouwbare ondertekenplatformen (zoals bv. eSignFlow) genereren bij elke ondertekening altijd een gekwalificeerde tijdstempel via een QTSP, ongeacht het gebruikte ondertekenmiddel.

Conclusie

- Elektronische handtekeningen zijn een krachtig middel om te bewijzen **wie** een document heeft ondertekend, op **welk tijdstip** en dat het document (behoudends specifiek toegelaten uitzonderingen) sindsdien **niet gewijzigd** is.
- Gebruik **betrouwbare software** en **duidelijke procedures** om ervoor te zorgen dat de handtekeningen in je documenten rechtsgeldig blijven.
- Dankzij de **eIDAS-Verordening** van de Europese Unie en gekwalificeerde ondertekenmiddelen zoals de Belgische eID, Itsme of HSM-certificaten van een (Q)TSP, kun je juridisch sluitend digitaal handtekenen, voor zover (niet-toegelaten) wijzigingen van het document na ondertekening worden vermeden.

LINK » [eIDAS 2.0: Verordening \(EU\) 2022/858 online.](#)

Als je een ondertekend document wijzigt, worden eerdere handtekeningen ongeldig. Om dit te vermijden, is het belangrijk om het document na volledige ondertekening met rust te laten. Afwijken van die regel vergt bewaring van elk ondertekend exemplaar.

Wees extra aandachtig bij documenten waarbij handtekeningen worden geplaatst met een mix van ondertekensystemen, of waarbij papieren en elektronische handtekeningen worden gecombineerd.

Ontdek het ondertekenplatform op maat gemaakt voor lokale besturen

Wil je meer te weten komen over **eSignFlow** en hoe we processen omzetten in slimme digitale stromen met beveiligde en juridisch bindende elektronische ondertekening en verzending, aarzel zeker niet om ons te contacteren op **www.esignflow.be**.



Verander je processen in slimme digitale stromen. Met beveiligde en juridisch sluitende elektronische ondertekening en verzending.



1. Indienen

Leg zonder rompslomp de juiste documenten aan de juiste persoon voor.



2. Goedkeuren

Behoud steeds het overzicht over de documenten die in omloop zijn.



3. Ondertekenen

Onderteken met enkele muisklikken al je documenten, waar en wanneer je wil.



4. Verzenden

Verzend de digitaal ondertekende documenten via een kanaal naar keuze (post, e-mail, eBox ...).



5. Verifiëren

Ga met een unieke code snel en eenvoudig de rechtsgeldigheid van een document na.

Ontdek meer op www.esignflow.be