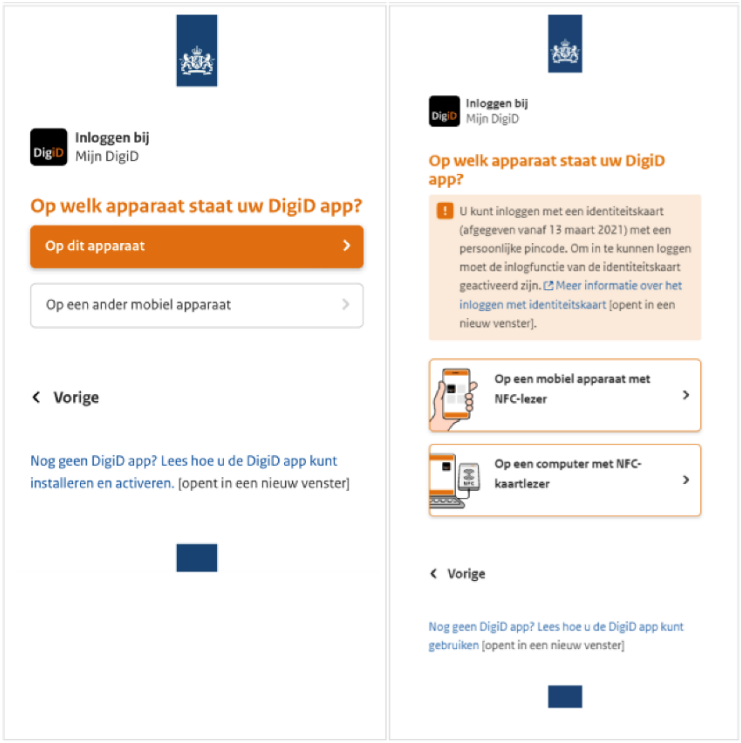
13-12-2023

Rapportage Onderzoek Elektronisch Ondertekenen Documenten



Inhoud

Inhoud

Management Samenvatting

Context

Verschillende processen, zoals keuzes rond pensionering, afkoop klein pensioen, waardeoverdracht, keuzes met betrekking tot pensionering vereisen een handtekening van de deelnemer en soms ook van de partner van de deelnemer. Deze processen zijn juridisch bindend en beïnvloeden de pensioenhoogte en -duur. Elektronisch ondertekenen biedt voordelen maar brengt uitdagingen met zich mee, zoals rechtsgeldigheid, veiligheid en documentbeheer.

Opdrachtomschrijving

De opdracht heeft verschillende aspecten:

- Leg het juridisch kader rond het zetten van een elektronische handtekening uit.
- Geef aan welke uitdagingen een pensioenuitvoerder heeft als gaat om het (laten) zetten van een elektronische handtekening. Laat zien wat hier verantwoorde keuzes zijn.
- In de huidige praktijk bevestigen deelnemers steeds vaker gemaakte keuzes in een portaal van de pensioenuitvoerder. Dit nadat ze met DigiD zij ingelogd. Geef aan in hoeverre dit een verantwoorde werkwijze is.
- Geef tevens aan of we stappen kunnen nemen om het elektronisch ondertekenen in de pensioensector te uniformeren voor met name deelnemers en partners van deelnemers.

Afbakening werkgebied en aanpak

We definiëren het werkgebied, leggen sleutelbegrippen vast en verduidelijken wat buiten de scope valt.

Het verschil tussen elektronische en digitale handtekeningen wordt uitgelegd, waarbij digitale handtekeningen als subset van elektronische handtekeningen worden benoemd. In dit rapport geven we de voorkeur aan de term elektronische handtekening ook al omdat we hiermee aansluiten bij eIDAS.

De aanpak omvat bureauonderzoek, onderzoek bij leveranciers en navraag via de werkgroep IDP om onderzoeksvragen te beantwoorden.

Voordelen van elektronische handtekeningen worden besproken, waaronder efficiëntie, kostenverlaging en beveiliging. Mogelijke nadelen zoals beveiligingszorgen, technologische afhankelijkheid en initiële kosten stellen we ook aan de orde. Het belang van authenticatie wordt benadrukt voor elektronische handtekeningen, met verschillende registratieprocessen om een sterke binding tussen identificatiemiddel en persoon te creëren.

Vervolgens stellen we het gebruik van elektronische handtekeningen in de pensioensector en de ervaringen van pensioenuitvoerders aan de orde. Voorts vermelden we verschillende situaties waarbij handtekeningen nodig zijn. We geven voorbeelden van toepassingen bij verschillende pensioenuitvoerders. Verschillende benaderingen en technieken voor ondertekening worden geïllustreerd.

Conclusies

De conclusies zijn geformuleerd in perspectief van de gestelde onderzoeksvragen.

Leg het juridisch kader rond het (laten) zetten van een elektronische handtekening uit
Dit kader is uitgebreid aan de orde gesteld in hoofdstuk 4 en Bijlage A t/m C.

Geef aan welke uitdagingen een pensioenuitvoerder heeft als gaat om het zetten van een elektronische handtekening. Laat zien wat hier verantwoorde keuzes zijn.
Het implementeren van elektronische handtekeningen in de pensioensector brengt verschillende uitdagingen met zich mee voor pensioenuitvoerders:

- Juridische en regelgevingsuitdagingen;

- Beveiligingsuitdagingen;
- Technologische infrastructuur;
- Gebruikersacceptatie;
- Diverse processen en partijen;
- Verandering in werkstromen;
- Privacy en gegevensbescherming;
- Onderhoud en updates.

In de huidige praktijk bevestigen deelnemers steeds vaker gemaakte keuzes in een portaal van de pensioenuitvoerder. Dit nadat ze met DigiD zij ingelogd. Geef aan in hoeverre dit een verantwoorde werkwijze is.
DigiD is ontworpen om een bepaald niveau van betrouwbaarheid te bieden bij het verifiëren van de identiteit van gebruikers voor veel online transacties. Echter, de mate van betrouwbaarheid kan variëren afhankelijk van het specifieke gebruik en de context.
Hoewel DigiD geen elektronische handtekening is, kan het worden gebruikt als een methode om te bevestigen wie een handeling heeft uitgevoerd. Het niveau van authenticatie met DigiD is op zich voldoende voor een geavanceerde elektronische handtekening. Maar omdat de handtekening niet wordt vastgehecht aan de ondertekende gegevens is er geen sprake van een elektronische handtekening, zoals bedoeld in het Burgerlijk Wetboek (3:15a).

Het rapport bespreekt de betrouwbaarheidsniveaus van DigiD (Basis, Midden, Substantieel en Hoog) en hoe deze niveaus overeenkomen met eIDAS-niveaus.

Geadviseerd wordt DigiD op minstens niveau substantieel af te dwingen, de gemaakte keuzes te bevestigen en de deelnemer te vragen om binnen een bepaalde termijn te reageren als het niet in orde is. De pensioenuitvoerder moet hierbij rekening houden met de wetgeving rond elektronische informatieverstrekking.

Geef tevens aan of we stappen kunnen nemen om het elektronisch ondertekenen in de pensioensector te uniformeren voor met name deelnemers.
In de markt zijn verschillende aanbieders met verschillende processen en werkwijzen. Dit maakt het creëren van een uniforme gebruikerservaring bij het ondertekeningsproces - zodat bijvoorbeeld deelnemers gemakkelijk en consistent door het proces kunnen navigeren, ongeacht het type document – lastig.

Aanbevelingen

Dwing DigiD substantieel af, bevestig keuzes van deelnemers en bied de mogelijkheid om bezwaar te maken
Geadviseerd wordt DigiD op minstens niveau substantieel af te dwingen, de gemaakte keuzes te bevestigen en de deelnemer te vragen om binnen een bepaalde termijn te reageren (bezwaar te maken) als het niet in orde is. De pensioenuitvoerder moet hierbij rekening houden met de wetgeving rond elektronische informatieverstrekking.

Zet Websiteanalysetools in
Websiteanalysetools zijn instrumenten die pensioenuitvoerders kunnen inzetten om het gedrag van bezoekers op hun portalen te meten, analyseren en rapporteren. Deze tools bieden waardevolle inzichten in hoe gebruikers interacteren met een portaal, ook op individueel niveau. Zie ook lijst met begrippen.

Zoek balans
Het is onnodig elk document op het hoogste niveau te ondertekenen. Het gebruik van het hoogste niveau van zekerheid, zoals een gekwalificeerde handtekening, brengt vaak extra kosten met zich mee. Het is belangrijk om de juiste balans te vinden tussen de benodigde zekerheid en de kosten en moeite die ermee gemoeid zijn. Ook de gebruikersvriendelijkheid speelt een rol. Voor minder belangrijke documenten of situaties waarbij een lager zekerheidsniveau volstaat, kan een geavanceerde

handtekening gebruikt worden. Op deze manier kan een pensioenuitvoerder efficiënter opereren zonder onnodige kosten te maken. De keuze van de zekerheid hangt af van de waarde en het risico dat ermee gemoeid is. Het is een keuze die een pensioenuitvoerder zelf moet maken.

Win juridisch advies in
Het is verstandig om advies in te winnen bij juridische professionals als een pensioenuitvoerder van plan is elektronische handtekeningen te gebruiken voor belangrijke juridische transacties. In sommige gevallen kunnen bevestigingen na inloggen op een hoog betrouwbaarheidsniveau mogelijk als rechtsgeldig worden beschouwd, afhankelijk van de toepasselijke wetgeving en de aard van de transactie of de keuzes die worden bevestigd. Het is echter belangrijk om juridisch advies in te winnen om te bepalen of deze bevestigingen als volwaardige rechtsgeldige handtekeningen kunnen worden beschouwd in de context van specifieke juridische vereisten.

Gekwalificeerde handtekening voorkomt bewijsproblemen
Gebruikt een pensioenuitvoerder elektronische overeenkomsten bij het zaken doen, dan is een zogenaamde gekwalificeerde elektronische handtekening te prefereren. Daarmee voorkomt deze uitvoerder bewijsproblemen mocht een geschil ontstaan met de partij die ondertekend heeft.

Daarbij geldt dat de feitelijke bewijsbaarheid van de elektronische handtekening beter is in elektronische vorm dan op papier. Een ‘natte’ handtekening is immers eenvoudig te vervalsen. Als de pensioenuitvoerder kiest voor de geavanceerde elektronische handtekening, let dan goed op het verzamelen van voldoende bewijslast, bijvoorbeeld een videogesprek waarbij je foto en persoon vergelijkt en dan de handtekening laat zetten. De kwaliteit wordt in hoge mate bepaald door de deugdelijkheid van de implementatie van het proces.

Andere vormen van ondertekening: ga na of methode voldoende betrouwbaar is
Gebruikt de uitvoerder een andere manier van elektronische ondertekening, dan is het van belang dat deze uitvoerder nagaat dat de gebruikte methode voldoende betrouwbaar is. Hoe groter het belang van het te ondertekenen document, hoe betrouwbaarder de handtekening moet zijn.

Trekken lessen uit jurisprudentie
De belangrijkste les die uit jurisprudentie rondom de elektronische handtekening getrokken kan worden, is dat je vooraf goed moet nadenken welk betrouwbaarheidsniveau passend is voor het soort het document dat je gaat ondertekenen. Het is belangrijk om een duidelijk bedrijfsbeleid te hebben en medewerkers goed te informeren. De voorlichting over de voordelen van digitaal gemak met de ondertekening moeten hand in hand gaan met uitleg over de risico’s. Zo voorkom je dat een contract of overeenkomst teniet wordt gedaan, omdat de handtekening geen stand houdt.

EU ID-wallet: volg de ontwikkelingen
Op termijn (2025) kan met de EU ID-wallet authenticatie op het hoogste betrouwbaarheidsniveau plaats vinden en tevens een gekwalificeerde elektronische handtekening gezet worden.

1 Inleiding

Deze inleiding geeft onder meer het doel en de doelgroep van het rapport aan. Het doel van het rapport is om de resultaten van het onderzoek 'Onderzoek Elektronisch Ondertekenen Documenten' te presenteren. De doelgroep zijn professionals die betrokken zijn bij het zoeken naar oplossingen voor elektronisch ondertekenen van documenten bij pensioenuitvoerders. De inleiding bevat een lijst van de leden van de projectgroep. De opdrachtgever van het rapport zijn de stuurgroep DSO en de stuurgroep GZD. De opzet van het rapport komt uitgebreid aan de orde.

1.1 Doel

Dit rapport presenteert de resultaten van het project ‘’Onderzoek Elektronisch Ondertekenen Documenten’’.

1.2 Doelgroep

1.2.1 Stuurgroep DSO

Organisatie	Naam
Achmea Pensioenservices	Evelien Kops
APG	René Steenhart (voorzitter)
AZL	Pieter van Eijden
MN	Ralf Rikze
Pensioenfederatie	Edith Maat
PGB Pensioendiensten	Harry Vossebeld
PGGM	Alexandra Phillippi
TKP	Joke Westenbrink
SIVI	Peter Mols
SIVI	Gerhard Gerritsen (secretaris)

1.2.2 Stuurgroep GZD

Organisatie	Naam
Achmea, SIVI Bestuur	Albert Spijkman
Sector Leven Verbond	Harold Herbert
Pensioenfederatie	Edith Maat
PGGM, SDSO	Alexandra Phillippi
SIVI Bestuur	Wim Henk Steenpoorte
TKP, SDSO	Joke Westenbrink
SIVI	Peter Mols
SIVI	Gerhard Gerritsen (secretaris)

1.3 Projectgroep

Organisatie	Naam
Achmea	Engbert Walinga
Rail & OV	Dirk Neuhaus (projectleider)
MN	William Vrasdonk
SIVI	Gerhard Gerritsen
SIVI	Duco Mansvelder

1.4 Opzet

De structuur van het rapport is als volgt.

Hoofdstuk	Inhoud
1	Inleiding Deze inleiding geeft onder meer het doel en de doelgroep van het rapport aan. Het doel van het rapport is om de resultaten van het onderzoek 'Onderzoek Elektronisch Ondertekenen Documenten' te presenteren. De doelgroep zijn professionals die betrokken zijn bij het zoeken naar oplossingen voor elektronisch ondertekenen van documenten bij pensioenuitvoerders. De inleiding bevat een lijst van de leden van de projectgroep. De opdrachtgever van het rapport zijn de stuurgroep DSO en de stuurgroep GZD. De opzet van het rapport komt uitgebreid aan de orde.
2	De opdracht Dit hoofdstuk behandelt context en uitdagingen bij elektronisch ondertekenen in de pensioensector. De opdracht omvat: uitleg juridisch kader, pensioen-uitdagingen, verantwoorde keuzes, DigiD-gebruik en uniformiteit elektronisch ondertekenen in de sector.
3	Afbakening van het werkgebied en aanpak Dit hoofdstuk behandelt de afbakening van het onderwerp documenten & elektronische handtekeningen. Het legt uit wat elektronische handtekeningen zijn volgens de belangrijkste definitie onder meer uit de eIDAS-verordening. Het verschil met digitale handtekeningen wordt uitgelegd. Het rapport volgt de voorkeur voor de term "elektronische handtekening" en beschrijft de aanpak van het onderzoek.
4	Juridisch kader Dit hoofdstuk beschrijft het doel en het juridisch belang van handtekeningen, vooral elektronische handtekeningen, bij het tot stand komen van overeenkomsten. Ook worden elektronische zegels en tijdstempels besproken. Uitspraken van rechtbanken worden genoemd, waarbij de geldigheid van 2FA en geavanceerde handtekeningen wordt besproken. In Bijlage A t/m C staat een aanvullende toelichting.
5	Kenmerken elektronische handtekening In dit hoofdstuk gaan we in op verschillende kenmerken van elektronische handtekeningen. Verschillende authenticatiemethoden en methoden voor digitaal ondertekenen worden beschreven. Ook wordt de EU ID-wallet en vertrouwensdiensten geïntroduceerd. Tot slot komen duurzaam toegankelijke Pdf's en metadata voor elektronische handtekeningen aan de orde.
6	Elektronische handtekening in de pensioensector

Hoofdstuk	Inhoud
	Dit hoofdstuk laat zien tijdens welke processen in de pensioensector het ondertekenen van documenten een rol speelt. Het hoofdstuk toont toepassingen, voordelen en methoden. Tevens gaan we in op ervaringen van pensioenuitvoerders.
7	Conclusies en aanbevelingen In dit hoofdstuk komt het volgende aan de orde: • Conclusies zijn antwoorden op de onderzoeksvragen. • Aanbevelingen zijn adviezen gericht op de pensioenuitvoerders.
8	Bijlage A – eIDAS Deze bijlage geeft een toelichting op eIDAS.
	Bijlage B – DigiD Pensioenuitvoerders kunnen – gelet op hun publieke taak en wettelijk geoorloofd gebruik van BSN – deelnemers (artikel 94 Pensioenwet) laten inloggen met DigiD. Dit is een goede reden in te gaan op de verschillende betrouwbaarheidsniveaus in relatie tot DigiD.
	Bijlage C – Wetteksten Deze bijlage laat relevante wetteksten zien.
	Bijlage D - EU ID-wallet In 2025 zijn één of meer nationale ID-wallets én andere Europees erkende ID-wallets in Nederland te gebruiken. Daarmee kunnen burgers hun bronidentiteit (een digitale versie van de identiteitsgegevens die de overheid van burgers heeft geregistreerd) en bijbehorende gegevens en documenten gebruiken om digitaal zaken te doen in het publieke én het private domein.
	Bijlage E - Checklist Een checklist die helpt de beste oplossing voor een pensioenuitvoerder te kiezen.
	Bijlage F - Begrippen en afkortingen In deze bijlage een begrippenlijst en een lijst met de gebruikte afkortingen.

1.5 Links

Het rapport bevat links, veelal bronvermeldingen. Deze zijn **blauw** gekleurd. Door op de link te klikken komt de lezer bij de desbetreffende webpagina of het desbetreffende rapport/artikel.

1.6 Herkomst afbeelding op de titelpagina

Bron: **Logius Handleiding DigiD**, januari 2023.
In het geval van een mobiel apparaat, kan een natuurlijk persoon de DigiD app op twee manieren gebruiken:

- de DigiD app op hetzelfde apparaat openen.
- de DigiD app op een ander apparaat openen en koppelen door het invoeren van een koppelcode en het scannen van een QR-code.

2 Opdracht

Dit hoofdstuk behandelt context en uitdagingen bij elektronisch ondertekenen in de pensioensector. De opdracht omvat uitleg juridisch kader, pensioen-uitdagingen, verantwoorde keuzes, DigiD-gebruik en uniformiteit elektronisch ondertekenen in de sector.

2.1 Context

Een aantal processen in de pensioensector vraagt om een handtekening. In de volgende processen is bijvoorbeeld een handtekening van de deelnemer vereist:

- Waardeoverdracht: Dit is het proces waarbij een deelnemer zijn opgebouwde pensioenaanspraken overdraagt van de ene naar de andere pensioenuitvoerder. De deelnemer moet hiervoor een aanvraagformulier invullen en ondertekenen.
- Afkoop klein pensioen: Dit is het proces waarbij een deelnemer zijn kleine pensioen in één keer laat uitbetalen. De deelnemer moet hiervoor een afkoopformulier invullen en ondertekenen.
- Keuzes met betrekking tot pensionering, zoals:
    - Ingang pensioen (vervroegen, uitstellen);
    - Deeltijdpensioen;
    - Uitruil van ouderdomspensioen met partnerpensioen en omgekeerd;
    - Hoog-Laagconstructies;
    - AOW overbrugging;
    - Variabele of vaste uitkering.
- Ook de handtekening van de partner kan van belang zijn. Dit speelt bij die situaties waarbij gemaakte keuzes impact hebben op het partnerpensioen. Zoals bij:
    - Uitruil ouderdomspensioen met partnerpensioen (en omgekeerd)
    - Waardeoverdracht.

2.2 Uitdagingen

De hierboven genoemde processen hebben allemaal gemeen dat ze juridisch bindend zijn en dat ze gevolgen hebben voor de hoogte en duur van het pensioen van de deelnemer. Mede in het kader van nieuwe wetgeving zal het genoemde belang verder toenemen, bijvoorbeeld voor:

- Keuze bedrag ineens;
- Voortzetting risicoverzekering nabestaandenpensioen;
- Lifecycle keuze (binnen DC regelingen komt dit nu al voor, maar dit gaat qua omvang toenemen.)

Daarom is het belangrijk dat de handtekening van de deelnemer geldig en betrouwbaar is, ook als de handtekening langs elektronische weg tot stand komt.

Elektronisch ondertekenen kan veel voordelen hebben, zoals meer efficiëntie, veiligheid en duurzaamheid. Maar er zijn ook enkele uitdagingen waar je rekening mee moet houden als je elektronisch wilt ondertekenen. Denk hierbij aan rechtsgeldigheid, veiligheid, implementatie en veranderingen in het beheren van documenten.

2.3 Opdracht

De opdracht heeft verschillende aspecten:

- Leg het juridisch kader rond het zetten van een elektronische handtekening uit.
- Geef aan welke uitdagingen een pensioenuitvoerder heeft als gaat om het (laten) zetten van een elektronische handtekening. Laat zien wat hier verantwoorde keuzes zijn.
- In de huidige praktijk bevestigen deelnemers steeds vaker gemaakte keuzes in een portaal van de pensioenuitvoerder. Dit nadat ze met DigiD zij ingelogd. Geef aan in hoeverre dit een verantwoorde werkwijze is.
- Geef tevens aan of we stappen kunnen nemen om het elektronisch ondertekenen in de pensioensector te uniformeren voor met name deelnemers en partners van deelnemers.

3 Afbakening werkgebied en aanpak

Dit hoofdstuk behandelt de afbakening van het onderwerp documenten & elektronische handtekeningen. Het legt uit wat elektronische handtekeningen zijn volgens de belangrijkste definitie onder meer uit de eIDAS-verordening. Het verschil met digitale handtekeningen wordt uitgelegd. Het rapport volgt de voorkeur voor de term "elektronische handtekening" en beschrijft de aanpak van het onderzoek.

3.1 Afbakening van het onderwerp

Een document is volgens Wikipedia een verzameling gegevens vastgelegd op een gegevensdrager. Dit kan zijn in schriftelijke vorm op papier of digitaal, maar ook op bijvoorbeeld een microfiche.

Het gaat enerzijds om het ondertekenen van documenten, anderzijds om het ondertekenen van teksten op websites en dergelijke. Door het ondertekenen is de wil van de desbetreffende persoon vast te stellen met betrekking tot de tekst bij of boven de handtekening, dat wil zeggen de inhoud van het document.

Definitie
We volgen de definitie uit de Handreiking Elektronische handtekening, VNG, Den Haag 2021:
‘’Een elektronische handtekening is een verzameling gegevens in elektronische vorm, die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen’’.

Dit sluit aan bij de definitie in de eIDAS verordening. Kort gezegd komt dit op het volgende neer:
(1) een elektronische handtekening bestaat uit een verzameling digitale gegevens, zoals een afbeelding of een cryptografische codereeks, die (2) verbonden is met andere digitale gegevens, zoals een pdf-document of afbeelding, en die (3) door de ondertekenaar gebruikt wordt om die digitale gegevens te ondertekenen.

Verschil met digitale handtekening
Een digitale handtekening is volgens Wikipedia een methode voor het bevestigen van de juistheid van digitale informatie door middel van bijvoorbeeld technieken van de asymmetrische cryptografie, op een wijze vergelijkbaar met het ondertekenen van papieren documenten aan de hand van een geschreven handtekening. Over het algemeen bestaat een digitale handtekening uit twee algoritmen: één om te bevestigen dat de informatie niet door derden veranderd is, de andere om de identiteit te bevestigen van degene die de informatie "ondertekent". De combinatie van de resultaten van deze twee algoritmen vormt de digitale handtekening. De technieken worden toegepast met behulp van een Public Key Infrastructure.

Het enige onderscheid tussen elektronische handtekeningen en digitale handtekeningen is dat digitale handtekeningen het gebruik van een code of algoritme vereisen om de authenticiteit van een document te ondertekenen en te authenticeren. Digitale handtekeningen zijn een subset van elektronische handtekeningen. In dit rapport geven we daarom de voorkeur aan de term elektronische handtekening ook al omdat we hiermee aansluiten bij eIDAS.

3.2 Aanpak

Door bureauonderzoek (rapporten, artikelen), onderzoek bij leveranciers en navraag via de werkgroep IDP zochten we antwoord op de verschillende onderzoeksvragen.

4 Juridisch kader

Dit hoofdstuk beschrijft het doel en het juridisch belang van handtekeningen, vooral elektronische handtekeningen, bij het tot stand komen van overeenkomsten. Ook worden elektronische zegels en tijdstempels besproken. Uitspraken van rechtbanken worden genoemd, waarbij de geldigheid van 2FA en geavanceerde handtekeningen wordt besproken.
In Bijlage A t/m C staat een aanvullende toelichting.

4.1 Het doel van de handtekening

Een handtekening heeft meerdere functies:
1. Het vaststellen van iemands identiteit;
2. Het vaststellen van de wil van de desbetreffende persoon met betrekking tot de tekst bij of boven de handtekening.
3. Het bieden van een waarborg dat de inhoud niet is veranderd;
4. Het bieden van een waarborg tegen overhaast optreden.

4.2 Het juridisch belang van een handtekening

Voor documenten, die meerdere personen tot bepaalde verplichtingen binden (zoals contracten) is de handtekening van belang, omdat deze aangeeft dat men de inhoud van de tekst kent en er akkoord mee gaat.

Schriftelijke vastlegging en een handtekening geven aldus duidelijkheid over:
1. wie er aan de overeenkomst zijn gebonden;
2. waarop de wil van de personen is gericht (inhoud van de overeenkomst);
3. wanneer men precies aan de overeenkomst gebonden is.

Deze drie aspecten hebben te maken met rechtszekerheid.

4.3 Totstandkoming overeenkomst

Waarom is geldigheid relevant?
De geldigheid van een elektronische handtekening is relevant voor de vraag of er een overeenkomst tot stand is gekomen. Het juridisch kader voor de totstandkoming van overeenkomsten en de elektronische handtekening wordt gevormd door artikel 6:227a BW en 3:15a BW en de eIDAS Verordening.

Vereisten voor totstandkoming overeenkomst zijn vormvrij
De vereisten voor de totstandkoming van een overeenkomst zijn aanbod en aanvaarding (artikel 6: 217 BW). Aanbod en aanvaarding zijn in beginsel vormvrij (artikel 3:37 BW) en zijn gebaseerd op de wilsvertrouwensleer (artikel 3:33 en 3:35 BW). Hieruit volgt dat voor de totstandkoming van een overeenkomst in beginsel geen vormvereiste geldt en deze tevens langs elektronische weg kan geschieden.

Totstandkoming van een overeenkomst waarvoor het schriftelijkheidsvereiste geldt
Op het beginsel dat aanbod en aanvaarding vormvrij zijn, bestaan uitzonderingen, waardoor voor bepaalde overeenkomsten een schriftelijkheidsvereiste geldt.'

Op grond van artikel 6:227a BW kan een overeenkomst waarvoor het schriftelijkheidsvereiste geldt ook elektronisch tot stand komen. Indien uit de wet voortvloeit dat een overeenkomst slechts in schriftelijke vorm geldig of onaantastbaar tot stand komt, is aan deze eis tevens voldaan indien de overeenkomst langs elektronische weg is totstandgekomen en
a. raadpleegbaar door partijen is;
b. de authenticiteit van de overeenkomst in voldoende mate gewaarborgd is;
c. het moment van totstandkoming van de overeenkomst met voldoende zekerheid kan worden vastgesteld; en
d. de identiteit van de partijen met voldoende zekerheid kan worden vastgesteld.

Voorwaarde uit 6:227a BW	**Toelichting** ontleend aan **kamerstuk**
De overeenkomst dient door partijen raadpleegbaar te zijn;	Dit betekent dat de elektronische overeenkomst raadpleegbaar moet zijn door de partijen bij de overeenkomst. Deze dient op zodanige wijze te worden vastgelegd, dat de partijen in staat zijn om de inhoud daarvan ter latere kennisneming te ontsluiten en te bewaren. Dit vereiste kan meebrengen dat de partij, die daarbij gebruik wil maken van een bepaalde techniek, gehouden zal zijn om de wederpartij over de juiste technische middelen te doen beschikken om de inhoud van de overeenkomst te kunnen raadplegen, indien deze daarover niet beschikt. Daarbij kan onder meer van belang zijn of gekozen wordt voor een bijzondere techniek of voor een techniek waarover een gebruiker in het algemeen geacht mag worden te beschikken.
de authenticiteit van de overeenkomst in voldoende mate gewaarborgd is;	De inhoud van elektronische berichten of bestanden kan daarentegen vrij eenvoudig en ongemerkt gemanipuleerd worden, indien er niet voldoende maatregelen zijn genomen ter beveiliging daarvan. Daarom wordt gesteld dat de authenticiteit van de overeenkomst in voldoende mate gewaarborgd is. Ter uitvoering van dit voorschrift dienen partijen de elektronische overeenkomst op zodanige wijze vast te leggen dat er in voldoende mate vertrouwd kan worden op de juistheid van de inhoud daarvan. Aangezien de woorden «in voldoende mate» een relatief criterium vormen, zal het antwoord op de vraag of hieraan voldaan wordt, mede afhankelijk zijn van de omstandigheden van het geval, zoals de stand van de techniek, de aard van de overeenkomst en de hoedanigheid van de partijen. Tevens kan van belang zijn of aan het gebruik van een veiliger techniek dan de daadwerkelijk gebruikte bijvoorbeeld kosten verbonden zouden zijn geweest die gelet op het belang van de overeenkomst disproportioneel moeten worden geacht. Partijen kunnen aan de onderhavige voorwaarde voldoen door een overeenkomst in een elektronisch bestand vast te leggen dat voorzien is van een elektronische handtekening zoals omschreven in de artikelen 15a tot en met 15c van Boek 3 van het Burgerlijk Wetboek, omdat de elektronische handtekening op zodanige wijze aan het bestand wordt verbonden, dat elke wijziging achteraf van de gegevens opgespoord kan worden. Partijen kunnen aan de onderhavige voorwaarde voldoen door een overeenkomst in een elektronisch bestand vast te leggen dat voorzien is van een elektronische handtekening zoals omschreven in de artikelen 15a tot en met 15c van Boek 3 van het Burgerlijk Wetboek, omdat de elektronische handtekening op zodanige wijze aan het bestand wordt verbonden, dat elke wijziging achteraf van de gegevens opgespoord kan worden.
het moment van totstandkoming van de overeenkomst met voldoende zekerheid kan worden vastgesteld; en	Dit betekent dat het moment van de totstandkoming van de overeenkomst met voldoende zekerheid kan worden vastgesteld. Deze eis wordt gesteld omdat het in veel gevallen belangrijk is om te weten op welk tijdstip een overeenkomst tussen partijen tot stand is gekomen, bijvoorbeeld om te kunnen bepalen vanaf wanneer partijen verplichtingen ten opzichte van elkaar hebben of sprake is van een tekortkoming in de nakoming van een verbintenis die uit de overeenkomst voortvloeit. Of het moment van totstandkoming van de overeenkomst «met voldoende zekerheid» kan worden vastgesteld is mede afhankelijk van de omstandigheden van het geval, zoals de

Voorwaarde uit 6:227a BW	**Toelichting** ontleend aan **kamerstuk**
	stand van de techniek, de aard van de overeenkomst en de hoedanigheid van partijen.
de identiteit van de partijen met voldoende zekerheid kan worden vastgesteld.	Deze houdt in dat de identiteit van partijen met voldoende zekerheid kan worden vastgesteld op het moment dat de overeenkomst langs elektronische weg wordt gesloten. Partijen kunnen bijvoorbeeld hieraan voldoen door de overeenkomst van een elektronische handtekening te voorzien zoals omschreven in de artikelen 15a tot en met 15c van Boek 3 van het Burgerlijk Wetboek. Voor zover een vormvereiste meebrengt dat een schriftelijke overeenkomst ondertekend moet worden om tot stand te kunnen komen, zijn partijen verplicht om deze elektronisch te ondertekenen overeenkomstig zojuist genoemde wetsartikelen.

4.4 Soorten handtekeningen vanuit juridisch perspectief

Vanuit juridisch perspectief kunnen we drie soorten elektronische handtekeningen onderscheiden:
1. “Gewone” elektronische handtekening (SES);
2. Geavanceerde elektronische handtekening (AES);
3. Gekwalificeerde elektronische handtekening (QES).

In de onderstaande tabel – ontleend aan DOCCO op ondertekenwijzer.nl - volgt uitleg.

Beknopte overzichtstabel	SES (eenvoudig)	AES (geavanceerd)	QES (gekwalificeerd)
Betrouwbaarheid	★☆☆☆☆ (laag)	★★★★☆[1] (substantieel)	★★★★★ (hoog)
Kosten	€	~~€€~~	~~€€€~~
Voorbeeld	Scan, krabbel, vinkje, akkoord	Ondertekening na (online) controles / met digitaal certificaat	Ondertekening met een gekwalificeerd certificaat
Identiteitsverificatie	Geen/gering	Meerdere verificatie stappen[1]	Door verificatie van identiteitskaart of paspoort
Mag worden aangedragen als digitale handtekening[2]	J	J	J
Juridisch (automatisch) gelijk aan de ‘natte’ handtekening	N	N	J
Bij wie ligt de bewijslast / wie dient aan te kunnen tonen,	Bij jou	Bij jou	Bij de ander

Beknopte overzichtstabel	SES (eenvoudig)	AES (geavanceerd)	QES (gekwalificeerd)
dat de handtekening geldig is?			
Geldigheid in EU-lidstaten.	Afhankelijk van nationale wetgeving in lidstaat	Afhankelijk van nationale wetgeving in lidstaat	Als zodanig erkend in gehele alle EU-lidstaten

1] de betrouwbaarheid hangt zeer sterk af van de wijze waarop de software bepaalde maatregelen voor bewijslast geïmplementeerd heeft.

2] een rechter kan de handtekening bijvoorbeeld niet weigeren, enkel en alleen omdat deze in een digitale vorm is. Dit wordt soms vertaald door aanbieders in de term '100% rechtsgeldig'.

Drempel is hoog
De gekwalificeerde elektronische handtekening is nog lang niet altijd de standaard. EU-burgers kunnen al jaren een persoonlijk gekwalificeerd certificaat krijgen. Door relatief hoge kosten en een gebrek aan een digitale identiteit (eID) op hoog niveau om een dergelijk certificaat eenvoudig te verkrijgen, is de drempel echter hoog, aldus DOCCO.

4.5 Elektronische zegels

Uit de Handreiking Elektronische handtekening (VNG, Den Haag 2021) blijkt dat het elektronische zegel in de eIDAS-verordening op dezelfde manier is geregeld als de elektronische handtekening. ''Het verschil is dat de persoon (ondertekenaar) is vervangen door de rechtspersoon (organisatie). Een zegel is dus niet verbonden aan een persoon, maar aan een organisatie. Er zijn net als bij ondertekeningen drie smaken: gewoon, geavanceerd en gekwalificeerd, waarbij de definities hetzelfde werken als bij ondertekeningen.'' (p.13/14).

''Een zegel is procedureel makkelijker om te gebruiken, want er is geen ondertekenaar bij betrokken. Een zegel kan daarnaast bijvoorbeeld een rol spelen om de bewijswaarde van een document te verhogen of bij de digitalisering van processen'''(p.14).

4.6 Elektronische tijdstempels

Uit de Handreiking Elektronische handtekening (VNG, Den Haag 2021) blijkt dat een tijdstempel gegevens aan een tijdstip verbindt. ''Met een tijdstempel op een (uiteraard elektronisch) document kunnen we aantonen dat het document op het gegeven tijdstip bestond, maar het is mogelijk dat de inhoud sindsdien is gewijzigd.

In de eIDAS-verordening wordt een juridisch kader gegeven voor tijdstempels, die gewoon en gekwalificeerd kunnen zijn. Een gekwalificeerd tijdstempel is eigenlijk een tijdstempel gecombineerd met een gekwalificeerde ondertekening of een gekwalificeerd zegel'' (p.14). Een gekwalificeerd tijdstempel heeft dus juridische geldigheid en kan worden gebruikt als bewijs in gerechtelijke procedures om aan te tonen dat een document op een bepaald moment in zijn huidige vorm bestond. Dit helpt de betrouwbaarheid en geloofwaardigheid van elektronische documenten te vergroten.

4.7 Uitspraken rechtbank

Tweefactor Authenticatie
De rechtbank Zeeland/West-Brabant heeft op 7 oktober 2020 een uitspraak gedaan over de rechtsgeldigheid van een digitale handtekening die tot stand komt door middel van e-mail en SMS-authenticatie. De kantonrechter benadrukte het belang van de overeenkomst, in dit geval een borgstellingsovereenkomst, en waarschuwde tegen lichtvaardig gebruik van digitale ondertekening

vanwege mogelijke misbruik mogelijkheden. Hoewel eerder goedgekeurde zaken vergelijkbare 2FA-methoden gebruikten, vond de kantonrechter in dit geval de 2FA niet voldoende. Dit komt doordat de mobiele telefoon die de SMS ontving, ook door iemand anders dan de eigenaar gelezen zou kunnen zijn, wat een directe link tussen de ondertekenaar en de overeenkomst in twijfel trekt.

De uitspraak roept discussie op over de betrouwbaarheid van 2FA op basis van e-mail en SMS. Het is nog onduidelijk of deze analyse stand zal houden in een vervolgprocedure, vooral omdat hogere instanties vergelijkbare 2FA-methoden al hebben goedgekeurd. De uitspraak heeft beperkte impact op de praktijk, maar benadrukt de noodzaak van zorgvuldige technische implementatie van 2FA. Andere vormen van authenticatie, zoals iDIN of gekwalificeerde digitale handtekeningen, kunnen ook overwogen worden in specifieke contracten. Het gebruik van een gekwalificeerd certificaat via de cloud voor digitale ondertekening is ook een mogelijkheid. Al met al blijft de discussie over de rechtsgeldigheid van digitale handtekeningen met 2FA voortduren

Geneeskundige verklaring met minimaal geavanceerde handtekening
De Hoge Raad oordeelde op 14 juni 2019 (ECLI:NL:HR:2019:957) over de elektronische ondertekening van een geneeskundige verklaring voor dwangopname. De verklaring moet door de geneesheer-directeur zelf worden ondertekend, vereisend dat een geavanceerde of gekwalificeerde elektronische handtekening wordt gebruikt om persoonlijke binding en integriteit te waarborgen, vergelijkbaar met een handgeschreven handtekening.

Elektronische handtekening op bijvoorbeeld een tablet
Recent (maart 2022) heeft de Rechtbank Noord-Holland daar een uitspraak over gedaan.
Een bedrijf dat software ontwikkelt en verkoopt stelt een overeenkomst te hebben gesloten met een slagerij en vordert een betaling van een factuur van ruim € 4.000,-. De slager weigert te betalen. De slager erkent een elektronische handtekening gezet te hebben op een tablet tijdens het bezoek van de verkoper. Dat was volgens de slager voor vrijblijvende informatie. Dit omdat hij eerste wilde zien wat de software inhoudt. Een bestelformulier met overeenkomst is niet getekend, aldus de slager.

Een dergelijk elektronische handtekening kan als bewijs gelden, maar dan vereist dat de methode van ondertekening voldoende betrouwbaar is (artikel 3:15a BW). De rechter oordeelt dat dit niet het geval is. De handtekening wordt namelijk gezet op een tablet die de verkoper bij zich draagt in een omgeving die door het desbetreffende softwarebedrijf of een door haar ingeschakelde partij wordt beheerd. Het is daarom niet voldoende te controleren wat er met de handtekening gebeurt.

5 Kenmerken elektronische handtekeningen

In dit hoofdstuk gaan we in op verschillende kenmerken van elektronische handtekeningen. Het belang van authenticatie in digitale ondertekening wordt onderstreept, waarbij de mate van binding tussen persoon en identificatiemiddel zorgt voor zekerheid.

5.1 Voordelen elektronische handtekening

- Efficiëntie: het proces van het ondertekenen kan worden geautomatiseerd, waardoor alle handmatige taken zoals het verkrijgen van een handtekening, afdrukken, scannen, posten, archiveren en verifiëren, komen te vervallen. Op afstand ondertekenen mogelijk, ondertekenaars hoeven zich niet te verplaatsen. Documenten zijn overal online beschikbaar. Dit levert ook klanttevredenheid op.
- Kostenverlaging: Je verbruikt minder papier, geen postzegels en inkt, je hebt geen fysiek archief of scanfaciliteiten meer nodig.
- Beveiliging: Met elektronische handtekeningen kun je je documenten beveiligen met een hoog veiligheids- en bewijsniveau. Een fraudebestendig zegel, waarschuwt als het document na ondertekening op enigerlei wijze wordt veranderd. Afhankelijk van de vertrouwelijkheid kan de beveiliging worden aangepast.
- Tijdsbesparing: Het proces van het opstellen, versturen, ondertekenen en retourneren van documenten kan worden verkort
- Plaats onafhankelijk: Door het digitaliseren van het ondertekeningsproces is het tegenwoordig makkelijk om overal te ondertekenen.
- Milieuvriendelijk: Aangezien er geen fysieke documenten en papier nodig zijn.
- Bewijsbaarheid: Elektronische handtekeningen worden vaak ondersteund door audit trails en tijdstempels, wat betekent dat elke stap in het ondertekeningsproces kan worden vastgelegd en geverifieerd. Dit kan nuttig zijn in gevallen waar juridische bewijslast nodig is.
- Minder fouten: Doordat de handmatige handtekening te vermijden kunnen processen volledig digitaal (STP) afgehandeld worden. Dit voorkomt bijvoorbeeld tussenkomst van een administratief medewerker en verlaagt de kans op foutief overnemen van de gemaakte keuzes.

5.2 Mogelijke nadelen elektronische handtekening

- Beveiligingszorgen: Het risico van cyberaanvallen, hacks en frauduleuze activiteiten bestaan.
- Afhankelijkheid van technologie: Elektronische handtekeningen zijn afhankelijk van technologische infrastructuren. Als er technische storingen optreden, zoals stroomuitval of internetstoringen, kan dit leiden tot vertragingen bij het ondertekeningsproces.
- Kosten: Hoewel elektronische handtekeningen op de lange termijn kostenbesparend kunnen zijn, kan de initiële implementatie en training op het gebruik van de technologie initieel kosten met zich meebrengen.
- De gekwalificeerde elektronische handtekening is nog lang niet altijd de standaard. EU-burgers kunnen al jaren een persoonlijk gekwalificeerd certificaat krijgen. Door relatief hoge kosten en een gebrek aan een digitale identiteit (eID) op hoog niveau om een dergelijk certificaat eenvoudig te verkrijgen, is de drempel echter hoog, aldus DOCCO.

5.3 Mate van binding met authenticatiemiddel zeer relevant

Bij elektronisch ondertekenen is authenticatie cruciaal. Immers alleen als voldoende zekerheid bestaat over de identiteit van een bepaalde persoon dan kan sprake zijn van een elektronische handtekening. Naarmate de binding tussen de persoon en het identificatiemiddel sterker is, zal sprake zijn van meer zekerheid.

Als een deelnemer – laten we zeggen de heer Pieter Janssen – online zijn pensioenen wil inzien of wijzigen, dan zal de pensioenuitvoerder er zeker van willen zijn dat de juiste Pieter Janssen toegang krijgt.

Om Pieter Janssen zich te laten identificeren heeft hij een middel nodig. Dit identificatiemiddel gebruikt hij tijdens het online-inlogproces bij de pensioenuitvoerder. Als 't goed is, dan leidt dit tot de bevestiging van de identiteit van Pieter Janssen.

Om een identificatiemiddel te kunnen gebruiken moet Pieter Jansen dat natuurlijk wel hebben. Identificatiemiddelen kunnen op verschillende manieren verstrekt worden. Om het middel te verkrijgen en te kunnen gebruiken moet Pieter Jansen een registratieproces doorlopen. Dit is het proces dat de middelenuitgever heeft ingericht om Pieter Janssen kenmerken van zichzelf vast te laten leggen. Pas na controle van de gegevens door de middelenuitgever wordt het middel verstrekt. Hierna staan een paar voorbeelden van registratieprocessen die Pieter Janssen kan doorlopen[1]. Afhankelijk van de aard van het registratieproces is sprake van een bepaalde mate van binding tussen het identificatiemiddel en de unieke persoon Pieter Janssen. Hoe sterker de binding des te meer betrouwbaar is het middel.

Registratieproces A
Pieter Janssen geeft op wat zijn emailadres is. De pensioenuitvoerder stuurt naar dit emailadres een email met een code die Pieter Janssen bevestigt via de website van de pensioenuitvoerder. In het vervolg kan Pieter Janssen bij die pensioenuitvoerder inloggen met als gebruikersnaam het opgegeven emailadres en een wachtwoord dat Pieter Janssen zelf heeft gekozen en voldoet aan bepaalde eisen (lengte, hoofdletter, kleine letter, leesteken en dergelijke). Dit identificatiemiddel heeft alleen binding met het emailadres, het verband tussen Pieter Jansen en zo'n identificatiemiddel is daarom niet erg betrouwbaar. Dat verband kan verstrekt worden door Pieter Janssen ook zijn mobiele telefoonnummer te laten opgeven en een code naar deze telefoon te sturen. Als Pieter Janssen deze code invoert tijdens het registratieproces dan ontstaat binding met emailadres en het mobiele telefoonnummer. Maar alle andere gegevens die Pieter Janssen opgeeft zijn niet zeker voor de pensioenuitvoerder. Wel kan tijdens het inloggen iedere keer een code naar de telefoon van Pieter Janssen gestuurd worden. Dit heet inloggen met twee factoren: iets wat Pieter Janssen weet (emailadres en wachtwoord) en iets wat hij bezit (zijn mobiele telefoon). Het hele proces heet twee-factor-authenticatie.

Registratieproces B
Pieter Janssen legt bij de pensioenuitvoerder een aantal gegevens van zichzelf vast. Vervolgens leest hij met een App van de pensioenuitvoerder zijn identiteitskaart met chip uit. Dit kan onder meer met ReadID technologie. Hierbij wordt gebruik gemaakt van het gegeven dat in Nederland 100% van de paspoorten, identiteitskaarten, verblijfsvergunningen en ~75% van de rijbewijzen een chip bevat met persoonsgegevens. Via de Smartphone kan Pieter Janssen die met NFC-technologie uitlezen (NFC = Near Field Communication). Door gebruik te maken van ReadID vindt online identificatie plaats: de gegevens die Pieter Janssen heeft opgegeven worden gecontroleerd tegen de gegevens die worden uitgelezen van zijn identiteitskaart, onder meer: voor- en achternaam, geboortedatum, geslacht, nationaliteit en pasfoto. Ook hier kan de mobiele telefoon na controle als tweede factor ingezet worden, naast gebruikersnaam en wachtwoord. Het emailadres (niet noodzakelijkerwijs de gebruikersnaam) zal ook gecontroleerd worden door hier een code naar toe te sturen die bevestigd moet worden.

Registratieproces C
Pieter Janssen legt bij de pensioenuitvoerder een aantal gegevens van zichzelf vast. Vervolgens krijg hij thuis bezoek van een persoon die zijn identiteit komt controleren. Hierbij moet Pieter Janssen zich legitimeren met een geldig identiteitsbewijs, en wordt ook ter plekke een code naar de mobiele telefoon van Pieter Janssen gestuurd. Hij moet ook nog laten zien dat hij mail ontvangt op het opgegeven emailadres. De binding tussen de persoon Pieter Janssen en zijn middel (gebruikersnaam, wachtwoord, mobiele telefoon) is nu sterk. Dit registratieproces is (veel) duurder dan Registratieproces B. Daarom heeft registratieproces B in de praktijk veelal de voorkeur.

Als het middel dat Pieter Janssen gaat gebruiken overal gebruikt kan worden voor inloggen dan biedt dat voor Pieter Janssen veel gemak. Zeker als met het middel zowel bij de overheid als bij bedrijven ingelogd

[1] De voorbeelden zijn primair illustratief. Uiteraard moeten pensioenuitvoerders voldoen aan de (steeds veranderende) wetgeving.

kan worden. Het kan ook zijn dat Pieter Janssen een andere persoon wil machtigen om namens hem te handelen. Dit kan bij onder meer DigiD. DigiD is een systeem waarmee Nederlandse overheden op internet iemands identiteit kunnen verifiëren.

5.4 Handtekeningen en authenticatie

Het zetten van een handtekening kan al dan niet worden vooraf gegaan door authenticatie.

5.4.1 Handtekening zonder Authenticatie

De belangrijkste:

- Handmatige handtekening
  - Een eenvoudige, handmatige handtekening kan op het scherm worden gezet met de muis of touchpad of met een vinger of stylus op een touchscreen. Dit wordt ook beschouwd als een digitale handtekening.
- Getypte handtekening
  - Met deze ondertekeningsmethode typ je je naam met behulp van een toetsenbord.
- Goedkeuringsknop
  - Een simpele muisklik op een goedkeuringsknop.

5.4.2 Handtekening met authenticatie

De belangrijkste:

- Login en wachtwoord (inclusief SSO);
- Ondertekenen met een smartcard of token (USB);
- Met een eenmalig wachtwoord (OTP) via sms of e-mail;
- Mobiele identiteiten IRMA, Itsme® in België;
- Publiek/overheidsinitiatief (DigiD);
- Bankauthenticatie (iDIN);
- eIDAS.

Pensioenuitvoerders kunnen/moeten – gelet op hun publieke taak en wettelijk geoorloofd gebruik van BSN – deelnemers (artikel 94 Pensioenwet) laten inloggen met DigiD. Dit is een goede reden in te gaan op de verschillende betrouwbaarheidsniveaus in relatie tot DigiD, zie Bijlage B.

DigiD

DigiD is een middel voor authenticatie, een middel waardoor (met bepaalde betrouwbaarheid) vastgesteld wordt wie een handeling heeft verricht. DigiD is geen elektronische handtekening. Het kan echter wel gebruikt worden als handtekening, als bij het document (vaak de aanvraag) vastgelegd wordt dat die aanvraag gedaan werd door een bepaalde gebruiker op een bepaald moment, die geldig geauthentiseerd was met DigiD. De crux zit hem in ‘gehecht aan of logisch verbonden’ uit art.3 lid 10 eIDAS-verordening: ‘’ elektronische handtekening”: gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen;’’.
Het niveau van authenticatie met DigiD is op zich voldoende voor een geavanceerde elektronische handtekening. Maar omdat de handtekening niet wordt vastgehecht aan de ondertekende gegevens is er geen sprake van een elektronische handtekening, zoals bedoeld in het Burgerlijk Wetboek (3:15a). ‘’Het is in feite niets meer dan een authenticatie plus een akkoordverklaring’’, aldus https://www.ondertekenwijzer.nl/uitleg-ondertekenen

Voor de gekwalificeerde elektronische handtekening is een ontmoeting nodig of een remote proces waarbij de identiteitskaart of het paspoort van de desbetreffende persoon wordt gecontroleerd.
Voor de geavanceerde handtekening worden meerdere vormen (soms in combinatie) gebruikt om eveneens tot een hoge mate van betrouwbaarheid te komen. Hieronder een aantal voorkomende methoden:

- SMS-verificatie. De meest bekende, maar door vervalsingsmogelijkheden steeds minder populaire methode. Daarom wordt deze methode soms vervangen door een andere authenticator op de smartphone.
- IDIN-verificatie. Hiermee identificeer je je via je bank(rekening).
- NFC-verificatie. Hierbij wordt via de smartphone de NFC-chip uitgelezen van een paspoort of ID-kaart.
- AI-verificatie. De nieuwste methode maakt gebruik van kunstmatige intelligentie om gezichtspunten ter herkennen. Dit noemen we ook wel 'biometrische gezichtsauthenticatie'.

5.4.3 Wet Digitale Overheid (Wdo)

De Wdo treedt gefaseerd in werking. Hij gaat pas gelden als een instantie technisch en organisatorisch klaar is om aan te sluiten.
Na inwerkingtreding:

- moeten de pensioenuitvoerders hun digitale diensten indelen naar betrouwbaarheidsniveau;
- hebben zij een acceptatieplicht voor toegelaten inlogmiddelen;
- moeten zij hun informatiebeveiliging op orde hebben;
- moeten zij meebetalen voor het gebruik van inlogmiddelen door burgers.

- Inloggen met private inlogmiddelen is mogelijk op basis van Europese eIDAS regels. Een aantal partijen in de Tweede Kamer heeft bij Wdo behandeling gevraagd om systeem van open toelating met private middelen. Andere landen hebben al private middelen (zoals Itsme in België). In Nederland zijn nog geen private middelen erkend, waarmee ook kan worden ingelogd in Nederland. Mensen krijgen daar – nadat deze middelen zijn erkend - de vrije keuze in.
- De Wdo regelt voor Nederland het toelaten van private inlogmiddelen naast publieke middel DigiD, maar stelt daar extra eisen aan en regelt toezicht daarop, zoals privacy-eisen en eisen die in de novelle van de Wdo zijn opgenomen.
- Het publieke middel DigiD blijft voor burgers beschikbaar, voor bedrijven komt een publiek middel beschikbaar.
- Als een middel uitvalt hebben gebruikers een terugvaloptie.

Regels voor het bepalen van het betrouwbaarheidsniveau van authenticatie en machtiging voor een elektronische dienst (eIDAS substantieel of hoog)
De overheid biedt een Regelhulp betrouwbaarheidsniveaus.

5.5 Opties om te ondertekenen

Verschillende opties zijn beschikbaar om een document te ondertekenen, variërend van eenvoudige methoden tot meer geavanceerde benaderingen. Hier zijn enkele veelgebruikte opties:

- **Digitale handtekeningsoftware:** Verschillende digitale handtekeningplatforms en software bieden gebruikers de mogelijkheid om documenten elektronisch te ondertekenen. Deze platforms bieden vaak functies voor het maken, verzenden en ondertekenen van documenten, inclusief de mogelijkheid om handtekeningen toe te voegen, de documentintegriteit te waarborgen en audittrails te genereren. Voorbeelden van dergelijke platforms zijn Evidos platform, DocuSign, Adobe Sign, HelloSign en SignRequest.
  Vergelijkingen van de oplossingen zijn beschikbaar.
- **Gecertificeerde digitale certificaten:** Gecertificeerde digitale certificaten zijn een geavanceerde methode voor digitale ondertekening waarbij gebruik wordt gemaakt van een vertrouwde derde partij, een certificaatautoriteit (CA). Gebruikers kunnen digitale certificaten aanvragen die hun identiteit verifiëren en vervolgens deze certificaten gebruiken om documenten digitaal te ondertekenen. Dit biedt een hoog niveau van vertrouwen en veiligheid. Microsoft Office biedt bijvoorbeeld de mogelijkheid om digitale handtekeningen te maken en te verifiëren met behulp van digitale certificaten.
- **Blockchain-gebaseerde ondertekening:** Blockchain-technologie kan worden gebruikt om digitale handtekeningen te verifiëren en de integriteit van ondertekende documenten te waarborgen. Eenmaal ondertekend en vastgelegd op een blockchain, kan een document niet worden gewijzigd

zonder dat dit zichtbaar wordt. Dit kan vooral handig zijn bij situaties waarin permanente, onveranderlijke archivering belangrijk is.

De keuze voor een specifieke methode hangt af van factoren zoals het vereiste beveiligingsniveau, gebruiksgemak, wettelijke vereisten en de beschikbare technologieën.

https://www.idin.nl/bedrijven/idin-ondertekenen/

iDIN is een product van de Nederlandse banken waarmee je online documenten kunt ondertekenen. Het werkt door gebruik te maken van de inlogmiddelen van de bank, zodat de consument zich online kan identificeren ten behoeve van het online ondertekenen van documenten.

Bedrijven die iDIN Ondertekenen willen gebruiken dienen hiervoor iDIN Ondertekenen af te nemen bij een Digital Identity Service Provider (DISP) met een specifiek certificaat voor het leveren van ondertekendiensten. Alleen een gecertificeerde DISP kan zijn zakelijke klanten de mogelijkheid aanbieden om iDIN Ondertekenen op hun website te integreren[1].

5.6 Toegankelijkheid documenten

De Handreiking voor de Rijksoverheid, Digitale Overheid 2022, Duurzaam digitaal toegankelijke pdf's, stelt dat veel gepubliceerde pdf-documenten niet gemaakt zijn met digitale toegankelijkheid in het achterhoofd. De ISO-standaard PDF/UA staat op de lijst van door Forum Standaardisatie (overheid) aanbevolen standaarden voor pdf-bestanden die digitaal toegankelijk moeten zijn. Een PDF/UA document is een PDF 1.7-document dat voldoet aan aanvullende afspraken voor digitale toegankelijkheid. Het is dan ook het meest geschikte pdf-formaat om aan de wettelijke toegankelijkheidsverplichting te voldoen.

Bij het creëren van duurzaam toegankelijke PDF-documenten moet een pensioenuitvoerder in ieder geval de volgende stappen volgen:

- Gebruik van juiste software: Gebruik professionele software zoals Adobe Acrobat, Microsoft Word met ingebouwde PDF-conversie, of andere tools die voldoen aan toegankelijkheidsstandaarden.
- Gebruik van lettertypen: Gebruik standaardlettertypen en -groottes om ervoor te zorgen dat tekst consistent en leesbaar blijft, zelfs als het PDF-bestand wordt vergroot.
- PDF/UA-conformiteit: Gebruik de PDF/UA-norm voor digitale toegankelijkheid, die specifiek is ontworpen voor het maken van toegankelijke PDF-documenten.

De Handreiking Elektronische handtekening (VNG, Den Haag 2021) (pagina 49 en verder) gaat hier nader op in relatie tot de elektronische handtekening.

De Archiefregeling en normen zoals NEN 2082 en NEN-ISO 16175 stellen eisen aan het bewaren van metadata over het validatieproces van elektronische handtekeningen, inclusief informatie over de ondertekenaar, het moment van validatie, het resultaat, en het certificaat. Deze metadata moeten worden opgeslagen om het proces en de authenticiteit van de ondertekening te kunnen reproduceren. Implementatie van elektronische handtekeningen in systemen moet rekening houden met deze eisen, en bij aanbestedingen kunnen pensioenuitvoerders deze specifieke metadatavelden benoemen.

5.7 EU ID-wallet

In 2025 zijn één of meer nationale ID-wallets én andere Europees erkende ID-wallets in Nederland te gebruiken. Daarmee kunnen burgers hun bronidentiteit (een digitale versie van de identiteitsgegevens die

de overheid van burgers heeft geregistreerd) en bijbehorende gegevens en documenten gebruiken om digitaal zaken te doen in het publieke én het private domein.

Deelnemers kunnen zich met één klik op een hoog betrouwbaarheidsniveau authenticeren bij pensioenuitvoerders. Daarna kan de deelnemer gericht gegevens delen. Bedenk hierbij dat deze gegevens authentiek zijn, voorzien van datum/tijd stempel en dat de deelnemer de gegevens niet kan wijzigen.

Met de EU ID-wallet kan een gekwalificeerde elektrische handtekening gezet worden. Dit wordt getest in grootschalige projecten.

Voor een verdere toelichting: zie **Bijlage D**.

5.8 Aanbieders van diensten

Een organisatie die nadenkt over elektronische handtekeningen, maar nog een aanbieder moet kiezen? DocuSign zet de belangrijkste te stellen vragen op een rijtje. Ook DOCCO biedt iets vergelijkbaars.

Qualified trust service providers (QTSPs)
Nieuw is dat EU-burgers met hun wallet-ID in heel Europa niet alleen met overheden maar ook met gecertificeerde bedrijven zaken kunnen doen. Artikel 22 van de eIDAS-verordening verplicht de lidstaten om vertrouwenslijsten op te stellen, bij te houden en te publiceren. Deze lijsten moeten informatie bevatten met betrekking tot de gekwalificeerde vertrouwensdienstverleners waarvoor zij verantwoordelijk zijn, en informatie met betrekking tot de gekwalificeerde vertrouwensdiensten die door hen worden verleend. De lijsten worden op een beveiligde manier gepubliceerd, elektronisch ondertekend of verzegeld in een formaat dat geschikt is voor geautomatiseerde verwerking. Nationale toezichthouders moeten hun ‘zegen’ geven over publieke en private dienstaanbieders, die zich na certificatie ‘qualified trust service provider’ mogen noemen.

Door EU erkende Trust Service Providers in Nederland staan in de bijlage.

6 Elektronische handtekening in de pensioensector

Dit hoofdstuk laat zien tijdens welke processen in de pensioensector het ondertekenen van documenten een rol speelt. Het hoofdstuk toont toepassingen, voordelen en methoden. Tevens gaan we in op ervaringen van pensioenuitvoerders..

6.1 Voorliggende keuzes

Als een pensioenuitvoerder een elektronische handtekening wil gebruiken, dan moet deze volgens de Handreiking Elektronische handtekening (VNG, Den Haag 2021) twee juridische vragen met “ja” beantwoorden (zie pagina 16 van genoemde handreiking).

‘’Vraag-1: Vormt de beoogde techniek een elektronische handtekening?
Voldoet de techniek die de pensioenuitvoerder voor ogen heeft, of de ondertekening die de pensioenuitvoerder ontvangen heeft, aan de definitie uit art. 3 lid 10 van de eIDAS-verordening? Gaat het dus om “gegevens in elektronische vorm die gehecht zijn of logische verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen?’’

‘’Vraag-2: Is de elektronische handtekening voldoende betrouwbaar voor het beoogde doel?
De gekwalificeerde vorm is, ongeacht de toepassing, voldoende betrouwbaar. Dat betekent echter niet dat andere (lagere) vormen niet voldoende betrouwbaar zijn.’’

6.2 Partijen en processen

6.2.1 Betrokken partijen

In de aan pensioenuitvoering gerelateerde processen bevestigen de volgende partijen al dan niet via een handtekening de gemaakte afspraken, keuzes, wijzigingen en dergelijke:

- Accountant
- Administratiekantoor (namens werkgever)
- Adviseur deelnemer
- Adviseur werkgever
- Bewindvoerder
- Curator
- Deelnemer
- Erfgenaam
- Ex-partner
- Fonds
- Gemachtigde
- Huidige partner
- Kind (wees)
- Werkgever (rechtstreeks verzekerd)
- Werkgever (verplicht aan te sluiten)
- Werkgever (vrijwillige aansluiting)
- Wettelijke vertegenwoordiger

6.2.2 Deelnemer processen waarbij handtekening een rol kan spelen

Categorie gegevens	Proces
Persoonsgegevens	Gewijzigd bankrekeningnummer
Persoonsgegevens	Doorgeven loonheffingskorting
Persoonsgegevens	Bewijs relatie (huwelijk/samenleving)
Persoonsgegevens	Gemoedsbezwaar kenbaar maken
Persoonsgegevens	Doorgeven Bewindvoering - door bewindvoerder zelf
Uit elkaar gaan	Verwerken scheiding - verevening
Uit elkaar gaan	Verwerken scheiding - conversie
Uit elkaar gaan	Verwerken scheiding - afstand Bijzonder Partnerpensioen
Waardeoverdracht	Akkoord inkomende waardeoverdracht
Waardeoverdracht	Akkoord uitgaande waardeoverdracht
Waardeoverdracht	Bezwaar tegen collectieve uitgaande waardeoverdracht
Persoonlijke keuzes	Beleggingskeuzes
Persoonlijke keuzes	Optioneel ANW-hiaat kiezen
Persoonlijke keuzes	Optioneel Excedentpensioen kiezen
Persoonlijke keuzes	Vrijwillig bijstorten
Einde dienstverband	Keuzes bij einde dienstverband (uitruil)
Einde dienstverband	Vrijwillige voortzetting
Pensioneren	Opvragen keuze variabel pensioen
Pensioneren	Pensioen keuzes (exclusief uitruil Partnerpensioen Ouderdomspensioen)
Pensioneren	Uitruil Ouderdomspensioen Partnerpensioen door deelnemer
Pensioneren	Uitruil Partnerpensioen Ouderdomspensioen door deelnemer
Pensioneren	Uitruil Partnerpensioen Ouderdomspensioen door partner
Pensioneren	Akkoord shoppen
Pensioneren	Akkoord afkoop (handtekening partner kan nodig zijn)
Overlijden	Aanvraag Partnerpensioen
Overlijden	Aanvraag Wezenpensioen
Overlijden	Afkoop Partnerpensioen
Overlijden	Afkoop Bijzonder Partnerpensioen na scheiding
Overlijden	Afkoop Bijzonder Partnerpensioen na overlijden
Overlijden	Afkoop Wezenpensioen
Bewijs in leven	Attestatie de Vitae
Bewijs van studie	Studieverklaring (stempel school nodig)

6.2.3 Voorbeelden handtekening zetten door huidige partner, wees en werkgever

Het is niet alleen de deelnemer die eventueel een handtekening moet zetten. Voorbeelden voor de huidige partner en een kind (wees).

Huidige partner

Deelnemer leeft

- Uitruil Partner Pensioen Ouderdomspensioen

Deelnemer overleden

- Gewijzigd bankrekeningnummer
- Doorgeven loonheffing korting
- Afkoop nabestaandenpensioen
- Attestatie de Vitae

Kind (wees)

Deelnemer overleden

- Gewijzigd bankrekeningnummer
- Afkoop Wezenpensioen
- Studieverklaring
- Attestatie de Vitae

Werkgevers

Relevante processen:

- Indien verzoek om offerte;
- Verzoek tot aansluiting;
- Accorderen voorstellen;
- Accorderen offertes;
- Afsluiten contracten;
- Aanleveren beoordelingsgegevens;
- Aanleveren aansluitgegevens;
- Deelname aanvullende regeling;
- Wijziging bankrekening nummer;
- Verlengen contracten.

Bij het afsluiten en verlengen van contracten is of een natte handtekening vereist of een gekwalificeerde elektronische handtekening.

Een accountant stuurt - namens een zzp'er aangesloten bij beroepspensioenfonds - getekende verklaring ''winst uit onderneming'' op naar de pensioenuitvoerders.

6.3 Voorbeelden van toepassingen

6.3.1 PGB (2018)

Digitaal ondertekenen is met ValidSign in eerste instantie primair ingezet voor externe documentatie. Dit betreft de pensioencontracten (aansluitcontracten) richting de werkgevers.

"Via de digitale handtekening van ValidSign kunnen wij documenten plaats- en tijdsonafhankelijk (laten) ondertekenen. Digitaal ondertekenen levert ons een enorme tijdswinst op. Ook is het door ValidSign inzichtelijk waar documenten in het proces zich bevinden en wie nog dient te ondertekenen."

"We hebben vaak documenten die door acht of meer personen ondertekend moeten worden. Als dit per post gaat is het hartstikke lastig om te volgen waar het document ligt. Door de digitale handtekening oplossing is dit wél inzichtelijk", zegt Frans van Veen.

PGB onderkent de volgende voordelen:

- Tijdwinst;
- inzicht in het ondertekenproces;
- het versimpelen van ondertekenen;
- kostenbesparingen;
- verhoogt de duurzaamheid.

6.3.2 BeFrank

BeFrank ondertekent sinds 2016 overeenkomsten digitaal met Stiply. De documenten die ondertekend worden zijn overeenkomsten en machtigingen. BeFrank maakt ook gebruik van een aanvullende authenticatiemethode, namelijk SMS. Een ondertekenaar ontvangt het ondertekenverzoek via e-mail én een code per SMS. ''Deze maatregel hebben wij getroffen omdat het belangrijk is om de identiteit van de persoon met wie wij zaken doen op een betrouwbare manier vast te stellen.'

De voordelen die digitaal ondertekenen met Stiply voor BeFrank hebben opgeleverd zijn tijdsbesparing en flexibiliteit. ''Tijdsbesparing omdat de documenten veel sneller retour komen dan hiervoor het geval was. En flexibiliteit omdat we niet meer hoeven te wachten op de fysieke aanwezigheid van een ondertekenaar om een akkoord te krijgen. Iemand zou bij wijze van spreken in de trein terug naar huis nog een handtekening kunnen zetten via Stiply. Dat is echt een uitkomst voor ons.''

6.3.3 Zwitserleven

Zwitserleven laat deelnemers (en hun partners) de keuzes in een digitaal proces ondertekenen:

- De persoon kiest in zijn e-mail de knop ''Ik maak mijn pensioenkeuzes'';
- De persoon logt in met zijn DigiD of met zijn e-mailadres en wachtwoord;
- Kies daarna Naar ondertekenen;
- Kies Verstuur SMS;
- De persoon vult bij ''Voer uw ontvangen code in'' de 7-cijferige sms code in die hij ontvangt;
- De persoon ontvangt een bevestiging: ''Bedankt. Dank u wel dat u uw pensioen bij Zwitserleven heeft gekocht''.

6.3.4 Stipp

Stipp laat werkgever met behulp van Adobe formulieren ondertekenen:

- Invullen en digitaal ondertekenen van formulieren
- Download en open het formulier in Adobe Reader;
- Vul het formulier volledig in;
- Klik op het handtekeningenveld om de PDF te ondertekenen;
- Configureer en maak een digitale id. aan;
- Selecteer Een nieuwe digitale id. maken;
- Selecteer Opslaan in bestand en sla dit bestand lokaal op;

- Kies een wachtwoord voor de beveiliging van uw id.;
- Klik op Doorgaan en selecteer de optie Document vergrendelen na ondertekening;
- Voer uw wachtwoord in en klik op Ondertekenen;
- Sla de PDF op en stuur het digitaal ondertekende formulier naar ons op via de knop 'Verstuur digitaal' op het formulier.

PFZW doet iets vergelijkbaars. Zowel Stipp als PFZW maken voor de pensioenadministratie gebruik van PGGM.

6.3.5 Overig

APG maakt in de diverse processen geen gebruik van een digitale handtekenening. Vanuit deelnemers perspectief gebruikt APG alleen DigiD als digitale ondertekening. Dit is een veel voorkomende oplossing, ook bij andere organisaties.
Een van de fondsen gebruik Ondertekenen.nl (Evidos) bij sommige deelnemer processen.

Detailhandel maakt voor het alle processen waarbij deelnemer inbreng gevraagd wordt (bijvoorbeeld bij het doorgeven van de keuzes ten aanzien pensionering, acceptatie van waardeoverdracht), gebruik van DigiD. Voor werkgeverinbreng wordt gebruik gemaakt van de aanmeldopties eIDAS of eigen user ID + wachtwoord. Gemaakte keuzes worden bevestigd in het document die afhankelijk van de persoonlijke instelling digitaal of per post wordt verzonden. Hierbij wordt niet gemeld dat het document elektronisch ondertekend is. De ondertekening zelf wordt wel geregistreerd.

Rail & OV gebruikt DigiD wel als authenticatie mechanisme, maar niet voor elektronisch ondertekenen. Er is begonnen met toepassing van ondertekenen.nl voor een beperkt aantal processen.

7 Conclusies en aanbevelingen

In dit hoofdstuk komt het volgende aan de orde:
- **Conclusies zijn antwoorden op de onderzoeksvragen.**
- **Aanbevelingen zijn adviezen gericht op de pensioenuitvoerders.**

7.1 Conclusies

We trekken hierna conclusies in perspectief van de gestelde onderzoeksvragen uit hoofdstuk 2.

Leg het juridisch kader rond het (laten) zetten van een elektronische handtekening uit
Dit kader is uitgebreid aan de orde gesteld in hoofdstuk 4 en Bijlage A t/m C.

Geef aan welke uitdagingen een pensioenuitvoerder heeft als gaat om het zetten van een elektronische handtekening. Laat zien wat hier verantwoorde keuzes zijn.
Het implementeren van elektronische handtekeningen in de pensioensector brengt verschillende uitdagingen met zich mee voor pensioenuitvoerders:
- Juridische en regelgevingsuitdagingen: Pensioenuitvoerders moeten ervoor zorgen dat de elektronische handtekeningen die zij gebruiken voldoen aan de geldende juridische en regelgevende vereisten. Pensioenuitvoerders moeten ervoor zorgen dat de gebruikte technologieën en processen aan deze vereisten voldoen.
- Beveiligingsuitdagingen: Elektronische handtekeningen vereisen een hoog niveau van beveiliging om ervoor te zorgen dat de identiteit van de ondertekenaar wordt geverifieerd en dat het ondertekende document niet kan worden gemanipuleerd. Pensioenuitvoerders moeten robuuste beveiligingsmaatregelen implementeren om de vertrouwelijkheid, integriteit en authenticiteit van de ondertekende documenten te waarborgen.
- Technologische infrastructuur: Het implementeren van elektronische handtekeningen vereist mogelijk aanpassingen aan de bestaande technologische infrastructuur van een pensioenuitvoerder. Dit kan investeringen vergen in digitale handtekeningplatforms, authenticatiemethoden en integratie met bestaande systemen.
- Gebruikersacceptatie: Het introduceren van nieuwe technologieën en processen kan leiden tot weerstand bij medewerkers, deelnemers en andere belanghebbenden. Pensioenuitvoerders moeten ervoor zorgen dat er voldoende training en communicatie is om de acceptatie van elektronische handtekeningen te bevorderen.
- Diverse processen en partijen: In de pensioensector is sprake van verschillende processen waarbij ondertekening een rol speelt en betrokken partijen zoals deelnemers, werkgevers, adviseurs en meer. Het implementeren van een uniforme elektronische handtekeningmethode die voor al deze variabele processen voldoet, kan complex zijn.
- Verandering in werkstromen: Het overgaan van handmatige ondertekeningsprocessen naar elektronische kan leiden tot veranderingen in bestaande werkstromen en procedures. Het is belangrijk om deze wijzigingen zorgvuldig te plannen en te testen om operationele verstoringen te minimaliseren.
- Privacy en gegevensbescherming: Het gebruik van elektronische handtekeningen houdt in dat er persoonlijke gegevens worden verwerkt en gedeeld. Pensioenuitvoerders moeten ervoor zorgen dat ze voldoen aan de geldende privacywetgeving en de gegevens van deelnemers en andere belanghebbenden adequaat beschermen.
- Onderhoud en updates: Elektronische handtekeningoplossingen vereisen regelmatig onderhoud en updates om beveiligingsrisico's te minimaliseren en ervoor te zorgen dat de gebruikte technologieën up-to-date blijven.

In de huidige praktijk bevestigen deelnemers steeds vaker gemaakte keuzes in een portaal van de pensioenuitvoerder. Dit nadat ze met DigiD zij ingelogd. Geef aan in hoeverre dit een verantwoorde werkwijze is.

DigiD is ontworpen om een bepaald niveau van betrouwbaarheid te bieden bij het verifiëren van de identiteit van gebruikers voor veel online transacties. Echter, de mate van betrouwbaarheid kan variëren afhankelijk van het specifieke gebruik en de context.
Hoewel DigiD geen elektronische handtekening is, kan het worden gebruikt als een methode om te bevestigen wie een handeling heeft uitgevoerd. Het niveau van authenticatie met DigiD is op zich voldoende voor een geavanceerde elektronische handtekening. Maar omdat de handtekening niet wordt vastgehecht aan de ondertekende gegevens is er geen sprake van een elektronische handtekening, zoals bedoeld in het Burgerlijk Wetboek (3:15a). Het is in feite een authenticatie plus een akkoordverklaring.

Het rapport bespreekt de betrouwbaarheidsniveaus van DigiD (Basis, Midden, Substantieel en Hoog) en hoe deze niveaus overeenkomen met eIDAS-niveaus.

DigiD kan na overlijden van een persoon nog 1 jaar gebruikt worden door naasten en andere direct betrokkenen.

Geadviseerd wordt DigiD op minstens niveau substantieel af te dwingen, de gemaakte keuzes te bevestigen en de deelnemer te vragen om binnen een bepaalde termijn te reageren (bezwaar te maken)

Wtp 2023 p 73
1. De pensioenuitvoerder verstrekt de informatie elektronisch, schriftelijk of via een website, waarbij informatieverstrekking via een website wordt gecombineerd met persoonlijk attenderen als er nieuwe of gewijzigde informatie op de website staat.
2. Indien de deelnemer, gewezen deelnemer, gewezen partner of pensioengerechtigde niet heeft bepaald op welke wijze hij informatie wil ontvangen, verstrekt de pensioenuitvoerder de informatie schriftelijk, elektronisch of via een website. Bij verstrekking via een website wordt de deelnemer, gewezen deelnemer, gewezen partner of pensioengerechtigde persoonlijk geattendeerd op deze website en op de mogelijkheid te kiezen voor een andere wijze van informatieverstrekking. De pensioenuitvoerder meldt op de website dat informatie ook elektronisch of schriftelijk kan worden verstrekt en biedt op de website de mogelijkheid om de wijze van informatieverstrekking te regelen. Het persoonlijk attenderen gebeurt elektronisch, indien het email adres bij de pensioenuitvoerder bekend is, of schriftelijk.
3. Er wordt ten hoogste een maal per jaar gewisseld in de wijze waarop informatie wordt verstrekt.

als het niet in orde is. De pensioenuitvoerder moet hierbij rekening houden met de wetgeving rond elektronische informatieverstrekking.

Op termijn kan met de EU ID-wallet authenticatie op het hoogste betrouwbaarheidsniveau plaats vinden en tevens een gekwalificeerde elektronische handtekening gezet worden.

Geef tevens aan of we stappen kunnen nemen om het elektronisch ondertekenen in de pensioensector te uniformeren voor met name deelnemers.
In de markt zijn verschillende aanbieders met verschillende processen en werkwijzen. Dit maakt het creëren van een uniforme gebruikerservaring bij het ondertekeningsproces - zodat bijvoorbeeld deelnemers gemakkelijk en consistent door het proces kunnen navigeren, ongeacht het type document – lastig.

Door de volgende stappen te volgen, kan de pensioensector elektronische ondertekening meer uniform en gestandaardiseerd maken voor deelnemers, wat zorgt voor een efficiënter proces en een verbeterde gebruikerservaring.

- Standaardisatie van processen: Definieer uniforme procedures en processen waar elektronische handtekeningen vereist zijn. Maak een duidelijke lijst van documenten en situaties waarbij elektronische ondertekening op een bepaald niveau nodig is.

- Gebruik van erkende platforms: Kies (door EU) erkende en veilige platforms voor elektronische handtekeningen die voldoen aan de wettelijke normen en regelgeving. Dit zorgt voor consistentie en vertrouwen bij deelnemers.
- Informeer deelnemers over het gebruik van elektronische handtekeningen, hun voordelen en de veiligheidsmaatregelen die worden genomen om hun privacy te beschermen.
- Zorg ervoor dat de gekozen elektronische ondertekeningsmethode toegankelijk is voor alle deelnemers, inclusief diegenen met beperkingen op het gebied van digitale vaardigheden of technologie.
- Betrek alle relevante belanghebbenden, waaronder juridische experts, om een uniforme aanpak te ontwikkelen en ervoor te zorgen dat aan alle wettelijke vereisten wordt voldaan.
- Evalueer regelmatig de implementatie van elektronische ondertekening in de pensioensector om eventuele knelpunten of verbeteringen te identificeren en aan te pakken.

7.2 Aanbevelingen

Dwing DigiD substantieel af, bevestig keuzes van deelnemers en bied de mogelijkheid om bezwaar te maken
Geadviseerd wordt DigiD op minstens niveau substantieel af te dwingen, de gemaakte keuzes te bevestigen en de deelnemer te vragen om binnen een bepaalde termijn te reageren (bezwaar te maken) als het niet in orde is. De pensioenuitvoerder moet hierbij rekening houden met de wetgeving rond elektronische informatieverstrekking.

Zet Websiteanalysetools in
Websiteanalysetools zijn instrumenten die pensioenuitvoerders kunnen inzetten om het gedrag van bezoekers op hun portalen te meten, analyseren en rapporteren. Deze tools bieden waardevolle inzichten in hoe gebruikers interacteren met een portaal, ook op individueel niveau. Zie ook lijst met begrippen.

Zoek balans
Het is onnodig elk document op het hoogste niveau te ondertekenen. Het gebruik van het hoogste niveau van zekerheid, zoals een gekwalificeerde handtekening, brengt vaak extra kosten met zich mee. Het is belangrijk om de juiste balans te vinden tussen de benodigde zekerheid en de kosten en moeite die ermee gemoeid zijn. Ook de gebruikersvriendelijkheid speelt een rol. Voor minder belangrijke documenten of situaties waarbij een lager zekerheidsniveau volstaat, kan een geavanceerde handtekening gebruikt worden. Op deze manier kan een pensioenuitvoerder efficiënter opereren zonder onnodige kosten te maken. De keuze van de zekerheid hangt af van de waarde en het risico dat ermee gemoeid is. Het is een keuze die een pensioenuitvoerder zelf moet maken.

Win juridisch advies in
Het is verstandig om advies in te winnen bij juridische professionals als een pensioenuitvoerder van plan is elektronische handtekeningen te gebruiken voor belangrijke juridische transacties.
Bijvoorbeeld: In sommige gevallen kunnen bevestigingen na inloggen op een hoog betrouwbaarheidsniveau mogelijk als rechtsgeldig worden beschouwd, afhankelijk van de toepasselijke wetgeving en de aard van de transactie of de keuzes die worden bevestigd. Het is echter belangrijk om juridisch advies in te winnen om te bepalen of deze bevestigingen als volwaardige rechtsgeldige handtekeningen kunnen worden beschouwd in de context van specifieke juridische vereisten.

Gekwalificeerde handtekening voorkomt bewijsproblemen
Gebruikt een pensioenuitvoerder elektronische overeenkomsten bij het zaken doen, dan is een zogenaamde gekwalificeerde elektronische handtekening te prefereren. Daarmee voorkomt deze uitvoerder bewijsproblemen mocht een geschil ontstaan met de partij die ondertekend heeft. Als je geen twijfel wilt hebben, kies voor een gekwalificeerde elektronische handtekening. Deze is qua rechtsgevolg gelijkgesteld aan de ‘natte’ handtekening. Daarbij geldt dat de feitelijke bewijsbaarheid van de elektronische handtekening beter is in elektronische vorm dan op papier. Een ‘natte’ handtekening is immers eenvoudig te vervalsen. Als de uitvoerder kiest voor de geavanceerde elektronische

handtekening, let dan goed op het verzamelen van voldoende bewijslast, bijvoorbeeld een videogesprek waarbij je foto en persoon vergelijkt en dan de handtekening laat zetten. De kwaliteit wordt in hoge mate bepaald door de deugdelijkheid van de implementatie van het proces.

Andere vormen van ondertekening: ga na of methode voldoende betrouwbaar is
Gebruikt de uitvoerder een andere manier van elektronische ondertekening, dan is het van belang dat deze uitvoerder nagaat dat de gebruikte methode voldoende betrouwbaar is. Hoe groter het belang van het te ondertekenen document, hoe betrouwbaarder de handtekening moet zijn.

Trekken lessen uit jurisprudentie
De belangrijkste les die uit jurisprudentie rondom de elektronische handtekening getrokken kan worden, is dat je vooraf goed moet nadenken welk betrouwbaarheidsniveau passend is voor het soort het document dat je gaat ondertekenen. Het is belangrijk om een duidelijk bedrijfsbeleid te hebben en medewerkers goed te informeren. De voorlichting over de voordelen van digitaal gemak met de ondertekening moeten hand in hand gaan met uitleg over de risico's. Zo voorkom je dat een contract of overeenkomst teniet wordt gedaan, omdat de handtekening geen stand houdt.

Belangrijkste aanbevelingen voor het implementeren van elektronische handtekeningen
Het implementeren van elektronische ondertekeningen kan de efficiëntie verbeteren. Hier zijn enkele aanbevelingen:

- Wet- en regelgeving: Zorg ervoor dat je op de hoogte bent van wetten en voorschriften met betrekking tot elektronische handtekeningen, zoals de eIDAS-verordening in de EU. Zorg ervoor dat de gebruikte technologie voldoet aan de vereisten voor juridisch bindende elektronische handtekeningen.
- Beveiliging: Kies een betrouwbare ondertekening provider die sterke beveiligingsmaatregelen biedt, zoals encryptie en identiteitsverificatie.
- Gebruiksvriendelijkheid: Kies een platform dat gemakkelijk te gebruiken is voor zowel interne medewerkers als externe partijen.
- Training en acceptatie: Zorg voor training en communicatie om medewerkers en klanten vertrouwd te maken met het nieuwe proces.
- Opslag en archivering: Zorg voor een veilige en gestructureerde opslag van elektronisch ondertekende documenten voor toekomstige referentie.
- Schaalbaarheid: Kies een oplossing die kan meegroeien met de behoeften van je organisatie naarmate het gebruik van elektronische ondertekeningen toeneemt.
- Testen: Voer uitgebreide tests uit om ervoor te zorgen dat de elektronische ondertekening processen soepel verlopen en eventuele problemen tijdig worden opgelost.

EU ID-wallet: volg de ontwikkelingen
Op termijn kan met de EU ID-wallet authenticatie op het hoogste betrouwbaarheidsniveau plaats vinden en tevens een gekwalificeerde elektronische handtekening gezet worden.

8 Bijlagen

8.1 Bijlage A – eIDAS

Deze bijlage geeft een toelichting op eIDAS.

8.1.1 Korte terugblik

eIDAS is ontstaan in 2014 als Europees raamwerk voor digitale identiteit en vertrouwensdiensten en is in 2016 als verordening ingevoerd en in Nederland met een aanpassingswet in 2018 in het Burgerlijk Wetboek opgenomen.

1992: Eerste Europese Richtlijn voor elektronische handtekeningen
Introductie elektronische handtekening

2013: Wet elektronische handtekening
Introductie 'geavanceerde' en 'gekwalificeerde' elektronische handtekening

2016: Electronic identification and trust services: eIDAS
Gelijktrekking niveaus van elektronische handtekeningen op Europees niveau
Middels een uitvoeringswet van kracht in Nederlands sinds 2018

8.1.2 Doelen

1. Alle EU-burgers toegang geven tot openbare diensten in de hele EU met behulp van elektronische identificatiemiddelen (eID) die in hun eigen land zijn uitgegeven.
2. Vertrouwen in elektronische transacties op de interne markt vergroten door het bieden van standaarden voor veilige en naadloze elektronische interactie tussen burgers, bedrijven en overheden.

8.1.3 Drie soorten handtekeningen

Vanuit juridisch perspectief kunnen we drie soorten elektronische handtekeningen onderscheiden:
1. "Gewone" elektronische handtekening (SES);
2. Geavanceerde elektronische handtekening (AES);
3. Gekwalificeerde elektronische handtekening (QES).

In de onderstaande tabel volgt uitleg.

eIDAS Elektronische handtekeningen	
Simpel (SES)	**Kenmerken** Elke digitale blijk van acceptatie. Bijvoorbeeld een scan van een 'natte' handtekening, een met een computerprogramma gegenereerde weergave van een handgeschreven handtekening, een in een vakje getypte of een uitgetypte naam. Kortom: alles waaruit de identiteit van een persoon blijkt. **Identiteit van de ondertekenaar** De identiteit van de ondertekenaar wordt niet gecontroleerd. **Verificatie** Niet zeker dat de handtekening tot stand is gekomen onder de uitsluitende controle van de ondertekenaar. **Hardware** Niet nodig.

eIDAS Elektronische handtekeningen	
	Voorbeelden • De PDA van een pakketbezorger; • De ‘akkoord’-knop voor de voorwaarden van een app; • Het typen van een naam onderaan een e-mail.
Geavanceerd (AES)	**Kenmerken** Een geavanceerde handtekening heeft de volgende kenmerken: • De ondertekenaar moet via de handtekening uniek identificeerbaar zijn. De handtekening moet aan de ondertekenaar zijn gekoppeld. • De ondertekenaar heeft volledige controle over de data die worden gebruikt bij het creëren van de handtekening • Er kan worden vastgesteld of iemand het document na ondertekening heeft aangepast. Als er iets is gewijzigd, wordt de handtekening ongeldig. **Identiteit van de ondertekenaar** Hoge waarschijnlijkheid van identificatie van de ondertekenaar. **Verificatie** Zeker dat de handtekening tot stand is gekomen onder de uitsluitende controle van de ondertekenaar. Meerfactorauthenticatie is optioneel. **Hardware** Secure Signature Creation Device (SSCD) nodig. **Voorbeelden:** • Het versturen van een eenmalig wachtwoord via SMS of e-mail om een login te verifiëren. • Arbeidscontracten. • Bancaire documenten. • Brieven; • Offertes; • Opdrachtbevestigingen; • Beperkte machtigingen.
Gekwalificeerd (QES)	**Kenmerken** Een gekwalificeerde handtekening heeft alle kenmerken van de geavanceerde handtekening. Daarnaast: • moet hij worden gegenereerd middels een Qualified Signature Creation Device (QSCD). • moet de ondertekenaar worden geverifieerd in een persoonlijke ontmoeting. Een gelijkwaardig proces, zoals een video call, mag ook. • is het gebruik van meervoudige authenticatie vereist om de geldigheid te waarborgen. Een QES werkt als volgt: • Een gekwalificeerde trust service provider (QTSP) genereert een digitaal certificaat. Dit zorgt ervoor dat de handtekening alleen door de ondertekenaar kan worden gebruikt. • De Qualified Signature Creation Device (QSCD) genereert een privésleutel en een publieke sleutel. Dit zorgt ervoor dat de handtekening van de ondertekenaar uniek is en niet kan worden vervalst.

eIDAS Elektronische handtekeningen	
	• De ondertekenaar gebruikt de privésleutel om het document te ondertekenen. • De ontvanger gebruikt de publieke sleutel om de identiteit van de ondertekenaar te verifiëren. **Identiteit van de ondertekenaar** Identificatie van de ondertekenaar is 100% zeker. Persoonlijke verificatie of een gelijkwaardig proces vooraf is vereist. **Verificatie** Zeker dat de handtekening tot stand is gekomen onder de uitsluitende controle van de ondertekenaar. Meerfactorauthenticatie is vereist. **Hardware** Qualified Signature Creation Device (QSCD) nodig. **Voorbeelden (documenten met grote rechtsgevolgen):** • Notariële akten; • Gepubliceerde jaarstukken; • Verzekeringspolissen; • Grote commerciële overeenkomsten; • Belangrijke verkoopcontracten; • Hypotheekstukken; • Kredietovereenkomsten; • Accountantsverklaringen (SBR Assurance); • Arbeidscontracten; • Aanbestedingen. .

Elektronische handtekeningen	
	Rechtsgevolg
Simpel **Geavanceerd**	• Jij moet bewijslast kunnen aandragen dat de handtekening wel of niet is geplaatst. • Is volgens de wet niet in alle gevallen passend: ”... hebben dezelfde rechtsgevolgen als een handgeschreven handtekening, indien voor deze beide elektronische handtekeningen de methode voor ondertekening die gebruikt is voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische handtekening is gebruikt en op alle overige omstandigheden van het geval” (3:15a BW).
Gekwalificeerd	• Bewijslast ligt bij de aanklager. • Gelijkgesteld aan natte handtekening: “Zij heeft dezelfde rechtsgevolgen als een handgeschreven handtekening.” (3:15a BW).

Onderstaande tabel vergelijkt de soorten handtekeningen op een aantal eigenschappen:

Bron: https://www.cm.com/nl-nl/sign/elektronische-handtekening/			
Eigenschap	**Standaard**	**Geavanceerd**	**Gekwalificeerd**
Rechtsgeldig	Ja	Ja	Ja
Gebonden aan andere gegevens	Ja	Ja	Ja
Uniek verbonden met de ondertekenaar	Optioneel	Verplicht	Verplicht
Identificatie van ondertekenaar	Optioneel	Verplicht	Verplicht
Twee-factor Authenticatie (2FA)	Optioneel	Verplicht	Verplicht
Beveiligd tegen wijzigingen	Optioneel	Verplicht	Verplicht
Beveiligd met een certificaat	Optioneel	Optioneel	Verplicht
Certificaat uitgegeven door een TSP	Optioneel	Optioneel	Verplicht
Ingesloten gegevens ter validatie	Optioneel	Optioneel	Verplicht

8.1.4 eIDAS Vertrouwensdiensten (niet uitputtend)

Qualified Trust Service Providers leveren de volgende diensten:

- Elektronische handtekening;
- Gekwalificeerde certificaten;
- Tijdsstempels;
- Website authenticatie;
  - Hierdoor kan een persoon erop vertrouwen dat de persoon zich op de gewenste website bevindt en niet op een namaaksite. De persoon ziet dit aan het slotje in de linkerbovenhoek van de. Vaak in combinatie met de groene kleur van de adresbalk. Websitecertificaten worden veel gebruikt als bron van vertrouwen in websites. Denk aan internetbankieren, overheidswebsites en webwinkels.
- Elektronische leveringsdiensten;
  - Gekwalificeerde elektronische leveringsdiensten leveren het bewijs dat een document of elektronisch bericht op een bepaald tijdstip bij een geadresseerde is afgeleverd. Dit mechanisme is ontworpen om de verzending en de correcte ontvangst van deze gegevens vast te leggen.
- Het bewaren van elektronische handtekeningen, zegels of certificaten;
- Vertrouwenslijsten;
- Gekwalificeerde methodes en apparaten om te verzegelen.

Door EU erkende Trust Service Providers in Nederland:

QTSP	**URL – gekwalificeerde dienst**	**Overheid J/N**
Aangetekend B.V.	**https://www.aangetekendmailen.nl/** Qualified electronic registered delivery service	N
CIBG	**https://www.uziregister.nl/** Qualified certificate for electronic signature	J
Cleverbase ID B.V.	**https://cleverbase.com/** Qualified certificate for electronic signature	N
Digidentity B.V.	**https://www.digidentity.eu/nl/** Qualified certificate for electronic signature Qualified certificate for electronic seal	N

QTSP	URL – gekwalificeerde dienst	Overheid J/N
KPN B.V.	https://certificaat.kpn.com/elektronische-opslagplaats/repository/ Qualified certificate for electronic signature Qualified certificate for electronic seal Qualified certificate for website authentication	N
Ministerie van Defensie	https://cps.ca.pkidefensie.nl/ Qualified certificate for electronic signature	J
Ministerie van Infrastructuur en Waterstaat	https://bct.tsp.minienw.nl/index_en.html Qualified certificate for electronic signature	J
QuoVadis Trustlink B.V.	https://www.quovadisglobal.com/repository/ Qualified certificate for electronic signature Qualified certificate for electronic seal Qualified certificate for website authentication Qualified time stamp	N

8.2 Bijlage B - DigiD

Pensioenuitvoerders kunnen – gelet op hun publieke taak en wettelijk geoorloofd gebruik van BSN – deelnemers (artikel 94 Pensioenwet) laten inloggen met DigiD. Dit is een goede reden in te gaan op de verschillende betrouwbaarheidsniveaus in relatie tot DigiD.

8.2.1 Inleiding

DigiD is een middel voor authenticatie, een middel waardoor (met bepaalde betrouwbaarheid) vastgesteld wordt wie een handeling heeft verricht. DigiD is geen elektronische handtekening. Het kan echter wel gebruikt worden als handtekening, als bij het document (vaak de aanvraag) vastgelegd wordt dat die aanvraag gedaan werd door een bepaalde gebruiker op een bepaald moment, die geldig geauthentiseerd was met DigiD. De crux zit hem in ‘gehecht aan of logisch verbonden’ uit art.3 lid 10 eIDAS-verordening: ‘’ elektronische handtekening”: gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen;’’.

Bouwstenen rond DigiD	Toelichting
DigiD	Een voorziening waarmee overheidsorganisaties en publieke dienstverleners online de identiteit van burgers en kunnen vaststellen.
DigiD Machtigen	Een voorziening waarmee een burger een andere burger kan machtigen om namens hem zaken met de overheid te regelen.
Digitoegankelijk	De wettelijke afspraak om websites en mobiele apps toegankelijk te maken voor mensen met een functiebeperking (zoals dyslectici, kleurenblinden, slechtzienden en blinden), door de standaard EN 301 549 (WAGC 2.1) toe te passen en daar een toegankelijkheidsverklaring over te publiceren.
eIDAS	Een EU-afsprakenstelsel over begrippen, digitale identiteiten van burgers, betrouwbaarheidsniveaus en het onderlinge gebruik van digitale infrastructuren, waardoor Europese burgers en bedrijven met hun eigen nationale toegangsmiddel kunnen inloggen bij publieke dienstverleners van de andere Europese lidstaten.

Bouwstenen rond DigiD	Toelichting
Inzageregister (voor inzage in machtigingen)	Via het inzageregister kan iedereen zelf zien welke middelen er aan zijn of haar BSN zijn gekoppeld. Als blijkt dat een onbekend middel is gekoppeld, dan kan de persoon zelf actie ondernemen. Dit inzageregister wordt momenteel gebouwd door Logius.
Machtigingenregister	In het machtigingenregister staat welke organisatie gemachtigd is voor het digitaal ophalen van berichten en gegevens voor een specifieke klant. In de praktijk zijn dit vaak intermediairs, die namens hun klanten berichten en gegevens uitwisselen met de Belastingdienst of het Uitvoeringsinstituut Werknemersverzekeringen (UWV). Logius beheert het machtigingenregister en maakt de juiste koppelingen.

8.2.2 DigiD Machtigen

Met DigiD Machtigen kan een persoon iemand machtigen die namens hem optreedt. Dit is handig als een gebruiker zelf niet goed met een computer of digitale dienstverlening overweg kan of dat wil uitbesteden. Een gemachtigde kan bijvoorbeeld een familielid, een zorgverlener of een belastingadviseur zijn. De machtiging geldt voor een specifieke tijdsperiode en voor 1 afgebakende digitale dienst.

Het huidige DigiD Machtigen gaat echter niet voorzien in het terugkoppelen van bevoegdheden van wettelijke vertegenwoordigers, zoals voor bewindvoering en bij de ouder-kindrelatie. Op dit moment wordt DigiD Machtigen doorontwikkeld tot een nieuwe machtigingsvoorziening die hierin wel gaat voorzien.

8.2.3 Verschillende betrouwbaarheidsniveaus en DigiD

De Wet digitale overheid (WDO) hanteert de 3 Europese eIDAS-betrouwbaarheidsniveau (Laag, Substantieel en Hoog).

DigiD	eIDAS
Basis	Laag
Midden	Laag
Substantieel	Substantieel
Hoog	Hoog

Niveau DigiD	Inlogmiddel
Basis	**Gebruikersnaam en wachtwoord** De gebruiker identificeert zich met een gebruikersnaam en een wachtwoord.
Midden	**Gebruikersnaam / wachtwoord en sms-controle** De gebruiker identificeert zich met een gebruikersnaam, een wachtwoord én een sms-code. DigiD stuurt deze sms-code naar het geregistreerde telefoonnummer van de gebruiker, nadat de gebruiker ingelogd heeft met gebruikersnaam en wachtwoord. Deze sms-code dient als extra controlemiddel om de identiteit van de gebruiker vast te stellen.
Midden	**DigiD app** De gebruiker identificeert zich met de DigiD app, welke gekoppeld is aan het DigiD account. Informatie over de DigiD app is te vinden in de Functionele beschrijving DigiD app.

Niveau DigiD	Inlogmiddel
Substantieel	**DigiD app met ID-check** De gebruiker identificeert zich met de DigiD app, welke gekoppeld is aan het DigiD account en waarmee de eenmalige ID-check succesvol is uitgevoerd. Informatie over de DigiD app met ID-check is te vinden in de Functionele beschrijving DigiD app.
Hoog	**Identiteitskaart / rijbewijs** De gebruiker identificeert zich met zijn/haar Nederlandse identiteitskaart of Nederlands rijbewijs en een (bijbehorende) pincode. Sinds 13 maart 2021 worden hiervoor geschikte identiteitskaarten afgegeven. De voor DigiD Hoog geschikte rijbewijzen komen in de toekomst beschikbaar.

eIDAS Laag en DigiD Basis en DigiD Midden
In Nederland hanteert DigiD op dit moment 4 betrouwbaarheidsniveaus (Basis, Midden, Substantieel en Hoog). Van deze niveaus zijn er 2 op niveau eIDAS Laag, dat zijn:

- DigiD Basis (eIDAS Laag): De gebruiker logt in met een gebruikersnaam en wachtwoord.
- DigiD Midden (eIDAS Laag): Dit is een tweefactorauthenticatie: De gebruiker kiest voor inloggen met de DigiD app of voor gebruikersnaam/wachtwoord aangevuld met een sms-controle.

Het eIDAS-betrouwbaarheidsniveau Laag gaat uit van tenminste een tweefactor authenticatie. Het niveau DigiD Basis voldoet dus niet aan het eIDAS Laag niveau en zal na inwerkingtreding van de Wet digitale overheid uitgefaseerd worden. In de huidige wettekst wordt een termijn van 3 jaar genoemd.

Een klein deel van de DigiD inlogs zijn nog op niveau Basis. Een pensioenuitvoerder kan zijn deelnemers attent maken op het bestaan van de DigiD app (digid.nl). Deze is gebruiksvriendelijk en heeft de tweefactorauthenticatie.

eIDAS substantieel en DigiD substantieel
Sommige gegevens zijn extra privacygevoelig, bijvoorbeeld informatie met betrekking tot het wijzigen van een afspraak met een zorgverlener. Om deze gegevens te kunnen inzien of wijzigen kunnen gebruikers steeds vaker alleen met de DigiD app inloggen. Voor de veiligheid en om de privacy te waarborgen is daar een eenmalige ID-check (digid.nl) van een paspoort, rijbewijs of identiteitskaart aan toegevoegd: hiermee komt de DigiD app op het betrouwbaarheidsniveau Substantieel en kan de gebruiker inloggen op online diensten die op betrouwbaarheidsniveau Substantieel worden aangeboden.

Hoe kunnen inwoners hun DigiD ophogen naar betrouwbaarheidsniveau Substantieel?
De ID-check (digid.nl) kan op dit moment worden uitgevoerd met de DigiD app op de meest gebruikte smartphones met NFC-lezer. De NFC-lezer op de telefoon kan gegevens uitlezen van de chip op bijvoorbeeld een paspoort of rijbewijs. De gebruiker doet dit door de telefoon op het paspoort, rijbewijs of identiteitskaart te leggen. De smartphone moet wel uitgerust zijn met een NFC-lezer.

Wat heeft de gebruiker nodig?

- DigiD app (geactiveerd)
- Android apparaat met NFC-lezer (Android-versie 6.0 of hoger).
- iPhone, model 7 of hoger (iOS-versie 13.2)
- Nederlands identiteitsbewijs (rijbewijs uitgegeven na 14 november 2014, identiteitskaart of paspoort)

Wat als een inwoner geen geschikte smartphone heeft?
Een deel van de DigiD-gebruikers kan op dit moment geen identiteitsbewijs scannen (ID-check), omdat hun smartphone niet beschikt over de NFC-lezer. Hiervoor is een aparte app ontwikkeld: de CheckID app van DigiD. Met deze CheckID app kan iemand anders de gebruiker helpen.

De CheckID-app werkt als volgt: degene die een smartphone heeft met NFC-lezer downloadt de CheckID-app (Android / iOS). Met de app op deze telefoon wordt het identiteitsbewijs (ID-check) gescand

van de persoon die geholpen wil worden. Vervolgens wordt via een beveiligde verbinding de ID-check toegevoegd aan de DigiD-app van deze persoon. De telefoon van de helper wordt alleen als kaartlezer gebruikt, er worden geen gegevens opgeslagen via de app.

Niet iedereen kan uit de voeten met bovenstaande oplossingen. Daarom werkt BZK/Logius ook aan oplossingen voor inwoners zonder telefoon of inwoners die graag iemand willen machtigen om online zaken voor hen te regelen.

Praktijkbeproevingen
Het ministerie van BZK is op zoek naar oplossingen om minder-digivaardige burgers te helpen bij het verhogen van hun DigiD niveau. De VNG werkt mee aan praktijkbeproevingen om te onderzoeken of voorgestelde oplossingen uitvoerbaar zijn.

eIDAS Hoog en DigiD Hoog
Sommige gegevens zijn zo privacygevoelig dat hiervoor het hoogste betrouwbaarheidsniveau wordt gevraagd, bijvoorbeeld medische informatie. Om gebruik te kunnen maken van DigiD Hoog, is een speciaal onderdeel nodig van de chip (de zogenoemde applet) op identiteitsdocumenten. Nog niet alle identiteitsdocumenten hebben deze chip. Rijbewijzen uitgegeven vanaf 26 juni 2018 hebben deze applet. De Nationale Identiteitskaart bevat sinds 4 januari 2021 deze applet, en wordt dan aangeduid als de eNIK. Paspoorten krijgen deze applet voorlopig niet en kunnen niet worden ingezet voor DigiD Hoog.

DigiD Hoog is in ontwikkeling en sinds januari 2021 beschikbaar in combinatie met de eNIK. De nieuwe rijbewijzen kunnen hiervoor worden ingezet na inwerkingtreding van de Wet digitale overheid.
In opdracht van onder andere het ministerie van BZK en in samenwerking met de VNG heeft VNG Realisatie de afgelopen jaren impactanalyses en uitvoeringstoetsen uitgevoerd. In maart 2016 is een impactanalyse (pdf, 830 kB) uitgevoerd op de proef voor het uitgifteproces van het publieke eID-middel. In juni 2021 is een onderzoek gestart naar de gemeentelijke ondersteuningsrol bij aanvraag, activatie en gebruik van DigiD Hoog. Lees de resultaten van dit onderzoek (pdf, 1,3 MB)

Hoe kunnen inwoners hun DigiD ophogen naar betrouwbaarheidsniveau Hoog?
De activatie of ophoging kan op dit moment alleen worden uitgevoerd met een eNIK, uitgegeven na 4 januari 2021, in combinatie met de DigiD app op een smartphone met NFC-lezer. De NFC-lezer op de telefoon kan gegevens uitlezen van de chip op de eNIK. Vervolgens moet een activatiecode worden ingevoerd, die per briefpost naar het huisadres van de kaarthouder is verstuurd. Deze code is een andere code dan de PIN-code die de gebruiker al heeft ingesteld voor de DigiD app.

Wat heeft de gebruiker nodig?
- DigiD app (geactiveerd);
- Android apparaat met NFC-lezer (Android-versie 6.0 of hoger) of
- iPhone, model 7 of hoger (iOS-versie 13.2);
- Nederlandse identiteitskaart (uitgegeven na 4 januari 2021);
- Brief met activatiecode, verstrekt vanuit DigiD en bezorgd op het GBA adres van de kaarthouder.

8.2.4 DigiD en overlijden
Indien uit de gegevens bij de BRP blijkt dat de persoon is overleden, is het niet mogelijk om:
- een DigiD aan te vragen;
- een DigiD te activeren;
- wijzigingen aan het DigiD account te doen, onder andere uit te breiden / gegevens te wijzigen (zie ook paragraaf Mijn DigiD).

8.2.5 Recente ontwikkelingen
Wet digitale overheid
Op 1 juli 2023 trad de Wet digitale overheid (Wdo) in werking.

- De nieuwe regels om digitale dienstverlening op het juiste betrouwbaarheidsniveau te classificeren werden 1 juli van kracht. Pensioenuitvoerders kunnen beginnen met het classificeren van betrouwbaarheidsniveaus van hun digitale diensten aan burgers en bedrijven. Zie de handreiking betrouwbaarheidsniveaus van het Forum Standaardisatie en de regelhulp van de overheid.
- De komende jaren wordt de Wdo stap voor stap ingevoerd. Zo komen er naast DigiD ook private inlogmiddelen beschikbaar om in te loggen bij de overheid. Deze middelen moeten aan strenge eisen voldoen. De techniek en organisatie achter het nieuwe stelsel daarvoor zijn naar verwachting in 2024 klaar.
- Aansluitschema (art 29, lid 3 Wdo):
  Pensioenuitvoerders moeten tussen 1 januari 2024 en eind 2026 aansluiten;
  Pensioenuitvoerders kunnen zelf het moment van aansluiting bepalen;
  Op datum van aansluiting geldt acceptatieplicht, binnen een termijn van 36 maanden.
- DigiD machtigen en wettelijke vertegenwoordiging:
  DigiD machtigen is onder Wdo niet verplicht;
  Wettelijke vertegenwoordiging valt niet onder Wdo.

Planning DigiD 2024 (ontleend aan concept GDI-programmeringsplan 2024)
- Plan opstellen voor verantwoorde uitfasering van lage niveaus DigiD;
- Aansluitmogelijkheden optimaliseren op de voorzieningen (onder andere gecombineerd DigiD en Machtigen);
- Oplossingen DigiD substantieel verbreden, zodat het mogelijke bereik groter wordt (waaronder balie-uitgifte en oplossingen voor vreemde nationaliteiten, vreemdelingen en/of gedetineerden).

DigiD Machtigen:
- Gebruiksvriendelijkheid verbeteren/ digitale inclusie;
- Aansluitmogelijkheden optimaliseren op de voorzieningen (onder andere gecombineerd DigiD en Machtigen);
- Betrouwbaarder maken van register vrijwillig machtigen;
- Uitbreiden oplossing voor machtigen aan de balie.

8.3 Bijlage C – Wetteksten

Deze bijlage laat relevante wetteksten zien.

8.3.1 Verordening (EU) nr. 910/2014 elektronische identificatie en vertrouwensdiensten

VERORDENING (EU) Nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG

Artikel 3 eIDAS
"**10.** „elektronische handtekening": gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen;
11. „geavanceerde elektronische handtekening": een elektronische handtekening die voldoet aan de eisen in artikel 26;
12. „gekwalificeerde elektronische handtekening": een geavanceerde elektronische handtekening die is aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen;
……..
15. "gekwalificeerd certificaat voor elektronische handtekeningen": een certificaat voor elektronische handtekeningen, dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage I;"

Artikel 25 eIDAS
"Rechtsgevolgen van elektronische handtekeningen
1. Het rechtsgevolg van een elektronische handtekening en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures mogen niet worden ontkend louter op grond van het feit dat de handtekening elektronisch is of niet aan de eisen voor gekwalificeerde elektronische handtekeningen voldoet.
2. Een gekwalificeerde elektronische handtekening heeft hetzelfde rechtsgevolg als een handgeschreven handtekening.
3. Een gekwalificeerde elektronische handtekening die op een in een lidstaat afgegeven gekwalificeerd certificaat is gebaseerd, wordt in alle andere lidstaten als een gekwalificeerde elektronische handtekening erkend."

Artikel 26 eIDAS
"Eisen voor geavanceerde elektronische handtekeningen
a) zij is op unieke wijze aan de ondertekenaar verbonden;
b) zij maakt het mogelijk de ondertekenaar te identificeren;
c) zij komt tot stand met gegevens voor het aanmaken van elektronische handtekeningen die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitende controle kan gebruiken, en
d) zij is op zodanige wijze aan de daarmee ondertekende gegevens verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord."

Bijlage I bij de eIDAS verordening:
"EISEN VOOR GEKWALIFICEERDE CERTIFICATEN VOOR ELEKTRONISCHE HANDTEKENINGEN
Gekwalificeerde certificaten voor elektronische handtekeningen bevatten:

a) een vermelding, ten minste in een vorm die geschikt is voor automatische verwerking, dat het certificaat afgegeven is als een gekwalificeerd certificaat voor elektronische handtekeningen;

b) een reeks gegevens die ondubbelzinnig verwijzen naar de gekwalificeerde verlener van vertrouwensdiensten die de gekwalificeerde certificaten afgeeft, met inbegrip van ten minste de lidstaat waarin de verlener is gevestigd en
—voor een rechtspersoon: de naam en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers,
—voor een natuurlijke persoon: de naam van de persoon;

c) op zijn minst de naam van de ondertekenaar of een pseudoniem; als er een pseudoniem wordt gebruikt, wordt dat duidelijk aangegeven;
d) gegevens voor de validering van elektronische handtekeningen, die overeenkomen met de gegevens voor het aanmaken van de elektronische handtekening;
e) informatie over begin en einde van de geldigheidsduur van het certificaat;
f) de identiteitscode van het certificaat, die uniek moet zijn voor de gekwalificeerde verlener van vertrouwensdiensten;
g) de geavanceerde elektronische handtekening of het geavanceerde elektronische zegel van de afgevende gekwalificeerde verlener van vertrouwensdiensten;
h) de locatie waar het certificaat ter ondersteuning van de geavanceerde elektronische handtekening of het geavanceerde elektronische zegel als bedoeld onder g) gratis beschikbaar is;
i) de locatie van de diensten waar informatie kan worden opgevraagd over de geldigheidsstatus van het gekwalificeerde certificaat;
j) indien de gegevens voor het aanmaken van een elektronische handtekening die gekoppeld zijn aan de gegevens voor de validering van de elektronische handtekening zich bevinden in een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen, een passende vermelding hiervan, ten minste in een vorm die geschikt is voor automatische verwerking."

8.3.2 Burgerlijk Wetboek

Boek 3

Afdeling 1A. Elektronisch vermogensrechtelijk rechtsverkeer

Artikel 15a
Evenals een elektronische gekwalificeerde handtekening als bedoeld in artikel 3, onderdeel 12, van verordening (EU) nr. 910/2014 van het Europees parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronisch transacties in de interne markt en tot intrekking van richtlijn 1999/93/EG (PbEU 2014, L 257) hebben een geavanceerde elektronische handtekening als bedoeld in onderdeel 11, en een andere elektronische handtekening als bedoeld in onderdeel 10, van artikel 3 van deze verordening dezelfde rechtsgevolgen als een handgeschreven handtekening, indien voor deze beide elektronische handtekeningen de methode voor ondertekening die gebruikt is voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische handtekening is gebruikt en op alle overige omstandigheden van het geval.

Artikel 15d
Degene die een dienst van de informatiemaatschappij verleent, maakt de volgende gegevens gemakkelijk, rechtstreeks en permanent toegankelijk voor degenen die gebruik maken van deze dienst, in het bijzonder om informatie te verkrijgen of toegankelijk te maken:
a. zijn identiteit en adres van vestiging;
b. gegevens die een snel contact en een rechtstreekse en effectieve communicatie met hem mogelijk maken, met inbegrip van zijn elektronische postadres;
c. voor zover hij in een handelsregister of een vergelijkbaar openbaar register is ingeschreven: het register waar hij is ingeschreven en zijn inschrijvingsnummer, of een vergelijkbaar middel ter identificatie in dat register;
d. voor zover een activiteit aan een vergunningsstelsel is onderworpen: de gegevens over de bevoegde toezichthoudende autoriteit;
e. voor zover hij een gereglementeerd beroep uitoefent:
–de beroepsvereniging of -organisatie waarbij hij is ingeschreven,
–de beroepstitel en de lidstaat van de Europese Unie of andere staat die partij is bij de Overeenkomst betreffende de Europese Economische Ruimte waar die is toegekend,
–een verwijzing naar de beroepsregels die in Nederland van toepassing zijn en de wijze van toegang daartoe;
f. voor zover hij een aan de BTW onderworpen activiteit uitoefent: het btw-identificatienummer zoals bedoeld in artikel 2a, eerste lid, onder g, van de Wet op de Omzetbelasting 1968.

2 De dienstverlener geeft aanduidingen van prijzen in een dienst van de informatiemaatschappij duidelijk en ondubbelzinnig aan, met de uitdrukkelijke vermelding of, en zo mogelijk welke, belasting en leveringskosten daarbij inbegrepen zijn.
3 Onder dienst van de informatiemaatschappij wordt verstaan elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van de afnemer van de dienst wordt verricht zonder dat partijen gelijktijdig op dezelfde plaats aanwezig zijn. Een dienst wordt langs elektronische weg verricht indien deze geheel per draad, per radio, of door middel van optische of andere elektromagnetische middelen wordt verzonden, doorgeleid en ontvangen met behulp van elektronische apparatuur voor de verwerking, met inbegrip van digitale compressie, en de opslag van gegevens.

Boek 6, art. 227a
1 Indien uit de wet voortvloeit dat een overeenkomst slechts in schriftelijke vorm geldig of onaantastbaar tot stand komt, is aan deze eis tevens voldaan indien de overeenkomst langs elektronische weg is totstandgekomen en
a raadpleegbaar door partijen is;
b de authenticiteit van de overeenkomst in voldoende mate gewaarborgd is;
c het moment van totstandkoming van de overeenkomst met voldoende zekerheid kan worden vastgesteld; en
d de identiteit van de partijen met voldoende zekerheid kan worden vastgesteld.

2 Lid 1 is niet van toepassing op overeenkomsten waarvoor de wet de tussenkomst voorschrijft van de rechter, een overheidsorgaan of een beroepsbeoefenaar die een publieke taak uitoefent.

Artikel 227b
1 Voordat een overeenkomst langs elektronische weg tot stand komt verstrekt degene die een dienst van de informatiemaatschappij verleent als bedoeld in artikel 15d lid 3 van Boek 3 de wederpartij ten minste op duidelijke, begrijpelijke en ondubbelzinnige wijze informatie over:
a.de wijze waarop de overeenkomst tot stand zal komen en in het bijzonder welke handelingen daarvoor nodig zijn;
b. het al dan niet archiveren van de overeenkomst nadat deze tot stand zal zijn gekomen, alsmede, indien de overeenkomst wordt gearchiveerd, op welke wijze deze voor de wederpartij te raadplegen zal zijn;
c.de wijze waarop de wederpartij van door hem niet gewilde handelingen op de hoogte kan geraken, alsmede de wijze waarop hij deze kan herstellen voordat de overeenkomst tot stand komt;
d.de talen waarin de overeenkomst kan worden gesloten;
e.de gedragscodes waaraan hij zich heeft onderworpen en de wijze waarop deze gedragscodes voor de wederpartij langs elektronische weg te raadplegen zijn.
2 De dienstverlener stelt voor of bij het sluiten van de overeenkomst de voorwaarden daarvan, niet zijnde algemene voorwaarden als bedoeld in artikel 231, op zodanige wijze aan de wederpartij ter beschikking, dat deze door hem kunnen worden opgeslagen zodat deze voor hem toegankelijk zijn ten behoeve van latere kennisneming.
3 Lid 1 is niet van toepassing op overeenkomsten die uitsluitend door middel van de uitwisseling van elektronische post of een soortgelijke vorm van individuele communicatie tot stand zijn gekomen.
4 Een overeenkomst die tot stand is gekomen onder invloed van het niet naleven door de dienstverlener van zijn in lid 1, aanhef en onder a, c of d, genoemde verplichtingen, is vernietigbaar. Indien de dienstverlener zijn in lid 1, aanhef en onder a of c genoemde verplichting niet is nagekomen, wordt vermoed dat een overeenkomst onder invloed daarvan tot stand is gekomen.
5 Gedurende de tijd dat de dienstverlener de informatie, bedoeld in lid 1, onder b en e en lid 2, niet heeft verstrekt, kan de wederpartij de overeenkomst ontbinden.
6 Tussen partijen die handelen in de uitoefening van een beroep of bedrijf kan van lid 1 worden afgeweken.

Artikel 227c
1 Degene die een dienst van de informatiemaatschappij als bedoeld in artikel 15d lid 3 van Boek 3 verleent, stelt de wederpartij passende, doeltreffende en toegankelijke middelen ter beschikking

waarmee de wederpartij voor de aanvaarding van de overeenkomst van door hem niet gewilde handelingen op de hoogte kan geraken en waarmee hij deze kan herstellen.

2 Indien een wederpartij van een dienstverlener langs elektronische weg een verklaring uitbrengt die door de dienstverlener mag worden opgevat hetzij als een aanvaarding van een door hem langs elektronische weg gedaan aanbod, hetzij als een aanbod naar aanleiding van een door hem langs elektronische weg gedane uitnodiging om in onderhandeling te treden, bevestigt de dienstverlener zo spoedig mogelijk langs elektronische weg de ontvangst van deze verklaring. Zolang de ontvangst van een aanvaarding niet is bevestigd, kan de wederpartij de overeenkomst ontbinden. Het niet tijdig bevestigen van de ontvangst van een aanbod geldt als verwerping daarvan.

3 Een verklaring als bedoeld in lid 2 en de ontvangstbevestiging worden geacht te zijn ontvangen, wanneer deze toegankelijk zijn voor de partijen tot wie zij zijn gericht.

4 De leden 1 en 2 zijn niet van toepassing indien de overeenkomst uitsluitend door middel van de uitwisseling van elektronische post of een soortgelijke vorm van individuele communicatie tot stand komt.

5 Een overeenkomst die tot stand is gekomen onder invloed van het niet naleven door de dienstverlener van zijn in lid 1 genoemde verplichting, is vernietigbaar. Indien de dienstverlener zijn in lid 1 genoemde verplichting niet is nagekomen, wordt vermoed dat een overeenkomst onder invloed daarvan tot stand is gekomen.

6 Van dit artikel kan slechts worden afgeweken tussen partijen die handelen in de uitoefening van een beroep of bedrijf.

8.3.3 Wet elektronische handtekeningen

De wet elektronische handtekeningen trad op 21 mei 2003 in werking. De wet geeft het juridisch kader voor het gebruik van elektronische handtekeningen en is onderdeel van het Burgerlijk Wetboek.

De wet bepaalt niet met welke techniek een elektronische handtekening moet worden aangemaakt. Wel zijn er eisen aan de veiligheid en betrouwbaarheid.

Eisen aan een elektronische handtekening

De handtekening moet op unieke wijze aan de ondertekenaar zijn verbonden. Ook moet de handtekening zijn gemaakt met middelen die de ondertekenaar helemaal onder zijn controle kan houden. Wijzigingen die achteraf aan de handtekening zijn aangebracht, moeten op te sporen zijn. Als een elektronische handtekening aan al die eisen voldoet, wordt ze juridisch gelijkgesteld aan een 'gewone' handtekening. Ze heeft dan dezelfde rechtskracht als een handgeschreven handtekening in dezelfde omstandigheid zou hebben.

Verdere toelichting

Zie: Memorie van toelichting

Zie: tekst Besluit elektronische handtekeningen

8.4 Bijlage D - EU ID-wallet

In 2025 zijn één of meer nationale ID-wallets én andere Europees erkende ID-wallets in Nederland te gebruiken. Daarmee kunnen burgers hun bronidentiteit (een digitale versie van de identiteitsgegevens die de overheid van burgers heeft geregistreerd) en bijbehorende gegevens en documenten gebruiken om digitaal zaken te doen in het publieke én het private domein.

Status

Begin november 2023 toonde de Europese Commissie zich ingenomen met het definitieve akkoord dat kort daarvoor is bereikt door het Europees Parlement en de Raad van de EU tijdens de slottrialoog over de verordening tot invoering van Europese digitale identiteitsportefeuilles.

Impact

Deelnemers kunnen zich met één klik op een hoog betrouwbaarheidsniveau authenticeren bij pensioenuitvoerders. Daarna kan de deelnemer gericht gegevens delen. Bedenk hierbij dat deze

gegevens authentiek zijn, voorzien van datum/tijd stempel en dat de deelnemer de gegevens niet kan wijzigen.

Kenmerken
- eIDAS betrouwbaarheidsniveau hoog.
- Wallet is gratis voor gebruiker.
- Voor burgers en bedrijven.
- Publieke en private sector.

Algemene toepassingen, bijvoorbeeld:
- Identiteit bewijzen (SCA = sterke klant authenticatie);
- Elektronische documenten delen;
- Documenten digitaal ondertekenen met een gekwalificeerde elektronische handtekening (QES);
    - EU – eSignature Get Started
    - EU – eSignature FAQ
- Data delen.

Welke gegevens staan gevalideerd in de wallet
- Huidige familienaam of familienamen;
- Huidige voornaam of voornamen
- Geboortedatum;
- Unieke identificatiecode, door de lidstaat van verzending vastgesteld volgens de technische specificatie voor grensoverschrijdende identificatie, zodanig dat deze zo lang mogelijk stabiel blijft.
- Geboorteplaats;
- Adres;
- Leeftijd;
- Geslacht;
- Burgerlijke staat;
- Gezinssamenstelling;
- Nationaliteit:
- Onderwijskwalificaties, -titels en -diploma's;
- Beroepskwalificaties, -titels en -licenties;
- Openbare vergunningen en licenties;
- Financiële en bedrijfsgegevens.

Specifieke toepassingen, bijvoorbeeld:
- Openbare diensten zoals het opvragen van geboorteakten, medische attesten, het doorgeven van een adreswijziging;
- Openen van een bankrekening;
- Het doen van belastingaangiftes;
- Solliciteren naar een universiteit, thuis of in een andere lidstaat;
- Het bewaren van een medisch recept dat overal in Europa gebruikt kan worden;
- Bewijs van uw leeftijd;
- Auto huren met digitaal rijbewijs;
- Inchecken in een hotel.

Wat regelt het voorstel voor een 'Europese Digitale Identiteit'?
- Alle lidstaten geven verplicht één of meer wallets uit.
- Regie op gegevens: Burgers en bedrijven kunnen hun digitale (bron)identiteit en gegevens, zoals diploma's, zelf delen via een wallet-applicatie op hun smartphone.
- Gebruik in private sector: Wallets kunnen gebruikt worden, niet alleen in het publieke domein, maar ook in het private domein, in het bijzonder op grote platforms (Google, Facebook, Amazon, etc.).

- Gebruik is gratis voor natuurlijke personen, wallet voldoet aan toegankelijkheidseisen en aan hoogste niveau van betrouwbaarheid bij uitgifte en gebruik.
- Wallets zijn geschikt voor offline gebruik zonder internet.
- Wallets moeten de vertrouwensdiensten elektronische handtekening en zegel bevatten (samenloop met beleidsterrein EZK). Daarnaast verplichte nationale certificering door in NL Agentschap Telecom (EZK).

Planning
- In 2023 een eerste NL-versie van een publieke open source voorbeeld ID-wallet beschikbaar.
- In 2023 start NL (indien EU gegund) met deelname enkele grensoverschrijdende Large Scale Pilots met ID-wallets. NL gaat deelnemen in Potential, een Consortium van 19 lidstaten op initiatief van overheden.
- In 2025 kunnen alle burgers en bedrijven gebruik maken van een hoogwaardige ID-wallet binnen het Europese digitale identiteit raamwerk.

Zie ook:
Waarden, kansen en uitdagingen rond het Europese Digitale Identiteit raamwerk
Van Huffelen, 26 juli 2022.

8.5 Bijlage E - Checklist (kiezen oplossing)

Een checklist die helpt de beste oplossing voor een pensioenuitvoerder te kiezen.

Bron:
Connective, De complete gids over digitale handtekeningen, Update 2021

8.5.1 Efficiëntie
- Kun je de bestandstypes ondertekenen die je gewoonlijk gebruikt (bijv. PDF, DOC, DOCX, TXT, XML etc.?)
- Werkt het met je bestaande toepassingen?
- Is het mogelijk documenten te traceren via een intuïtief dashboard?
- Biedt de oplossing ingebouwde geautomatiseerde handtekeningstromen?
- Kan de oplossing worden geïntegreerd met je bestaande toepassingen of met toepassingen die je in de toekomst mogelijk wilt gebruiken, bijvoorbeeld contractbeheer of HR-diensten?
- Kent en begrijpt de leverancier je bedrijf?
- Is er ruimte voor om het product aan te passen aan de look en feel (bijvoorbeeld: logo, kleuren,…) van je bedrijf?

8.5.2 Juridisch
- Voldoet de oplossing aan de regelgeving die voor je organisatie van belang is (eIDAS, GDPR, etc....)? Kun je de oplossing internationaal gebruiken?
- Voldoet de oplossing aan de meest recente eIDAS-verordening voor Europa?
- Ondersteunt ze geavanceerde en gekwalificeerde elektronische handtekeningen (AES en QES) voor documenten met meerdere ondertekenaars?
- Kan iedereen de handtekening valideren, zelfs zonder toegang tot het systeem? Met andere woorden: vormen de documenten op zichzelf staand bewijs? Zo niet, dan heb je de ondertekenaar later mogelijk nodig in geval van een geschil.
- Biedt de oplossing WYSIWYS: wat je ziet is wat je tekent? Als je er zeker van wilt zijn dat het hele document wordt gelezen voordat het wordt ondertekend, is deze functie een must in de oplossing die je kiest. Het zorgt ervoor dat het document pas kan worden ondertekend wanneer het helemaal is gelezen.

8.5.3 Gebruikerservaring

- Is het gemakkelijk om documenten voor te bereiden voor ondertekening?
- Spreekt de oplossing voor zich en is deze intuïtief? Zorg ervoor dat je gebruikers geen training hoeven te volgen of een handleiding hoeven te lezen om de oplossing te gebruiken.
- Kun je de volgorde van de ondertekenaars bepalen?
- Biedt de oplossing uiteenlopende ingebouwde handtekeningmethoden (code via sms en mail, challenge responseauthenticatie, eID, andere digitale certificaten, enzovoort)?
- Kun je je ondertekenaars verschillende ondertekeningsmethoden aanbieden (zodat ze het apparaat kunnen gebruiken dat ze bij de hand hebben)?
- Kun je documentenpakketten ondertekenen?
- Kun je er op elk gewenst apparaat mee ondertekenen?
- Kan iedereen binnen of buiten de organisatie de handtekening valideren, zelfs zonder toegang tot het systeem?
- Ondersteunt de oplossing meerdere talen, zowel voor initiatiefnemers als voor ondertekenaars?

8.5.4 Technische eisen

- Wil je een cloudoplossing gebruiken of de oplossing zelf hosten? Is de oplossing beschikbaar op de manier waar jij voorkeur voor hebt? Biedt de software het vereiste niveau van beveiliging?
- Maakt de oplossing een digitale handtekening en hash voor elke ondertekenaar in de transactie? Met andere woorden: wordt het document van ondertekenaar tot ondertekenaar onmanipuleerbaar verzegeld volgens de eIDAS-vereisten?
- Is het compatibel met de laatste versies van alle gangbare besturingssystemen (zowel desktop als mobiel)?
- Biedt het een volledig responsief ontwerp? Kunnen gebruikers ook op hun smartphone of tablet tekenen?
- Is de oplossing apparaat onafhankelijk?
- Heeft het een flexibele Application Programming Interface (API)? Is de oplossing gemakkelijk te implementeren?
- Zijn er out-of-the-box connectors beschikbaar voor programma's als Microsoft Power Automate of Salesforce? KOSTEN

8.5.5 Kosten

- Wat is het prijsmodel van de oplossing?
- Betaal je per handtekening of voor de volledige oplossing?
- Moet je de oplossing kopen of is SaaS (abonnement) ook een optie?

8.6 Bijlage F – Begrippen en Afkortingen

In deze bijlage een begrippenlijst en een lijst met de gebruikte afkortingen.

8.6.1 Begrippen

Begrip	Omschrijving
(e)Seal	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Een elektronisch zegel, geplaatst d.m.v. van een (gekwalificeerd) eSeal certificaat die verkrijgbaar is bij een QTSP en bedoeld is, om de handtekening aan het ondertekende stuk te verbinden en wijzigingen achteraf te voorkomen.

Begrip	Omschrijving
Aanmaker van een zegel	Bron: eIDAS verordening Een rechtspersoon die een elektronisch zegel aanmaakt.\
Abonneehouder	Bron: Gids 'digitaal ondertekenen in de praktijk', 2021 De bij de QTSP geregistreerde contactpersoon voor de uitgifte en het beheer van certificaten binnen een organisatie of op persoonlijke titel in geval van het beroepscertificaat.
Afgeleid digitaal/elektronisch identificatiemiddel	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P. Een middel om een (rechts)persoon aan een bepaalde geregistreerde identiteit te linken. Deze identiteit is afgeleid van een digitale bronidentiteit van een (rechts)persoon zoals door de overheid vastgelegd.
Afnemend dienstverlener (Relying Party)	Een aanbieder van online-dienstverlening, die authenticatie laat plaatsvinden (afneemt) via een netwerk voor authenticatie. In het Engels wordt deze partij vaak aangeduid met de term Relying Party.
Afsprakenstelsel	Set van vastgelegde specificaties, regels en afspraken om samenwerking en zekerheid te garanderen op het gebied van technische functionaliteiten, beveiliging en privacy voor het uitwisselen van persoonlijke data. Eisen kunnen van technische aard zijn, bijvoorbeeld door het gebruik van bepaalde standaarden af te dwingen, maar kunnen bijvoorbeeld ook ingaan op het verdienmodel van een oplossing. Horizontale afsprakenstelsels Een afsprakenstelsel kan sectoronafhankelijk zijn. Dit is een horizontaal afsprakenstelsel. Een voorbeeld is het afsprakenstelsel van de overheid voor Elektronische Toegangsdiensten.
Afsprakenstelsel Elektronische toegangsdiensten.	Het afsprakenstelsel is een set van technische, functionele, juridische en organisatorische afspraken op basis waarvan eHerkenning wordt geleverd. De afspraken hebben als doel om samenwerking en zekerheid in het Netwerk te garanderen. Tegelijkertijd bieden de afspraken ook voldoende vrijheid aan de deelnemers om competitieve proposities te leveren aan hun klanten. Het afsprakenstelsel wordt inhoudelijk compleet beschreven in diverse documenten: eHerkenning valt onder het afsprakenstelsel Elektronische Toegangsdiensten.
Akte	Bron: Wikipedia Een akte is een officieel document.

Begrip	Omschrijving
	Het Nederlandse Wetboek van Burgerlijke Rechtsvordering definieert een akte als: "ondertekend geschrift, bestemd om tot bewijs te dienen" Er zijn wettelijk twee soorten akten: 1. authentieke akten. Deze worden opgemaakt door een bevoegd openbaar ambtenaar, als bijvoorbeeld een notaris of een rechter. 2. onderhandse akten. Deze kunnen door eenieder worden opgesteld. Een overheidsinstelling kan een akte afgeven. Een door een notaris vastgelegde akte heet een notariële akte. Om ongeautoriseerde wijzigingen in een papieren akte duidelijker te kunnen zien worden getallen vaak in letters geschreven, en de ruimten aan het eind van elke regel opgevuld met lijntjes.
Audittrail	Bron: Gids 'digitaal ondertekenen in de praktijk', 2021 Een logboek met een verzameling van feiten en controles (transacties) waaruit de identiteit van ondertekenaar, het tijdstip en het document (met een hashcontrole) blijkt.
Authenticatie	Bron: eIDAS verordening Een elektronisch proces dat de bevestiging van de elektronische identificatie van een natuurlijke persoon of rechtspersoon, of van de oorsprong en integriteit van gegevens in elektronische vorm mogelijk maakt.
Authenticatie (authenticeren)	Authenticatie is het proces dat nagaat of een gebruiker daadwerkelijk is wie hij/zij beweert te zijn. Dat wil zeggen: daadwerkelijk de identiteit bezit die hij/zij opgeeft. Deze vastgestelde identiteit bepaalt of de betreffende gebruiker gerechtigd is om een bepaalde handeling te verrichten of een service af te nemen; deze volgende stap noemen we autorisatie. Authenticatie bestaat uit twee stappen. Bij de registratiefase wordt eenmalig een account gemaakt op basis van persoonsgegevens. Hoe grondig hierbij wordt gecontroleerd of de persoonsgegevens daadwerkelijk bij de betreffende persoon horen, bepaalt de betrouwbaarheid: face-to-face-controle met een paspoort bij een balie, leidt tot een hogere mate van betrouwbaarheid dan een gebruiker die online zijn/haar gegevens invoert. Heeft de gebruiker eenmaal een account, dan kan hij/zij zich hier voortaan mee authenticeren. In deze inlogfase wordt vanaf nu alleen nog vastgesteld dat het om dezelfde gebruiker gaat als die ook de account aanmaakte. Ook hier hangt de betrouwbaarheid af van de mate waarin dit gecontroleerd wordt: enkel het invullen van een wachtwoord wordt als

Begrip	Omschrijving
	minder betrouwbaar verondersteld dan bijvoorbeeld een gezichtsscan of het invoeren van een extra code via de gsm van de gebruiker.
Authenticatiefactor	Bron: NORA Een factor waarvan is bevestigd dat deze gebonden is aan een bepaalde persoon en die onder een van de drie volgende categorieën valt Op bezit gebaseerde authenticatiefactor: een authenticatiefactor waarvan de betrokkene moet aantonen dat deze in zijn bezit is. Op kennis gebaseerde authenticatiefactor: een authenticatiefactor waarvan de betrokkene moet aantonen dat hij ervan kennis draagt. Inherente authenticatiefactor: een authenticatiefactor die op een fysiek kenmerk van een natuurlijke persoon is gebaseerd en waarbij de betrokkene moet aantonen dat hij dat fysieke kenmerk bezit.
Authenticatiefraude	Bron: NORA Authenticatie namens een persoon zonder diens toestemming.
Authenticatiemiddel	Het middel dat de gebruiker aanwendt bij authenticatie; iets wat de gebruiker weet, bezit of is.
Authentiseren	Bron: ICTU Referentiearchitectuur ROG Authentiseren is de activiteit waarbij iemand nagaat of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij beweert te zijn. Bij de authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken, bijvoorbeeld een in het systeem geregistreerd bewijs.
Autorisatie	Autorisatie is het verlenen van toestemming (een bevoegdheid) aan een geauthenticeerde partij om toegang te krijgen tot een bepaalde dienst of toestemming om een bepaalde actie uit te voeren. Een autorisatie kan worden vastgelegd in toegangsrechten. Het verlenen van toegang kan (mede) gebaseerd zijn op die in toegangsrechten vastgelegde autorisatie. Autorisatie is geen synoniem voor machtiging.
Autorisatie	Bron: eIDAS regulering, art 3. ‘Definities’ Bepalen of iemand geautoriseerd is/in aanmerking komt om toegang te krijgen tot een dienst of informatie etc.
Autorisatie	Bron: NORA Het proces van het toekennen van rechten voor de toegang tot geautomatiseerde functies en/of gegevens in ICT

Begrip	Omschrijving
	voorzieningen (NORA 3.0 Principes voor samenwerking en dienstverlening).
Betrouwbaarheidsniveau	Een betrouwbaarheidsniveau is een relatief niveau van de sterkte van het bewijsmateriaal aangaande een authenticatie. Dit niveau wordt bepaald door een samenhangend geheel van factoren, zoals de sterkte van de identiteitsverificatie tijdens de registratie en uitgifte van het authenticatiemiddel, de sterkte van het middel zelf en de sterkte het authenticatiemechanisme. Een betrouwbaarheidsniveau zegt iets over de betrouwbaarheid van: Het eHerkenningsmiddel: een certificaat (EH4) is sterker dan een gebruikersnaam-wachtwoord combinatie (EH1). De registratie van het eHerkenningsmiddel: een gebruiker die live verschijnt is betrouwbaarder dan een kopie van een paspoort. De uitgifte van het eHerkenningsmiddel: het middel persoonlijk uitreiken is betrouwbaarder dan dat dit per post wordt toegestuurd. Een betrouwbaarheidsniveau geeft dus de mate van zekerheid aan dat de juiste persoon over het gebruikte middel beschikt, in combinatie met de mate van zekerheid dat de gebruiker daadwerkelijk namens het bedrijf mag inloggen op die specifieke dienst.
Betrouwbaarheidsniveau	Bron: NORA Mate waarin vertrouwen kan worden gesteld in een identificatiemiddel, gebaseerd op de mate van zekerheid waarmee attributen, identiteiten, identificatiemiddelen en/of bevoegdheden zijn vastgesteld.
Betrouwbaarheidsniveaus DigiD	Bron: **Logius Handleiding DigiD**, januari 2023. DigiD kent vier betrouwbaarheidsniveaus die de mate van zekerheid bepalen over de identiteit van de zich authentiserende gebruiker: • **DigiD Basis:** gaat uit van iets dat een persoon weet en wat alleen hij weet. Bijvoorbeeld een wachtwoord. DigiD Basis kan gebruikt worden wanneer een beperkt aantal persoonsgegevens van de gebruiker wordt vastgelegd, bijvoorbeeld gegevens over een arbeidsrelatie of een klantrelatie. • **DigiD Midden:** gaat uit van de combinatie van iets dat een persoon weet en iets dat een persoon heeft. Deze combinatie maakt het inlogmiddel veiliger. DigiD Midden kan gebruikt worden als het gaat om uitwisseling van financieel-economische gegevens van gebruikers of bijzondere persoonsgegevens (godsdienst, politieke gezindheid, gezondheid).

Begrip	Omschrijving
	• **DigiD Substantieel:** gaat uit van de combinatie van iets dat een persoon weet en iets dat een persoon heeft. Daarnaast is geverifieerd dat de persoon in het bezit is van een Nederlands paspoort, Nederlandse identiteitskaart of rijbewijs dat de opgegeven identiteit vertegenwoordigt. DigiD Substantieel kan gebruikt worden als het gaat om uitwisseling van gegevens die extra privacygevoelig zijn zoals medische gegevens. • **DigiD Hoog:** gaat uit van de uitgifte van het inlogmiddel bij een balie ('face-to-face') en van de combinatie van iets dat een persoon heeft (inlogmiddel) en iets dat een persoon weet (bijbehorende pincode).
Beveiligingsincident	Bron: Afsprakenstelsel Elektronische Toegangsdiensten Een gebeurtenis die een bedreiging vormt of kan vormen voor de betrouwbaarheid, vertrouwelijkheid of beschikbaarheid van een elektronische toegangsdienst en/of een inbreuk op beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.
Biometrie	Bron: Biometrie voor identiteitsverificatie, Verkenning van de mogelijkheden, InnoValor 2020 Biometrische identiteit: Unieke set van onveranderlijke dan wel langdurig stabiele fysieke, fysiologische of gedrag gerelateerde kenmerken van een persoon. Deze kenmerken zijn uniek identificerend en worden gebruikt in biometrische systemen om iemand te herkennen en de identiteit vast te stellen.
Biometrische identiteit	Bron: Biometrie voor identiteitsverificatie, Verkenning van de mogelijkheden, InnoValor 2020 Unieke set van onveranderlijke dan wel langdurig stabiele fysieke, fysiologische of gedrag gerelateerde kenmerken van een persoon. Deze kenmerken zijn uniek identificerend en worden gebruikt in biometrische systemen om iemand te herkennen en de identiteit vast te stellen.
Certificaat	Bron: Wikipedia Een **certificaat** is een computerbestand dat fungeert als een digitaal paspoort voor de eigenaar van dat bestand en wordt gebruikt binnen de Public key infrastructure. Een digitaal certificaat is een combinatie van identiteit en openbare sleutel die gewaarmerkt is door de uitgever c.q. certificaatautoriteit (CA). Een certificaat bevat: • geregistreerde naam van de eigenaar c.q. certificaathouder; • publieke sleutel c.q. openbare sleutel van de eigenaar c.q. certificaathouder;

Begrip	Omschrijving
	• geldigheidsperiode van het certificaat; • identiteit van de uitgever c.q. certificaatautoriteit van het certificaat; • locatie van de 'Certificate Revocation List' (bij de uitgever van het certificaat); • samenvatting van bovenstaande gegevens, aangemaakt door een hashfunctie, en vervolgens vercijferd met de geheime sleutel van de uitgever c.q. certificaatautoriteit. Dit wordt een waarmerk of digitale handtekening genoemd en dient om de geldigheid c.q. authenticiteit van bovenstaande gegevens te waarborgen. Waarborgen authenticiteit c.q. geldigheid van een certificaat: • ontvanger van het certificaat berekent zelf de samenvatting van bovenstaande gegevens met behulp van de gebruikte hashfunctie; • ontvanger vraagt de openbare sleutel van de uitgever op (de meeste webbrowsers bevatten openbare sleutels van een groot aantal uitgevers); • ontvanger ontcijfert de ontvangen samenvatting in het certificaat met behulp van de openbare sleutel van de uitgever; • ontvanger vergelijkt of beide samenvattingen overeenstemmen (bij verschil is het ontvangen certificaat na uitgifte aangepast en niet meer authentiek en geldig)
Certificaat	Bron: https://www.cm.com/nl-nl/sign/elektronische-handtekening/ Certificaten worden uitgegeven door speciale Certificate Authorities (CA). Certificaten kunnen verlopen en worden ingetrokken, waardoor de geldigheid van documenten ook na lange tijd te valideren is. Volgens eIDAS is een certificaat niet verplicht voor een geavanceerde elektronische handtekening, toch wordt dit in de praktijk vrijwel altijd gebruikt. Dit komt omdat een certificaat de meest gangbare manier is om aan de andere eisen van een geavanceerde elektronische handtekening te voldoen. PDF documenten zijn van zichzelf al moeilijk aan te passen voor de gemiddelde persoon. Toch zou het mogelijk kunnen zijn dat iemand jouw ondertekende documenten wijzigt. Bijvoorbeeld door de voorwaarden van een contract aan te passen. Dankzij een digitaal certificaat kunnen elke aanpassing aan het originele document opgespoord worden. Simpel gezegd komt de digitale handtekening van het certificaat niet meer overeen met het document zodra deze wordt aangepast. Dankzij cryptografische berekeningen die maar 1 kant op werken is dit niet te vervalsen.
Certificaat voor elektronische handtekeningen	Bron: eIDAS verordening Een elektronische attestering die valideringsgegevens voor elektronische handtekeningen aan een natuurlijke persoon

Begrip	Omschrijving
	koppelt en ten minste de naam of het pseudoniem van die persoon bevestigt.
Certificaat voor elektronische zegels	Bron: eIDAS verordening Een elektronische attestering die valideringsgegevens van elektronische zegels aan een rechtspersoon verbindt en de naam van die rechtspersoon bevestigt.
Certificaat voor websiteauthenticatie	Bron: eIDAS verordening Attestering die het mogelijk maakt de authenticiteit van een website vast te stellen en die de website verbindt aan de natuurlijke of rechtspersoon aan wie het certificaat is afgegeven.
Conformiteitsbeoordelingsinstantie	Bron: eIDAS verordening Een instantie omschreven in artikel 2, punt 13, van verordening (eg) nr. 765/2008, die in overeenstemming met die verordening geaccrediteerd is om een conformiteitsbeoordeling te verrichten van een gekwalificeerde verlener van vertrouwensdiensten en van de door hem verleende vertrouwensdiensten.
CRL	Een Certificate Revocation List (CRL) is een lijst met certificaat serienummers die herroepen zijn, niet meer geldig zijn en niet meer te vertrouwen zijn voor gebruikers. Een CRL wordt periodiek gemaakt. De CRL wordt altijd uitgegeven (vaak elke 24 uur) door een Certificate Authority (CA) die zich alleen toespitst op hun eigen certificaten. Alle CRL's hebben een (vaak korte) periode waarin ze geldig zijn. Deze CRL's kunnen worden geraadpleegd door applicaties met PKI functionaliteit. Om spoofing of denial-of-service aanvallen te voorkomen zijn CRL's vaak digitaal ondertekend door de CA van de CRL. Een andere methode voor het controleren van de geldigheid van certificaten is het Online Certificate Status Protocol.
Dataminimalisatie	Bron: AVG Dataminimalisatie houdt in dat bij het verzamelen en verwerken van persoonsgegevens niet meer gegevens mogen worden gebruikt dan nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken.
Dataminimalisatie	Bron: Afsprakenstelsel Elektronische Toegangsdiensten Het zodanig inrichten van een gegevensverwerking dat er zo weinig mogelijk identificerende gegevens bekend hoeven te zijn bij zo weinig mogelijk partijen.
Dienst voor elektronisch aangetekende bezorging	Bron: eIDAS verordening

Begrip	Omschrijving
	Een dienst die het mogelijk maakt gegevens via elektronische middelen tussen derden te verzenden en die bewijs verschaft ten aanzien van het hanteren van de verzonden gegevens, met inbegrip van bewijs van het verzenden en ontvangen van de gegevens, en die de verzonden gegevens beschermt tegen het risico van verlies, diefstal, beschadiging of onbevoegde wijzigingen.
Digitaal ondertekenen	Bij digitaal ondertekenen wordt een handtekening toegevoegd door middel van een elektronische transactie. Hierbij wordt ook een tijdstempel gebruikt. De elektronische handtekening is het feitelijke bestand met gegevens van de transactie. Het technische proces bestaat uit deze stappen: • De software berekent met behulp van een algoritme de hashwaarde van het document. • De hashwaarde wordt versleuteld met de (geheime) privésleutel van de ondertekenaar. • Deze versleuteling vormt de elektronische handtekening. De controle: • De ontvanger ontcijfert de handtekening met behulp van de software. dankzij de publieke sleutel die samenhangt met de privé sleutel. • Als de uitkomst (de berekende hashwaarde) hetzelfde is, kan worden vastgesteld, dat de ondertekening heeft plaatsgevonden door de ondertekenaar, die in het bezit is van de privé sleutel én dat het document niet is gewijzigd.
Digitale bron identiteit (DBI)	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Een unieke, betrouwbare, inclusieve, veilige en door de overheid uitgegeven en erkende digitale identiteit voor entiteiten.
Digitale bronidentiteit	Bron: NORA Een verzameling van betrouwbare gegevens die een entiteit (persoon, organisatie, object of apparaat) representeren in het digitale domein.
Digitale handtekening	Bron: Connective, De complete gids over digitale handtekeningen Digitale handtekeningen zijn het meest geavanceerde en best beveiligde type elektronische handtekeningen. Ze gebruiken de standaarden en procedures van Public Key Infrastructure (PKI) om elektronische gegevens te ondertekenen met een cryptografische sleutel. De inhoud van het bericht kan niet worden gewijzigd of gemanipuleerd zonder de geldigheid van de digitale handtekening te schenden.

Begrip	Omschrijving
Digitale identiteit	Bron: Visiebrief Digitale Identiteit, kabinet 2021 Een digitale identiteit is een verzameling van betrouwbare gegevens waarmee een entiteit (persoon, organisatie, object of apparaat) zich digitaal kan identificeren en identiteitsgegevens en officiële documenten in elektronisch formaat kan opslaan en beheren.
Digitale identiteit	Bron: NORA Een identiteit die een digitale representatie is van een persoon.
Digitale/elektronische identificatie	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Het proces van het gebruiken van persoonsidentificatiegegevens in elektronische vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden.
Digitale/elektronische identiteit	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Een identiteit in de onlinewereld voor entiteiten. Een digitale identiteit kan bestaan uit verschillende aspecten (attributen) die over een bepaalde entiteit geregistreerd staan. ISO/IEC stelt: een digitale identiteit is een set attributen die te relateren zijn aan een entiteit.
Digitale/elektronische identiteit infrastructuur	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Het geheel van stelsels, afspraken, standaarden en voorzieningen, rond de digitale identiteit van (rechts)personen.
eIDAS	eIDAS staat voor Electronic Identification (eID) and Trust Services (AS). Het is een initiatief van de Europese Commissie met als doel om elektronische interacties tussen ondernemingen, burgers en organisaties veiliger en efficiënter te maken en alle EU-landen elkaars eID en AS erkennen.
eIDAS-verordening	Bron: Afsprakenstelsel Elektronische Toegangsdiensten EU verordening nr. 910/2014 van het Europees Parlement en de Raad (23 juli 2014) en de Uitvoeringsverordening EU 2015/1501 en 2015/1502 (8 september 2015), betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt. Niet alleen EU-lidstaten implementeren de eIDAS-verordening, daarom wordt er aan implementerende landen gerefereerd met "eIDAS-lidstaten". De eIDAS-verordening is integraal te lezen.
Elektronisch document	Bron: eIDAS verordening

Begrip	Omschrijving
	Elke inhoud die is opgeslagen in elektronische vorm, in het bijzonder tekst of geluid, beeld of audiovisuele opname.
Elektronisch identificatiemiddel	Bron: eIDAS verordening Een materiële en/of immateriële eenheid die persoonsidentificatiegegevens bevat en die gebruikt wordt voor authenticatie bij een onlinedienst.
Elektronisch zegel	Bron: eIDAS verordening Gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die worden gebruikt om de oorsprong en integriteit daarvan te waarborgen.
Elektronische handtekening	Bron: Handreiking Elektronische handtekening, VNG, Den Haag 2021 Een elektronische handtekening is een verzameling gegevens in elektronische vorm, die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen.
Elektronische handtekening	Bron: eIDAS verordening Gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen.
Elektronische identificatie	Bron: eIDAS verordening Het proces van het gebruiken van persoonsidentificatiegegevens in elektronische vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden.
Elektronische tijdstempel	Bron: eIDAS verordening Gegevens in elektronische vorm die andere gegevens in elektronische vorm verbinden aan een bepaald tijdstip en die bewijzen dat die laatstgenoemde gegevens op dat tijdstip bestonden.
ETSI	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Het European Telecommunications Standards Institute (ETSI) coördineert op Europees niveau standaarden rondom o.a. elektronische communicatie.

Begrip	Omschrijving
ETSI TA 119 312	De ETSI TS 119 312 standaard definieert algoritmes en sleutellengtes. De algoritmes worden gebruikt voor het plaatsen van een hash over een document of transactie, en is de eerste stap naar de digitale ondertekening van een bericht.
EULA	Bron: Gids 'digitaal ondertekenen in de praktijk', 2021 De end-user-license-agreement is een gebruikers(licentie) overeenkomst die softwareleveranciers hun eindgebruikers aanbieden, waarin algemene leveringsvoorwaarden zijn opgenomen. Dit kan van belang zijn, indien ondertekensoftware door (eind)gebruikers wordt gebruikt waarmee geen licentie- en/of contractrelatie bestaat.
Extern beheer	Bron: Gids 'digitaal ondertekenen in de praktijk', 2021 Het uit handen geven van de opslag van gekwalificeerde certificaten aan een QTSP.
Geavanceerd elektronisch zegel	Bron: eIDAS verordening Een elektronisch zegel dat voldoet aan de eisen in artikel 36.
Geavanceerde elektronische handtekening	Bron: eIDAS verordening Een elektronische handtekening die voldoet aan de eisen in artikel 26.
Geavanceerde elektronische handtekening	Bron: Handreiking Elektronische handtekening, VNG, Den Haag 2021 Een geavanceerde elektronische handtekening kent meer waarborgen dan een 'gewone' elektronische handtekening, en maakt gebruik van wiskundige technieken om een unieke code aan een bericht te koppelen. Deze code wordt afgeleid uit het bericht zelf en uit de identiteit van de afzender. Daarmee is de code niet te gebruiken bij een vervalst bericht, zodat zo'n geavanceerde elektronische handtekening al snel als betrouwbaar en dus rechtsgeldig wordt gezien. Deze vorm wordt ook wel aangeduid als de "digitale handtekening". De Wet elektronische handtekeningen stelt er de volgende eisen aan: • de handtekening is op een unieke manier aan de ondertekenaar verbonden; • de handtekening maakt het mogelijk de ondertekenaar te identificeren; • de manier waarop de handtekening wordt gemaakt, staat onder exclusieve controle van de ondertekenaar; • de handtekening is op dusdanige wijze met het bestand - waarvoor het geldt - verbonden, dat elke naderhand aangebrachte wijziging kan worden opgespoord.

Begrip	Omschrijving
	Dit is in lijn met artikel 26 uit de eIDAS verordening. Hoe in te richten In dit geval is de elektronische handtekening nog steeds op meerdere manieren in te richten, maar kan niet worden volstaan met alleen het plakken van een plaatje. Het moet duidelijk af te leiden zijn wie de ondertekenaar is, dat de handtekening wordt gezet door de persoon aan wie de handtekening toebehoort en dat de ondertekenaar in staat is de handtekening voor zichzelf te houden. Denk hierbij in de simpelste vorm aan een gebruikersnaam en wachtwoord dat uniek aan de ondertekenaar wordt toebedeeld. Ten slotte is het laatste vereiste dat de integriteit van de boodschap bewaard blijft, en dat dit achteraf aangetoond moet kunnen worden. Hierbij kun je denken aan het loggen van bepaalde acties tijdens het proces, het vastleggen van de originele boodschap, of het gebruiken van een certificaat om de integriteit van een bestand te waarborgen. De geavanceerde elektronische handtekening in de praktijk: • Is vaak aangeboden door middel van validatie op basis van e-mailadres en/of een tweede validatiestap via bijvoorbeeld 06-nummer of iDIN. • Kan ook plaatsvinden middels uitgebreidere identificatie op basis van identificatiebewijs en geavanceerd persoonlijk certificaat uitgegeven door een (Q)TSP. De geavanceerde elektronische handtekening is geschikt voor overeenkomsten met beperkt juridisch gevolg, bijvoorbeeld: • Brieven; • Offertes; • Opdrachtbevestigingen; • Beperkte machtigingen.
Geavanceerde ondertekening	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Een elektronische handtekening die voldoet aan de (vier) wettelijke eisen van deze vorm en daarmee extra waarborgen bevat, die helpen bij het verkrijgen van bewijslast. In sommige situaties kan de handtekening ook dezelfde rechtsgevolgen hebben als een natte handtekening.
Gebruiker	Bron: NORA Iedere persoon, organisatie of functionele eenheid die gebruik maakt van een informatiesysteem.
Gegevens voor het aanmaken van elektronische handtekeningen	Bron: eIDAS verordening Unieke gegevens die door de ondertekenaar worden gebruikt om een elektronische handtekening aan te maken.

Begrip	Omschrijving
Gegevens voor het aanmaken van elektronische zegels	Bron: eIDAS verordening Unieke gegevens die door de aanmaker van het elektronische zegel worden gebruikt om een elektronisch zegel aan te maken.
Geïnformeerde uitdrukkelijke toestemming	Bron: Afsprakenstelsel Elektronische Toegangsdiensten De geïnformeerde uitdrukkelijke toestemming die wordt gevraagd voorafgaand aan registratie en verstrekking van aanvullende attributen. Dit houdt in dat degene die verantwoordelijk is voor de verwerking van persoonsgegevens ervoor zorgt dat voorafgaande aan de uitdrukkelijke toestemming van de betrokkene informatie wordt verstrekt over het doel van de verwerking van persoonsgegevens, welke gegevens worden verwerkt, of er sprake is van derdenverstrekking en zo ja, met welk doel alsmede de rechten die betrokkenen tegen de gegevensverwerking kunnen uitoefenen.
Gekwalificeerd certificaat voor elektronische handtekeningen	Bron: eIDAS verordening Een certificaat voor elektronische handtekeningen, dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage i.
Gekwalificeerd certificaat voor elektronische zegels	Bron: eIDAS verordening Een certificaat voor een elektronische zegel dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage iii.
Gekwalificeerd certificaat voor websiteauthenticatie	Bron: eIDAS verordening Certificaat voor websiteauthenticatie dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage iv.
Gekwalificeerd elektronisch zegel	Bron: eIDAS verordening Een geavanceerd elektronisch zegel dat aangemaakt is door een gekwalificeerd middel voor het aanmaken van elektronische zegels en dat gebaseerd is op een gekwalificeerd certificaat voor elektronische zegels.
Gekwalificeerd middel voor het aanmaken van elektronische handtekeningen	Bron: eIDAS verordening Een middel voor het aanmaken van elektronische handtekeningen dat voldoet aan de eisen van bijlage ii.
Gekwalificeerd middel voor het aanmaken van elektronische zegels	Bron: eIDAS verordening Een middel voor het aanmaken van elektronische zegels dat mutatis mutandis voldoet aan de eisen van bijlage ii.

Begrip	Omschrijving
Gekwalificeerde ondertekening	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Een elektronische handtekening met behulp van een persoonlijk (al dan niet-beroepsgebonden) certificaat en een ondertekenmiddel die aan hoge betrouwbaarheidsvereisten voldoet. Met dezelfde rechtsgevolgen als een natte handtekening.
Gekwalificeerde dienst voor elektronisch aangetekende bezorging	Bron: eIDAS verordening Een dienst voor elektronisch aangetekende bezorging die voldoet aan de in artikel 44 vastgestelde eisen.
Gekwalificeerde elektronische handtekening	Bron: eIDAS verordening Een geavanceerde elektronische handtekening die is aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen.
Gekwalificeerde elektronische handtekening	Bron: Handreiking Elektronische handtekening, VNG, Den Haag 2021 De gekwalificeerde elektronische handtekening is de zwaarste variant en kent de volgende definitie in de eIDAS-verordening: „gekwalificeerde elektronische handtekening”: een geavanceerde elektronische handtekening die is aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen. In de definitie zie je dat er een extra eis wordt gesteld, boven op de eisen voor de geavanceerde elektronische handtekening. Het grote verschil is dat er een gekwalificeerd middel en gekwalificeerd certificaat gebruikt moet worden om te ondertekenen. Aan zowel de gekwalificeerde certificaten als de gekwalificeerde middelen stelt de eIDAS-verordening strenge eisen. De in de praktijk meest gebruikte toepassing van de gekwalificeerde elektronische handtekening houdt in dat de ondertekenaar een persoonlijk PKI-certificaat krijgt toegewezen, waarvoor hij of zij zich in levende lijven zal moeten identificeren. Het certificaat wordt op een externe token of kaart gezet en ter beschikking gesteld aan de ondertekenaar. De combinatie van het certificaat en het middel maakt dat voldoende betrouwbaar kan worden vastgesteld wie de ondertekenaar is. Een certificaat is conform de Wet elektronische handtekeningen een elektronische bevestiging die gegevens voor het verifiëren van een elektronische handtekening met een bepaalde persoon verbindt en de identiteit van die persoon bevestigt. Een

Begrip	Omschrijving
	gekwalificeerd certificaat is een certificaat dat onder strikte voorwaarden is uitgegeven aan de houder, zodanig dat er een grote zekerheid is over de koppeling met de houder. Gekwalificeerde certificaten zijn in verregaande mate gestandaardiseerd. Dit is de meest betrouwbare handtekening. Daar is een gekwalificeerde verlener van vertrouwensdiensten voor nodig. Deze gekwalificeerde dienstverleners staan onder publiekrechtelijk toezicht. Gekwalificeerde handtekeningen zullen duurder zijn dan de geavanceerde. Gekwalificeerde elektronische handtekening is geschikt voor overeenkomsten en verklaringen met een hoog juridisch gevolg en daar waar wettelijk verplicht, onder meer: • Kredietovereenkomsten; • Accountantsverklaringen (SBR Assurance); • Arbeidscontracten; • Aanbestedingen. Een gekwalificeerd certificaat kan men aanvragen bij een bedrijf dat op de vertrouwenslijst van de Europese Commissie staat. De Rijksinspectie Digitale Infrastructuur (RDI) (voorheen Agentschap Telecom) controleert deze bedrijven.
Gekwalificeerde elektronische tijdstempel	Bron: eIDAS verordening Een elektronische tijdstempel die voldoet aan de in artikel 42 vastgelegde eisen.
Gekwalificeerde verlener van vertrouwensdiensten	Bron: eIDAS verordening Een verlener van vertrouwensdiensten die één of meerdere gekwalificeerde vertrouwensdiensten verleent en van het toezichthoudende orgaan de status van gekwalificeerde heeft gekregen.
Gekwalificeerde vertrouwensdienst	Bron: eIDAS verordening Een vertrouwensdienst die voldoet aan de toepasselijke eisen zoals vastgelegd in deze verordening.
Gewone elektronische handtekening	Bron: Handreiking Elektronische handtekening, VNG, Den Haag 2021 Hieronder valt bijvoorbeeld een ‘scan van de fysieke handtekening’. De betrouwbaarheid daarvan is betrekkelijk, want eenvoudig na te maken. De ontvanger kan wellicht wel controleren of de handtekening overeen komt, maar zekerheid dat deze ook écht door de wederpartij is gezet heeft hij niet. Dit is in feite een kopie van een echte handtekening, heeft dus

Begrip	Omschrijving
	weinig tot geen bewijskracht en is niet ‘voldoende betrouwbaar’ zoals het BW dat voorschrijft. De bekendste toepassing van de gewone elektronische handtekening is weliswaar het gescande plaatje van de natte handtekening, maar het is van belang om op te merken dat de ‘gewone’ elektronische handtekening allerlei (andere) vormen kent. Andere voorbeelden van de ‘gewone’ elektronische handtekeningen zijn het typen van een naam in een document op de plaats waar moet worden ondertekend. Ook het ‘plakken’ van een gescand exemplaar van een ‘papieren’ handtekening valt binnen deze categorie. Deze handtekening is slechts geschikt voor overeenkomsten met een laag juridisch risico.
Hash	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Een cryptografische berekening volgens een algoritme waarbij een waarde wordt vervangen door een tekenreeks. Het wordt gebruikt voor pseudonimisering en in het elektronische ondertekenproces als controlemiddel bij het vaststellen van de afzender en wijzigingen in bijvoorbeeld documenten. Hierbij wordt de huidige tekenreeks vergeleken met de oorspronkelijke tekenreeks. Hashing is een essentieel onderdeel van de elektronische ondertekening.
HSM	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Een Hardware Security Module is een beveiligde omgeving waarbinnen gekwalificeerde certificaten opgeslagen kunnen worden. Wanneer een HSM is ondergebracht bij een QTSP, die onder toezicht staat wordt gesproken over een gekwalificeerde HSM.
Identificatie	Bron: eIDAS regulering, art 3. ‘Definities’ Registratie van een unieke identiteit (vaststelling en creatie) en vervolgens het uitgeven van een identificatiemiddel om personen in staat te stellen om deze identiteit te laten verifiëren.
Identificatie/Identificeren	Het overleggen van attributen van een entiteit om deze in een bepaalde context uniek aan te duiden.
Identificeerbaar	Bron: ICTU Referentiearchitectuur ROG Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Identificeren	Bron: ICTU Referentiearchitectuur ROG

Begrip	Omschrijving
	Vaststellen wie is een gebruiker, een andere computer of applicatie is.
Identiteit	Bron: BZK, Presentatie 16 juli 2020, Klantportaal A&P Een identiteit bestaat uit de geregistreerde aspecten (attributen) die in voldoende mate bepalen wie iemand of iets is.
Identiteit	Bron: NORA Identiteit is de eenheid van wezen, volkomen overeenstemming en gelijkheid. Dat wat uniek of eigen is aan iets of iemand. Het kan daarbij gaan om zowel personen als organisaties of landen.
iDIN	Bron: DNB iDIN Een dienst van de banken waarmee hun klanten zich met hun eigen inlogmiddelen van hun bank, online kunnen identificeren bij andere organisaties. Zo hoef je geen aparte toegangscodes aan te vragen en te onthouden van bijvoorbeeld verzekeringsmaatschappijen, overheidsinstanties of webwinkels
Inlogmiddel	Zie authenticatiemiddel.
iProov	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Biometrische (gezichtsherkennings)oplossing voor identiteits-verificatie die bijvoorbeeld bij banken in gebruik is om(nieuwe) klanten te verifiëren.
Itsme	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Belgische oplossing (app) voor het beheer van je digitale identiteit. Met de app kunnen gebruikers zich bijvoorbeeld identificeren, transacties bevestigen en documenten ondertekenen.
LTV	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Longterm Validation of Lange-termijn validatie. Het op de juiste wijze toepassen en vastleggen van metagegevens als het tijdstempel, zodat in de toekomst kan worden vastgesteld of ondertekening in het verleden op de juiste wijze heeft plaatsgevonden. Zo wordt voorkomen, dat een ongeldige handtekening wordt gepresenteerd, doordat bijvoorbeeld certificaten intussen verlopen zijn.
Machtigen	Bron: ICTU Referentiearchitectuur ROG Machtigen (het verlenen van een volmacht) heeft hier betrekking op het verlenen van toestemming aan een dienstverlener om in het kader van een offerte nader gespecificeerde gegevens die zich in de administratie van de overheid bevinden op te halen en rechtstreeks aan

Begrip	Omschrijving
	die dienstverlener te verstrekken. Onderdeel van machtigen is ook het beheren van de machtigingen (dus overzicht geven, verlenen, wijzigen en intrekken). Een andere vorm van volmacht verlening is de vertegenwoordiger (zoals schuldhulpverlener, echtscheidingsconsulent e.d.) die in opdracht van de vertegenwoordigde burger namens deze burger optreedt.
Machtigen (eHerkenning)	Bron: KvK Als een gebruiker met eHerkenning een online-dienst wil afnemen, dan moet deze daarvoor gemachtigd zijn. Zonder machtiging werkt eHerkenning niet. Een machtiging is, net als eHerkenning, persoonsgebonden. Een machtiging kan alleen worden gegeven door iemand in de organisatie die tekenbevoegd is volgens het Handelsregister van de Kamer van Koophandel. Als er meerdere personen tekenbevoegd zijn moeten zij mogelijk ook tekenen, dat is afhankelijk van de statuten van het bedrijf. De 'tekenbevoegde' kan ook een machtigingenbeheerder aanstellen die dan de machtigingen kan verstrekken. Een machtigingenbeheerder neemt de tekenbevoegde veel werk uit handen.
Machtiging	Bron: ICTU Referentiearchitectuur ROG Een toestemming van de burger aan de dienstverlener om namens hem gegevens over hem in te winnen bij de overheid. Deze toestemming kan ook vooraf gegeven worden bij de bron: de overheid machtigt de overheid om (onder bepaalde condities) persoonsgegevens te leveren aan een dienstverlener indien deze daarom vraagt.
MFA	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Multifactor authenticatie, ook wel 2-staps-verificatie genoemd, is een inlogmethodiek, waarbij naast een gebruikersnaam en wachtwoord extra informatie (stap) nodig is om een identiteit te verifiëren, bijvoorbeeld d.m.v. SMS of token(app) verificatie.
Middel voor het aanmaken van elektronische handtekeningen	Bron: eIDAS verordening Geconfigureerde software of hardware die wordt gebruikt om een elektronische handtekening aan te maken.
Middel voor het aanmaken van elektronische zegels	Bron: eIDAS verordening Geconfigureerde software of hardware die wordt gebruikt om een elektronisch zegel aan te maken.
Middelenuitgever	Verantwoordelijk voor de uitgifte van authenticatiemiddelen en alle daaraan verbonden processen: aanvraag, registratie, activering, blokkering/heractivering, inname en opheffing. Vaak treedt de middelenuitgever ook op als authenticatiedienst.

Begrip	Omschrijving
Multifactor Authenticatie (MFA)	Dit is een authenticatie methode waarbij de onlinegebruiker twee stappen succesvol moet doorlopen om ergens toegang tot te krijgen.
Netwerk voor authenticatie	Bron: Afsprakenstelsel Elektronische Toegangsdiensten De verzameling onderling verbonden componenten die gereguleerd worden door het afsprakenstelsel en gezamenlijk authenticatiediensten leveren.
Ondertekenaar	Bron: eIDAS verordening Een natuurlijke persoon die een elektronische handtekening aanmaakt.
PAdES	Bron: Gids 'digitaal ondertekenen in de praktijk', 2021 De technologische standaard voor de implementatie van pdf-ondertekening op geavanceerde, elektronische wijze (zogenaamde ETSI-norm) en in Nederland verplicht is bij de toepassing in het (semi)overheidsdomein. Het tijdstempel is hierin een vereiste voor lange termijn validatie (LTV).
Persoonsidentificatiegegevens	Bron BZK, Presentatie 16 juli 2020, Klantportaal A&P Een reeks gegevens aan de hand waarvan de identiteit van een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, kan worden vastgesteld.
Persoonsidentificatiegegevens	Bron: eIDAS verordening Een reeks gegevens aan de hand waarvan de identiteit van een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, kan worden vastgesteld.
Polymorfe pseudonimisering	Bron: Afsprakenstelsel Elektronische Toegangsdiensten Een vorm van versleuteling, waarbij specifieke pseudoniemen voor een gebruiker worden gevormd per Ontvangende Partij, zonder dat de vormende partij het specifiek pseudoniem kan herleiden of de identiteit van de gebruiker bij gebruik hoeft te kennen. Polymorfe pseudonimisering is gebaseerd op cryptografie, waardoor het onder andere de bovengenoemde eigenschappen kan bieden.
Public Key Infrastructure	Bron: Connective, De complete gids over digitale handtekeningen Update 2021 Digitale handtekeningen werken met een specifiek protocol: een 'public key infrastructure' of PKI. Dit protocol gebruikt cryptografische algoritmen om twee lange cijferreeksen te

Begrip	Omschrijving
	genereren: de 'sleutels'. Eén sleutel is openbaar, de andere privé. Om de digitale handtekening van elke ondertekenaar uniek te maken, worden documenten steeds ondertekend met de privésleutel. Deze wordt veilig bewaard door de ondertekenaar en staat steeds in zijn of haar handtekening. Kort gezegd koppelt de digitale handtekening de ondertekenaar aan het document met behulp van een code. Naast deze sleutel bevat de handtekening ook het certificaat van de ondertekenaar. Dit certificaat bevat de openbare sleutel en aanvullende informatie, zoals de datum en het tijdstip van ondertekening. Voordat de handtekening wordt geplaatst, maakt een cryptografische functie een 'message digest' of 'hash' aan (vergelijkbaar met een stukje data). Daarna wordt deze hash versleuteld met de privésleutel van de ondertekenaar en in de digitale handtekening opgenomen. Wanneer het document op zijn bestemming aankomt, wordt er een tweede hash gemaakt. Nadat de hash in de handtekening is ontsleuteld, wordt deze vergeleken met de hash die voor het document is aangemaakt. Als ze niet overeenstemmen, ziet de ontvanger dat het document gemanipuleerd is en is de digitale handtekening ongeldig.
QES	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Een Qualified Electronic Signature: de toepassing van de gekwalificeerde elektronische handtekening onder eIDAS.
QTSP	Een Qualified Trusted Service Provider is een gekwalificeerde dienstverlener die bijvoorbeeld certificaten mag verstrekken. De dienstverlener opereert binnen de EU/staat op de EU trusted List en onder toezicht van Agentschap Telecom.
Rendering	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Het proces waarbij data in een elektronisch formaat (XML, XBRL) visueel wordt gepresenteerd.
SBR Assurance	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 Methodiek waarbij een ‘handtekeningbestand’ gemaakt wordt met eigenschappen van de gekwalificeerde ondertekening én hashwaarden van (meerdere) databestanden. Hierbij wordt de handtekening verbonden aan de bestanden. Gebruikt in specifieke branches.
Self Sovereign Identity	Bron: NORA Het concept van Self Sovereign Identity (SSI) legt de controle en de macht over een digitale identiteit volledig bij de entiteit die deze digitale identiteit representeert. Dit vereist volledige

Begrip	Omschrijving
	onafhankelijkheid van een centraal register of centrale autoriteit.
Self-sovrin identity	Self-sovrin identity is een digitale identiteit waarbij de gebruiker en diens privacy centraal staat. De gebruiker kan met SSI zelf zijn identiteit bewaren. In tegenstelling tot de klassieke identiteiten waarbij een gebruiker, òf bij elke organisatie opnieuw moet inloggen met een andere identiteit, òf bij elke organisatie inlogt via een andere organisatie (denk aan knoppen met tekst 'Login met DigiD' of 'Login met Google') en deze haar identiteit vervolgens doorgeeft aan die organisatie. In SSI krijgt de gebruiker eenmalig, van bijvoorbeeld DigiD, een digitaal identiteit met daarin al haar gegevens en kan deze vervolgens met andere organisaties delen. Met de self-sovereign identiteit die de gebruiker zelf bezit, kan de gebruiker buiten DigiD om, zelf inloggen bij andere partijen, zonder dat DigiD daarvan op de hoogte is. Bij het inloggen middels een 'login met DigiD of Google', weten deze partijen op welke sites een gebruiker zijn identiteit gebruikt. Met SSI heeft de gebruiker dus meer privacy. Er zijn verschillende voorbeelden die als SSI benoemd kunnen worden, zoals Sovrin, welke een blockchain gebruikt en IRMA, welke het Idemix protocol gebruikt.
SES	Bron: Gids 'digitaal ondertekenen in de praktijk', 2021 Een Simpel Electronic Signature: de toepassing van de eenvoudige / gewone elektronische handtekening onder eIDAS.
Smartcard	Bron: Gids 'digitaal ondertekenen in de praktijk', 2021 Een pas die samen met een USB-pashouder gebruikt wordt en waarop een certificaat staat, dat gebruikt wordt bij gekwalificeerde ondertekening.
SMS-verificatie	Bron: Gids 'digitaal ondertekenen in de praktijk', 2021 Een stap waarbij een natuurlijk persoon een SMS-code ontvangt, die als controlewaarde dient om diens identiteit te bevestigen.
Stelsel voor elektronische identificatie	Bron: eIDAS verordening Een stelsel voor elektronische identificatie waarbinnen elektronische identificatiemiddelen worden uitgegeven aan natuurlijke personen, rechtspersonen of natuurlijke personen die rechtspersonen vertegenwoordigen.
Tekenbevoegd	Mensen die tekenbevoegd zijn, mogen namens de onderneming bepaalde rechtshandelingen uitvoeren. Iemand kan volledig tekenbevoegd zijn, maar er kunnen ook beperkingen zijn.

Begrip	Omschrijving
	In het KVK Handelsregister, en de vergelijkbare buitenlandse registers is informatie te vinden over bedrijven, bevoegde personen en bijvoorbeeld faillissementen en jaarrekeningen. In het uittreksel van een bedrijf staat wie er mag tekenen, en of er beperkingen zijn. Daarmee kan je nagaan wie er op dat moment namens een bedrijf een contract mag sluiten. Vaak mag een persoon alleen samen met een andere vennoot of bestuurder een belangrijke overeenkomst sluiten. Wie er tekenbevoegd zijn, verschilt per rechtsvorm. In dit overzicht vind je de tekenbevoegdheid per rechtsvorm.
Tijdstempel	Bron: Gids 'digitaal ondertekenen in de praktijk', 2021 Ook wel timestamp genoemd en is een (beveiligde) vastgestelde tijd die wordt verkregen van een tijdstempelserver. Het toont aan, dat een document op het moment van ondertekenen daadwerkelijk bestond. Deze wordt idealiter opgenomen in de ondertekening.
Toestemming van de betrokkene	Bron: AVG Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling de hem of haar betreffende verwerking van persoonsgegevens aanvaardt.
Toestemming/consent	Bron: AVG Twee van de eisen die de AVG stelt aan 'toestemming' zijn dat deze 'geïnformeerd' en 'specifiek' gegeven is. Om geldige toestemming aan te tonen is het dan ook essentieel dat een organisatie kan laten zien op basis van welke informatie de betrokken personen de toestemming heeft gegeven. Het is dus onvoldoende om alleen de toestemming zelf vast te leggen.
Token(app)-verificatie	Bron: Gids 'digitaal ondertekenen in de praktijk', 2021 Een stap waarbij een natuurlijk persoon een code ontvangt via een app op een smartphone, die als controlewaarde dient om diens identiteit te bevestigen.
Trust Framework	Bron: ICTU Referentiearchitectuur ROG Een vertrouwensraamwerk bestaat uit afspraken op juridisch, organisatorisch, financieel, communicatief, semantisch en technisch gebied, zodat personen en dienstaanbieders op een veilige en efficiënte manier kunnen samenwerken. Partijen die deelnemen committeren zich aan de afspraken, en kunnen diensten aanbieden op basis van de reeds overeengekomen afspraken. Een canvas voor zo'n vertrouwensraamwerk voor het delen van gegevens is uitgewerkt in Data Sharing Canvas. Binnen Regie op Gegevens van de overheid wordt het

Begrip	Omschrijving
	vertrouwensraamwerk uitgewerkt in het *Vertrouwensraamwerk Regie op Gegevens*.
Tweestapsverificatie	Tweestapsverificatie wordt ook wel tweefactorautorisatie of sterke klantauthenticatie genoemd. In het Engels: strong customer authentication of SCA. Het is een veilige manier om een betaling goed te keuren met twee verschillende dingen waar alleen de rechtmatige pashouder of rekeninghouder over beschikt. Aan de kassa is dat meestal een persoonlijke pinpas in combinatie met een geheime pincode. Met iDEAL en internetbankieren is dat vaak een persoonlijk inlogapparaatje, ook weer in combinatie met een geheime pincode. Bij mobiel bankieren is het een persoonlijke smartphone, bijvoorbeeld in combinatie met gezichtsherkenning.
USB-token	Bron: Gids 'digitaal ondertekenen in de praktijk', 2021 Een USB-stick waarop een certificaat staat die wordt gebruikt bij gekwalificeerde ondertekening.
User consent	Bron: Afsprakenstelsel Elektronische Toegangsdiensten De geïnformeerde uitdrukkelijke toestemming die wordt gevraagd voorafgaand aan registratie en verstrekking van aanvullende attributen. Dit houdt in dat degene die verantwoordelijk is voor de verwerking van persoonsgegevens ervoor zorgt dat voorafgaande aan de uitdrukkelijke toestemming van de betrokkene informatie wordt verstrekt over het doel van de verwerking van persoonsgegevens, welke gegevens worden verwerkt, of er sprake is van derdenverstrekking en zo ja, met welk doel alsmede de rechten die betrokkenen tegen de gegevensverwerking kunnen uitoefenen.
Validering	Bron: eIDAS verordening Proces waarmee wordt nagegaan of en bevestigd dat een elektronische handtekening of een elektronisch zegel geldig is.
Valideringsgegevens	Bron: eIDAS verordening Gegevens die worden gebruikt om een elektronische handtekening of elektronisch zegel te valideren.
Verifiable credentials	Een credential is een uitspraak over een persoon door een entiteit, die gecontroleerd kan worden. Denk bijvoorbeeld aan een paspoort, deze bewijst vanuit de overheid je identiteit. Dit kan gecontroleerd worden aan de echtheidskenmerken van een paspoort of door het uitlezen van de cryptografisch beveiligde chip in het document. Ook een diploma is een voorbeeld van een credential, deze bevat vaak de schriftelijke handtekening van de onderwijsinstelling.

Begrip	Omschrijving
	In de digitale wereld hebben we vergelijkbare credentials met hun echtheidskenmerken en deze worden verifiable credentials genoemd. Deze echtheidskenmerken kunnen variëren, van een copy van een document met handtekening tot cryptografische ondertekende documenten. Een digitale handtekening met behulp van asymmetrische encryptie, is een mooi voorbeeld. De entiteit gebruikt zijn cryptografische privé sleutel om een credential uit te geven, andere partijen kunnen de publieke sleutel gebruiken om te controleren dat de credential echt is uitgegeven door de entiteit. Het is in PDM belangrijk dat de data die van de gebruiker naar andere partijen gestuurd wordt ook gecontroleerd kan worden op echtheid, verifiable credentials zouden daarvoor gebruikt kunnen worden. Een voorbeeld van een open standaard van verifiable credential is gemaakt door W3C, deze wordt veel gebruikt in SSI-oplossingen. Ook Idemix, wat gebruikt wordt in IRMA, is een vorm van verifiable credentials.
Verlener van vertrouwensdiensten	Bron: eIDAS verordening Een natuurlijke persoon of rechtspersoon die een of meer vertrouwensdiensten verleent als een gekwalificeerde of als een niet-gekwalificeerde verlener van vertrouwensdiensten.
Vertrouwende partij	Bron: eIDAS verordening Vertrouwende partij: een natuurlijke persoon of een rechtspersoon die vertrouwt op een elektronische identificatie of een vertrouwensdienst.
Vertrouwensdienst	Bron: eIDAS verordening Een elektronische dienst die gewoonlijk tegen betaling wordt verricht en het onderstaande inhoudt: • Het aanmaken, verifiëren en valideren van elektronische handtekeningen, elektronische zegels of elektronische tijdstempels, diensten voor elektronisch aangetekende bezorging en op deze diensten betrekking hebbende certificaten of • Het aanmaken, verifiëren en valideren van certificaten voor authenticatie van websites, of Het bewaren van elektronische handtekeningen, zegels of certificaten die op deze diensten betrekking hebben.
Waarmerk	Bron: ICTU Referentiearchitectuur ROG Een waarmerk is een extra kenmerk van (een set van) gegeven(s) waaruit blijkt dat de uitgever van het waarmerk (meestal na onderzoek) de juistheid van het gegeven onderschrijft (“voor waar aanmerkt”).

Begrip	Omschrijving
Waarmerken Elektronische identiteit	Bron: ICTU Referentiearchitectuur ROG Een gegeven of een set van gegevens wordt hiermee voorzien van bewijs van de identiteit van de betrokkene. Komt overeen met elektronische identiteitsbewijs uit eIDAS.
Waarmerken Elektronisch dateren	Bron: ICTU Referentiearchitectuur ROG Een gegeven of set van gegevens wordt hiermee voorzien van een datum zodat vastgelegd is wat de datum van creëren/levering is. Komt overeen met *elektronische tijdstempel* uit eIDAS (op eur.lex.europa.eu, amendement artikel 3 punt 16).
Waarmerken Elektronisch ondertekenen	Bron: ICTU Referentiearchitectuur ROG Een gegeven of set van gegevens wordt hiermee voorzien van een elektronische verklaring van de afzender dat deze ook daadwerkelijk de afzender is. Komt overeen met elektronische ondertekening uit eIDAS.
Waarmerken Elektronische identiteit bewijzen	Bron: ICTU Referentiearchitectuur ROG Een gegeven of een set van gegevens wordt hiermee voorzien van bewijs van de identiteit van de betrokkene. Komt overeen met elektronische identiteitsbewijs uit eIDAS.
Waarmerken Elektronisch verzegelen	Bron: ICTU Referentiearchitectuur ROG Een gegeven of set van gegevens wordt hiermee voorzien van een elektronisch waarborg dat de set overeenkomt met de inhoud van de bron/verklaring van de afzender nadat deze door de afzender verzonden is (integriteit van de inhoud en afzender). Komt overeen met elektronisch zegel uit eIDAS.
Wallet	Bron: NORA Een apparaat (ook wel Bron: NORA device), onlineservice of softwareprogramma dat vertrouwelijke gegevens kan bevatten, zoals persoonlijke attributen, identificatiegegevens, inloggegevens en bankpassen, en dat de bezitter in staat stelt digitale transacties uit te voeren, zoals aantonen van zijn identiteit, attributen verstrekken en betalingen te doen.
Websiteanalysetools	Websiteanalysetools zijn instrumenten die pensioenuitvoerders kunnen inzetten om het gedrag van bezoekers op hun portalen te meten, analyseren en rapporteren. Deze tools bieden waardevolle inzichten in hoe gebruikers interacteren met een portaal. Webanalysetools kunnen verschillende analyses uitvoeren om inzicht te bieden in het gedrag van gebruikers op een portaal. Dit betreft onder andere de volgende veelvoorkomende analyses:

Begrip	Omschrijving
	• Gebruikersgedrag: Inzicht in hoe gebruikers zich op de site bewegen. • Doelconversies: Het bijhouden van de voltooiing van specifieke doelen, zoals het invullen van formulieren of het downloaden van documenten. • Event tracking: Bijhouden van specifieke gebeurtenissen op de site, zoals het klikken op knoppen, het bekijken van video's of het downloaden van bestanden. Sommige webanalysetools bieden functies voor het vastleggen van het gedrag van specifieke gebruikers. Deze functies stellen een pensioenuitvoerder in staat om het gedrag van individuele bezoekers op de website te volgen. Hier zijn enkele manieren waarop webanalysetools het gedrag van specifieke gebruikers kunnen vastleggen: • **Gebruikers-ID-tracking:** Sommige tools bieden de mogelijkheid om unieke gebruikers te identificeren door ze een unieke gebruikers-ID toe te wijzen. Hierdoor kan de pensionuitvoerder het gedrag van die specifieke gebruiker over verschillende sessies volgen. • **Sessie-opnames:** Dit is een functie waarmee je letterlijk sessies van individuele gebruikers kunt opnemen. De pensioenuitvoerder ziet hoe gebruikers door de site navigeren, welke pagina's ze bezoeken en hoe ze met verschillende elementen op de pagina omgaan. • **Individuele gebruikerspaden:** Sommige tools bieden de mogelijkheid om de specifieke paden van individuele gebruikers door de website te volgen, waardoor je een gedetailleerd inzicht krijgt in hun interacties. • **Gebeurtenistracking:** Het bijhouden van specifieke gebeurtenissen of acties die een gebruiker onderneemt. Dit kan het klikken op knoppen, het bekijken van video's of andere interacties op de site omvatten.
XAdES	Bron: Gids ‘digitaal ondertekenen in de praktijk’, 2021 De technologische standaard voor de implementatie van XML-ondertekening op geavanceerde, elektronische wijze (zogenaamde ETSI-norm). Deze is in Nederland verplicht bij de toepassing in het (semi) overheidsdomein. Het tijdstempel is hierin een vereiste voor lange termijn validatie (LTV).
Zero Knowledge Proof	Een zero knowledge proof is een wiskundige manier om te bewijzen dat je kennis hebt van een zeker gegeven, zonder dat gegeven daadwerkelijk te laten zien. Dit gegeven kan dus ook een persoonlijk gegeven zijn. Dit draagt bij aan dataminimalisatie en voegt waarde toe vanuit privacy perspectief. Zero knowledge proofs worden gebruikt in Idemix, het protocol dat bijvoorbeeld gebruikt wordt in IRMA.

8.6.2 Afkortingen

Afkorting	Omschrijving
2FA	Twee Factor Authenticatie
AES	Een Advanced Electronic Signature: de toepassing van de geavanceerde elektronische handtekening onder eIDAS
AFM	Autoriteit Financiële Markten
AI	Artificiële intelligentie (AI) of kunstmatige intelligentie Dit kan gebruikt worden in het ondertekenproces om kenmerken van een foto, identiteitsbewijs en/of gezicht(punten) te verifiëren
AI	Artificial Intelligence
AP	Autoriteit Persoonsgegevens
ARF	Architectural Reference Framework
AT	Agentschap Telecom
AVG	Algemene Verordening Gegevensbescherming
BES	Basic Electronic Signature Ook wel Simple Electronic Signatures (eIDAS) genoemd
BRP	Basisregistratie Personen
BZK	Het ministerie van Binnenlandse Zaken
CA	Certification Authority
CRL	Een Certificate Revocation List (CRL) is een lijst met certificaat serienummers die herroepen zijn, niet meer geldig zijn en niet meer te vertrouwen zijn voor gebruikers
DBI	Digitale Bron Identiteit
DDTF	Dutch Digital Trust Framework
DES	Data Encryption Standard
DNB	De Nederlandse Bank
DSO	Digitale Standaardisatie & Ontwikkeling
EC	Europese Commissie
EDI	Europese Digitale Identiteit
eID	Elektronische identiteit
eIDAS	Electronic Identities And Trust Services
EIOPA	European Insurance and Occupational Pensions Authority (EIOPA)
ESSIF	European Self-sovereign Identity Framework
ETD	Elektronische toegangsdiensten
ETSI	European Telecommunications Standards Institute (ETSI)
EU	Europese Unie
EULA	End-user-license-agreement
FBS	Federatief Berichten Stelsel
GDI	Generieke Digitale Infrastructuur
GZD	Gezamenlijk Domein
HSM	Hardware Security Module
I&A	Identificatie & Authenticatie
IAK	Integraal Afwegingskader
ICTU	ICT Uitvoeringsorganisatie
iDIN	Identificeren Inloggen
IDP	Innovatie Digitale Pensioenuitvoering
IRMA	I Reveal My Attributes, een techniek waarmee een persoon alleen die persoonlijke gegevens hoeft te delen die op dat moment relevant zijn ter controle
LSP	Large Scale Pilot
LTW	Longterm Validation
MFA	Multi Factor Authenticatie
MIDO	Meerjarenprogramma Infrastructuur Digitale Overheid

Afkorting	Omschrijving
MKBA	Maatschappelijke Kosten Baten Analyse
MPO	MijnPensioenOverzicht
NFC	Near-field Communication is een contactloze communicatiemethode op korte afstand een NFC-chips uit te lezen. Een identiteitsbewijs kan zo'n chip bevatten die kan worden uitgelezen als verificatiestap
NORA	Nederlandse Overheid Referentie Architectuur
NVB	Nederlandse Vereniging van Banken
OBDO	Overheidsbreed Beleidsoverleg Digitale Overheid
OOP	Only Once Principe
PET	Privacy Enhancing Technologies
PGDI	Programmeringsraad GDI
PID	Personal Identification Data
PKI	Public Key Infrastructure
PT	Programmeringstafel
QCSD	Een Qualified Signature Creation Device ofwel gekwalificeerd ondertekenmiddel onder eIDAS, die benodigd is bij de totstandkoming van de gekwalificeerde ondertekening Een USB-token of smartcard kan hier een voorbeeld van zijn
QES	Een Qualified Electronic Signature: de toepassing van de gekwalificeerde elektronische handtekening onder eIDAS
QTSP	Een Qualified Trusted Service Provider is een gekwalificeerde dienstverlener die bijvoorbeeld certificaten mag verstrekken De dienstverlener opereert binnen de EU/staat op de EU trusted List en onder toezicht van Agentschap Telecom
RA	Registration Authority
RDI	Rijksinspectie Digitale Infrastructuur
RvIG	Rijksdienst voor Identiteitsgegevens
RVO	Rijksdienst voor ondernemend Nederland
SCA	Strong Customer Authentitication
SES	Een Simpel Electronic Signature: de toepassing van de eenvoudige / gewone elektronische handtekening onder eIDAS
SSI	Self Sovereign Identity De gebruiker kan met SSI zijn identiteit bewaren in een soort digitale portefeuille en bepalen welke gegevens gedeeld worden met dienstverleners
SWO	Softwareontwikkelaar
vID	Virtueel identiteitsbewijs
Wdo	Wet Digitale Overheid
WID	Wet op de Identificatieplicht
WRR	Wetenschappelijke Raad Regeringsbeleid