

ZAKELIJKE EN JURIDISCHE COMPLIANCE MET MAXIMAAL VERTROUWEN

Vertrouwen en identiteit zijn noodzakelijk in een wereld vol digitale documenten

Papieren processen worden steeds meer vervangen door digitale documenten. Daardoor groeit de behoefte aan betrouwbare digitale ondertekening snel. Zonder vertrouwen kunnen bedrijven, overheden en individuen er niet zeker van zijn dat mensen en organisaties legitiem zijn en ontstaat het risico van manipulatie en fraude voor transacties, overeenkomsten en contracten.

DigiCert Document Signing Manager bewijst identiteit en biedt vertrouwen

Ook op het gebied van digitale ondertekening zijn niet alle oplossingen gelijkwaardig. DigiCert Document Signing Manager is gebouwd op Public Key Infrastructure, een beproefde technologie voor versleuteling, authenticatie en identiteit. Met Document Signing Manager wordt een document ondertekend met een cryptografisch beveiligde identiteit. Daardoor kan iedereen zien wie het heeft ondertekend en dat het document niet is gewijzigd.



Wat is een gekwalificeerde verlener van vertrouwensdiensten?

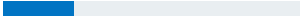
De regels voor ondertekening die worden voorgeschreven door de Europese Unie en de ETSI (European Technical Standard Institute) zijn de wereldwijde benchmark voor veilige ondertekening en identiteit. Binnen deze normen biedt een gekwalificeerde verlener van vertrouwensdiensten, ook wel Qualified Trust Service Provider of QTSP genoemd, de hoogste mate van zekerheid. Sinds de overname van QuoVadis wordt DigiCert door de EU en ETSI erkend als een van de beperkte groep partijen die voldoen aan de ondertekeningsnormen die zijn vastgelegd in de eIDAS-wetgeving. Ook komt DigiCert tegemoet aan de vereisten voor gekwalificeerde handtekeningen van ZertES, de Zwitserse wetgeving op dat gebied.

De documentondertekening van DigiCert + QuoVadis wordt beschouwd als equivalent aan een handgeschreven handtekening en geldt op veel plaatsen als bewijs van identiteit, gelijkwaardig aan een door de overheid uitgegeven identiteitsbewijs.

De ondertekeningsoplossingen van DigiCert voldoen dan ook ruimschoots aan de strengste normen voor veilige ondertekening, authenticatie en identiteit overal ter wereld.

Verschillende zekerheidsniveaus voor verschillende documenten

Afhankelijk van de mate van zekerheid die een individu of organisatie nodig heeft, verschillen de vereisten voor en validatie van erkende digitale handtekeningen.

Soort handtekening	Basic/Standard Electronic Signature (SES)	Advanced Plus Digital Signature (ADS/AATL)	Qualified Electronic Digital Signature (QES)
Vereisten voor handtekeningen	Een elektronische handtekening die een ondertekenaar toevoegt aan een document als bewijs van acceptatie of goedkeuring. Dit kan een als afbeelding gescande handtekening zijn of een druk op de knop 'Ik ga akkoord'.	Een digitale handtekening die voldoet aan specifieke vereisten, die een hoger niveau biedt aan identiteitsverificatie, beveiliging en bewijs dat een document niet is gemanipuleerd.	Een digitale handtekening die voldoet aan de strengste vereisten en wordt geleverd door een gekwalificeerde verlener van vertrouwensdiensten (QTSP) die voorkomt op de EU Trusted List (ETL) en is gecertificeerd door een EU-lidstaat of een QTSP op de Zwitserse Trusted List. Deze geavanceerde digitale handtekening wordt gebruikt als equivalent voor een traditionele handtekening.
Vereisten met betrekking tot zekerheid en identiteitsvalidatie	Geen	Handtekening gekoppeld aan unieke ondertekenaar Ondertekenaar identificeerbaar door nationaal identiteitsbewijs, maar zonder garantie De handtekening wordt gemaakt met specifieke identiteitsgegevens waarover alleen de ondertekenaar controle heeft De handtekening is gekoppeld aan de ondertekende gegevens, waarin wijzigingen detecteerbaar zijn De handtekening is gekwalificeerd voor de Adobe Approved Trust List (AATL)	De QTSP moet de integriteit en authenticiteit van de ondertekenaar controleren: 1. De gegevens waarmee de elektronische handtekening is aangemaakt, zijn beveiligd en vertrouwelijk 2. De identiteit van de ondertekenaar kan worden aangetoond door de QTSP op basis van een persoonlijke ontmoeting of vergelijkbaar streng proces ter verificatie van de identiteit
Voorbeelden	Medewerkers tekenen documenten tijdens onboarding Commerciële overeenkomsten tussen zakelijke entiteiten Consumentenovereenkomsten Softwarelicenties	Overeenkomsten voor kredieten en leningen voor consumenten Collectieve arbeidscontracten Arbeidsovereenkomst tussen een agent en medewerker	Lease-, overdrachts- en onroerendgoedcontracten Documenten op het gebied van familierecht Oprichtingsakte van een vennootschap met beperkte aansprakelijkheid
eIDAS Level of Assurance (LoA)	Lage zekerheid 	Aanzienlijke zekerheid 	Hoge mate van zekerheid 
Validatieniveau	Geen validatie	Gedeeltelijke validatie	Maximale (grondige) validatie

Twee manieren om te tekenen

Als individu (eSignature)

Een natuurlijke persoon kan als individuele ondertekenaar gemakkelijk documenten ondertekenen zoals persoonlijke overeenkomsten voor onroerendgoedtransacties, bankrekeningen en vertrouwelijke informatie zoals medische gegevens.

Als organisatie (eSeal)

Bij bedrijven en overheden kan een rechtspersoon als organisatie-ondertekenaar tekenen namens een bedrijf of entiteit om te garanderen dat een document niet kan worden gewijzigd. Eventueel kunnen er vele documenten tegelijk worden ondertekend.

Het voordeel van documentondertekening

Geef uw klanten de mogelijkheid om overal en altijd digitaal te ondertekenen. Onze totaaloplossing omvat opties voor certificaten, technologie en automatisering die zowel een concurrentievoordeel als een betere klantervaring bieden.

Functionaliteit

Maatwerkworkflows voor ondertekening

Maak uitgebreide workflows met opties voor meerdere technologieën zoals Ascertia SigningHub, Adobe Acrobat Sign of DocuSign.

Moeiteloze validatie

Laat uw klanten op afstand en in een paar minuten een veilige identiteit maken met behulp van Verify by DigiCert powered by IDNow.

Vereenvoudigd sleutelbeheer

Bescherm sleutels in een Qualified Signature Creation Device die wordt gehost in een betrouwbare omgeving.

Gestroomlijnd beheer

Maak het beheerders gemakkelijk met gecentraliseerd beleid en controle over gebruikers en ondertekenaars.

Gedetailleerde tracking

Maak overzichten en controleer audittrails om te voldoen aan de voorschriften en beleidsregels van bedrijven en overheden.

Strengere beveiliging

Zorg voor een strengere beveiliging met opties voor meervoudige authenticatie.

Eenvoudige integratie

Integreer webservices en workflows van derden zoals Adobe Acrobat Sign, Ascertia Signing Hub enzovoort.

Flexibele implementatieopties

Werk met een gehoste of on-premises oplossing.

Belangrijkste voordelen

- Verlaag de kosten van papier, administratie en verzending
- Verbeter de loyaliteit en ervaring van klanten met eenvoudige onboarding- en ondertekeningsvereisten
- Verkort de doorlooptijd van transacties van dagen naar minuten
- Vergroot de beveiliging van waardevolle transacties
- Wek vertrouwen met rechtsgeldige handtekeningen
- Garandeer bedrijfscontinuïteit en werk aan een concurrentievoordeel
- Voldoe aan wereldwijde voorschriften en wetgeving

Technische specificaties en integratie

Protocollen voor digitale ondertekening

- Rest API
- CSC API

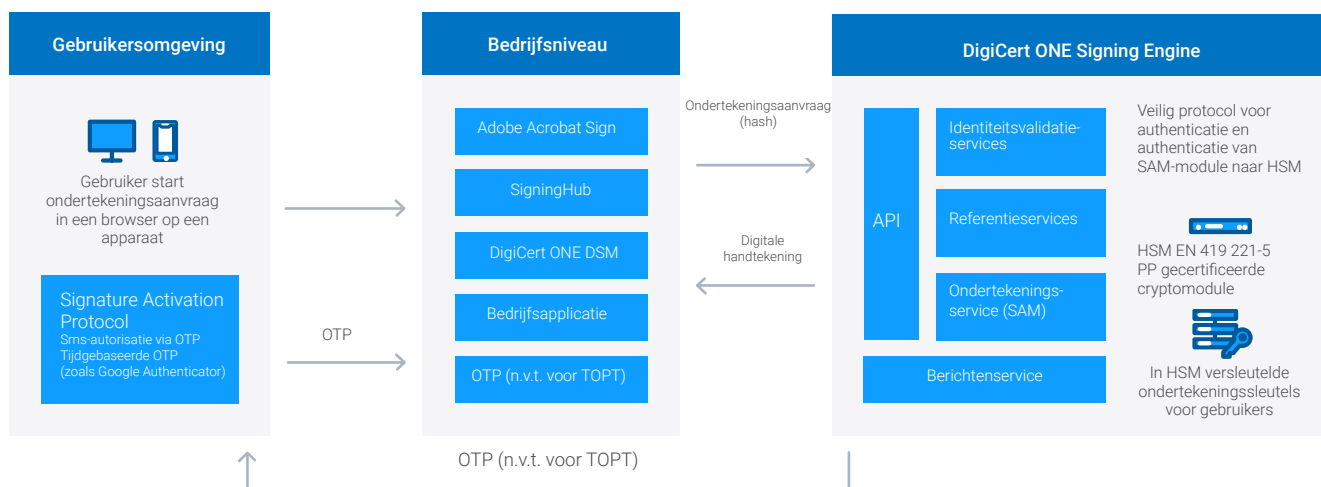
Beschikbare integratie

- Adobe Acrobat Sign
- Ascertia SigningHub
- DocuSign

Compatibel met

- Microsoft Office®
- Adobe® Acrobat & Adobe Reader
- LibreOffice®
- Open Office™
- Andere oplossingen van derden, zoals DocuSign
- Documenten in allerlei soorten bestandsindelingen, waaronder pdf, odf, docx en xml

Ondertekeningsarchitectuur in de cloud



DigiCert® ONE

Document Signing Manager is onderdeel van DigiCert ONE™, een moderne, holistische benadering van PKI-beheer. DigiCert ONE heeft een geavanceerde architectuur die is gebaseerd op containers. Daarmee implementeert u services in een fractie van de tijd die het voorheen kostte en beheert u grote aantallen eindgebruikers en apparaten.

Voor meer informatie over DigiCert® Document Signing Manager neemt u contact op met een van onze PKI-specialisten via docsigning@digicert.com.

De vertrouwde leverancier van PKI

Bij DigiCert draait alles om het vinden van een betere manier om internet te beveiligen. Daarvoor zetten we ons al in sinds het allerprilste begin van ons bestaan. Dat is dan ook precies de reden waarom onze certificaten overal worden vertrouwd en miljoenen keren per dag worden gebruikt door bedrijven over de hele wereld. En daarom geven onze klanten ons al jarenlang de hoogste scores voor service en support. Dat is onze motivatie om toonaangevend te blijven in de sector en te blijven werken aan een innovatieve en veilige toekomst. DigiCert is de niet zo gemene deler van SSL, IoT, PKI en meer.