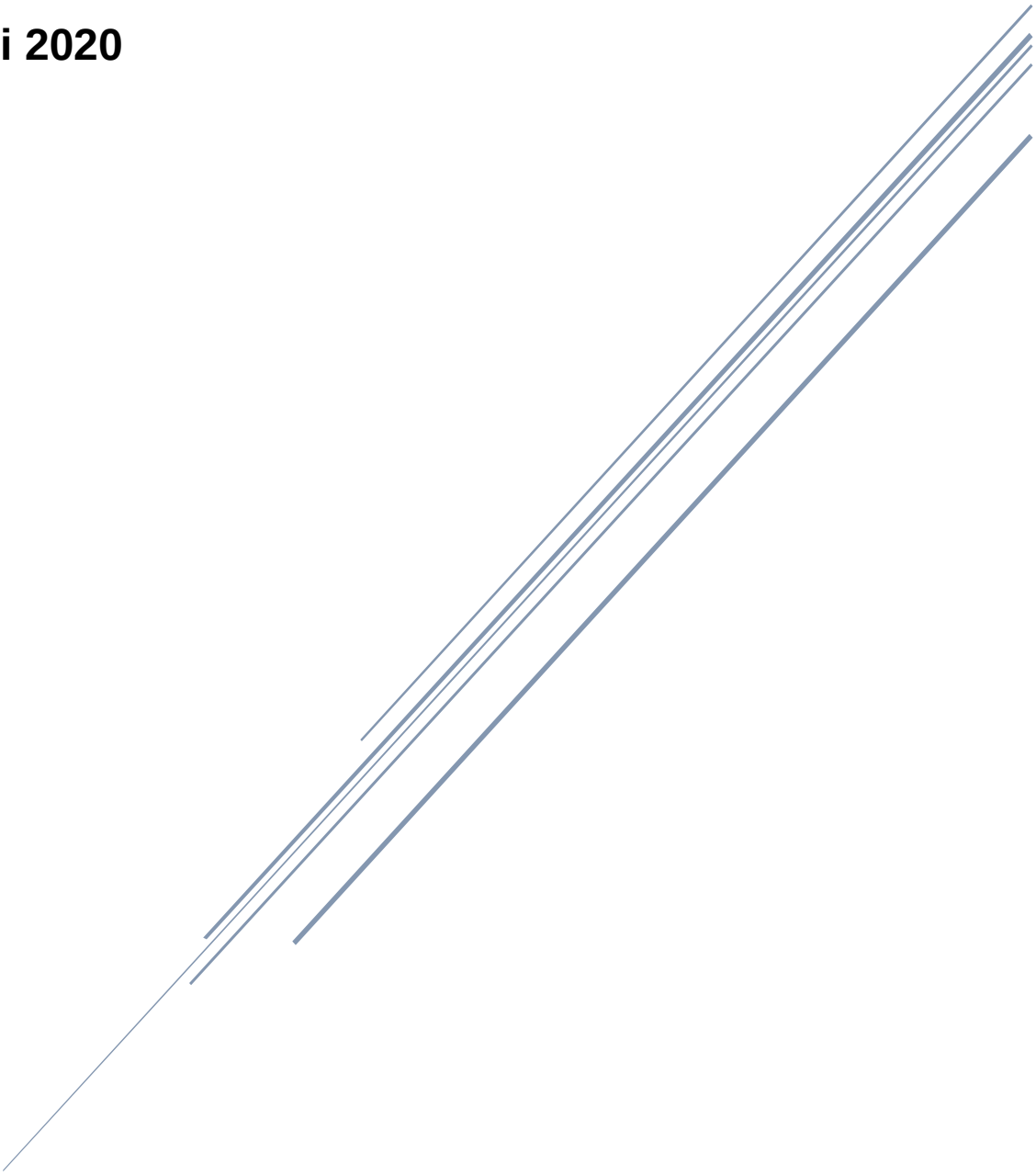
# Stappenplan migratie

# Digitaal Paspoort naar eHerkenning

# Handleiding voor online dienstverleners

**22 juni 2020**



# Inhoud

# 1 Context

## 1.1 Achtergrond migratie

Het Digitaal Paspoort is al meer dan twintig jaar de branchestandaard voor inloggen in de verzekeringsbranche. Automatische toegang tot extranetten van verzekeraars en serviceproviders en tot portalen van online dienstverleners als de Stichting CIS is de belangrijkste reden voor de brede spreiding van het gebruik van het Digitaal Paspoort. Het Digitaal Paspoort kent echter ook grote nadelen en is vanuit beveiligingsperspectief over de houdbaarheidsdatum. Het Digitaal Paspoort verdwijnt om deze reden. Dienstverleners en gebruikers in de verzekeringsbranche die het Digitaal Paspoort toepassen en gebruiken, hebben daarom tot en met december 2021 de tijd om over te stappen op eHerkenning. eHerkenning is dé standaard voor B2B authenticatie in heel Nederland, ook buiten de verzekeringssector. Zakelijk inloggen bij de overheid loopt verplicht via eHerkenning. In de verzekeringsbranche is eHerkenning niet verplicht, maar wordt het gebruik sterk aangeraden. Voor een financieel adviseur is het een voordeel om met een veilig middel overal in te kunnen loggen, of zelfs eenmalig in te loggen waarna automatisch toegang wordt verschaft tot meerdere applicaties van verschillende verzekeraars en serviceproviders.

## 1.2 Proposities voor migratieperiode

Tijdens de overgangsperiode kunnen zowel gebruikers (onder andere financiële adviseurs) als online dienstverleners (bijvoorbeeld verzekeraars) gebruik maken van methodes om de overgang te vereenvoudigen. Hiertoe is In juli 2019 een raamcontract getekend door Digidentity en SIVI.

Omdat tijdens de overgangsperiode nog niet alle verzekeraars en andere Relying Parties[1] direct overgaan op eHerkenning, is het van belang dat zij tot in ieder geval het einde van de overgangsperiode kunnen inloggen met hun Digitaal Paspoort. Bij Digidentity kan het Digitaal Paspoort vanaf **1 september 2020** alleen nog verlengd worden in combinatie met een eHerkenningsmiddel. Concreet betekent dit:

1. Gebruikers kunnen vanaf 1 september 2020 hun Digitaal Paspoort alleen nog verlengen als ze een eHerkenningsmiddel van Digidentity hebben.
2. Gebruikers hebben tussen 1 september 2020 en 1 januari 2022 het Digitaal Paspoort nodig, omdat nog niet alle Relying Parties direct eHerkenning accepteren.
3. Gebruikers kunnen vanaf 1 januari 2022 overal in de branche inloggen met een eHerkenningsmiddel. Het Digitaal Paspoort is dan uitgefaseerd, financiële adviseurs en andere gebruikers kunnen hun eHerkenningsmiddel dan bij elke willekeurige eHerkenningsleverancier aanschaffen en zijn niet langer gebonden aan Digidentity.

Voor toekomstige gebruikers van eHerkenning is een apart stappenplan bij SIVI beschikbaar.

## 1.3 Stappenplan

De migratie van Digitaal Paspoort naar eHerkenning brengt veel vragen met zich mee. Met eHerkenning stappen gebruikers over op een nieuwe systematiek van inloggen. Tweefactorauthenticatie wordt de norm, middelen worden veiliger en persoonlijk en het machtigen wordt op een andere manier ingeregeld. Zo is het Digitaal Paspoort feitelijk een werkplek-inlog: de dienstverlener wist daardoor niet wie er op zijn systeem inlogde. Via eHerkenning weet de dienstverlener straks wie er op het systeem inlogt. Voor dienstverleners is dit een verandering met de nodige impact. Waar moet je rekening mee houden? En waar moet je extra goed op letten? Om de meest voor de hand liggende vragen te beantwoorden en houvast te bieden bij de migratie heeft SIVI dit stappenplan opgesteld voor een succesvolle migratie van Digitaal Paspoort naar eHerkenning. Vragen en/of opmerkingen met betrekking tot de migratie in het algemeen of dit stappenplan in het bijzonder, kunnen gesteld worden aan support@sivi.org.

[1] Een Relying Party is een aanbieder van online dienstverlening, die authenticatie laat plaatsvinden (afneemt) via een netwerk voor authenticatie. In dit document worden met Relying Parties de verzekeraars, service providers en andere portaalaanbieders (zoals Stichting CIS) bedoeld.

### 1.4 Meer informatie

SIVI heeft een landingspagina voor de migratie. Hier treft u een FAQ en actuele informatie.
https://www.sivi.org/eherkenning/

Voorts kunt u zich abonneren op de SIVI Nieuwsbrief voor de laatste updates en stand van zaken:
https://www.sivi.org/tag/nieuws/

## 2 Voer een impactanalyse uit

Een impactanalyse helpt om inzicht te krijgen in de gevolgen van de migratie van het Digitaal Paspoort naar eHerkenning (en wat nodig is om de migratie te verwezenlijken) en inzicht in de gevolgen (voor wie en wat) van de veranderingen.

### 2.1 Welke diensten worden toegankelijk via eHerkenning?

Een impactanalyse helpt om inzicht te krijgen in de gevolgen van de migratie van het Digitaal Paspoort naar eHerkenning (en wat nodig is om de migratie te verwezenlijken) en inzicht in de gevolgen (voor wie en wat) van de veranderingen.

### 2.2 Welke diensten worden toegankelijk via eHerkenning?

De dienstverlener bepaalt zelf welke diensten via eHerkenning worden ontsloten en op welke wijze deze diensten gepubliceerd worden in de dienstencatalogus van eHerkenning. De dienstencatalogus van eHerkenning bevat de volgende elementen:

- Naam en omschrijving van de dienst (herkenbaar en betekenisvol voor de gebruiker). Hieruit moet de eindgebruiker – of diegene die de machtigingen beheert – kunnen afleiden wat "de dienst" inhoudt.
- Het vereiste betrouwbaarheidsniveau voor afname van de dienst.
- Of de dienst met Single Sign On (SSO)[2] kan worden afgenomen.
- Welk dienstafnemers krijgen toegang tot de dienst.

In de dienstencatalogus van eHerkenning staan alle diensten van alle aangesloten dienstverleners binnen het afsprakenstelsel Elektronische Toegangsdiensten (ETD)[3]. Logius beheert deze dienstencatalogus. Het vullen van de dienstencatalogus loopt via de Herkenningsmakelaars, waarmee dienstverleners een contract sluiten om aan te kunnen sluiten op eHerkenning.

Met behulp van de dienstencatalogus zijn de dienstverleners in staat te bepalen om één dienst – of een beperkt aantal diensten – in de dienstencatalogus te op te nemen, en in eigen huis de autorisaties voor de onderliggende diensten te regelen.

### 2.3 Op welk betrouwbaarheidsniveau zijn de diensten beschikbaar?

eHerkenning kent vijf betrouwbaarheidsniveaus (1, 2, 2+, 3 en 4). De dienstverlener bepaalt het betrouwbaarheidsniveau waarmee de gebruiker inlogt. Hoe hoger het niveau, hoe meer zekerheid de dienstverlener krijgt over de online identiteit van de gebruikers.

- https://www.eherkenning.nl/aansluiten-op-eherkenning/betrouwbaarheidsniveaus/bepalen-van-juiste-niveau

[2] Als de laatste authenticatie langer dan twee uur geleden is, dan vindt opnieuw authenticatie bij eHerkenning plaats. De maximale sessieduur kan door de dienstverlener zelf worden ingekort: een dienstverlener kan er ook voor kiezen om SSO niet te ondersteunen en áltijd om herauthenticatie te vragen.

[3] eHerkenning valt onder het Afsprakenstelsel Elektronische Toegangsdiensten.

In de verzekeringsbranche wordt eHerkenning ingesteld op niveau drie (3), dit is gelijk aan het niveau voor authenticatie bij het UWV en de Belastingdienst. Omdat dit niveau vanuit compliance-perspectief acceptabel is voor verreweg de meeste transacties, is in overleg met stakeholders ook voor dit niveau gekozen in de verzekeringsbranche. Voor bepaalde diensten – rond medische gegevens – wordt een hoger niveau vereist.

Onderstaande tabel geeft een toelichting op de diverse aspecten van betrouwbaarheidsniveau drie.

| Aspect | Toelichting |
|---|---|
| Inlogmethode via eHerkenning niveau 3 | U logt in met een gebruikersnaam en wachtwoord, aangevuld met een tweede factor (sms-code, token, pincode, etc.). |
| Aanvraagprocedure | Bij de meeste erkende leveranciers vindt de aanvraag volledig online plaats. Het kan voorkomen dat het middel deels online en deels offline (per post) moet worden aangevraagd. Het ondertekende aanvraagformulier + benodigde documenten dient de aanvrager per post op te sturen. |
| Controlebevoegdheid tijdens aanvraagproces | De relatie tussen de aanvrager en het bedrijf wordt gecontroleerd aan de hand van de Kamer van Koophandel-registratie. Persoonsgegevens worden gecontroleerd door op locatie het originele identiteitsbewijs te tonen. Bij sommige eHerkenningsleveranciers gebeurt dit inmiddels ook volledig online. |
| Uitgifte van het middel | Het uitgeven aan gebruikers gebeurt op basis van een betrouwbaar brondocument. De middelen worden online of offline verstuurd, bijvoorbeeld per aangetekende post. |
| Verschil met niveau 2 | Extra ingebouwde veiligheidsmaatregelen in de controle van bevoegdheden (check persoonsgegevens via origineel identiteitsbewijs) en uitgifte online of d.m.v. aangetekende post. |
| Te gebruiken bij onder andere | Alle diensten waar eHerkenning niveau 1, 2, 2+ of 3 wordt gevraagd. Zoals UWV en Belastingdienst. |

Voor betrouwbaarheidsniveau drie bestaan momenteel verschillende inlogmethodes. De meest voorkomende methode is een combinatie van een speciale authenticatie-app op de smartphone en het scannen van een QR-code op de site van de Relying Party. Ook veel gebruikt is de combinatie van gebruikersnaam en wachtwoord en een tweede factor in de vorm van een token of sms-code.

### 2.4 Hoe implementeer ik aansluiting op achterliggende processen?

Uiteraard doet zich ook de vraag voor hoe de backoffice en achterliggende processen ingericht worden en aansluiten op de onlinediensten die via eHerkenning ontsloten worden. De gekozen eHerkenningsmakelaar kan hierbij helpen.

### 2.5 Biedt mijn bedrijf naast eHerkenning ook alternatieve inlogmethoden?

Veel online dienstaanbieders laten gebruikers kiezen: of inloggen met eHerkenning, of inloggen met gebruikersnaam/wachtwoord. De laatste optie is vanuit compliance-perspectief niet de beste route en onhandig voor gebruikers die bij veel dienstverleners inloggen.

Hier geldt:

- Over alternatieve inlogmethoden zijn geen afspraken gemaakt.
- Het is aan de dienstverlener welke inlogmethoden toegepast worden.
- Gebruikersnaam/wachtwoord lijkt niet voldoende; minimaal is Multi-Factor Authenticatie (MFA) vereist. Het is aan de dienstverlener om eventueel naast eHerkenning ook een alternatieve MFA in te richten. Als alle intermediairs en andere gebruikers eHerkenning omarmen, dan is hier geen noodzaak voor.

Naarmate de adoptie van eHerkenning toeneemt, zullen partijen vaker overwegen om alleen eHerkenning aan te bieden.

## 2.6 Welke makelaar gaat mijn diensten aansluiten op eHerkenning?

Om aan te sluiten op eHerkenning dient een dienstverlener zich aan te sluiten op een koppelvlak van het netwerk via een eHerkenningsmakelaar.
De eHerkenningsmakelaars zijn:

- Digidentity (www.digidentity.eu/nl/home/#eHerkenning)
- iWelcome (www.iWelcome.com)
- KPN (www.eHerkenning.KPN.com)
- Reconi (voorheen CreAim) (https://www.reconi.nl/eherkenning/)
- We-ID (voorheen Connectis) (https://we-id.nl/eherkenning/)

Deze marktpartijen voldoen allemaal aan dezelfde eisen en zijn erkend door de overheid. Ze verschillen onder andere in kwaliteit van dienstverlening/service en prijs.

De eHerkenningsmakelaar kan een implementatiemanager leveren, eventueel ondersteunt door development-specialisten. Nieuw ontwikkelde koppelvlakken zijn doorontwikkelingen van het bestaande koppelvlak voor eHerkenning dat al in gebruik is. Als een bedrijf al een aansluiting op eHerkenning heeft, dan is het advies om in gesprek te gaan met de gekozen eHerkenningsmakelaar. Bespreek het gewenste technische en economisch haalbare scenario om een keuze te kunnen maken voor een koppelvlak dat het beste bij de desbetreffende situatie past.

Dienstverleners hebben tijdens de transitiefase twee opties om aan te sluiten op eHerkenning:

1. Digidentity Broker:
    - Met aansluiting op de Digidentity Broker wordt de dienstverlener tegelijk aangesloten op eHerkenning én het Digitaal Paspoort.
    - Dienstverleners herkennen een eHerkenninggebruiker aan het e-mailadres dat ook in het Digitaal Paspoort werd/wordt gebruikt, en anders zorgt Digidentity voor de koppeling.
    - De Digidentity Identity Broker geeft de mogelijkheid verschillende oplossingen te ondersteunen op het gebied van authenticatie. Met andere woorden, Relying Parties kunnen hiermee verschillende inlogmethodes combineren, zoals eHerkenning en het X509-certificaat (Digitaal Passport). Er vindt een vertaalslag plaats naar het achterliggende landschap van de Relying Party. Dit betekent dat je met diverse protocollen de gewenste attributen kan ontvangen. Denk hierbij aan oAuth, SAML en OpenID Connect (OIDC). Daarnaast krijgt de achterliggende applicatie de juiste set attributen mee. In veel gevallen is dit een combinatie tussen attributen van het certificaat, eHerkenning en eventuele klantsystemen. Ook machtigingsstructuren die zijn ingeregeld voor applicaties bij de Relying Party kan de Digidentity Identity Broker opnemen. Na de migratieperiode en uitfasering van het Digitaal Paspoort staat het de Relying Party natuurlijk vrij om te beslissen of ze de diensten voor eHerkenning laat doordraaien op de huidige makelaar, of een nieuwe uitvraag doet in de markt.
    - Voor wat betreft de Digidentity Broker heeft SIVI medio 2019 een raamcontract met Digidentity gesloten. Dit raamcontract is via SIVI opvraagbaar. Het raamcontract zorgt voor een faire prijs en zekerheid over de geleverde dienstverlening gedurende de transiatie (én DP én eHerkenning).
2. Losse aansluiting op eHerkenning:
    - De dienstverlener sluit regulier aan op eHerkenning bij een van de beschikbare makelaars (waaronder Digidentity). Koppelingen tussen gebruikers van DP en eHerkenning maakt de dienstverlener zelf.
    - De dienstverlener moet faciliteren dat – tijdens de transitiefase – gebruikers met het Digitaal Paspoort kunnen inloggen.

## 2.7 Welke randvoorwaarden zijn nodig?

Voor het aansluiten op eHerkenning zijn organisatorische en technische randvoorwaarden nodig:

- Een ontwikkelaar met voldoende kennis om een SAML-verbinding tot stand te brengen.
- Een beheerder die na implementatie diverse acties kan uitvoeren.
- Een applicatie en/of connector die SAML-berichten kan versturen en ontvangen volgens de eHerkennings-specificaties. De applicatie kan van de dienstverlener zelf zijn (als zij applicaties

ontwikkelt), maar is vaak van een leverancier. Een eHerkenningsmakelaar of een derde partij kan een connector leveren.
- Een testomgeving én een productieomgeving. Een testomgeving is door het afsprakenstelsel - waarvan eHerkenning deel uit maakt - niet verplicht voor dienstverleners. Afhankelijk van het aansluitproces bij de makelaar kan dit wel verplicht zijn. Een mogelijk scenario is dat de eHerkenningsmakelaar de gebruiker aansluit op een preproductie/acceptatie/test-omgeving, die zoveel mogelijk lijkt op de productieomgeving. Testen kan dan plaatsvinden tijdens het aansluitproces met niet-productie testmiddelen die de Herkenningsmakelaar beschikbaar stelt.
- De ontwikkelde doelarchitectuur voor aansluiting op de eHerkenning infrastructuur is in beginsel gebaseerd op koppelvlak versie 1.13. Houd de website van Logius in de gaten om te kijken wanneer welke versie in productie komt of vraag uw Herkenningsmakelaar u op de hoogte te houden.

## 2.8 Met welke kosten voor de makelaar moet ik rekening houden?

Aan de aansluiting zijn kosten verbonden: eenmalige aansluitkosten die variëren per organisatie, afhangen van de bestaande infrastructuur en het kennisniveau van de medewerkers. Daarnaast rekent de makelaar maandelijkse kosten plus variabele kosten afhankelijk van het gebruik.
Vermoedelijk liggen de kosten per aansluiting in de volgende orde van grootte:

| Soorten kosten | Indicatie kosten |
|---|---|
| Eenmalige aansluitkosten | € 600 - € 2500<br>Verschillende typen aansluitingen mogelijk afhankelijk van de kennis in de interne organisatie, en de noodzaak tot aanschaf van PKI Overheid-certificaten voor het ondertekenen van documenten. Daarnaast optioneel extra support op urenbasis voor de implementatie indien uw organisatie niet over de benodigde expertise beschikt. |
| Structurele maandelijkse kosten | € 0 - € 500 per maand |
| Variabele kosten | Staffelkosten tot 50.000 transacties: €250 per maand.<br>Tussen 50.000 en 125.000 transacties: €475 per maand<br>Tussen 125.000 en 250.000 transacties: €680 per maand<br>Tussen 250.000 en 500.000 transacties: €860 per maand<br>Tussen 500.000 en miljoen transacties: €1025 per maand |

## 2.9 Waar moet ik bij de keuze voor een makelaar op letten?

Vanuit SIVI wordt geen voorkeur uitgesproken voor een makelaar. SIVI raadt aan om zelf de verschillende makelaars te benaderen en een keuze te maken. De volgende keuzecriteria kunnen als voorbeeld dienen:
- Kosten;
- Ondersteuning: aansluiting op backoffice, implementatie koppelvlak, hulp met ontsleutelsoftware Logius;
- Mogelijkheden rondom aansluiting op koppelvlak eIDAS[4] (relevant voor pensioenverzekeraars);
- Ondersteuning van ketenmachtigingen;
- Expertise;

[4] eHerkenning verbindt publieke en private dienstverleners met het Europese eIDAS-stelsel. Europese inwoners kunnen worden geïdentificeerd met een zeker betrouwbaarheidsniveau.

- Omvang, stabiliteit en toekomstvastheid van de eigen organisatie;
- Service-afspraken over performance, downtime, enzovoort;
- ICT-beveiligingsaspecten;
- Testomgevingen, beheerste procedures om wijzigingen in systemen door te voeren;
- Eventuele ondersteuning van oudere versies van het koppelvlak bij een nieuwe release;
- Soort makelaar: commercieel of stichting.

## 2.10 Hoe herken ik de gebruiker?

De makelaar kan op basis van een inlog diverse attributen leveren aan de dienstverlener. Elk attribuut moet verantwoord worden. Er is onderscheid naar attributen van natuurlijke personen (bijvoorbeeld BSN-nummer, NAW-gegevens en/of geboortedatum) en niet-natuurlijke personen (bijv. bedrijfsnaam, KvK en/of RSIN). Hiermee kan de dienstverlener de koppeling leggen naar personen of bedrijven in de eigen administratie.

Gevalideerde attributen die standaard beschikbaar zijn:
- KvK-nummer
- vestigingsnummer

Beschikbaar met toestemming van de gebruiker zijn:
- e-mail
- naam
- geboortedatum
- BSN (mits toegestaan om te verwerken)
- adresgegevens (niet gevalideerd)

Aan elke combinatie van gebruiker en dienstverlener wordt een uniek pseudoniem gekoppeld.

Dit pseudoniem is per dienstverlener anders en kan niet tussen dienstverleners gematched worden.

Zie voor meer informatie: http://afsprakenstelsel.etoegang.nl/display/as/attribuutcatalogus.

Wanneer zowel eHerkenning als het Digitaal Paspoort bij Digidentity aangeschaft worden, is het pseudoniem op beide middelen gelijk. Dit geldt natuurlijk niet als het eHerkenningsmiddel bij een andere provider wordt aangeschaft.

**Let op:**
- Het is voor gebruikers die een eHerkenningsmiddel bij Digidentity aanschaffen niet verplicht om ook een Digitaal Paspoort aan te schaffen.
- Gebruikers kunnen ook bij een andere partij een eHerkenningsmiddel aanschaffen.
- Een Digitaal Paspoort kan uitsluitend nog vanuit het Digidentity profiel aangevraagd worden. Hetzelfde geldt voor bedrijfscertificaten.
- Voor Aplaza koppelingen blijven certificaten de authenticatiemethode om transacties, documenten en berichten op te halen. Aplaza gaat hiervoor de bedrijfscertificaten stimuleren (maar vooralsnog niet verplichten).

## 2.11 Hoe worden de gebruikers gemachtigd?

Voor het inloggen met eHerkenning krijgt een specifieke gebruiker binnen een organisatie de juiste machtiging om van een beschikbare dienst gebruik te maken. Veel Nederlandse bedrijven hebben al medewerkers die eHerkenning als inlogmiddel gebruiken, bijvoorbeeld om zaken te doen met de Belastingdienst, het UWV, DNB of andere instanties. Voor veel organisaties is eHerkenning dus niet nieuw; het is één inlogmiddel dat ze bij meerdere dienstverleners gebruiken om in te loggen.

### 2.11.1 Machtigingen

Iemand die met eHerkenning een online dienst wil afnemen, moet daarvoor gemachtigd zijn: zonder machtiging werkt een eHerkenningsmiddel niet. Een machtiging wordt aangevraagd en is persoonsgebonden, het is een eHerkenningsmiddel. Een machtiging wordt alleen verstrekt door iemand met tekenbevoegd volgens het Handelsregister van de Kamer van Koophandel. Deze tekenbevoegde kan ervoor kiezen om een machtigingenbeheerder aan te stellen die deze rol overneemt en machtigingen kan verstrekken.

In het machtigingenregister wordt de koppeling gelegd tussen het authenticatiemiddel van de gemachtigde en diens bevoegdheid. Op basis van deze gegevens kan het netwerk met een bepaald betrouwbaarheidsniveau verklaren dat iemand met een bepaald authenticatiemiddel namens een bepaald bedrijf mag handelen voor de afname van een bepaalde dienst. De procedure voor het vastleggen van bevoegdheden varieert naar gelang het betrouwbaarheidsniveau. Hoe hoger het niveau, des te meer bewijzen iemand moet overleggen.

Per bedrijf is het verstandig minstens één ‘administrator’ eHerkenning aan te stellen. Dit hoeft niet dezelfde persoon te zijn als de tekenbevoegde KvK, maar deze persoon moet wel diens officiële toestemming hebben.

Deze bedrijfsbeheerder kan per eHerkennings-gebruiker binnen zelfde organisatie:

- Middelen (de)activeren;
- Instellen welke diensten de gebruiker mag afnemen (machtigingen).

In het Self Service Portaal van Digidentity ziet de bedrijfsbeheerder (machtigingenbeheerder) wie er van het bedrijf een eHerkenningsmiddel en Digitaal Paspoort heeft. Hierdoor hebben de beheerders een overzicht van alle machtigingen die een persoon heeft en op welk niveau. Bij het inloggen met eHerkenning krijgt de gebruiker een lijst te zien van de bedrijven waarvoor hij/zij een machtiging heeft. De gebruiker dient een van deze machtigingen te selecteren. De machtiging voor het gekozen bedrijf wordt dan gebruikt en verstuurd naar de dienstverlener na inloggen. Als een ‘beheerder’ niet als zodanig in het KvK staat opgenomen (bij het aanvragen van een eHerkenningsmiddel bij Digidentity), dan hoeft de KvK de inschrijving niet aan te passen. Digidentity voegt dan handmatig die persoon toe met de rol beheerder.

Bij werkgevers, adviseurs/bemiddelaars zijn dus machtigingen ingeregeld. Aan de kant van de dienstverlener is veelal ook sprake van een inregeling van rechten. Mogelijk kunnen deze rechten door een super-user aan de kant van de gebruiker geconfigureerd worden. Het is van belang dit te ontkoppelen van eHerkenning, omdat ook sprake zal zijn van alternatieve inlogmethoden. Wel is het belangrijk om een gebruiker die inlogt met eHerkenning te herkennen zodat de juiste rechten aan deze persoon gekoppeld worden.

### 2.11.2 Ketenmachtigingen

De ketenmachtiging vormt een alternatief voor de individuele machtiging. Met een ketenmachtiging kunnen organisaties andere organisaties machtigen om namens hen een online dienst af te nemen met eHerkenning. Ketenmachtigingen zijn vooral handig voor bedrijven die via een tussenpartij (een extern bureau of intermediair) gebruik willen maken van bepaalde diensten die met eHerkenning toegankelijk zijn. De medewerker of machtigenbeheerder van het bedrijf heeft dan niet per se zelf een eHerkenningsmiddel nodig. Het voordeel voor de tussenpartij is dat deze met één eHerkenningsmiddel namens meerdere bedrijven kan inloggen bij diensten waarvoor hij of zij is gemachtigd. Deze tussenpartij hoeft dan geen apart eHerkenningsmiddel aan te vragen voor elke partij die hij of zij vertegenwoordigt. De machtiging aan de tussenpartij moet schriftelijk of digitaal vastgelegd worden bij een erkende leverancier die ketenmachtigingen levert. Inmiddels leveren alle eHerkenningsleveranciers ketenmachtigingen.

## 3 Implementeer eHerkenning en test nieuwe Digitaal Paspoort

In het verlengde van de impactanalyse wordt eHerkenning geïmplementeerd. Een deel van de gebruikers beschikt tijdens de migratieperiode over een Digidentity, het combimiddel van eHerkenning en Digitaal Paspoort. Het is belangrijk dat tijdig getest wordt met dit middel. Het Digitaal Paspoort verschilt in het combimiddel van inhoud. Het belangrijkste is dat de Digitaal Paspoorten die vanaf 1 september 2020 uitgegeven gaan worden een andere root/certificate chain hebben.
Dit is aangegeven in onderstaande tabel.

| **Attribuut** | **Invulling** | | |
|---|---|---|---|
| | **vóór sept-19** | **vanaf sept-19** | **nieuwe DP vanaf september-20** |
| e-mail gebruiker | E-mailadres van de gebruiker. Dient een persoonlijk e-mailadres te zijn. | E-mailadres van de gebruiker. Dient een persoonlijk e-mailadres te zijn. | E-mailadres van de gebruiker. Dient een persoonlijk e-mailadres te zijn. |
| naam gebruiker | Volledige naam van de gebruiker. | Volledige naam van de gebruiker. | Volledige naam van de gebruiker. |
| pseudoniem gebruiker | - | Uniek getal om de gebruiker te identificeren. | Uniek getal om de gebruiker te identificeren. |
| achternaam gebruiker | - | - | Achternaam gebruiker zoals geregistreerd op identiteitsbewijs. |
| voornamen gebruiker | - | - | Voornamen gebruiker zoals geregistreerd op identiteitsbewijs. |
| naam organisatie | Naam van organisatie zoals geregistreerd in handelsregister. | Naam van organisatie zoals geregistreerd in handelsregister. | Naam van organisatie zoals geregistreerd in handelsregister. |
| id organisatie | - | Identificerend nummer van organisatie zoals geregistreerd in handelsregister (bijv. KvK-nummer). | Identificerend nummer van organisatie zoals geregistreerd in handelsregister (bijv. KvK-nummer). |
| land organisatie | - | Twee-letterige landcode van de locatie van de organisatie. | Twee-letterige landcode van de locatie van de organisatie. |
| uitgevende partij | Uitgevende partij van het certificaat (bijv. Solera Nederland). | - | - |
| land van uitgifte | Land van uitgifte van het certificaat. | - | - |

## 4 Communiceer met de gebruikers

Eenmaal aangesloten op eHerkenning is het belangrijk dat de gebruikers tijdig worden voorbereid op het gebruik van eHerkenning. Maar ook intern is het nodige te communiceren; bijvoorbeeld naar medewerkers bij de klantenservice of naar medewerkers die betrokken zijn bij de desbetreffende dienst.

Dienstverleners hoeven geen klantenservice in te richten voor vragen over het aanvragen en gebruiken van eHerkenning; de erkende middelenleveranciers zijn hiervoor verantwoordelijk. De klantenservice va neen dienstverlener kan deze gebruikers doorverwijzen naar de leverancier waar de betreffende gebruiker zijn/haar eHerkenningsmiddel heeft aangevraagd.

Voor de hand liggende teksten op uw website:

- Heeft u al een eHerkenningsmiddel, maar nog niet op het juiste betrouwbaarheidsniveau? Neem contact op met uw leverancier om uw inlogmiddel te upgraden naar een hoger niveau en om uw machtiging te regelen.
- U heeft nog geen eHerkenning inlogmiddel. U kunt alleen een inlogmiddel aanvragen als u of uw organisatie staat ingeschreven bij de Kamer van Koophandel. Om in te kunnen loggen op deze dienst heeft u een eHerkenningsmiddel op (minstens) niveau 3 nodig.

  U kunt uw eHerkenningsmiddel alleen aanvragen bij een erkende eHerkenningsleverancier. U bent vrij om zelf een leverancier te kiezen. Alle leveranciers voldoen aan de strenge eisen vanuit de overheid. Leveranciers bieden verschillende typen inlogmiddel, prijzen en aanvraagprocedures.

  Gebruik het stappenplan op www.sivi.org. Dit stappenplan leidt u door de belangrijkste aspecten in het aanvraagproces.
- Ervaart u problemen met de aanvraag of het gebruik van eHerkenning? Neem dan contact op met de leverancier van uw eHerkenningsmiddel. Deze leverancier is in het bezit van uw gegevens en kan u eenvoudig verder helpen. Contactgegevens van de verschillende leveranciers staan op www.eHerkenning.nl/contact.