Rechtsgeldig en snel ondertekenen met een digitale handtekening

Inclusief handige checklist
voor een digitale handtekening
die past bij jouw bedrijf

pondres

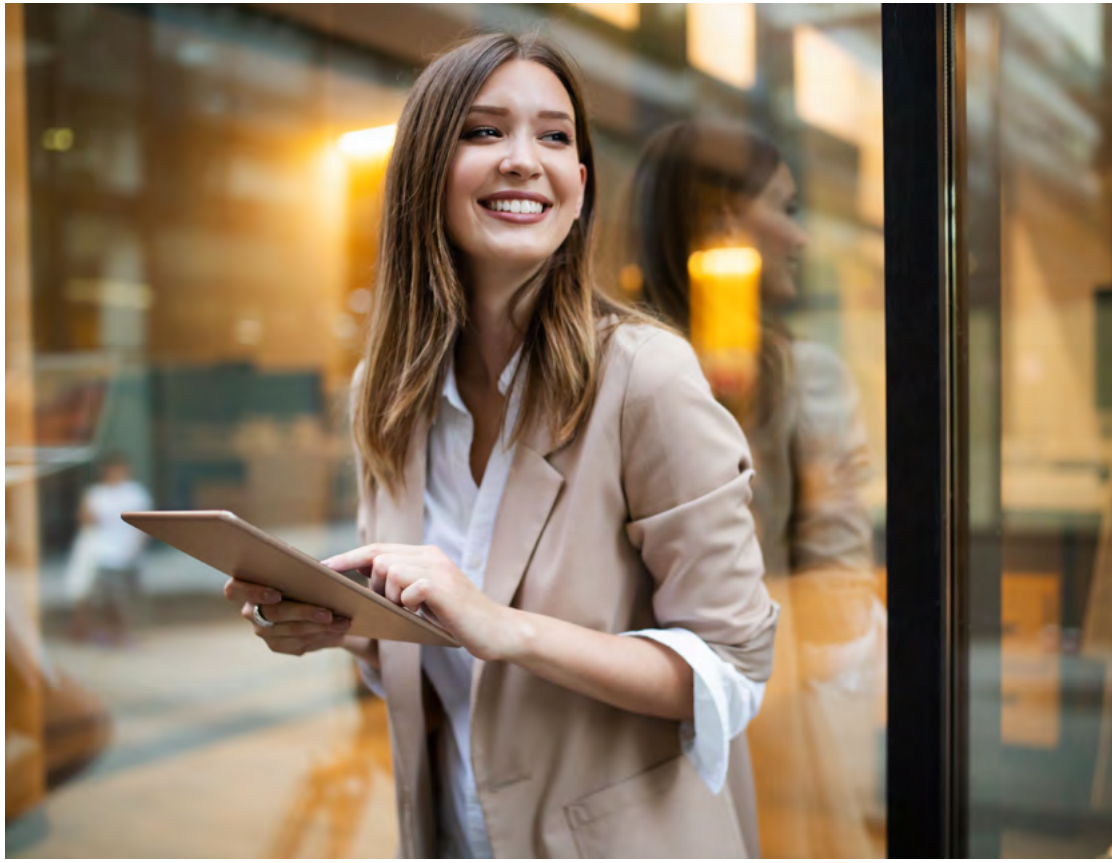
Inhoudsopgave

Inleiding

Digitalisering van bedrijfsprocessen staat bij veel bedrijven al jaren op de agenda. En dat is niet voor niets, want het helpt organisaties processen te versnellen en flexibeler te zijn. In 2020 heeft digitale transformatie bij veel organisaties op alle vlakken een enorme vlucht gemaakt. Door het coronavirus moesten bedrijfsprocessen sneller dan ooit aangepast worden. We werken meer thuis dan vanuit kantoor, we houden afstand en komen nog maar weinig op bezoek bij klanten en relaties. Daardoor is het laten ondertekenen van documenten nu vaak een tijdrovend proces.

De digitale handtekening brengt hier gelukkig verandering in. Daarmee kan immers het gehele ondertekenproces online worden afgerond; of het nu gaat om eenvoudige bestellingen, zakelijke contracten offor-mele documenten die rechtsgeldig ondertekend moeten worden. Zo realiseer je aanzienlijke besparingen in tijd, papier en kosten, bijvoorbeeld op het gebied van porti. Bovendien bied je je relaties een snelle, eenvoudige en veilige manier om een document digitaal rechtsgeldig te ondertekenen.

Maar hoe zorg je voor een goede aansluiting met bestaande interne IT-systemen? En wat is precies het verschil tussen een elektronische en een digitale handtekening? Hoe werkt een digitale handtekening en waarom kun je er als toekomstgericht bedrijf eigenlijk niet omheen? Het antwoord op deze en andere vragen vind je in deze whitepaper.



Wat is een digitale handtekening?

pondres

Inhoudsopgave

Wat is een digitale handtekening?

Een elektronische of digitale handtekening is simpelweg de digitale variant van de handgeschreven krabbel op papier. Technisch gezien is het een encrypted code die ervoor zorgt dat een document niet meer gewijzigd kan worden na ondertekening. Door middel van autorisatiemethoden controleert het ook de identificatie van een persoon. Zo weet je altijd zeker dat de juiste persoon de handtekening heeft gezet.

Verschil tussen een elektronische en digitale handtekening

De termen elektronische handtekening en digitale handtekening worden vaak door elkaar gebruikt. Er is echter een verschil. Een digitale handtekening kan namelijk dienen als juridisch, rechtsgeldig bewijs; een elektronische handtekening alleen als een rechter dit bepaalt. De juridische en technische kenmerken van de elektronische en digitale handtekening worden verder uitgelicht op pagina 6.

Drie soorten elektronische (digitale) handtekeningen

In 2018 is de Europese eIDAS-verordening ingegaan. Vanaf dat moment moeten publieke en private organisaties met een publieke taak Europees erkende inlogmiddelen accepteren binnen de digitale dienstverlening. Zo wordt het makkelijker en veiliger om binnen Europa online zaken te regelen. Hiervoor zijn drie soorten elektronische (digitale) handtekeningen beschikbaar, die verschillen in juridisch bewijs op de volgende drie vereisten:

- **Authenticiteit:** weet je zeker dat de handtekening echt is gezet door de ondertekenaar?
- **Identiteit:** is de identiteit van de ondertekenaar goed vast te stellen?
- **Integriteit:** zijn de data (documenten niet gewijzigd tijdens en na het ondertekenproces?

1. Basis elektronische handtekening (BES)

Een basis elektronische handtekening (BES) wordt gebruikt voor zaken waarbij de identiteit van de tekenaar niet verplicht gecontroleerd hoeft te worden. Denk aan het ondertekenen van een ontvangstbevestiging van een pakketje. De klant zet zelf een handtekening op een touchscreen of klikt op 'ik ga akkoord'. De BES kan echter de identiteit van de ondertekenaar niet checken of garanderen en is dus ongeschikt voor wettelijke bindende documenten.

2. Geavanceerde elektronische handtekening of digitale handtekening (AES)

De geavanceerde elektronische handtekening oftewel digitale handtekening (AES) gaat veel verder dan een gewone elektronische handtekening. De handtekening is op een unieke manier aan de ondertekenaar verbonden. Zo kan de identiteit worden gecheckt, maar niet 100% gegarandeerd. Ook zijn eventuele wijzigingen aan het ondertekende document achteraf traceerbaar.

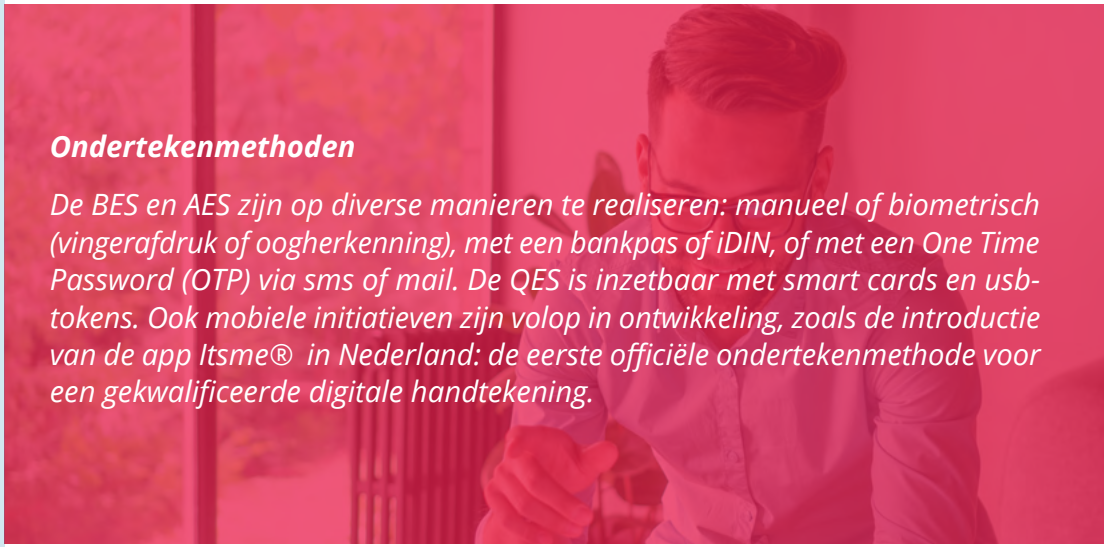
De AES voldoet volledig aan de eIDAS-verordening, is betrouwbaar en kan niet worden vervalst. Enkel voor bepaalde documenten voldoen identiteitscontroles mogelijk niet aan de strengste betrouwbaarheidsvereisten.

pondres

3. Gekwalificeerde geavanceerde elektronische handtekening of gekwalificeerde digitale handtekening (QES)

Is een 'natte' handtekening op papier volgens jou de enige veilige optie voor je document? Overweeg dan haar digitale tegenhanger: de gekwalificeerde digitale handtekening (QES). Bij de onweerlegbare (non-repudiative) QES is de identiteit van de ondertekenaar aan de handtekening verbonden door een persoonlijk, gekwalificeerd certificaat van een Qualified Trust Service Provider. Zo weet je dat de handtekening niet alleen geldig is in het EU-land waar ze is geplaatst, maar dat ze heel de EU wordt erkend als een geldige, wettelijk bindende handtekening. Daardoor leent deze handtekening zich voor documenten waar grote risico's mee gemoeid zijn, zoals levensverzekeringen en kredietaanvragen.

Uiteraard speelt ook de lokale wetgeving een rol. Zo dient de handtekeningsleutel van de gebruiker te worden beheerd in een device dat daarvoor gecertificeerd is (bijvoorbeeld een mobiele telefoon of usb-token) en is multifactor-authenticatie verplicht. Alleen met deze handtekening kun je de ondertekenaar (vooraf) met 100% zekerheid identificeren. Daarmee biedt de gekwalificeerde handtekening wettelijk en onweerlegbaar bewijs dat de handtekening daadwerkelijk is gezet door de ondertekenaars.



Ondertekenmethoden

De BES en AES zijn op diverse manieren te realiseren: manueel of biometrisch (vingerafdruk of oogherkenning), met een bankpas of iDIN, of met een One Time Password (OTP) via sms of mail. De QES is inzetbaar met smart cards en usb-tokens. Ook mobiele initiatieven zijn volop in ontwikkeling, zoals de introductie van de app Itsme® in Nederland: de eerste officiële ondertekenmethode voor een gekwalificeerde digitale handtekening.

pondres

Technische en juridische kenmerken van een digitale handtekening

Onderstaande tabel geeft in één oogopslag de technische en juridische kenmerken van de drie verschillende elektronische (digitale) handtekeningen weer.

Technische en juridische kenmerken	'Natte' handtekening	Basis elektr. handtekening (BES)	Geavanceerde elektr. handtekening = Digitale handtekening (AES)	Gekwalificeerde geavanceerde elektronische handtekening = Gekwalificeerde digitale handtekening (QES)
Juridische waarde	Kan dienen als bewijs, maar rechter bepaalt	Kan dienen als bewijs, maar rechter bepaalt	✓ Bewijs voor inhoud en identiteit, maar rechter bepaalt	✓ Non-repudiative; wettelijk bewijs
Authenticatie Controle identiteit ondertekenaar	✗ Check niet verplicht	✗ Check niet verplicht	✓ • Handtekening is verbonden aan ondertekenaar. • Multifactor-authenticatie is mogelijk	✓ Kan dienen als bewijs, maar rechter bepaalt
Integriteit Betrouwbaar	✗	✗	✓ Inhoud beveiligd tegen wijzigingen	✓ Inhoud beveiligd tegen wijzigingen
Vertrouwelijkheid	✗	✗	✓	✓
Non-repudiation Onweerlegbaar bewijs	✗	✗	✓	✓
Public Key Infrastructure Rechtsgeldige ondertekening met cryptografische sleutel	✗	✗	✓	✓
eIDAS-vereisten Voldoet aan eIDAS-wetgeving	✗	✗	✓	✓
Audit trail Transactiegegevens worden vastgelegd (timestamp, IP)	✗	✗	✓	✓

5 voordelen van een digitale handtekening

pondres

5 voordelen van een digitale handtekening

De maatschappij digitaliseert in rap tempo en klanten verwachten dat ze online geholpen en benaderd worden. We werken meer en meer vanuit verschillende locaties; vanuit huis, kantoor of de andere kant van de wereld. Klanten verwachten dat ze online geholpen en benaderd worden. Met de digitale handtekening kan deze klantreis worden geoptimaliseerd. We zetten deze voordelen van een digitale handtekening nog een keer op een rij.

Voordeel 1: Gebruiksvriendelijk

Een digitale handtekening is sneller en gemakkelijker dan een fysieke handtekening. Geen gedoe meer met het printen, versturen, scannen en archiveren van ondertekende papieren documentatie. Geen tijdsverlies door miscommunicatie. Maar een veilige en rechtsgeldige oplossing die door iedereen, binnen of buiten de organisatie, altijd en overal kan worden ingezet. Met communicatie die bovendien aangepast kan worden aan de eigen huisstijl voor herkenbaarheid, betrouwbaarheid en consistentie. En een online dashboard waarin je het ondertekenproces kunt monitoren en bijsturen.

Voordeel 2: Kostenbesparend

Met laagdrempelige koppelingen kan het gehele digitale goedkeurings- en ondertekeningproces aan de bestaande IT-infrastructuur worden gekoppeld. De digitale handtekening helpt bedrijfsprocessen te stroomlijnen, fouten te voorkomen en administratieve kosten te besparen. Ook kosten voor papier, inkt en porti zijn verleden tijd. Voor zowel de zender als de ontvanger een flinke kostenbesparing.

Voordeel 3: Veilig en rechtsgeldig

De afgelopen jaren is de internationale wetgeving op het gebied van digitale handtekeningen flink aangescherpt. In Europa we hebben dankzij de eIDAS-verordening goede afspraken over de validiteit van digitale handtekeningen voor samenwerking binnen de EU. Onder deze regeling worden alle soorten digitale handtekeningen gelijk behandeld in de Europese rechtspraak.

Met een digitale handtekening hebben zowel interne stakeholders als klanten de garantie dat de identiteit van de ondertekenaars is gecontroleerd en de handtekeningen daadwerkelijk door de betrokken personen zijn gezet. Hiervoor zijn verschillende ondertekenmethoden beschikbaar: van manueel tekenen, sms of e-mail met one time password (OTP) e-herkenning tot iDIN en Itsme©. Via OpenIDConnect protocol kunnen eenvoudig extra (landspecifieke) methodieken zoals DigiD, beID en Swiss ID, worden geïntegreerd.

Voordeel 4: Betrouwbaar

Als het om handtekeningen gaat, zijn authenticiteit en veiligheid prioriteiten. Dankzij de versleuteling van het document heb je de garantie dat het document na ondertekening ongewijzigd is gebleven. Met een digitale handtekening onderteken je altijd het hele document. Je weet zeker dat er geen pagina's achteraf zijn toegevoegd of verwijderd. Disclaimers, die nodig zijn conform de AVG-wetgeving kunnen worden bijgevoegd.

Voordeel 5: Innovatief

Afhankelijk van de leverancier die je kiest, biedt een digitale handtekening niet alleen de handtekening zelf. Je bent er ook zeker van dat alle software technisch up-to-date blijft en dat je op de hoogte blijft van de laatste innovaties in de markt. Zeker zo belangrijk is de oplossing blijft aansluiten op de actualiteit van Nederlandse én Europese wet- en regelgeving. Met een duidelijke roadmap houd je jouw doelen voor ogen, die meebewegen met alle ontwikkelingen.

Hoe werkt een digitale handtekening?

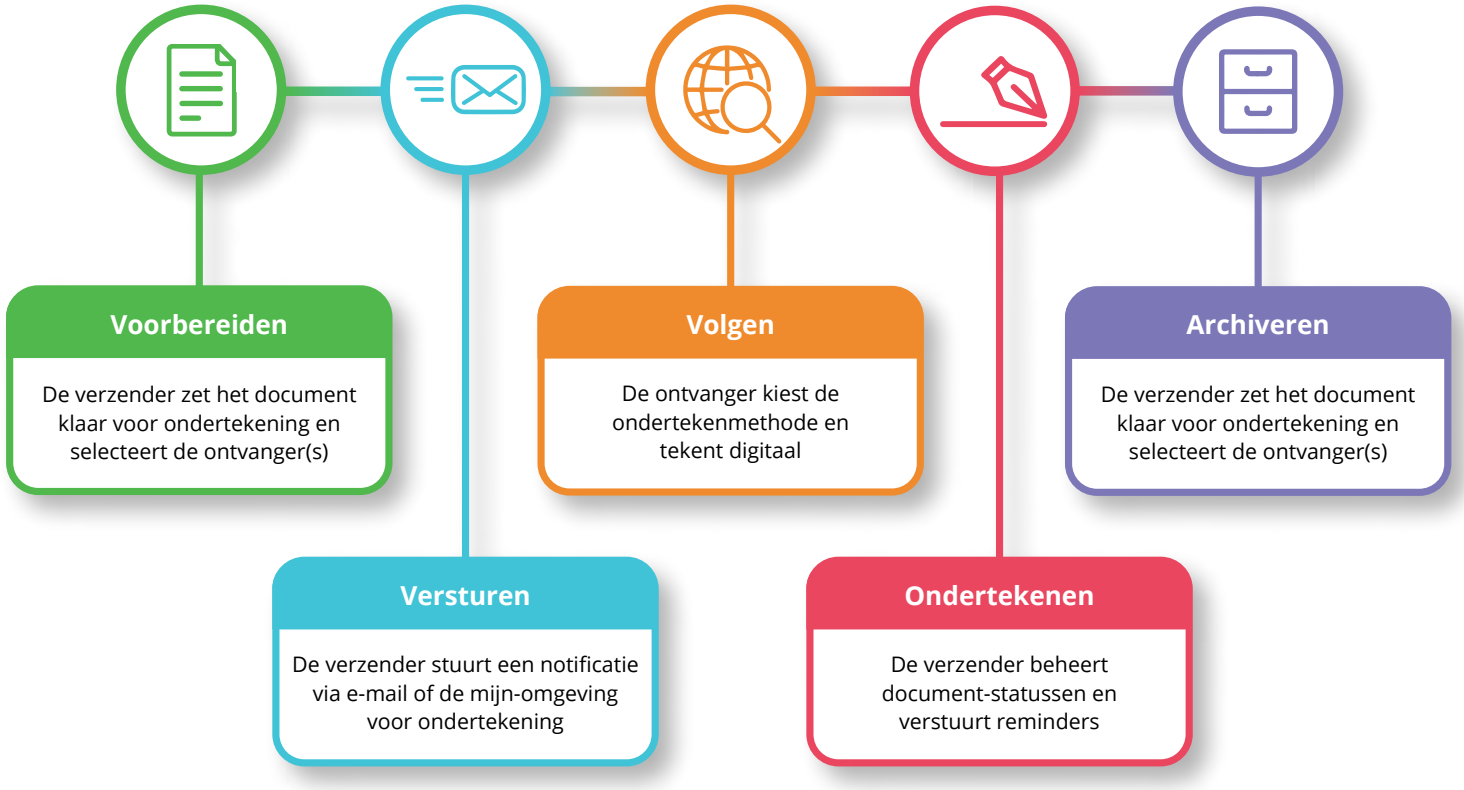
pondres

Hoe werkt een digitale handtekening?

Een digitale handtekening is efficiënt en gebruiksvriendelijk, maar hoe gaat het ondertekenproces precies in zijn werk? Hoe zit het met de versleuteling van de data? En wat vraagt de digitale handtekening op het gebied van integratie in bestaande systemen? De informatie vind je in de volgende paragrafen.

Een digitale handtekening in 5 stappen

Binnen enkele minuten creëer en verstuur je een te ondertekenen document, waarna de ontvanger hem controleert en tekent. Na ondertekening is het document direct beschikbaar voor download of archivering voor beide partijen.



Versleuteling

Digitale handtekeningen zijn gebaseerd op een specifiek protocol, genaamd Public Key Infrastructure (PKI). Dit protocol maakt gebruik van cryptografische algoritmen om twee unieke lange getallen (een hash) te creëren.

Op moment van ondertekening wordt er één hash door de privésleutel geëncrypteerd. De privésleutel - het woord zegt het al - blijft geheim, maar is gelinkt aan een publieke sleutel. Deze publieke sleutel wordt met de hash in het te ondertekenen document opgeslagen en naar ontvanger doorgestuurd.

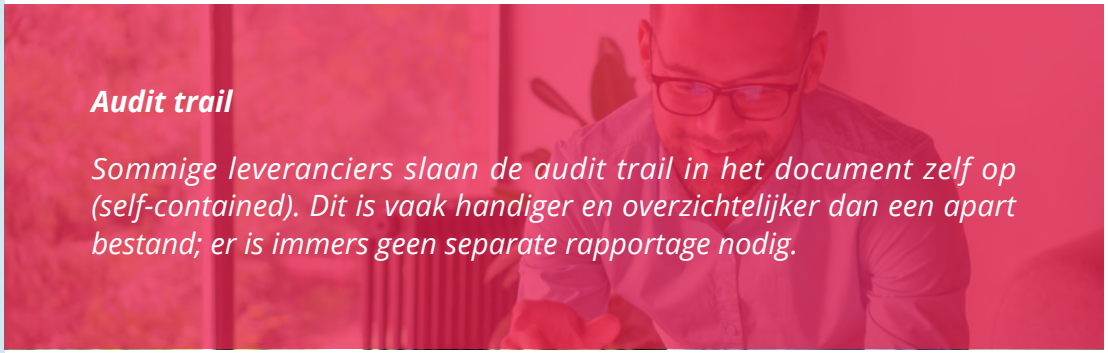
De ontvanger ondertekent het document. Om de handtekening te kunnen valideren en eventuele wijzigingen in het document te detecteren, wordt automatisch een tweede hash aangemaakt met de publieke sleutel. Een handtekening is geldig als beide hashes gelijk zijn.

Integratie met systemen en software

Een digitale handtekening maakt bedrijfsprocessen eenvoudiger en efficiënter. Voor een soepele overstap van jouw ondertekenproces is het belangrijk om de oplossing goed te integreren met bestaande IT-oplossingen in de eigen organisatie.

Heb je geen geautomatiseerd ondertekenproces en verwerking nodig? Dan kun je ook eenvoudig handmatig gebruik maken van de handtekeningtool via een digitaal portaal. Let bij je keuze goed op de klantreis en klantbehoeften.

De meeste oplossingen voor een digitale handtekening zijn clouddiensten; zo werk je altijd met de nieuwste besturingssystemen en software, en blijf je up-to-date met wet- en regelgeving. Het geautomatiseerde proces wordt geïntegreerd met een goed gedocumenteerde API.



Audit trail

Sommige leveranciers slaan de audit trail in het document zelf op (self-contained). Dit is vaak handiger en overzichtelijker dan een apart bestand; er is immers geen separate rapportage nodig.

In 4 checks naar de beste oplossing voor een digitale handtekening

In 4 checks naar de beste oplossing voor een digitale handtekening

De keuze om met digitale handtekeningen te gaan werken is misschien al gemaakt. Maar wat is nu de juiste oplossing? Om je te helpen bij deze keuze hebben we een aantal checks opgesteld waar de oplossing in onze ogen aan zou moeten voldoen. Zo weet je zeker dat je de oplossing kiest die het beste past bij je klanten, maar ook bij jouw organisatie.

Check 1: Gebruiksgemak

- ☐ De oplossing spreekt voor zich en het gebruik is intuïtief
- ☐ Het ondertekenproces is volledig digitaal (zonder overstappen naar andere kanalen)
- ☐ Ik kan op elk device ondertekenen (pc, tablet, smartphone; browser-onafhankelijk)
- ☐ Iedereen binnen of buiten mijn organisatie kan de handtekening valideren, zelfs zonder toegang tot het systeem
- ☐ Het ondertekenportaal is aan te passen aan de huisstijl van mijn organisatie of label.

Check 2: Efficiency en kosten

- ☐ Met de oplossing kan ik het hele goedkeurings- en ondertekenproces binnen mijn organisatie stroomlijnen, met minder fouten
- ☐ Ik kan de status van de documenten volgen (geopend, ondertekend, afgehandeld)
- ☐ De oplossing integreert met bestaande of toekomstige applicaties, zoals contractmanagement en HR-diensten
- ☐ Het kostenmodel sluit aan bij mijn organisatie (SaaS-oplossing met betaling per handtekening).
- ☐ Bij één transactie kunnen de digitale handtekeningen van meerdere personen gevalideerd worden, zodat ook partners indien nodig kunnen meetekenen
- ☐ De volgorde van de ondertekenaars kan ik zelf bepalen
- ☐ Het is mogelijk om een compleet pakket aan documenten in één keer te ondertekenen.

Check 3: Compliancy

- ☐ De oplossing voldoet aan onze voorschriften, zoals eIDAS, GDPR, US Sign act
- ☐ De organisatie die de oplossing biedt, beschikt over de benodigde certificeringen. Bijvoorbeeld ISO9001, ISO14001, ISO27001, ISAE3402 Type II
- ☐ De organisatie is of werkt samen met een gecertificeerde Trust Service Partner
- ☐ Er zijn verschillende ondertekenmethoden beschikbaar die passen bij de wettelijke vereisten. Denk aan manueel, biometrisch, bankkaart of iDIN, sms/e-mail met OTP, Itsme®, aanvullende ondertekenmethoden via het OpenIdConnect Protocol zoals DigiD en eHerkenning, of lokale methoden zoals belID, SwissID
- ☐ De handtekening is rechtsgeldig in andere Europese landen en ondersteunt meerdere talen, zowel voor de verzender als ondertekenaar
- ☐ De geavanceerde en gekwalificeerde digitale handtekening (AES en QES) voor documenten met meerdere ondertekenaars worden door de oplossing ondersteund
- ☐ Ik kan herleiden wie welk document heeft ondertekend en hoe (audit trail). Deze informatie is geseald in het document (self-contained), zodat er geen aparte rapportage hoeft te worden bewaard
- ☐ De oplossing biedt WYSIWYS (What You See Is What You Sign). Deze functie zorgt ervoor dat het document alleen ondertekend kan worden als het volledig is gelezen.

Check 4: Technische specificaties

- ☐ De oplossing voegt functionaliteit toe aan bestaande interne IT-oplossingen en werkt hier goed mee samen
- ☐ Ik kan de oplossing gefaseerd in gebruik nemen (er is een ontwikkel-, test-, acceptatie- en productieomgeving mogelijk, oftewel OTAP)
- ☐ De oplossing is eenvoudig te implementeren, bijvoorbeeld middels een laagdrempelige, goed gedocumenteerde API-koppeling
- ☐ De bestandsformaten die ik normaal gebruik bij het ondertekenen worden ondersteund (PDF, DOC, DOCX, TXT, XML)
- ☐ De software biedt het vereiste beveiligingsniveau
- ☐ De oplossing is compatibel met de nieuwste versies van alle gangbare besturingssystemen en voor verschillende devices
- ☐ Er zijn standaard connectoren beschikbaar voor programma's zoals MS Dynamics, Salesforce, , SAP en Oracle
- ☐ Mijn organisatie blijft zelf in controle over de data, zodat ik zeker weet dat er geen informatie achterblijft op het platform van de leverancier
- ☐ De leverancier biedt een duidelijke roadmap op basis van ontwikkelingen, en nieuwe technische en compliancy-standaarden in de markt.

pondres

Conclusie

Digitale communicatie is de nieuwe standaard: klanten verwachten een digitale klantreis. Een digitale handtekening is daar een onmisbaar onderdeel van. Hierbij kun je kiezen voor een BES, AES of QES, afhankelijk van het doel van het document en de vereiste juridische bewijsvoering: authenticiteit (uniek), identiteit, integriteit (betrouwbaar) en authenticatie (juistheid).

De voordelen van een digitale handtekening:

- **Gebruiksvriendelijk**
  door een geautomatiseerd, real-time online proces
- **Kostenbesparend,**
  bijvoorbeeld in ad-ministratie, papier, inkt, porti en archief
- **Veilig en rechtsgeldig,**
  conform eIDAS en lokale wetgeving
- **Betrouwbaar,**
  met bewijs van authenticiteit door unieke versleuteling
- **Innovatief,**
  up-to-date met technologie en regelgeving, en met duidelijke roadmap.

Toekomstbestendig

Steeds meer landen werken met een digitaal ID, een vorm van online identificatie. Daarmee kun je, ook over landsgrenzen heen, binnen enkele seconden je identiteit bevestigen. Deze digitale identificatie maakt ook de bewijsvoering voor authenticiteit en identiteit van de digitale handtekening nog eenvoudiger.

Afhankelijk van de leverancier die je kiest, biedt een digitale handtekening niet alleen de handtekening zelf. Je bent er ook zeker van dat alle software technisch up-to-date blijft en dat je op de hoogte blijft van de laatste innovaties in de markt. Zeker zo belangrijk is de oplossing blijft aansluiten op de actualiteit van Nederlandse én Europese wet- en regelgeving. Met een duidelijke roadmap houd je jouw doelen voor ogen, die meebewegen met alle ontwikkelingen.

pondres

Inhoudsopgave

Contact

Onze digitale transformatie-aanpak

Pondres ondersteunt haar klanten bij hun transitie naar digitale (transactionele) communicatie. Dat doen we door digitale klantcommunicatie eenvoudig en toegankelijk te maken met innovatieve oplossingen. Veel informatie-intensieve organisaties binnen het publieke en financiële domein maken gebruik van onze diensten. Deze sterk gereguleerde markten vragen om robuuste oplossingen die voldoen aan de strenge wet- en regelgeving. We werken voor klanten waar betrouwbaarheid, innovatie en kwaliteit voorop staan.

Ons Digitale Communicatieportfolio geeft jou toegang tot een groot aantal digitale verzendkanalen. Denk aan een digitale handtekening, het veilig en aangetekend verzenden van (privacy- en bedrijfsgevoelige) informatie met secure e-mail of een digitale kluis. Op basis van jouw behoeften en wensen stellen we modules samen, op maat geconfigureerd in design en content. Manueel of automatisch (batch of on demand); jij bepaalt welke oplossing je wilt gebruiken, standalone of met één API-koppeling geïntegreerd in jouw systemen. Zo kun je efficiënt, relevant en onderscheidend communiceren, zonder maatwerk en tegen lagere kosten (TCO).

eSign voor jouw organisatie?

Wil je jouw documenten veilig en rechtsgeldig laten ondertekenen en wil je graag meer informatie over de mogelijkheden? Onze specialisten kijken graag welke toepassing en inrichting het best bij jouw onderneming past. Neem gerust contact met ons op via jouw vaste contactpersoon of één van onze specialisten. Dat kan via e-mail op info@pondres.nl of telefonisch via +31 88 949 41 00.

pondres

Inhoudsopgave

Bronnen

- Digitale overheid
- Connective

Kraaivenstraat 19 | 5048 AB Tilburg | info@pondres.nl | +31 88 949 41 00 | www.pondres.nl

pondres