

Handleiding voor bedrijfsbeheerders

Nederlandstalig

Date	9 Juli 2025
Author	Customer Succes
Version	2025-v1

Revisions

Version	Date	Author	Changes Made (*)
2025-v1	9 Juli 2025	Customer Success	Initial version

(*) All changes are marked in grey highlight.

1	Introductie	5
1.1	Introductie	5
1.2	Doelstellingen	5
2	Aan de slag.....	6
2.1	Vereisten	6
2.1.1	Digidentity Wallet.....	6
2.2	Appvereisten	6
2.2.1	Minimale app versie:.....	6
2.2.2	Documenten.....	6
2.3	My Digidentity	6
2.4	De Digidentity Wallet	7
2.4.1	Functies van de app	7
2.4.2	Wallet Maatwerk	7
2.5	Kleur:	7
2.5.1	Logo Specificaties:.....	7
3	Het Self-Service Portaal.....	8
3.1	Wat is het Self-Service Portaal?	8
3.1.1	Instructievideo: Een rondleiding door het Self-Service Portaal.....	8
3.2	Instructievideo: Medewerkers uitnodigen voor eHerkenning met rollen	8
3.2.1	Instructievideo: accepteren uitnodiging. (Engels en Nederlands beschikbaar)	9
4	eHerkenning / bedrijfsbeheerder	10
4.1	Digidentity Wallet app en authenticator	10
4.1.1	Persoonsgegevens aanleveren.....	10
4.1.2	Bedrijfsgegevens aanleveren	10
4.1.3	Instructievideo: registratie eHerkenning	10
4.1.4	Instructievideo: Een ondertekende brief uploaden met de Digidentity Wallet app.....	11
4.1.5	Instructievideo: paspoort uploaden.....	11
4.2	Bedrijfsbeheerderstatus aanvragen.....	11
4.3	Wat moet ik doen als er geen bestuurder is om te ondertekenen?.....	11
5	Ketenmachtigingen.....	12
5.1	Een ketenmachtiging verlenen aan uw intermediair	12
5.1.1	Instructievideo: Een ketenmachtiging geven aan een intermediair	12
5.2	Een ketenmachtiging aanvragen om in te loggen namens uw cliënt.....	12
5.2.1	Instructievideo: Een ketenmachtiging aanvragen als intermediair	13
5.2.2	Hoe kan ik controleren of de ketenmachtiging goed is ingesteld?.....	13
6	Ondertekening.....	14
6.1	Advanced Electronic Signature (AdES) en Qualified Electronic Signature (QES).....	14
6.2	Digidentity AdES & QES	14
6.2.1	AdES	14
6.2.2	QES	14
6.3	eSGN.com	16
6.3.1	Hoe upload ik een document om zelf te ondertekenen	16
6.3.2	Hoe upload ik een document dat iemand anders kan ondertekenen.....	16
6.3.3	Instructievideo: Een signflow starten op eSGN.com	16
6.4	Adobe Acrobat sign	16
6.4.1	Registratie	17
6.4.2	Adobe Sign Flow.....	17
6.4.3	Vereisten:	17
6.5	DocuSign	18
6.5.1	Instructievideo voor Docusign.....	18
7	ESeal.....	19
7.1	Wat is eSeal?.....	19
7.1.1	Kenmerken van een eSeal:.....	19
7.2	ESeal registreren	19
7.3	EPREL – Organisation identifier	19
8	Foutcodes en ondersteuning.....	20
8.1	Toegang tot ondersteuning.....	20

8.1.1 Contactgegevens20

8.2 Inlogproblemen20

8.2.1 Verwijder de app niet!.....20

8.2.2 Ik heb de app van mijn apparaat verwijderd20

8.2.3 Ik ben mijn wachtwoord/pincode vergeten.....20

8.2.4 Ik ontvang geen meldingen van de app.....21

8.3 Problemen bij het registreren.....21

8.3.1 Medewerker heeft de status 'in afwachting'.....21

8.4 Problemen bij het uploaden van het identiteitsbewijs21

8.4.1 Verlopen documenten.....21

8.4.2 Problemen met het scannen van het identiteitsbewijs21

8.5 App-foutcodes21

8.5.1 Orange Dolpin.....21

8.5.2 Purple Kangaroo22

8.5.3 Green Tiger22

8.5.4 Maroon Parrot22

8.5.5 Lemon Turtle22

8.5.6 White Whale/Yellow Pidgeon.....23

8.5.7 Technische documentatie23

8.6 Nieuwe telefoon toevoegen aan uw account.....23

8.7 Ik heb wél toegang tot mijn oude toestel en certificaat23

8.8 Ik heb geen toegang tot mijn oude toestel.....23

8.8.1 Certificaat herstellen24

1 Introductie

1.1 Introductie

Digidentity helpt je met alles rondom identiteits- en toegangsbeheer, op allerlei gebieden. Of je Digidentity nu gebruikt voor het verifiëren van iemands identiteit of voor het inloggen, in deze handleiding vind je alle info die je nodig hebt om snel aan de slag te gaan met het Digidentity Self-Service Portaal.

We leggen uit wat je nodig hebt om het systeem te gebruiken, hoe je ermee werkt, hoe je rapporten maakt en waar je terecht kunt bij problemen of vragen. Krijg je vragen van je gebruikers? Dan helpt deze handleiding je om snel een antwoord te vinden.

1.2 Doelstellingen

Deze handleiding is bedoeld voor alle bedrijfsbeheerders en helpt je met de belangrijkste info en stappen om soepel en efficiënt met het Digidentity Self-Service Portaal te werken. Zo haal je het beste uit de beschikbare functies én de ondersteuning.

2 Aan de slag

In dit deel van de handleiding lees je alles over de belangrijkste onderdelen van het Digidentity Self-Service Portaal, plus wat je nodig hebt om ermee aan de slag te gaan.

Wil je een van onze diensten afnemen? Stuur dan een mailtje naar ons salesteam via Sales@digidentity.com om een demo en adviesgesprek in te plannen.

2.1 Vereisten

1. Om gebruik te maken van de diensten van Digidentity, heb je de Digidentity Wallet app op je telefoon nodig. Voor sommige diensten, zoals identiteitsverificatie, moet je ook een geldig ID bij de hand hebben. In dit deel lees je wat je nodig hebt om de app te installeren en hoe je je documenten voorbereidt.

2.1.1 Digidentity Wallet

2. Om de Digidentity Wallet-app te gebruiken, heb je een smartphone of tablet nodig waarop je apps kunt installeren. De app kan niet worden geïnstalleerd op een computer of laptop.

App Icoon:



2.2 Appvereisten

Om de Digidentity Wallet-app te gebruiken, heeft u een mobiele telefoon nodig die voldoet aan de volgende minimale vereisten:

- IOS-versie 15 of hoger voor Apple iPhone.
- Android-versie 9 of hoger voor Android-smartphones.
- Een hoofdcamera (achterkant) en een selfiecamera (voorkant).

Voor de meest recente appvereisten kunt u de volgende pagina raadplegen: [Appvereisten](#)

Belangrijk (!) Android Go, unieke besturingssystemen zoals Oppo en Xiaomi, en telefoons die geroot of op een andere manier gewijzigd zijn, worden niet ondersteund.

2.2.1 Minimale app versie:

De minimale versie van de Digidentity app betreft 6.40.0 for Android en 6.35.0 for iOS. Lagere versies van de Digidentity app werken mogelijk niet of niet correct.

Geroot/Jailbroken Apparaten

Om veiligheidsredenen ondersteunt Digidentity Wallet geen gerootte/jailbroken apparaten.

Aanvullende eisen voor gekwalificeerde producten

Registreer je een eSGN(+) Qualified, eHerkenning niveau 4 of Digidentity Certificaatbeheerder product? Kijk dan op de volgende pagina voor aanvullende eisen aan jouw smartphone: [Eisen aan RemotelD](#).

2.2.2 Documenten

Digidentity biedt digitale identiteits- en vertrouwensproducten. Afhankelijk van het product kunnen de vereiste documenten variëren. Voor al onze producten gelden echter de volgende algemene documentvereisten:

- Documenten moeten geldig zijn en niet verlopen.
- Documenten mogen niet gestolen of vervalst zijn.
- Documenten moeten toebehoren aan de persoon die zich identificeert.
- Rijbewijzen en identiteitskaarten moeten een fotokaart zijn; papieren rijbewijzen worden niet geaccepteerd.

Heb je vragen over de documentvereisten voor een specifiek product? Neem contact op via: Customersuccess@digidentity.com.

2.3 My Digidentity

My Digidentity is jouw persoonlijke accountpagina bij Digidentity. Vanuit je account kun je onder andere het volgende doen:

- Je persoonlijke gegevens aanpassen
- Je accountinstellingen beheren (zoals 2FA updaten of je account deactiveren)
- Extra producten aanschaffen (via het tabblad 'Services')
- Naar het Self-Service Portaal gaan (via het tabblad 'Bedrijven')
- Verdergaan met een lopende registratie (ook via 'Services')

2.4 De Digidentity Wallet

De Digidentity Wallet-app is nodig voor je registratie en het dagelijks gebruik. Met deze veilige app kun je je makkelijk registreren en later veilig blijven inloggen. Je kunt de app downloaden op je smartphone of tablet via de Apple App Store of de Google Play Store.

2.4.1 Functies van de app

Document- en identiteitsverificatie: Onze app biedt een veilige manier om foto's van uw documenten en een selfie voor identiteitsverificatie te uploaden.

Twee-factor-authenticatie (2FA):

Voor extra veiligheid gebruik je de Digidentity Wallet-app om twee-factor-authenticatie in te stellen. Dit werkt vergelijkbaar met apps zoals Google Authenticator of Microsoft Authenticator. Je ontvangt via de app een veilige bevestiging wanneer je bijvoorbeeld inlogt of een belangrijke handeling uitvoert.

Daarom is het belangrijk dat je de app op je telefoon laat staan en niet verwijdert. Zonder de app kun je namelijk niet meer inloggen of je identiteit bevestigen.

Je gebruikt een eenvoudige 5-cijferige pincode om snel en veilig te bevestigen dat jij het bent.

eSGN Document Signing: Als u een abonnement heeft op ons eSignature-product, kunt u de app gebruiken om documenten veilig digitaal ondertekenen.

2.4.2 Wallet Maatwerk

De Digidentity Wallet is voorzien van een productkaart voor elk product dat je hebt gekocht. Deze kaarten kunnen worden aangepast om de branding van uw bedrijf weer te geven. In het volgende deel van de handleiding worden de noodzakelijke vereisten voor het personaliseren van de kaarten uiteengezet. Neem voor alle verzoeken om maatwerk contact op met uw Customer Success contactpersoon of stuur een e-mail naar customersuccess@digidentity.com. Hieronder vindt u de relevante specificaties en vereisten voor het personaliseren van uw productkaarten.

2.5 Kleur:

Specificaties van de kleur moeten worden ingediend in Hex Color-codes om ervoor te zorgen dat de kleur een nauwkeurige weergave is van het merk van het bedrijf. Bijv. #ef0604.

2.5.1 Logo Specificaties:

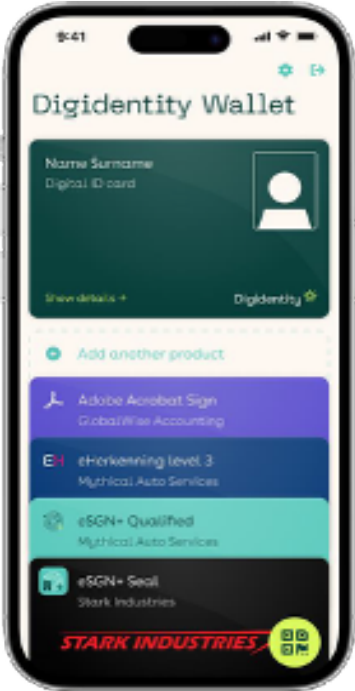
De volgende tabel geeft een overzicht van de specificatievereisten voor het bedrijfslogo op de productkaart.

Parameter	Waarde
Totale kaartgrootte	366 px breed x 230 px hoogte
Framemaat	1098 px breed x 690 px hoogte
Grootte van het logo	855 px breed x 165 px hoogte
Plaatsing van het logo	Gecentreerd in het veilige gebied van het frame
Formaat exporteren	Transparante PNG

Specificaties



Praktische toepassing



3 Het Self-Service Portaal

3.1 Wat is het Self-Service Portaal?

Het Self-Service Portaal (SSP) is een beveiligde online beheeromgeving. Om in te loggen op het Self-Service Portaal, ga naar: <https://selfservice.digidentity.eu>

Het SSP is ontworpen om beheerders te voorzien van alle benodigde tools om hun producten en diensten effectief te beheren. Het vergemakkelijkt ook het activeren van gebruikers, zodat zij efficiënt toegang krijgen tot en gebruik kunnen maken van de benodigde diensten. De belangrijkste functionaliteiten van de SSP zijn onder andere:

- Uitnodigen versturen voor registratie op een specifiek product
- Inzage in de status van de producten van medewerkers
- Facturen en facturatie-instellingen beheren
- Machtigingen beheren (inclusief rollen instellen, vernieuwen en intrekken)
- Abonnementen beheren

Dit gedeelte van de handleiding biedt een stapsgewijze uitleg over hoe de belangrijkste functionaliteiten van het SSP uitgevoerd kunnen worden. De video hieronder kunt u bekijken om een indruk te krijgen van de mogelijkheden binnen het SSP.

3.1.1 Instructievideo: Een rondleiding door het Self-Service Portaal



3.2 Instructievideo: Medewerkers uitnodigen voor eHerkenning met rollen

U kunt in het SSP ook medewerkers uitnodigen voor eHerkenning. Wij raden ten zeerste aan om voordat u dit doet eerst gebruik te maken van onze 'Rollen' functionaliteit. Hieronder kunt u een korte instructie video hiervan vinden.

Het 'Rollen' tabblad is gemaakt om het beheer van eHerkenning machtigingen van uw medewerkers eenvoudig en overzichtelijk te houden.



3.2.1 Instructievideo: accepteren uitnodiging. (Engels en Nederlands beschikbaar)

Hieronder vind je een video over hoe het accepteren van een uitnodiging in zijn werking gaat. Wat je hier goed kan zien is hoe het proces er voor nieuwe gebruikers uit ziet en wat ze tijdens de registratie allemaal moeten doen.



4 eHerkenning / bedrijfsbeheerder

Om bedrijfsbeheerder te worden dient u eerst minimaal een afgeronde eHerkenning niveau 3 compleet registratie in uw account te hebben.

Hoe u een registratie kunt starten en wat u kunt verwachten tijdens de registratie kunt u vinden in de instructievideo bij hoofdstuk 4.1.3

4.1 Digidentity Wallet app en authenticator

Voor de aanvraag van eHerkenning moet Digidentity uw identiteits- en uw bedrijfsgegevens vaststellen. Hiervoor dient u via een veilige omgeving enkele documenten naar ons te uploaden. Dit wordt gedaan via de gratis Digidentity Wallet app voor uw smartphone. U vindt deze in de Apple App Store (iPhone) of Google Play Store (Android).

U maakt ook een authenticator aan. Dit is een twee factor authenticatie methode, verzegeld door een, door u bedachte, pincode. Deze vindt u in de Digidentity Wallet app en wordt in het vervolg gebruikt om in te loggen.

4.1.1 Persoonsgegevens aanleveren

Tijdens het aanvraagproces controleren wij uw identiteit aan de hand van uw legitimatiebewijs en selfie. Deze kunt u aanleveren via de veilige omgeving in de Digidentity Wallet app.

Let op: Buitenlandse rijbewijzen worden niet geaccepteerd als onderdeel van het verificatie proces.

Als de registratie vraagt uw volledige naam in te voeren, zorg ervoor dat de naam die u opgeeft overeenkomt met die op het door u gebruikte legitimatiebewijs. U kunt geen roepnamen of afkortingen gebruiken.

4.1.2 Bedrijfsgegevens aanleveren

Naast uw persoonsgegevens hebben wij ook uw bedrijfsgegevens nodig. Wij gebruiken uw KVK-nummer om een uittreksel bij de Kamer van Koophandel op te halen. Wij controleren of u gemachtigd bent om in te loggen namens uw bedrijf. Zo niet, dan maken wij één of meerdere brieven aan voor de tekenbevoegde personen in uw organisatie. De brief wordt, door de tekenbevoegde vermeld op de brief, via de Digidentity Wallet app geüpload. Nadat de brieven zijn gekeurd door de servicedesk (Werkdagen van 09:00 tot 17:00) kunt u direct gebruik maken van uw product.

4.1.3 Instructievideo: registratie eHerkenning



4.1.4 Instructievideo: Een ondertekende brief uploaden met de Digidentity Wallet app



4.1.5 Instructievideo: paspoort uploaden

Heeft de persoon alleen een paspoort? Dan kan hij deze ook gebruiken tijdens het uploaden van een brief.



4.2 Bedrijfsbeheerderstatus aanvragen

Nadat u uw eHerkenning registratie heeft afgerond kunt u de bedrijfsbeheerdersrol aanvragen. Om de bedrijfsbeheerdersrol aan te vragen, kunt u de onderstaande stappen volgen:

1. Log in op my.digidentity.eu via uw PC
2. Ga naar de tab 'Bedrijven' Klik op het 'Bedrijf'.
3. Klik op 'Verzoek om bedrijfsbeheerder te worden'
4. Ga aan de slag met de brieven.
5. Wanneer deze zijn goedgekeurd heeft u direct toegang tot het Self-Service Portal.

4.3 Wat moet ik doen als er geen bestuurder is om te ondertekenen?

Staat er geen bestuurder in het KvK? In zulke gevallen is het mogelijk in het KvK register een beheerder eHerkenning aan te stellen. Een beheerder eHerkenning is gemachtigd om het volledige eHerkenning beheer uit te voeren, en eventueel zelfs nieuwe beheerders aan te stellen.

U kunt op de website van het KvK eenvoudig een machtiging binnen uw organisatie wijzigen of toevoegen: <https://www.kvk.nl/wijzigen/organisatie/>

Vul uw KvK nummer in en ga naar het tabblad '**Functionaris(sen)**' en klik op '**Bevoegdheid of volmacht wijzigen**' en volg de stappen in uw scherm. Voor meer informatie kunt u contact opnemen met het KvK: <https://www.kvk.nl/hulp-en-contact/>

5 Ketenmachtigingen

Een ketenmachtiging is een koppeling tussen de eHerkenning producten van twee bedrijven. Om een ketenmachtiging te verzoeken of te verlenen is het van belang dat beide partijen eHerkenning hebben bij een van de eHerkenning-leveranciers en daar de betreffende stappen uitvoeren.

Wanneer u bedrijfsbeheerder bent kunt u ketenmachtigingen verlenen of verzoeken aan een ander bedrijf. Om een ketenmachtiging op te zetten dient u de stappen exact te volgen.

Als u een ketenmachtiging verzoekt of verleend, maar de andere partij nog geen stappen heeft genomen, dan functioneert de ketenmachtiging niet.

Om een ketenmachtiging te verlenen aan een intermediair, moet u een afgeronde aankoop hebben van "eHerkenning niveau 3 Compleet" op uw account en daarnaast de status van bedrijfsbeheerder aanvragen. Het verlenen van een ketenmachtiging aan uw intermediair is kosteloos, aangezien de rekening naar uw intermediair wordt gestuurd.

5.1 Een ketenmachtiging verlenen aan uw intermediair

5.1.1 Instructievideo: Een ketenmachtiging geven aan een intermediair



Mocht u nog meer informatie willen over ketenmachtiging kunt u onze Faq pagina raadplegen: [Ketenmachtiging faq](#)

5.2 Een ketenmachtiging aanvragen om in te loggen namens uw cliënt

Om een ketenmachtiging aan te vragen om in te loggen namens uw cliënt, dient u de volgende stappen te volgen. Allereerst moet u de registratie voor 'eHerkenning niveau 3 Compleet' hebben voltooid en daarna de status van bedrijfsbeheerder aanvragen.

Het aanvragen van een ketenmachtiging bij uw cliënt kost €24,20 (inclusief btw). Het aanvragen van een ketenmachtiging bestaat uit twee stappen. Als u slechts één stap afrondt, zal de ketenmachtiging niet bruikbaar zijn. Hieronder een korte instructievideo over het aanvragen van een ketenmachtiging als intermediair:

5.2.1 Instructievideo: Een ketenmachtiging aanvragen als intermediair



5.2.2 Hoe kan ik controleren of de ketenmachtiging goed is ingesteld?

Omdat een ketenmachtiging opgezet is uit 2 delen, is proberen in te loggen met het product de enige manier om te controleren of het werkt. Als beide partijen de producten goed hebben ingesteld met de juiste diensten, dan werkt het product direct.

Het is daarom essentieel dat u goed met de andere partijen communiceert tijdens het opzetten van de ketenmachtiging.

6 Ondertekening

6.1 Advanced Electronic Signature (AdES) en Qualified Electronic Signature (QES)

Digidentity is een Qualified Trust Service Provider (QTSP) zoals gedefinieerd in EU-verordening 910/2014 (eIDAS). Digidentity biedt wereldwijd diensten voor elektronisch ondertekenen aan. De eIDAS-verordening definieert drie verschillende soorten elektronische handtekeningen:

- 1. Electronic Signature (basis)
- 2. Advanced Electronic Signature (Digitale handtekening)
- 3. Qualified Electronic Signature (Digitale handtekening).

Een vergelijking van deze soorten elektronische handtekeningen is hieronder te zien:

	Electronic Signature	Advanced Electronic Signature (AdES)	Qualified Electronic Signature (QES)
Legally Binding	Yes, but in case of dispute signature will not be accepted	Yes, but in case of dispute specialists are needed to accept signature	Yes, equal to handwritten signature
Identity Verification	No	Yes, high degree of certainty of identity of signer	Yes, completely certain of identity of signer
Access	Everyone	Sole Control by signer	Sole Control by signer
Protection against modification	No	Yes, signature becomes invalid when document is modified after signing	Yes, signature becomes invalid when document is modified after signing
Burden of Proof	Party that initiates signature must prove the requirements of reliability are met	Party that initiates signature must prove the requirements of reliability are met	Party that challenges its authenticity must prove its inaccuracy.
Created or Issued	Everyone	Certificate Authority	Qualified Trust Service Provider
PKI based	No	Yes, electronic certificate for advanced signature	Yes, electronic certificate for qualified signature
Hardware required	No	Yes, electronic signature creation device	Yes, qualified signature creation device (QSCD)

6.2 Digidentity AdES & QES

In verband met EU-verordening 910/2014 (eIDAS) biedt Digidentity twee soorten handtekeningen aan.

- 1. Advanced Electronic Signature (Digitale handtekening)
- 2. Qualified Electronic Signature (Digitale handtekening).

Onze Digidentity Advanced Signatures en Qualified Signatures zijn opgenomen in the EU Trust List en Adobe Approved Trust List (AATL).

6.2.1 AdES

In tegenstelling tot onze Qualified elektronische handtekening, vereist de geavanceerde handtekening een lager betrouwbaarheidsniveau bij het voltooiën van de identiteitsverificatie. Het onboardingproces kan op afstand worden voltooid door middel van het uploaden van uw identiteitsbewijs via de Digidentity Wallet-app. We gebruiken liveness-detectie, gezichtsvergelijkingstechnologie en handmatige controles om de identiteit van een levend persoon te verifiëren.

De Geavanceerde Elektronische Handtekening (AdES) is een digitale handtekening die veiligere en een beter beveiligde oplossingen biedt dan andere digitale handtekeningen.

Hoewel ook AdES uniek is gekoppeld aan een individuele ondertekenaar, ligt de bewijslast in juridische zaken bij de ondertekenaar zelf.

6.2.2 QES

Vergeleken met de AdES vertrouwt onze QES op het valideren van identiteitsdocumenten met behulp van het uitlezen van de gegevens in de NFC-chip. Hierdoor is er geen noodzaak om de identiteit van de natuurlijke persoon te verifiëren aan de hand van een face-to-face ontmoeting. De Digidentity Remote Identificatie-oplossing maakt gebruik van technologie om een digitale identiteit te verkrijgen op een eIDAS Level High en eIDAS Qualified.

Door middel van deze oplossing stelt de QES van Digidentity de gebruiker in staat om zich binnen vijf minuten te registreren voor een QES. Een gebruiker kan vervolgens een document ondertekenen met behulp van eSGN.com, de Digidentity eSigning API of via onze partners die de Cloud Signature Consortium API hebben geïmplementeerd.

De Gekwalificeerde Elektronische Handtekeningen (QES) van Digidentity bewijzen de identiteit van de ondertekenaar én hun akkoord met de inhoud van uw document. Een QES is een gekwalificeerde elektronische handtekening die wordt ondersteund door EU-regelgeving en een gekwalificeerd certificaat dat de ondertekenaar onweerlegbaar identificeert, waardoor het document wordt beschermd tegen manipulatie of vervalsing. Een QES is uniek gekoppeld aan elke ondertekenaar en is juridisch even bindend als een handgeschreven handtekening in het Verenigd koninkrijk en in de hele EU.

De onderstaande tabel geeft een overzicht van de verschillende gebruikersvereisten die nodig zijn om een QES- of AdES-handtekening van Digidentity te verkrijgen.

Qualified Signature (QES)	Advanced Signature (AdES)
Document vereisten	
Paspoort (Chip vereist)	Paspoort
Rijbewijs (Chip vereist)	Rijbewijs
Nationale identiteitskaart of verblijfsvergunning (chip vereist)	Nationale identiteitskaart of verblijfsvergunning
*Minimale apparaatvereisten	
Android:	Android:
Qualified Signature (QES)	Advanced Signature (AdES)
Versie 9 of hoger voor Android-smartphones	Versie 9 of hoger voor Android-smartphones.
Een hoofdcamera (naar achteren gericht) en een selfiecamera (naar voren gericht).	Een hoofdcamera (naar achteren gericht) en een selfiecamera (naar voren gericht).
Hardware-veilige keystore.	
Minimum App Versie	
Android:	Android:
6.40.0	6.40.0
IOS:	IOS:
6.35.0	6.35.0

Altijd op de hoogte zijn van de juiste app vereisten? Bezoek dan onze website: [Digidentity Wallet app vereisten](#)

"Android Go, unieke besturingssystemen zoals die van Oppo en Xiaomi, en telefoons die zijn geroot of op andere wijze zijn aangepast, worden niet ondersteund. Om veiligheidsredenen ondersteunt Digidentity Wallet geen gerootte of geïllegaliseerde apparaten."

6.3 eSGN.com

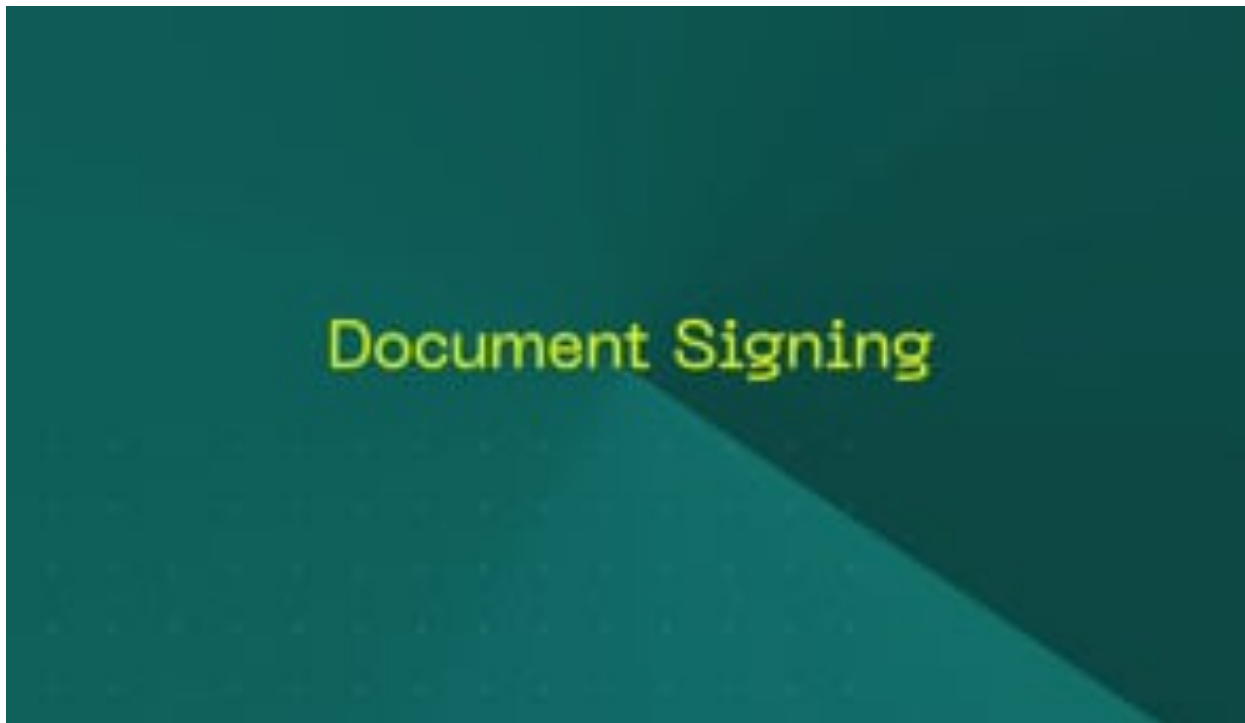
eSGN is het eSigning-platform van Digidentity dat kan worden gebruikt om elk PDF-document te ondertekenen waarvoor een digitale handtekening vereist is. eSGN is [hier](#) toegankelijk. Toegang tot het eSGN-portaal is inbegrepen in de prijs van het ondertekeningsproduct.

Vereisten voor gebruik:

1. Geldig QES/AdES Digidentity Signing Certificaat.
2. Documenten moeten in Pdf-formaat zijn.

6.3.1 Hoe upload ik een document om zelf te ondertekenen

De volgende instructie video geeft een beeld van hoe je een document kunt uploaden en direct ondertekenen, binnen het ondertekenplatform van Digidentity: eSGN.com



6.3.2 Hoe upload ik een document dat iemand anders kan ondertekenen.

De volgende instructie video geeft een beeld van hoe je een document kunt uploaden dat iemand anders kan ondertekenen, binnen het ondertekenplatform van Digidentity.

6.3.3 Instructievideo: Een signflow starten op eSGN.com



6.4 Adobe Acrobat sign

Als EU Qualified Trust Service Provider (QTSP) is Digidentity lid van de Adobe Approved Trust List, geïntegreerd met Adobe Acrobat Sign om digitale ondertekening mogelijkheden te vergemakkelijken. Adobe verkoopt onze geavanceerde en gekwalificeerde elektronische handtekeningen als onderdeel van het Adobe Acrobat Sign-aanbod.

6.4.1 Registratie

Het onboardingsproces voor het toewijzen van QES/AdES aan uw gebruikers kan variëren, afhankelijk van uw gebruikssituatie. De Adobe Sign-integratie biedt een extra registratieroute die het onderteken proces stroomlijnt. Dit aspect van de handleiding geeft een overzicht van beide scenario's en hoe het in de praktijk kan werken.

6.4.2 Adobe Sign Flow

De toegevoegde waarde van dit proces is dat het een gebruiker in staat stelt om binnen één workflow een document te registreren en te ondertekenen. Dit is vooral handig voor het verzenden van uitnodigingen naar eenmalige gebruikers voor het ondertekenen van contracten, enz. Het elimineert de noodzaak om eerst een uitnodiging te sturen met behulp van het Digidentity SSP.

6.4.3 Vereisten:

Digidentity Company Onboarding - Voordat dit proces kan worden ingeschakeld, moet een succesvolle onboarding op het Digidentity Platform worden voltooid. Zodra Digidentity het provision verzoek van Adobe ontvangt, neemt het Customer Succes Team contact op met de beheerder van je bedrijf om de onboarding te vergemakkelijken.

Adobe Account or Group ID – Om ervoor te zorgen dat de integratie actief is, moet Digidentity worden voorzien van het Adobe-account of de groeps-ID van je Adobe Admin Console.

- Een beheerder op accountniveau kan de account-ID vinden op het tabblad Algemene instellingen van het beheerdersmenu.
- De groeps-ID is te vinden door naar het tabblad Groepsinstellingen van de groep te gaan in het beheerdersmenu.

Meer informatie vindt u in Account-ID's en Groeps-ID's [hier](#).

Belangrijk (!)

De volgende effecten moeten in overweging worden genomen zodra de integratie is ingeschakeld:

Verzenden van documenten om te ondertekenen: Als een document wordt verzonden met het verzoek om een 'digitale handtekening', wordt dit afgetrokken van de vooraf aangeschafte hoeveelheid Digidentity-certificaten en worden ondertekening certificaten verstrekt aan gebruikers zonder een bestaand Digidentity-account. Daarom, als een QES/AdES niet vereist is, selecteer dan niet 'Digitale Handtekening' in de handtekeningvelden.

Meerdere aangekochte producten: Via de Adobe Reseller Overeenkomst biedt Digidentity twee soorten ondertekening certificaten aan: Onbeperkt Ondertekenen (eSignature+ Qualified) en certificaten voor eenmalig gebruik (eSignature Qualified 1 Sign).

Vanwege beperkingen kan de Adobe-workflow alleen onboarding voor één product faciliteren. Als u beide eSignature-producten heeft aangeschaft, moet u het Digidentity SSP gebruiken om uitnodigingen te verzenden voor het product dat niet door de integratie wordt ondersteund. Certificaten voor eenmalig gebruik (eSignature Qualified 1 Sign) zullen altijd het standaardproduct voor integratie zijn.

6.5 DocuSign

Digidentity is nu naadloos geïntegreerd in het DocuSign-platform, waardoor je je Digidentity Qualified Electronic Signature (QES) direct binnen het DocuSign-platform kunt gebruiken. Het volgende gedeelte van de handleiding beschrijft de stappen om dit proces te voltooien.

Belangrijk (!)

Om toegang te krijgen tot de Digidentity-diensten via je DocuSign-platform, moeten specifieke configuraties door DocuSign worden ingesteld. Als je deze wijzigingen moet aanvragen, neem dan rechtstreeks contact op met DocuSign voor hulp.

6.5.1 Instructievideo voor DocuSign



7 ESeal

7.1 Wat is eSeal?

eSeal kan het beste worden omschreven als een digitale stempel van een organisatie. Het is in feite een gekwalificeerde elektronische handtekening van een organisatie. De Qualified eSeal voldoet aan de hoogste eisen van eIDAS, de Europese wetgeving rond elektronische identificatie en authenticatie. Deze is vereist voor onder andere de EPREL-registratie.

Een eSeal (elektronische zegel) is een digitale variant van een bedrijfsstempel of -handtekening, bedoeld om de authenticiteit en integriteit van een elektronisch document of gegevens te waarborgen. Het wordt meestal gebruikt door bedrijven of organisaties (niet door individuen).

7.1.1 Kenmerken van een eSeal:

- Verifieert de herkomst: Laat zien dat het document afkomstig is van een specifieke organisatie.
- Garandeert integriteit: Je kunt zien of het document na het ondertekenen is gewijzigd.
- Gebaseerd op PKI (Public Key Infrastructure): Het is gekoppeld aan een gecertificeerd digitaal certificaat.

Verschil met een digitale handtekening:

Eigenschap	Digitale handtekening	eSeal
Wie ondertekent?	Natuurlijke persoon (individu)	Rechtspersoon (bedrijf)
Doel	Persoonlijke goedkeuring	Authenticatie door organisatie
Wettelijke waarde	Ja, onder eIDAS	Ja, onder eIDAS

7.2 ESeal registreren

Om de registratie te starten, moet je gebruikmaken van de onderstaande link. Zorg ervoor dat je tijdens dit proces een geldig identiteitsbewijs, telefoon en desktop bij de hand hebt.
[De registratie voor eSeal kan hier gestart worden](#)



7.3 EPREL – Organisation identifier

Wij bieden geen directe ondersteuning bij de EPREL-registratie. Een veelvoorkomende foutmelding bij de EPREL-registratie heeft betrekking op de ‘organisation identifier’. Vaak wordt aangegeven dat de Seal de organisatie niet match. Als dit gebeurt, moet het KVK-nummer handmatig worden ingevuld bij de EPREL-registratie en moet de '**Identity Type Reference code**' worden gewijzigd naar NTR. Mocht je hier niet uitkomen, neem dan direct contact op met EPREL via: ener-eprel-helpdesk@ec.europa.eu

Identificatie en machtiging

Om het certificaat te kunnen uitgeven, moet eerst de identiteit van de persoon die de Seal gaat gebruiken worden vastgesteld. De persoon die de registratie doorloopt, is dan ook de enige persoon die namens de organisatie de eSeal kan plaatsen, tenzij er een tweede registratie plaatsvindt. Degene die de eSeal gaat gebruiken, hoeft niet per definitie tekenbevoegd te zijn voor de organisatie. In het geval dat een medewerker een eSeal aanvraagt, kunnen machtigingsbrieven worden gebruikt die automatisch worden gegenereerd tijdens de registratie.

8 Foutcodes en ondersteuning.

In dit gedeelte van de handleiding vindt u gedetailleerde informatie over veelvoorkomende problemen en relevante foutcodes die van invloed kunnen zijn op gebruikers. Het bevat richtlijnen om u te helpen deze problemen effectief op te lossen, mochten deze zich voordoen.

8.1 Toegang tot ondersteuning

8.1.1 Contactgegevens

De contactgegevens van de betreffende Digidentity-afdelingen vind je in de onderstaande tabel:

Afdeling	Wanneer contact opnemen	Openingsuren	Contact
Klantenservice	Voor ondersteuning van eindgebruikers.	Maandag t/m vrijdag: 09:00 – 17:00 (CET)	helpdesk@digidentity.co.uk
Finance	Voor alle vragen over facturering.	Maandag t/m vrijdag: 09:00 – 17:00 (CET).	debiteuren@digidentity.com
Implementatie	Voor alle vragen over technische ondersteuning	Maandag t/m vrijdag: 09:00 – 17:00 (CET).	eid@digidentity.com .
Customer Success	Voor alle vragen met betrekking tot uw bedrijfsaccount en administratieve ondersteuning.	Maandag t/m vrijdag: 09:00 – 17:00 (CET).	customersuccess@digidentity.com

**Eindgebruikers die om ondersteuning vragen, moeten de volgende informatie verstrekken:*

- 1. Het product/de dienst waarvoor ze zich registreren*
- 2. De e-mail die aan hun account is gekoppeld.*
- 3. Bedrijf dat de uitnodiging heeft verstrekt.*

8.2 Inlogproblemen

8.2.1 Verwijder de app niet!

In geval van onverwachte problemen, verwijder niet de app van uw apparaat. Zodra uw account is beveiligd met een 5-cijferige pincode, functioneert de app als uw twee-factor authenticator. Als u de app verwijdert, wordt de authenticator ook verwijderd, waardoor u de toegang tot uw account verliest.

Als u problemen ondervindt, volgt u de stappen in dit document voor de specifieke app-foutcodes. Als het probleem met deze stappen niet is opgelost, neemt u contact op met de ondersteuning voor hulp in plaats van de app te verwijderen.

8.2.2 Ik heb de app van mijn apparaat verwijderd

Als u of een gebruiker de app van zijn apparaat heeft verwijderd, moet het herstelproces gestart worden.

8.2.3 Ik ben mijn wachtwoord/pincode vergeten.

Als een gebruiker zijn wachtwoord of 5-cijferige pincode vergeet, kan hij account herstel starten via www.digidentity.eu tijdens het inlogproces.

De gebruiker kan 'Wachtwoord vergeten' of 'Geen toegang' selecteren bij het inloggen op zijn account.

Als ze echter al hun inloggegevens (wachtwoord en pincode) kwijt zijn, is account herstel niet mogelijk. Zij moeten contact opnemen met de servicedesk.

Voor de meest actuele informatie over het herstellen van uw wachtwoord kunt u onze FAQ-pagina raadplegen:
[Hoe kan ik mijn vergeten wachtwoord herstellen](#)

Voor de meest actuele informatie over het herstellen van uw certificaat kunt u onze FAQ-pagina raadplegen:
[Certificaat herstellen](#)

8.2.4 Ik ontvang geen meldingen van de app

In zeldzame gevallen kan het voorkomen dat de melding die door de Digidentity Wallet-app wordt verzonden om in te loggen, niet aankomt.

In dit geval moet de gebruiker het volgende doen:

- 1. Controleer hun internetverbinding.
- 2. Check of notificaties zijn ingeschakeld voor de Digidentity Wallet App in de instelling van uw telefoon.
- 3. Controleer het meldingscentrum van uw apparaat om te zien of er meldingen zijn gemist
- 4. Klik op ‘Verstuur de melding opnieuw.’

Dit zou het probleem moeten oplossen. Maar als je nog steeds geen meldingen van de app ontvangt, neem dan contact op met de servicedesk.

8.3 Problemen bij het registreren

8.3.1 Medewerker heeft de status 'in afwachting'

Gebruikers kunnen soms afhaken bij het registratieproces voordat ze alle noodzakelijke stappen hebben voltooid. Ze moeten terugkeren naar hun registratie om de nodige stappen te voltooien voordat ze het product kunnen gaan gebruiken.

Gebruikers die hun registratie nog niet hebben voltooid, tonen een 'in afwachting' status op hun profiel in het SSP. Deze status betekent dat hun registratie onvolledig is.

Instructies registratie afronden:

- 1. Log in op <https://my.digidentity.eu/> met uw inloggegevens.
- 2. Zoek op de pagina 'Services' uw producten in behandeling onder ‘Ga verder met registreren’.
- 3. Klik op 'Ga verder' bij het product waarvan je de registratie wilt afronden.

8.4 Problemen bij het uploaden van het identiteitsbewijs

8.4.1 Verlopen documenten

Digidentity kan alleen documenten verifiëren die nog geldig zijn en de vervaldatum niet hebben overschreden. Voor het uploaden van verlopen documenten wordt de gebruiker geïnformeerd dat de vervaldatum van het document ongeldig is.

In dit geval wordt de gebruiker gevraagd om zijn documenttype te wijzigen in overeenstemming met de productvereisten. Als de gebruiker geen geldig identiteitsbewijs kan uploaden, kan hij niet doorgaan met de registratie.

8.4.2 Problemen met het scannen van het identiteitsbewijs

In sommige gevallen kunnen gebruikers problemen ondervinden bij het voltooien van het scan proces van hun identiteitsdocumenten. Omdat we NFC-technologie gebruiken om te controleren of er een NFC-chip aanwezig is.

De gebruiker moet ervoor zorgen dat hij het volgende nakijkt voor het geval hij problemen ondervindt bij het scannen van documenten:

- 1. Verwijder eventuele hoesjes van hun document of apparaat.
- 2. Zorg ervoor dat ze hun document waar mogelijk uploaden in een kamer met natuurlijk licht en voorkom reflecties.
- 3. Zorg ervoor dat NFC is ingeschakeld in de apparaat instellingen.

8.5 App-foutcodes

Voor de meest actuele informatie over algemene foutmelding kunt u onze FAQ-pagina raadplegen:

[Algemene foutmeldingen Digidentity wallet app](#)

8.5.1 Orange Dolpin

Foutmelding in de app	Uitleg van de foutmelding	Oplossing
Geen internetverbinding Het lijkt erop dat je apparaat geen verbinding heeft met internet. Controleer je internetverbinding, schakel tussen mobiele data en wifi, en probeer het opnieuw. → Probeer opnieuw → Annuleer	Geen internet Betekent dat er letterlijk geen internetverbinding is, dus Google.com zou ook niet werken. Bijvoorbeeld: het apparaat staat in vliegtuigmodus en is niet verbonden met wifi.	Controleer de internetverbinding → Zorg ervoor dat het mobiele apparaat van de eindgebruiker is verbonden met internet. → Adviseer de eindgebruiker om te switchen tussen mobiele data of wifi. → Zodra de verbinding is bevestigd, vraagt u de eindgebruiker om de

		knop "probeer het opnieuw" in het dialoogvenster te selecteren.
--	--	---

8.5.2 Purple Kangaroo

Foutmelding in de app	Uitleg van de foutmelding	Oplossing
Kon niet verbinden Je apparaat is verbonden met internet, maar de Digidentity wallet app kon de server niet bereiken. Controleer je internetverbinding, schakel tussen mobiele data en wifi, en probeer het opnieuw. → Probeer opnieuw → Annuleer	Onze backend is niet beschikbaar We kunnen geen verbinding maken met onze backend terwijl het apparaat wel met internet is verbonden. Mogelijke oorzaken zijn een VPN-probleem, proxy, DNS, een volledige storing van de backend of zelfs gewoon een zeer trage verbinding die tot een timeout leidt.	Verbinding aanpassen → Zorg ervoor dat het mobiele apparaat van de eindgebruiker is verbonden met internet. → Adviseer de eindgebruiker om te switchen tussen mobiele data en wifi. → Adviseer de eindgebruiker om alle actieve VPN-verbindingen uit te schakelen. → Zodra de verbinding is bevestigd, vraagt u de eindgebruiker om de knop "probeer het opnieuw" in het dialoogvenster te selecteren.

8.5.3 Green Tiger

Foutmelding in de app	Uitleg van de foutmelding	Oplossing
Kon niet verbinden Digidentity wallet app kon de server niet bereiken vanwege een probleem aan onze kant. Probeer het later nog eens of neem contact op met onze servicedesk om u verder te helpen. → OK	Onze backend werkt niet zoals verwacht Onze backend geeft onverwachte reacties terug, waaronder 5xx-fouten en soms zelfs 4xx-fouten in situaties die voor de app onverwacht zijn. Niet herstelbaar, geen knop "Opnieuw proberen".	Standaard probleemoplossing: → Update de app naar de nieuwste versie. → Sluit de app en start deze opnieuw op. Herstart eventueel het toestel. → Schakel tussen je Wifi en 4/5g verbinding

8.5.4 Maroon Parrot

Foutmelding in de app	Uitleg van de foutmelding	Oplossing
Niet ondersteund Apparaat wordt niet ondersteund Digidentity kan niet garanderen dat uw online identiteit veilig is omdat uw apparaat niet ondersteund wordt.	Apparaat is geïllegaliseerd (iOS) of geroot (Android) Volledig scherm blokkeert al het gebruik van de app omdat de gebruiker zijn iOS-apparaat heeft geïllegaliseerd of zijn Android-apparaat heeft geroot.	Unjailbreak/unroot het apparaat. De enige manier om met dit apparaat door te gaan, is door het apparaat te unjailbreaken/unrooten. Anders moet de eindgebruiker een apparaat gebruiken dat niet is geïllegaliseerd/geroot.

8.5.5 Lemon Turtle

Foutmelding in de app	Uitleg van de foutmelding	Oplossing
Je beschikt niet over de benodigde diensten om door te kunnen gaan en je kunt ze niet zelf registreren. Neem contact op met onze helpdesk voor meer informatie.	De service waartoe u toegang probeert te krijgen, kan alleen op uitnodiging worden verkregen.	Gebruikers moeten contact opnemen met de beheerders van hun bedrijf of contact opnemen met Digidentity Support voor verdere verduidelijking.

8.5.6 White Whale/Yellow Pidgeon

Foutmelding in de app	Uitleg van de foutmelding	Oplossing
Er ging iets mis Er ging iets mis, excuses voor het ongemak. Probeer het opnieuw. Als het probleem aanhoudt, probeer het dan later nog eens of neem contact op met onze servicedesk om u verder te helpen. → Probeer opnieuw → Annuleer	Algemene standaardfout Een standaardfoutcode wordt gebruikt voor fouten die niet in een van de andere categorieën kunnen worden ingedeeld.	Standaard probleemoplossing: → Update de app naar de nieuwste versie. → Sluit de app en start deze opnieuw op. → Schakel tussen je Wifi en 4/5g verbinding → Start uw apparaat opnieuw op. → Schakel de VPN op uw apparaat uit.

Voor de meest actuele informatie over Digidentity foutcodes kunt u onze FAQ-pagina raadplegen:

[Foutmeldingen FAQ](#)

8.5.7 Technische documentatie

Voor klanten die via onze API's (Application Programming Interface) of IDK (Integration Development Kit) verbonden zijn met het Digidentity platform, is alle benodigde informatie online te vinden in onze [Connection Documentation](#).

De volledige technische specificaties van de API's van Digidentity zijn te vinden op <https://docs.digidentity.com>.

8.6 Nieuwe telefoon toevoegen aan uw account

Wanneer u of een medewerker een nieuw toestel wilt gebruiken zijn er meerdere scenario's aanwezig. Hieronder zullen wij de mogelijkheden bespreken per geval.

8.7 Ik heb wél toegang tot mijn oude toestel en certificaat

Voor de meest actuele informatie over het vernieuwen van u certificaat kunt u onze FAQ-pagina raadplegen:

[Hoe vernieuw ik een certificaat?](#)

8.8 Ik heb geen toegang tot mijn oude toestel



8.8.1 Certificaat herstellen

Voor de meest actuele informatie over het herstellen van uw certificaat kunt u onze FAQ-pagina raadplegen:

[Hoe herstel ik een smartcard](#)