

# eHerkenning @ Digidentity

Hoe werkt eHerkenning?

<b>Titel</b>	eHerkenning @ Digidentity - Hoe werkt eHerkenning?
<b>Datum</b>	5 juli 2023
<b>Auteur</b>	Sander Remmerswaal
<b>Versie</b>	2023-v2
<b>Locatie</b>	<a href="https://www.digidentity.eu/en/documentation/">https://www.digidentity.eu/en/documentation/</a>
<b>Classificatie</b>	Openbaar

## Contents

<b>eHerkenning.....</b>	<b>3</b>
eHerkenningstelsel.....	3
eHerkenningmiddel (identificatie).....	4
Betrouwbaarheidsniveaus.....	4
Machtiging .....	5
Identificatie.....	8
Handelsregister.....	9
Protocollaire Basisadministratie (PROBAS).....	9
Gebruik in Europa.....	9
<b>Rollen in eHerkenning.....</b>	<b>10</b>
Dienstafnemer (gebruiker).....	10
Middelenuitgever (MU).....	10
Dienstverlener (DV).....	10
Authenticatiedienst (AD).....	11
Herkenningmakelaar (HM).....	11
Machtigingenregister (MR).....	11
Hoe werkt inloggen met eHerkenning? .....	12
<b>Bijlage – Regels eHerkenningsovereenkomst.....</b>	<b>13</b>

## eHerkenning

De volgende paragrafen beschrijven wat eHerkenning is, welke betrouwbaarheidsniveaus beschikbaar zijn en wat machtigingen zijn.

## eHerkenningstelsel

Het Afsprakenstelsel Elektronische Toegangsdiensten (eTD), bekend als eHerkenning, is een publiek-private samenwerking om bedrijven toegang te geven tot digitale dienstverlening van de overheid.

De basis van het Afsprakenstelsel is een samenwerking tussen overheidsorganisaties en commerciële bedrijven om toegangsdiensten te leveren. In deze samenwerking zijn verschillende rollen te onderscheiden voor het uitgeven van authenticatiemiddelen of het controleren van machtigingen.

Overheidsorganisaties sluiten aan op eHerkenning en ondernemers kopen een eHerkenningmiddel om in te kunnen loggen. Erkende bedrijven (makelaars) implementeren eHerkenning in uw organisatie en erkende eHerkenning leveranciers geven eHerkenning inlogmiddelen uit om in te kunnen loggen bij overheidsorganisaties en verzekeringsmaatschappijen.

Het Afsprakenstelsel beschrijft de eisen voor verschillende onderwerpen:

- \* rollen in het stelsel
- \* relaties tussen de rollen
- \* technische relaties
- \* infrastructuur
- \* identificatie van personen en organisaties
- \* uitgeven van machtigingen
- \* beveiliging van data

eHerkenning is de Nederlandse oplossing om te voldoen aan de eIDAS-verordening<sup>1</sup>. Daarmee worden de diensten van de aangesloten (publieke) Dienstverleners via het stelsel ontsloten voor gebruikers uit andere eIDAS-lidstaten.

Op dit moment zijn ruim 500 Dienstverleners aangesloten op eHerkenning en Digidentity en vijf andere leveranciers zijn erkend door het ministerie van Binnenlandse Zaken. Alleen erkende organisaties mogen eHerkenning leveren. De erkende organisaties als Digidentity voldoen aan dezelfde strenge eisen en staan onder toezicht van de overheid. Beveiliging en functionele kwaliteit is daarmee gegarandeerd.

eHerkenning is een persoonsgebonden inlogmiddel. Daarom moet u bij de aanvraag persoonsgegevens verstrekken aan uw erkende leverancier om uw identiteit vast te stellen.

---

<sup>1</sup> eIDAS verordening - <https://digital-strategy.ec.europa.eu/nl/policies/eidas-regulation>

Aantal eisen waaraan de leveranciers moeten voldoen zijn:

- \* Algemene Verordening Gegevensbescherming (AVG), onder toezicht van de Autoriteit Persoonsgegevens.
- \* ISO27001 certificering, de internationale standaard voor informatiebeveiliging, waar aantoonbaar moet zijn dat de leverancier voldoet aan wet- en regelgeving.
- \* Europese eIDAS-eisen (EU Verordening 910/2014).

eHerkenning is in het Engels vertaald als Dutch Trust Framework. De vertaling 'eRecognition' is onjuist.

Alle eisen uit het Afsprakenstelsel staan op internet: <https://afsprakenstelsel.etoegang.nl>.

## eHerkenningsmiddel (identificatie)

Het eHerkenningsmiddel is de identiteit waarmee de gebruiker bij de Dienstverlener inlogt. Het eHerkenningsmiddel kan een gebruikersnaam, wachtwoord en tweede factor (eenmalige code) zijn.

De gebruiker ontvangt het eHerkenningsmiddel van de Middelenuitgever die daarvoor de identiteit van de gebruiker vaststelt en de identiteit van de organisatie waarvoor de gebruiker de machtiging aanvraagt.

## Betrouwbaarheidsniveaus

Het betrouwbaarheidsniveau (Level of Assurance) van het eHerkenningsmiddel geeft de zekerheid van de identiteit aan. Hoe hoger het betrouwbaarheidsniveau, hoe strenger en nauwkeuriger de identificatie van de aanvrager is.

eHerkenning kent vier betrouwbaarheidsniveaus;

- \* eHerkenning niveau 2
- \* eHerkenning niveau 2+
- \* eHerkenning niveau 3
- \* eHerkenning niveau 4



Digidentity biedt betrouwbaarheidsniveaus eH2+, eH3 en eH4.

Per 1 juli 2021 is eHerkenning niveau 1 vervallen en niet meer beschikbaar.

## eHerkenning niveau 2 (eH2)

eHerkenning niveau 2 (eIDAS Laag) is te gebruiken voor overheidsdiensten waar een lage zekerheid van identiteit nodig is. eH2 eist een beperkte identificatie op basis van wettelijk identiteitsbewijs en controle in Handelregister. Inloggen op basis van gebruikersnaam en wachtwoord.

Digidentity biedt geen eH2 aan omdat de beveiliging op basis van gebruikersnaam en wachtwoord voor ons onvoldoende is.

## eHerkenning niveau 2+ (eH2+)

eHerkenning niveau 2+ (eIDAS Laag) is te gebruiken voor overheidsdiensten waar een lage zekerheid van identiteit nodig is. eH2+ eist een beperkte identificatie op basis van een wettelijk identiteitsbewijs en controle in Handelregister. Inloggen op basis van gebruikersnaam, wachtwoord en een tweede factor als pincode. Bijvoorbeeld: Aanvragen van een Verklaring omtrent Gedrag (VOG) kan met een eH2+ middel.



## eHerkenning niveau 3 (eH3)

eHerkenning niveau 3 (eIDAS Substantieel) is voor overheidsdiensten waar een substantiële zekerheid van identiteit nodig is. eH3 eist een identificatie op basis van een origineel wettelijk identiteitsbewijs, vergelijking van de aanvrager met het ID (fysieke controle of op afstand) en controle in Handelregister. Identiteitscontrole geldt ook voor de wettelijk vertegenwoordiger(s).



Inloggen met een gebruikersnaam en een tweede factor zoals een smart card met een pincode. Bijvoorbeeld: eH3 is nodig om belastingaangifte bij de Belastingdienst te doen.

eHerkenning niveau 3 zal het basisniveau worden.

## eHerkenning niveau 4 (eH4)

eHerkenning niveau 4 (eIDAS Hoog) is voor overheidsdiensten waar een hoge zekerheid van identiteit nodig is. eH4 eist een identificatie op basis van een origineel wettelijk identiteitsbewijs, vergelijking van de aanvrager met het ID (fysieke controle of op afstand) en controle in Handelregister. Identiteitscontrole geldt ook voor de wettelijk vertegenwoordiger(s).



Inloggen met een gebruikersnaam en een tweede factor zoals smart card met digitaal certificaat en een pincode. Bijvoorbeeld: eH4 is nodig om een verzoek tot gratie in te dienen bij Justis.

## Machtiging

Een gebruiker van eHerkenning moet een machtiging van een organisatie hebben om namens deze organisatie te handelen. Zonder machtiging werkt eHerkenning niet.

Een machtiging legt een driehoeksrelatie vast:

- [1] wie mag namens welke
- [2] organisatie gebruik maken van welke
- [3] diensten.

Als het eHerkenningmiddel een sleutel is, is de machtiging het slot waar de sleutel op past. Geen machtiging is hetzelfde als een sleutel zonder passend slot.

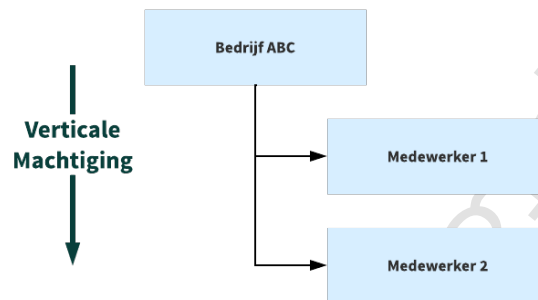
eHerkenning kent twee type machtigingen

[1] Persoonlijke machtiging (verticale machtiging)

[2] Ketenmachtiging (horizontale machtiging)

## Persoonlijke machtiging (verticale machtiging)

Machtigingen binnen één organisatie zijn verticale machtigingen. Een organisatie verstrekt deze machtigingen aan eigen medewerkers om namens deze organisatie te handelen (bijvoorbeeld belastingaangifte of indienen verzekeringsclaim).



Net als het eHerkenningsmiddel, is de machtiging persoonlijk. De machtiging legt vast bij welke dienst(en) de gebruiker namens de organisatie mag inloggen.

Een machtiging kan alleen door de wettelijk vertegenwoordiger(s) of machtigingenbeheerder van een bedrijf of organisatie worden verstrekt. De wettelijk vertegenwoordiger(s) kan een machtigingen-beheerder benoemen om binnen een bedrijf of organisatie de machtigingen te beheren.

Wanneer een wettelijk vertegenwoordiger (volledig bevoegd) een eHerkenningsmiddel aanvraagt, zal de machtiging direct worden goedgekeurd omdat deze persoon namens de organisatie mag handelen.

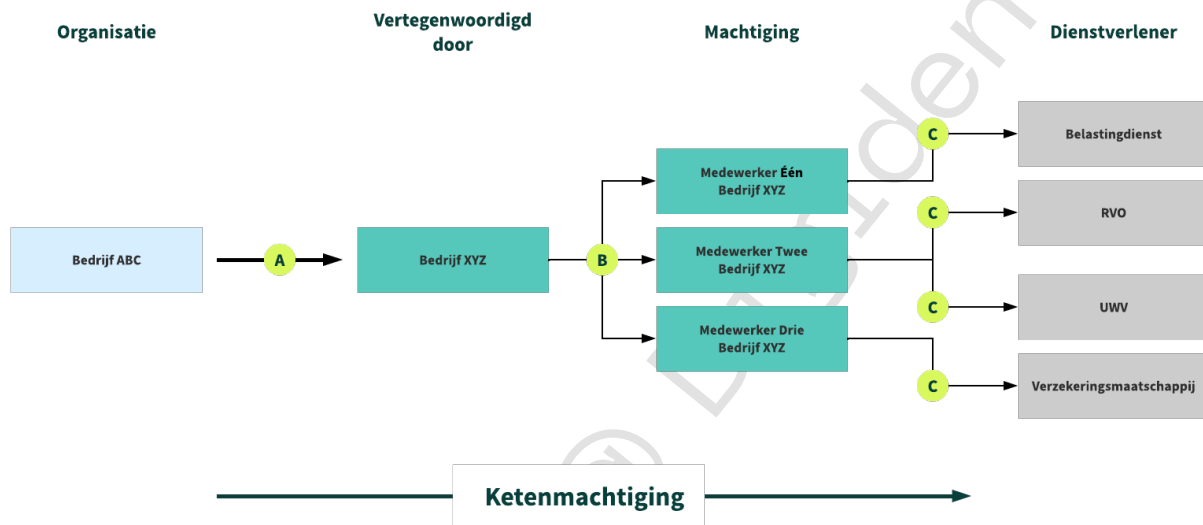
Wanneer iemand een machtiging aanvraagt maar geen wettelijk vertegenwoordiger (volledig bevoegd) is, zal een wettelijk vertegenwoordiger (of meerdere wettelijk vertegenwoordigers) de machtiging moeten goedkeuren.

Regels voor het verstrekken van een machtiging staan in Bijlage A.

**Let op! De Middelenuitgever (Digidentity) moet de wettelijk vertegenwoordiger(s) op hetzelfde betrouwbaarheidsniveau identificeren als de gebruiker van de machtiging.**

## Ketenmachtiging (horizontale machtigingen)

Machtigingen gegeven aan medewerkers van een andere organisatie zijn horizontale machtigingen. Deze horizontale machtigingen bieden de mogelijkheid om een organisatie (ABC) een andere organisatie (XYZ) (vaak een intermediair) te machtigen om namens organisatie (ABC) te handelen bij digitale diensten van de Nederlandse overheid (voorbeeld: doen van belastingaangifte of indienen verzekeringsclaim). De ketenmachtiging biedt de Bedrijfsbeheerder van de gemachtigde organisatie (XYZ) de mogelijkheid om medewerkers van organisatie (XYZ) te machtigen voor organisatie (ABC).



## Voorbeeld van een ketenmachtiging (horizontale machtiging)

Bedrijf ABC machtigt (A) het accountantskantoor Bedrijf XYZ om namens ABC te handelen met de Nederlandse overheid en verzekeringsmaatschappijen (doen van belastingaangiften, aanvragen subsidies, aanvragen vergunningen).

XYZ stelt een Bedrijfsbeheerder aan om medewerkers van XYZ te machtigen (B) om namens ABC te handelen bij Dienstverleners (C).

In bovenstaande afbeelding: de Bedrijfsbeheerder van XYZ machtigt Medewerker Drie om te handelen namens ABC bij de verzekeringsmaatschappij.

Het voordeel van de ketenmachtiging is dat ABC niet iedere individuele medewerkers van XYZ hoeft te machtigen. ABC machtigt XYZ en laat de Bedrijfsbeheerder van XYZ de individuele machtigingen uit te geven.

Een ketenmachtiging kan worden verstrekt of worden aangevraagd:

[a] Bedrijf ABC verstrekt een ketenmachtiging aan een andere organisatie (Bedrijf XYZ).

[b] Bedrijf XYZ vraagt een ketenmachtiging aan voor een andere organisatie (Bedrijf ABC). De verstrekende organisatie (ABC) moet de aangevraagde ketenmachtiging formeel goedkeuren.

## Machtigingenbeheerder

Een organisatie kan één of meerdere machtigingenbeheerders benoemen. Bij Digidentity zijn dit Bedrijfsbeheerder(s). Een machtigingenbeheerder kan machtigingen verstrekken, wijzigen en intrekken voor alle gebruikers binnen de organisatie.

De wettelijke vertegenwoordiger(s) benoemt/benoemen de machtigingenbeheerder(s). De machtigingenbeheerder(s) nemen beheren van de machtigingen over van de wettelijk vertegenwoordiger(s).

De machtigingenbeheerder mag alleen machtigingen beheren voor het niveau waarop de identificatie van de machtigingenbeheerder is uitgevoerd. Een beheerder geïdentificeerd op eH3 niveau mag geen machtigingen op eH4 beheren.

Bij Digidentity kan de wettelijk vertegenwoordiger de machtigingenbeheerder ook de bevoegdheid geven om nieuwe machtigingenbeheerders aan te stellen.

## Identificatie

Ieder eHerkenningmiddel kent een identificatieplicht. Afhankelijk van het betrouwbaarheidsniveau, is meer bewijs van identiteit noodzakelijk om de gewenste betrouwbaarheid te krijgen. De identificatie geldt voor zowel de aanvrager (gebruiker) van het eHerkenningmiddel als degene (tekenbevoegde of bedrijfsbeheerder) die de machtiging goedkeurt.

De eis is dat de Middelenuitgever de gebruiker en tekenbevoegde op hetzelfde betrouwbaarheidsniveau moet identificeren.

Voor de registratie en identificatie zijn bij Digidentity de volgende gegevens nodig:

- \* e-mailadres
- \* identiteitsdocument (paspoort, identiteitskaart of rijbewijs) - voor eH4 moet het ID een chip hebben
- \* selfies (om te kijken of je een levend persoon bent en te vergelijken met de foto op het paspoort)
- \* Kamer van Koophandel nummer (om de organisatie te identificeren)

Digidentity voert de gehele identificatie op afstand uit voor alle betrouwbaarheidsniveaus.

Digidentity heeft een goedgekeurd proces voor identificatie op afstand voor gekwalificeerde certificaten. Voor eHerkenning niveau 4 maakt Digidentity gebruik van het registratieproces voor een gekwalificeerd certificaat. Op basis van het gekwalificeerd certificaat, geeft Digidentity het eHerkenning niveau 4 middel uit zonder dat de gebruiker of tekenbevoegde(n) zich fysiek op locatie moeten identificeren. Digidentity is in Nederland de enige Middelenuitgever die eH4 op basis van volledige identificatie op afstand uitgeeft. De tekenbevoegde(n) kunnen de machtiging digitaal ondertekenen ter goedkeuring.



## Handelsregister

Het Handelsregister (Kamer van Koophandel) is de basisregistratie van alle rechtspersonen en ondernemingen in Nederland. Het Handelsregister is daarmee een gezaghebbende bron voor eHerkenning.

Het Handelsregister is de bron voor de identificatie van organisaties binnen eHerkenning. Wanneer een gebruiker een eHerkenningsmiddel aanvraagt, hoort daar een machtiging voor een organisatie bij. Tijdens de registratie moet de gebruiker het Kamer van Koophandel (KvK) nummer van de organisatie invoeren.

De Middelenuitgever vraagt de organisatiegegevens bij de Kamer van Koophandel op om de organisatie en haar wettelijk vertegenwoordigers (tekenbevoegde) te identificeren.

De Middelenuitgever controleert of de naam van de aanvrager (gebruiker) als tekenbevoegd in het Handelsregister is opgenomen. Is de aanvrager tekenbevoegd, dan kan de Middelenuitgever de machtiging afgeven. Staat de naam van de aanvrager niet in het Handelsregister, of is de aanvrager beperkt bevoegd, dan moeten één of meerdere tekenbevoegde(n) (afhankelijk van de bevoegdheden) de machtiging goedkeuren.

## Protocollaire Basisadministratie (PROBAS)

Een andere gezaghebbende bron voor eHerkenning is de Protocollaire Basisadministratie (PROBAS). PROBAS is een register van het ministerie van Buitenlandse Zaken met persoonsgegevens van medewerkers van ambassades, consulaten en internationale organisaties die actief zijn in Nederland. Deze organisaties staan niet in het Handelsregister.

Wanneer deze groep personen een eHerkenningsmiddel aanvraagt, controleert de Middelenuitgever de organisatie en tekenbevoegden in PROBAS.

## Gebruik in Europa

Een gebruiker kan het eHerkenningsmiddel gebruiken om bij Europese overheidsdiensten in te loggen.

Het is mogelijk om met een eHerkenningsmiddel bij de Italiaanse belastingdienst in te loggen. Hiervoor is een aparte machtiging nodig (eIDAS-Uit). Waar de gebruiker in Nederland met eHerkenning inlogt namens een organisatie, logt de gebruiker in Europa als persoon in.

## Rollen in eHerkenning

Binnen het eHerkenningstelsel zijn verschillende rollen te onderscheiden. Iedere rol heeft een eigen verantwoordelijkheid binnen eHerkenning.

eHerkenning kent de volgende rollen:

- \* Dienstafnemer (gebruiker)
- \* Middelenuitgever (MU)
- \* Dienstverlener (DV)
- \* Authenticatiedienst (AD)
- \* Herkenningmakelaar (HM)
- \* Machtigingenregister (MR)

### Dienstafnemer (gebruiker)

Een Dienstafnemer of gebruiker neemt digitale diensten af van overheidsorganisaties of private organisaties (bijvoorbeeld verzekeringsmaatschappijen). Om deze digitale diensten te gebruiken, moet de gebruiker een eHerkenningmiddel (om in te loggen) en machtiging (autorisatie voor toegang) aanschaffen bij een Middelenuitgever (MU).

De gebruiker kan met het eHerkenningmiddel zijn of haar identiteit aantonen en de machtiging geeft de bevoegdheden aan.

### Middelenuitgever (MU)

De Middelenuitgever identificeert de gebruiker en de organisatie. De Middelenuitgever geeft authenticatiemiddelen uit aan de gebruiker waarmee de gebruiker zich bij de Dienstverlener identificeert. De Middelenuitgever controleert of de gebruiker bevoegd is om namens de organisatie te handelen (controle op de machtiging).

Digidentity is een Middelenuitgever en levert eHerkenning niveau 2+, 3 en 4 middelen.

### Dienstverlener (DV)

De Dienstverlener is een organisatie die digitale diensten aanbiedt. Overheidsdiensten als Belastingdienst, RVO, UWV en Dienst Justis zijn Dienstverleners. Ook private organisaties als verzekeringsmaatschappijen bieden als Dienstverlener digitale diensten aan voor organisaties.

### **Authenticatiedienst (AD)**

De Authenticatiedienst zorgt voor de authenticatie van gebruikers die willen inloggen bij een Dienstverlener met een eHerkenningmiddel.

Wanneer de gebruiker wil inloggen bij een Dienstverlener, moet de gebruiker zijn of haar Middelenuitgever als Digidentity selecteren op de website van de Dienstverlener. De Herkenningmakelaar routeert de gebruiker naar de Authenticatiedienst van Digidentity.

De gebruiker logt in bij de Authenticatiedienst met zijn of haar eHerkenningmiddel. Als de authenticatie gelukt is, stuurt de Authenticatiedienst een toegangssleutel naar de Herkenningmakelaar. In het geval de authenticatie is afgewezen, stuurt de Authenticatiedienst een afwijzing naar de Herkenningmakelaar.

### **Herkenningmakelaar (HM)**

De Herkenningmakelaar sluit de Dienstverlener aan op eHerkenning. Iedere Dienstverlener heeft een Herkenningmakelaar. De Herkenningmakelaar routeert het authenticatieverkeer tussen de Dienstverlener en de verschillende Authenticatiediensten en Machtigingenregisters.

De Herkenningmakelaar zorgt namens de Dienstverlener voor de afhandeling van een verzoek om in te loggen. De Herkenningmakelaar routeert de gebruiker naar de Authenticatiedienst en geeft de resultaten door aan de Dienstverlener.

De Herkenningmakelaar raadpleegt het Machtigingenregister om vast te stellen of de gebruiker de juiste machtiging (autorisatie) heeft en geeft de resultaten door aan de Dienstverlener.

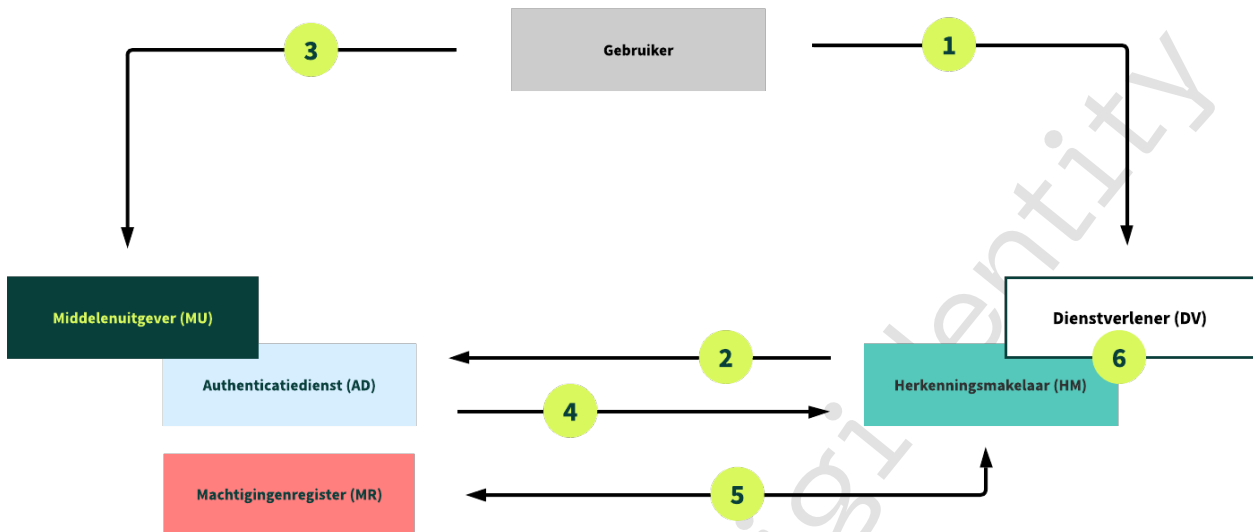
Digidentity levert Herkenningmakelaars aan Dienstverleners.

### **Machtigingenregister (MR)**

Het Machtigingenregister beheert de machtigingen voor de bijbehorende Middelenuitgever en Authenticatiedienst. De Middelenuitgever registreert, beheert en controleert de machtigingen die horen bij de uitgegeven eHerkenningmiddelen.

Het Machtigingenregister ontvangt een toegangssleutel van de Herkenningmakelaar met het verzoek de machtiging voor deze sleutel te controleren in het register. Wanneer de machtiging correct is voor de sleutel, stuurt het Machtigingenregister de geautoriseerde toegangssleutel naar de Herkenningmakelaar. In het geval de machtiging niet is afgegeven voor de toegangssleutel, stuurt het Machtigingenregister een afwijzing naar de Herkenningmaker van de Dienstverlener.

## Hoe werkt inloggen met eHerkenning?



- [1] Gebruiker wil inloggen bij een Dienstverlener (bijvoorbeeld de Belastingdienst). Op de inlogpagina van de Dienstverlener, selecteert de gebruiker zijn of haar Middelenuitgever.
- [2] De Herkenningmakelaar van de Dienstverlener routeert de gebruiker naar de Authenticatiedienst van de Middelenuitgever.
- [3] De gebruiker identificeert zich met zijn of haar eHerkenningsmiddel bij de Authenticatiedienst van de Middelenuitgever. De Authenticatiedienst authentificeert de gebruiker.
- [4] De Authenticatiedienst stuurt een toegangssleutel naar de Herkenningmakelaar van de Dienstverlener.
- [5] De Herkenningmakelaar stuurt de toegangssleutel naar het Machtigingenregister voor een controle van de machtiging van de gebruiker. Het Machtigingenregister bevestigt de machtiging en autoriseert de gebruiker aan de Herkenningmakelaar
- [6] De Herkenningmakelaar routeert de goedkeuring naar de Dienstverlener en de gebruiker is ingelogd.

## Bijlage – Regels eHerkenning

Het stelsel definieert per betrouwbaarheidsniveau de regels voor het goedkeuren van een eHerkenning afhankelijk van de bevoegdheden in het Handelsregister.

### eHerkenning 2+

Bevoegdheid in Handelsregister	Voorwaarden
Wettelijk vertegenwoordiger met volledige bevoegdheid, zelfstandige bevoegdheid of een volmacht	n.v.t.
Wettelijk vertegenwoordiger met gezamenlijke bevoegdheid	Minimaal twee vertegenwoordigers met gezamenlijke bevoegdheid
Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht	Minimaal twee vertegenwoordigers met beperkte bevoegdheid of beperkte volmacht
Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht voor eHerkenning	Expliciete autorisatie voor eHerkenning moet op KvK uittreksel staan

### eHerkenning 3

Bevoegdheid in Handelsregister	Voorwaarden
Wettelijk vertegenwoordiger met volledige bevoegdheid, zelfstandige bevoegdheid of een volmacht	n.v.t.
Wettelijk vertegenwoordiger met gezamenlijke bevoegdheid	Meerderheid van de vertegenwoordigers met gezamenlijke bevoegdheid (helft plus een)
Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht	Meerderheid van de vertegenwoordigers met beperkte bevoegdheid of beperkte volmacht (helft plus een)
Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht voor eHerkenning	Expliciete autorisatie voor eHerkenning moet op KvK uittreksel staan

### eHerkenning 4

Bevoegdheid in Handelsregister	Voorwaarden
Wettelijk vertegenwoordiger met volledige bevoegdheid, zelfstandige bevoegdheid of een volmacht	n.v.t.
Wettelijk vertegenwoordiger met gezamenlijke bevoegdheid	Alle vertegenwoordigers met gezamenlijke bevoegdheid
Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht	Alle vertegenwoordigers met beperkte bevoegdheid of beperkte volmacht
Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht voor eHerkenning	Expliciete autorisatie voor eHerkenning moet op KvK uittreksel staan

Deze regels zijn beschreven in het Afsprakenstelsel (<https://afsprakenstelsel.etoegang.nl>).