Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

# DBI Verdieping identiteitsecosysteem

Versie 1.0
31 maart 2022

# Inhoud

# 1. Inleiding

Dit document is een bijlage bij het *Onderzoeksrapport Digitale Bronidentiteit*.

## 1.1 Kaders voor overheidsdienstverlening

De Nederlandse Overheid Referentie Architectuur (NORA) introduceert het begrip 'kernwaarde'. Een kernwaarde is een 'fundamentele overtuiging, gebaseerd op maatschappelijke waarden, waar overheidsdienstverlening aan moet voldoen.'[1]

De NORA onderscheidt de volgende kernwaarden waaraan het overheidsgedeelte van het identiteits-ecosysteem dient te voldoen:[2]

| Kernwaarde | Omschrijving |
|---|---|
| Vertrouwen | De dienstverlening van de overheid is het vertrouwen waard dat burgers en bedrijven daar in stellen. |
| Veilig | Niemand hoeft bij dienstverlening van de overheid te vrezen voor gevaren en bedreigingen. |
| Toekomstgericht | De dienstverlening van de overheid is op de toekomst voorbereid. |
| Doeltreffend | De dienstverlening van de overheid bereikt de gestelde doelen en voldoet zo aan de verwachtingen van burgers en bedrijven. |
| Doelmatig | De dienstverlening van de overheid is zo ingericht dat met een optimale balans tussen kosten, tijdigheid en kwaliteit het beoogde doel wordt bereikt. |

## 1.2 Definities

Voor een goed begrip van dit hoofdstuk zijn de volgende definities van belang:

| Begrip | Definitie |
|---|---|
| Digitale bronidentiteit | Een door de overheid uitgegeven, erkende en in de wet en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector. Deze digitale bronidentiteit bevat een minimale set van identiteits-gegevens die nodig zijn in het maatschappelijk verkeer. ... De overheid creëert met de digitale bronidentiteit een 'gezaghebbende bron' van betrouwbare persoons-identificerende gegevens. ...<br>Dit biedt een belangrijk generiek bouwblok voor vertrouwen in de digitale wereld.<br>De DBI als 'gezaghebbende bron' maakt afgeleide digitale identiteits-middelen mogelijk ..."[3]<br>Zie de beantwoording van onderzoeksvraag 1 voor een detailuitwerking van 'de DBI'. |

[1] https://www.noraonline.nl/wiki/Kernwaarde_van_Dienstverlening_(Begrip) (01-03-2022). (De kernwaarden en de daarvan afgeleide kwaliteitsdoelen/principes zijn overigens nog in concept.)
[2] https://www.noraonline.nl/wiki/Kernwaarden_van_Dienstverlening (01--3-2022).
[3] Visiebrief digitale identiteit (18-2-2021)

| Begrip | Definitie |
|---|---|
| Europese portemonnee voor digitale identiteit.<br>• NL Wallet | Een product en dienst die de gebruiker in staat stelt zich te identificeren/ authentiseren en attributen met betrekking tot zijn/haar identiteit op te slaan, op verzoek aan vertrouwende partijen te verstrekken, voor online en offline authenticatie voor een dienst overeenkomstig artikel 6 bis te gebruiken, en gekwalificeerde elektronische handtekeningen en zegels aan te maken.[4] |
| Vertrouwensdienst | Een elektronische dienst die gewoonlijk tegen betaling wordt verricht en het onderstaande inhoudt:<br>a. het aanmaken, verifiëren en valideren van elektronische handtekeningen, elektronische zegels of elektronische tijdstempels, diensten voor elektronisch aangetekende bezorging, elektronische attestering van attributen en certificaten die betrekking hebben op deze diensten;<br>b. het aanmaken, verifiëren en valideren van certificaten voor authenticatie van websites;<br>c. het bewaren van elektronische handtekeningen, zegels of certificaten die op deze diensten betrekking hebben;<br>d. het elektronisch archiveren van elektronische documenten;<br>e. het beheer van middelen voor het aanmaken van elektronische handtekeningen en zegels op afstand;<br>f. het opslaan van elektronische gegevens in elektronische registers.[5] |
| Attribuut | Een eigenschap, kenmerk of kwaliteit van een natuurlijke of rechtspersoon of een entiteit, in elektronisch formaat.[6] |
| Elektronische attestering van attributen | Een attestering in elektronisch formaat aan de hand waarvan attributen kunnen worden geauthenticeerd.[7] |
| Gekwalificeerde elektronische attestering van attributen” | Een elektronische attestering van attributen die is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage V [van de concept-verordening].[8] |
| Authentieke bron | Een register of systeem, onder de verantwoordelijkheid van een publiekrechtelijk orgaan of particuliere entiteit, dat attributen omtrent een natuurlijke of rechtspersoon bevat en als de primaire bron van die informatie wordt beschouwd of krachtens nationaal recht als authentiek wordt erkend.[9] |
| Gekwalificeerde vertrouwensdienst | Een vertrouwensdienst die voldoet aan de toepasselijke eisen zoals vastgelegd in deze verordening.[10] |
| Verlener van vertrouwensdiensten | Een natuurlijke persoon of rechtspersoon die een of meer vertrouwensdiensten verleent als een gekwalificeerde of als een niet-gekwalificeerde verlener van vertrouwensdiensten.[11] |
| Gekwalificeerde verlener van vertrouwensdiensten | Een verlener van vertrouwensdiensten die één of meerdere gekwalificeerde vertrouwensdiensten verleent en van het toezichthoudende orgaan de status van gekwalificeerde heeft gekregen.[12] |
| Vertrouwende partij | Een natuurlijke persoon of een rechtspersoon die vertrouwt op een elektronische identificatie of een vertrouwensdienst.[13] |

[4] Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit, artikel 3(i)
[5] Ib., artikel 3(d)
[6] Ib., artikel 3(i)
[7] Ib.
[8] Ib.
[9] Ib., artikel 3(46)
[10] 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(17)
[11] Voorstel voor een VERORDENING., artikel 3(19)
[12] Ib., artikel 3(20)
[13] Ib., atikel 3(6)

| Begrip | Definitie |
|---|---|
| Gebruiker | Een natuurlijk of rechtspersoon die gebruik maakt van diensten van vertrouwende partijen en gekwalificeerde verleners van vertrouwensdiensten. |
| Elektronisch register | Middels elektronische registers beschikken gebruikers over bewijs en een vaststaand controlespoor voor de volgorde van transacties en gegevensbestanden.[14] |
| Gekwalificeerd elektronisch register | [Bewaart] gegevens op zodanige wijze dat het unieke karakter, de authenticiteit en de juiste volgorde van de ingevoerde gegevens onvervalsbaar worden verzekerd. Een elektronisch register combineert het effect van tijdstempels van gegevens met zekerheid over de gegevensbron, wat lijkt op een e-handtekening, met als bijkomend voordeel dat de governancemodellen meer kunnen worden gedecentraliseerd, wat voor samenwerking tussen meer partijen geschikt is.[15] |

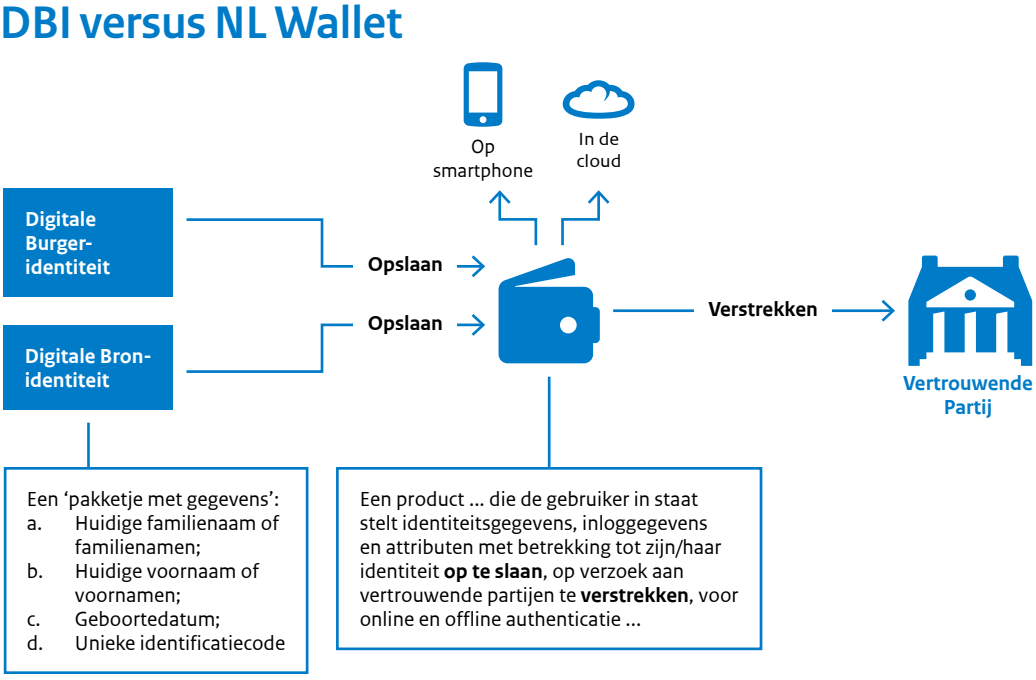
In het vervolg van dit hoofdstuk worden bovenstaande begrippen gebruikt.

[14] Ib., blz. 9.
[15] Ib., blz. 22.

# 2 DBI en positionering

## 2.1 De DBI en NL Wallet

***Afbeelding 1*** *DBI en de NL Wallet*




De overheid beheert nog meer identiteitsgegevens dan alleen deze 'minimale set van identiteitsgegevens. Denk bijvoorbeeld aan gegevens over de rijbevoegdheid van burgers of aan diploma's.[16] Die gegevensset noemen we de Digitale Burgeridentiteit. Deze is ook weergegeven in afbeelding 1.

Een burger kan zijn digitale bron- en burgeridentiteit ontvangen[17] van (gekwalificeerde) verleners van vertrouwensdiensten, zoals de gemeenten, RDW en DUO, en opslaan in zijn NL Wallet. Vanuit die wallet kan hij vervolgens die gegevens doorsturen naar vertrouwende partijen, zoals een autoverhuurbedrijf of een opleidingsinstituut.

## 2.2 De positionering van 'een DBI'

'De DBI' is het fundamentele bouwblok in het identiteitsecosysteem: digitale identiteiten die de burger gebruikt in het maatschappelijk verkeer (kunnen) zijn afgeleid van de Digitale Bronidentiteit van de burger.

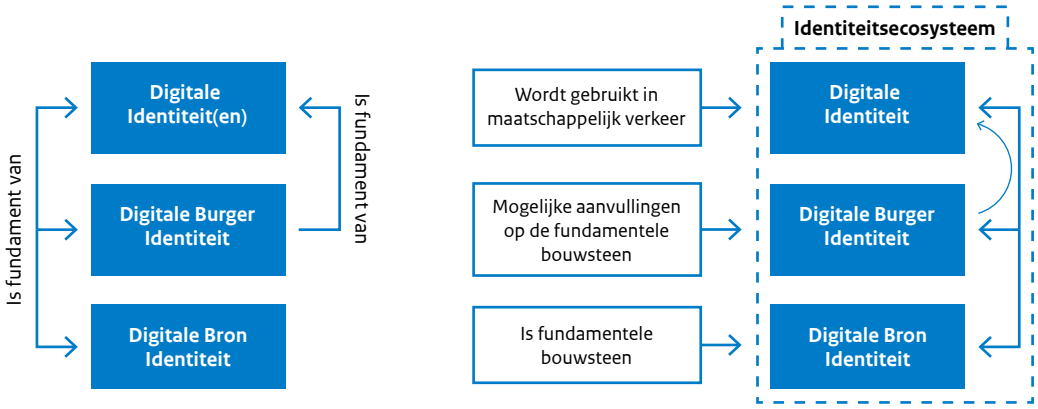
Indien wenselijk kan de burger (delen van) zijn digitale bronidentiteit aanvullen met identiteitsgegevens die uit de digitale burgeridentiteit.

De (delen van) digitale bronidentiteit en de gegevens uit de digitale burgeridentiteit tezamen vormen een

[16] Voor diploma's zie https://www.duo.nl/particulier/uittreksel-diplomagegevens-downloaden.jsp
[17] We doen hier nog geen uitspraak of de burger eerst die gegevens moete aanvragen ('pull'-methode) of dat de (gekwalificeerde) verlener de gegevens actief opstuurt ('push'-methode).

digitale identiteit die de burger kan gebruiken in het maatschappelijk verkeer.

***Afbeelding 2*** *DBI in het ecosysteem*



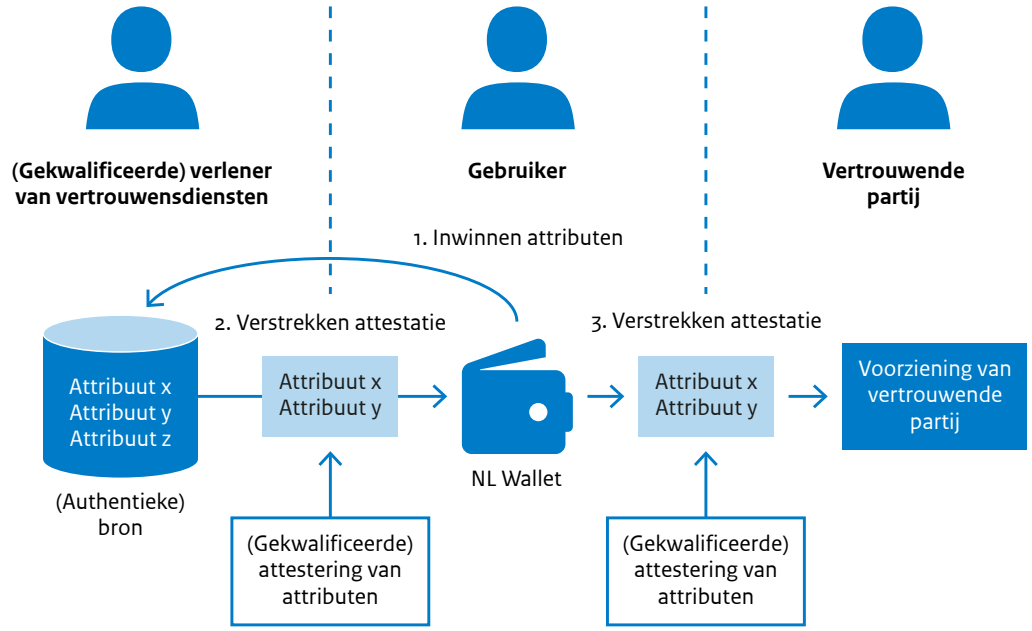

## 2.3 Een verdieping: (gekwalificeerde) elektronische attestaties van attributen

Een gebruiker kan zijn attributen verstrekken aan bijvoorbeeld een vertrouwende partij. Dat kan in het formaat van een elektronische attestatie. Zo'n attestatie bevat dus gegevens over de gebruiker.

Er zijn twee verschijningsvormen van elektronische attestaties van attributen (artikel 45 quater, lid 1, 3):

- Gekwalificeerd: deze elektronische attestaties voldoen aan de vereisten uit bijlage V van de conceptverordening.
  - Een gekwalificeerde attestatie kan worden ingetrokken. Vanaf dat moment is de attestatie niet meer geldig. Intrekking is definitief en kan niet ongedaan worden gemaakt.
- Niet-gekwalificeerd: deze voldoen niet aan de vereisten uit bijlage V van de conceptverordening.

*Afbeelding 3*



# 3 Het DBI eco-systeem

## 3.1 De noodzaak van een identiteitsecosysteem

Aan alleen zijn DBI en de NL Wallet heeft een burger niets. Hij moet de DBI kunnen gebruiken in het maatschappelijk verkeer om digitale diensten te kunnen afnemen van zowel publieke als private vertrouwende partijen.

Daarbij is het wel van belang dat de DBI betrouwbaar is op alle momenten van een dienstverlening. Dat stelt niet alleen eisen de betrouwbaarheid van de DBI zelf. Maar ook aan onder andere de betrouwbaarheid van de NL Wallet en aan de wijze waarop (gekwalificeerde) verleners van vertrouwensdiensten en vertrouwende partijen omgaan met de DBI (en zelfs bredere zin: de identiteitsgegevens) die zij aan burgers verstrekken c.q. van burgers ontvangen.

Om ervoor te zorgen dat een DBI op en betrouwbare, veilige, voorspelbare wijze wordt gebruikt in het maatschappelijk verkeer, is een zogenaamd identiteitsecosysteem nodig.

Met de term identiteitsecosysteem bedoelen wij het volgende: *het geheel aan (o.a.) wetten/afspraken, diensten/ producten, processen, applicaties, gegevensverzamelingen dat nodig is om ervoor te zorgen dat een burger zich op een betrouwbare en veilige wijze digitaal kan identificeren en authentiseren bij publieke en private dienstaanbieders.*[18]

Een goed werkend ecosysteem is uitermate belangrijk. Niet alleen omdat publieke én private vertrouwende partijen in dat ecosysteem concrete diensten met vertrouwen kunnen aanbieden aan burgers, maar ook omdat een helder afsprakenstelsel en de nodige ondersteunende diensten deel uitmaken van het ecosysteem.[19]

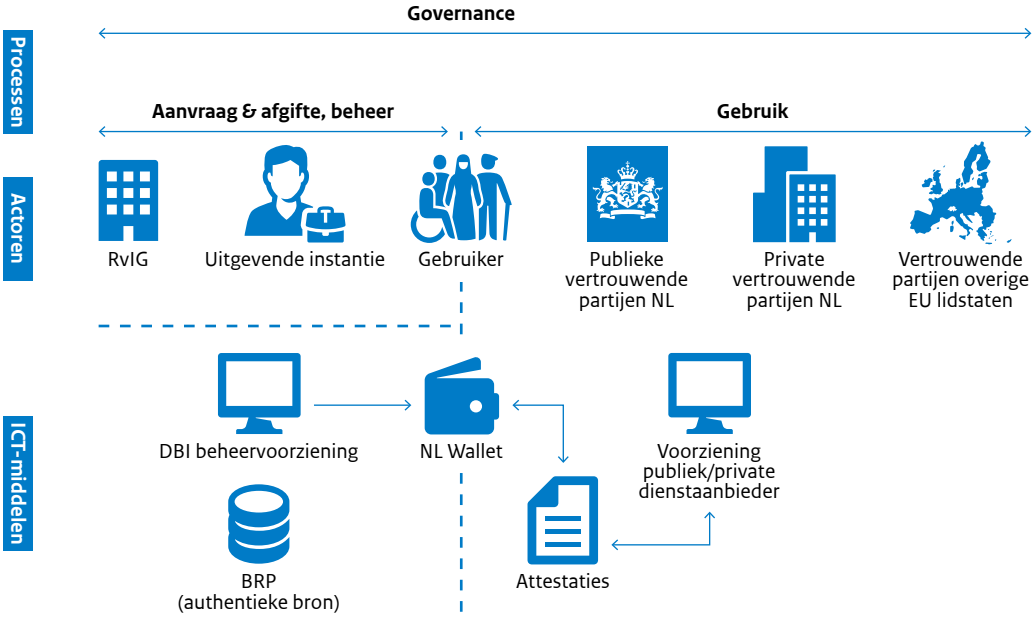
Bovenstaande definitie is opgesteld vanuit het gezichtspunt van de burger. Uiteraard hebben ook (gekwalificeerde) verleners van vertrouwensdiensten en vertrouwende partijen een groot belang bij een goed werkend ecosysteem (en dus onder andere bij een betrouwbare DBI en NL Wallet.)

[18] Gebaseerd op de definitie van de Wereldbank op: https://id4d.worldbank.org/guide/glossary 22-10-2021)

[19] In die zin kan een ecosysteem min of meer worden vergeleken met een ketenproces. In de 'visiebrief digitale identiteit' van de staatssecretaris van BZK d.d. 11-2-2021 wordt het identiteitsecosysteem 'digitale identiteit infrastructuur' genoemd.

Afbeelding 4 geeft een vereenvoudigd beeld van het identiteitsecosysteem.

***Afbeelding 4*** *Vereenvoudigde weergave van het identiteitsecosysteem*




In deze vereenvoudigde weergave bestaat het identiteitsecosysteem uit een drietal lagen:

1. Processen. Dit zijn enerzijds de processen die nodig zij voor de aanvraag en uitgifte van een DBI en voor het beheer ervan. Anderzijds betreft dit de processen die nodig zijn voor het gebruik van een DBI in het maatschappelijk verkeer.
2. Actoren. Dit zijn de actoren die (delen van) de processen uitvoeren om zo diensten te kunnen aanbieden en afnemen en he onderling te kunnen afstemmen.
3. ICT-middelen. Dit zijn de ICT-middelen die de uitvoering van de processen ondersteunen/mogelijk maken, zoals de DBI- beheervoorziening. Dit is vooralsnog een algemene aanduiding voor de voorzieningen die nodig zijn om een DBI te kunnen aanvragen, uitgeven en te beheren. Maar ook gebruikersondersteuning is een functionaliteit van deze voorziening. Op een later moment wordt de DBI-beheervoorziening verder uitgewerkt in één of meerdere voorzieningen

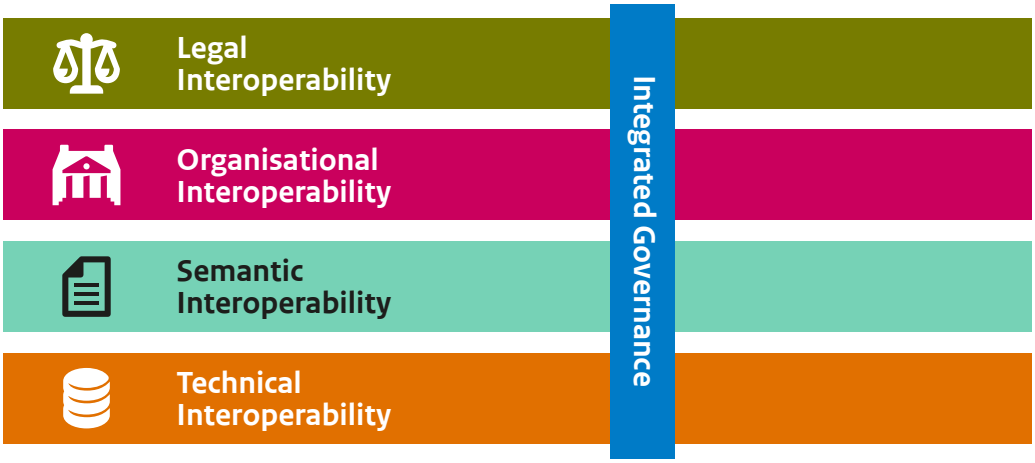
## 3.2 De noodzaak van interoperabiliteit

Interoperabiliteit staat voor het vermogen van organisaties (en hun processen en systemen) om effectief en efficiënt informatie te delen met hun omgeving.[20] Diensten en producten van de (gekwalificeerde) verleners van vertrouwensdiensten en vertrouwende partijen uit het identiteitsecosysteem moeten op elkaar aansluiten en ‘dezelfde taal spreken’.

Interoperabiliteit moet op verschillende manieren zijn geregeld voordat een goedwerkend ecosysteem kan worden gerealiseerd. In onderstaande afbeelding en tabel zijn alle mogelijke vormen van inter-operabiliteit weergegeven en beschreven.[21]

[20] https://www.noraonline.nl/wiki/Interoperabiliteit (24-11-2021).
[21] New European Interoperability Framework. Promoting seamless services and data flows for European public administrations (Europese Unie; Luxemburg, 2017), blz. 27-31.

***Afbeelding 5*** *Interoperabiliteitsraamwerk van de Europese Unie*




| Interoperabiliteits-vorm | Beschrijving | Gevolgen identiteits-ecosysteem |
|---|---|---|
| Juridisch | Wet- en regelgeving uit verschillende domeinen is onderling afgestemd. | Nationale wet- en regelgeving van Nederland en andere lidstaten mag niet strijdig zijn met Europese wet- en regelgeving, zoals de eIDAS-verordening. |
| Organisatorisch | Samenwerkende actoren hebben hun processen, verantwoordelijkheden en verwachtingen onderling afgestemd en toezicht op het ecosysteem is ingericht en operationeel. | Analoog aan de inrichting van keten-processen is de inrichting van primaire processen door individuele (gekwalificeerde) verleners van vertrouwensdiensten en vertrouwende partijen niet relevant; het gaat immers om diensten en producten. Verwachtingen en verantwoordelijkheden zijn daarentegen wel relevant: wie levert welk(e) dienst/ product? Wat zijn de onderlinge afhankelijkheden daarbij? Onderlinge afspraken en het houden van toezicht op de naleving daarvan is ook een belangrijk aspect van organisatorische interoperabiliteit. |
| Semantisch | Semantiek: samenwerkende actoren geven dezelfde betekenis aan gegevens die onderling worden uitgewisseld. | Semantiek: iedereen gebruikt dezelfde definitie van een attribuut of attestatie waaruit de Digitale Bron- c.q. Burger-identiteit kan bestaan. Bijvoorbeeld de *Core Person Vocabulary* van SEMIC.[22] |
| | Syntax: de schrijfwijze (vorm of syntax) van de uit te wisselen gegevens is eenduidig. | Syntax: attestaties hebben altijd dezelfde vorm, bijvoorbeeld *Verifiable Credentials* van W3C.[23] |
| Technisch | Systemen van samenwerkende actoren kunnen op het niveau van infrastructuur en software met elkaar gegevens uitwisselen. | Er zijn gestandaardiseerde koppelvlakken tussen ICT-componenten die onderling gegevens uitwisselen. |

[22] https://semiceu.github.io/Core-Person-Vocabulary/releases/2.00/ (24-11-2021; https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic (24-11-2021).
[23] https://www.w3.org/TR/vc-data-model/ (24-11-2021).

Ook tussen deze verschillende vormen van interoperabiliteit is afstemming nodig. Een interoperabiliteitsvorm legt immers kaders op aan de direct onderliggende interoperabiliteitsvorm.
Het is daarom van belang dat een Integrale governance – zowel nationaal als in EU-verband – wordt ingericht.[24]

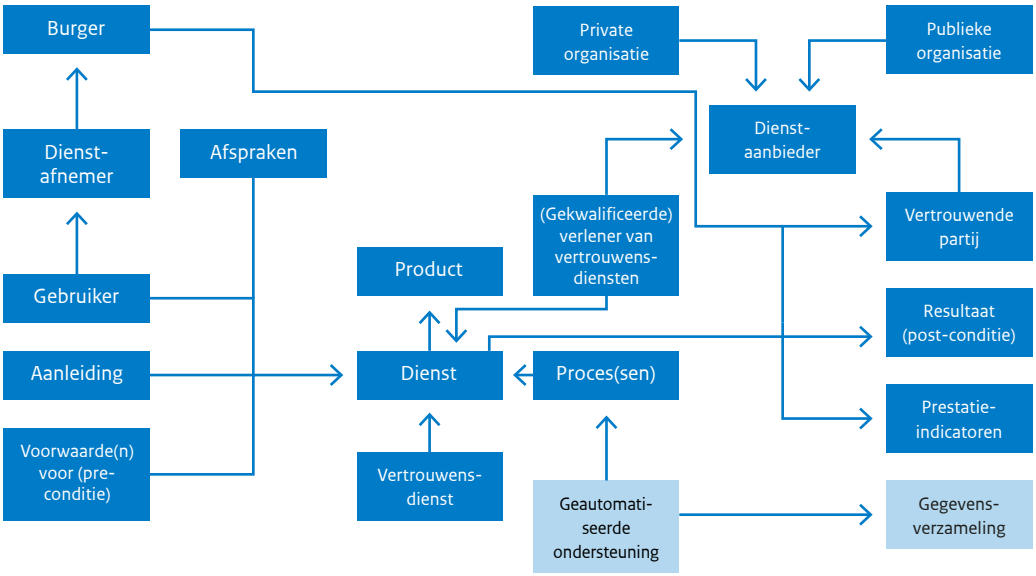
In onderstaande paragrafen is beschreven welke vormen van interoperabiliteit relevant zijn voor het identiteitsecosysteem.

[24] De Europese Commissie werkt aan een overzicht van (toe te passen) standaarden en binnenkort ook aan een voorstel voor governance. Het is raadzaam deze ontwikkelingen nauwkeurig in de gaten te houden.

## 3.3 Metamodel

Het identiteitsecosysteem wordt uitgewerkt volgens onderstaand model. Naarmate het ecosysteem verder wordt uitgewerkt, komt meer detail in dit model.

***Afbeelding 6*** *Metamodel identiteitsecosysteem*




Centraal in het ecosysteem staat de dienstverlening aan burgers van publieke en private organisaties, zoals bijvoorbeeld RvIG of een financiële instelling.

# 4 Uitwerking DBI eco-systeem

## 4.1 Diensten en producten

De Nederlandse Overheid Referentie Architectuur (verder: NORA) geeft de volgende definitie van een dienst: “Een afgebakende prestatie van een persoon of organisatie … die voorziet in een behoefte van haar omgeving”.[25] Aan elke dienst kunnen prestatie-indicatoren worden toegekend aan de hand waarvan kan worden bepaald of een dienst nog steeds voldoet aan de verwachtingen.

Er is altijd een aanleiding nodig om een dienst uit te voeren. In de context van DBI is dat de wens van een gebruiker om een digitale dienst of product af te nemen. Dit wil overigens niet zeggen dat een (gekwalificeerde) verleners van vertrouwensdiensten of vertrouwende partijen geen voorwaarden kan stellen aan het leveren van een dienst. Voldoet een gebruiker niet aan die, vooraf duidelijk kenbaar gemaakte voorwaarden, dan wordt de dienst niet geleverd (en het onderliggende proces niet uitgevoerd).

Dienstverlening heeft ook altijd een verwachte uitkomst. Vaak zal dat de levering van de door de gebruiker gewenste dienst of product zijn. Een afwijzing kan ook een verwachte – maar onverhoopte – uitkomst zijn van een dienst.

Producten kunnen tastbaar zijn. Denk bijvoorbeeld aan een papieren diploma. Maar in de context van DBI zijn producten niet-tastbaar. Het betreft immers digitale producten. Denk bijvoorbeeld aan een attestatie van een diploma.

Voor een goede dienstverlening zijn alle interoperabiliteitsvormen van groot belang; zie paragraaf 1.3.2

In onderstaande overzichten zijn de diensten/producten weergegeven die relevant zijn in het identiteitsecosysteem. Deze diensten en producten zijn voor een groot deel ook bepalend voor hoe het identiteitsecosysteem eruitziet.

Er is onderscheid gemaakt tussen primaire diensten. Primaire diensten zijn diensten die op de gebruikers zijn gericht, secundaire diensten zijn m.n. intern gericht.[26]

| Primaire dienst | Bijbehorende product(en) | Opmerking |
|---|---|---|
| Leveren ondersteuning aan dienstafnemers en -aanbieders (‘helpdesk’). | | |
| Melden verlies, fouten, vermoeden van fraude. | Digitale portemonnee, DBI, attestaties. | Wellicht kan dit worden belegd bij het Meldpunt Fouten in Overheids-registraties resp. Centraal Meldpunt Identiteits-fraude. |
| Blokkeren DBI/wallet. | | Wellicht hergebruik van StopID functionaliteit. |
| Uitgeven DBI. | DBI, transactiegeschiedenis. | |

[25] https://www.noraonline.nl/wiki/Dienst (23-11-2021)
[26] Vgl. https://www.lean.nl/achtergrond/wat-is-een-proces/ (29-11-2021)

| Primaire dienst | Bijbehorende product(en) | Opmerking |
|---|---|---|
| Uitgeven attestatie. | Attestatie, transactie-geschiedenis. | Voor nu is dit een verzamel-begrip. Op een later moment worden – i.s.m. de dienst-aanbieders en op basis van de prioriteit van de use cases - de uiteenlopende attestaties in detail uitgewerkt.<br>Zie concept-verordening artikel 45 sexies. |
| Intrekken attestatie. | Attestatie, transactie-geschiedenis (inden intrekking door burger zelf). | Zie concept-verordening artikel 45 quater lid 3 blz. 45. |
| Identificeren gebruiker – online. | Attestaties, transactie-geschiedenis. | Zie concept-verordening artikel 6 bis lid 4 (a)(3), artikel 12 ter lid 3 en artikel 12 quater lid 1. |
| Aanmaken elektronische handtekening op afstand. | Elektronische handtekening, transactiegeschiedenis. | Zie concept-verordening artikel 29 bis lid 1. |
| Leveren bewaringsdienst voor gekwalificeer-de elektronische handtekening. | | Zie concept-verordening artikel 34. |
| Aanmaken elektronische zegel op afstand. | Elektronische zegel, transactie-geschiedenis. | Zie concept-verordening artikel 39 bis. |
| Verifiëren NL Wallet. | NL Wallet. | Zie concept-verordening artikel 6 bis lid 5. |
| Verifiëren identiteit. | Attestatie(s). | Zie concept-verordening artikel 6 bis lid 5(b). |
| Verifiëren attribuut. | Attribuut. | Zie concept-verordening artikel 6 bis lid 4(a)(2) en lid 5(b), artikel 24 lid 1, artikel 45 quinquies lid 1. |
| Toekennen machtiging/vertegenwoordiging. | DBI. | |
| Intrekken machtiging/vertegenwoordiging. | DBI. | |
| Aantonen machtiging/vertegenwoordiging. | DBI. | |

| Secundaire dienst | Bijbehorende product(en) | Opmerking |
|---|---|---|
| Houden van toezicht op het identiteitsecosysteem. | -- | Dit is inclusief de tweejaarlijkse audit van 'gekwalificeerde verleners van vertrou-wensdiensten'.<br>Zie conceptverordening artikel 18. |
| Uitvoeren van governance van het identiteitsecosysteem . | | |
| Beheren DBI. | DBI. | |
| Ontwikkelen & beheren NL Wallet. | NL Wallet. | Dit is inclusief o.a. het opschorten van de afgifte c.q. intrekken van de geldigheid van de NL Wallet.<br>Zie conceptverordening artikel 10 bis. |
| Authentiseren vertrouwende partijen. | Register van vertrouwende partijen. | Zie conceptverordening artikel 6 ter lid 2. Dienstaanbieders (vertrouwende partijen) moeten hun voornemen om gebruik te maken van de NL Wallet, melden bij de Lidstaat waarin zij zijn gevestigd. |

| Secundaire dienst | Bijbehorende product(en) | Opmerking |
|---|---|---|
| Verifiëren authenticatie dienstaanbieder. | Register van geautoriseerde dienstaanbieders. | |
| Beheren Register van geautoriseerde vertrouwende partijen. | Register van geautoriseerde vertrouwende partijen. | |
| Certificeren en accrediteren (gekwalificeerde) verlener van vertrouwensdiensten. | Register van gekwalificeerde aanbieders van vertrouwensdiensten. | Zie conceptverordening, overweging artikel 35. |
| Verifiëren certificaat gekwalificeerde verlener van vertrouwensdiensten. | Register van gekwalificeerde aanbieders van vertrouwensdiensten. | |
| Beheren Register van gekwalificeerde verleners van vertrouwendiensten. | Register van gekwalificeerde aanbieders van vertrouwensdiensten. | |
| Beheren van middelen voor het aanmaken van elektronische zegels op afstand. | | Zie conceptverordening artikel 39 bis. |
| Opstellen & beheren dienstencatalogus. | Dienstencatalogus. | Alle primaire en secundaire diensten (en hun eventuele voorwaarden) worden opgenomen in een openbaar dienstencatalogus.<br>Zie conceptverordening artikel 6 ter lid 1 en 2. |
| Certificeren NL Wallets. | NL Wallet, Register van gecertificeerde NL Wallets. | Zie conceptverordening artikel 6 quarter. |
| Verifiëren certificaat NL Wallet. | NL Wallet, Register van gecertificeerde NL Wallets. | |
| Beheren Register van gecertificeerde NL Wallets. | Register van gecertificeerde NL Wallets. | |
| Verzamelen statistieken over de werking van de NL Wallet. | | Zie conceptverordening artikel 48 bis. |
| Verzamelen statistieken over de werking van gekwalificeerde vertrouwensdiensten. | | Zie conceptverordening artikel 48 bis. |

Bij het prioriteren van diensten en producten mag het burgerperspectief niet ontbreken. Als de eerste diensten/producten die beschikbaar worden gesteld niet aansluiten bij de (dagelijkse) behoeften van burgers, kan dat ten koste gaan van de acceptatie van DBI en de NL Wallet.

## 4.2 Verdieping: diensten in het kader van de Europese 'Toolbox'

De Europese Commissie werkt aan een Toolbox voor eIDAS-diensten. In dat kader worden in Europees verband de volgende *grensoverschrijdende use cases* uitgewerkt:[27]

| Use case | Dienstaanbieder | Opmerking |
|---|---|---|
| Identificeren burger – online. | RvIG. | |
| Elektronische handtekening. | | |
| Mobile Driving License. | RDW. | |

[27] The Toolbox Process, blz. 23 e.v.

| Use case | Dienstaanbieder | Opmerking |
|---|---|---|
| eHealth: Patient Summary & ePrescription. | | |
| Digital Travel Credential. | RvIG. | |
| Payments. | Banken, credit card-uitgevers, ... | |
| Sharing Diploma. | DUO. | |

*Processen*

Diensten ontstaan niet spontaan. Eén of meerdere processen worden uitgevoerd om een product of dienst te kunnen leveren. Voor de afnemer is het niet relevant hoeveel processen moeten worden uitgevoerd en door hoeveel personen. Het gaat de afnemer immers niet om het uitvoeren van processen maar om de dienst. Maar als de afnemer zelf delen van het proces moet uitvoeren, moet hij dat op een gebruikersvriendelijke kunnen doen.

Het is voor een goede werking van het identiteitsecosysteem niet relevant te weten welke processen een dienstaanbieder uitvoert om een bepaalde dienst te leveren. Het is aan een dienstaanbieder om een dienst te leveren conform de gemaakte afspraken (zie paragraaf XX over interoperabiliteit).
Welke processen de dienstaanbieder daarvoor moet uitvoeren, is volledig aan hem om te bepalen. Daarom worden processen in dit hoofdstuk niet verder uitgewerkt.

## 4.3 Actoren en rollen

Natuurlijke en rechtspersonen nemen diensten en/of producten af c.q. leveren diensten/producten. Ook voeren zij (delen van) processen uit. Dat doen zij vanuit een specifieke rol.

Voor het identiteitsecosysteem onderscheiden we de volgende actoren en rollen:

| Actor | Rol | Opmerking |
|---|---|---|
| Burger | Dienstafnemer: gebruiker Dienstaanbieder vertrouwende partij in geval van een burger  burger transactie. | Denk bijvoorbeeld aan een webwinkel. |
| Gemeente | Dienstaanbieder (uitgeven DBI): gekwalificeerde verlener van vertrouwensdiensten. | |
| Ambassade/consulaat | Dienstaanbieder (uitgeven DBI): gekwalificeerde verlener van vertrouwensdiensten. | |
| RvIG | Beheerder kernvoorzieningen (zie volgende paragraaf). | |
| ? | Leverancier/beheerder NL Wallet. | |
| ? | Leverancier/beheerder DBI-beheervoorziening. | |
| | Eigenaar/beheer van andere <relevante> apps. | Zie applicatielandschap. Denk bijvoorbeeld aan banken, luchtvaart-maatschappijen. Kunnen ook onder de rol dienstaanbieder vallen. |
| Publieke organisatie | Dienstaanbieder:<br>• (Gekwalificeerde) verlener van vertrouwensdienst; en<br>• Vertrouwende partij. | Dit betreft overheidsorganisaties; zowel Nederlandse als die van andere lidstaten. |

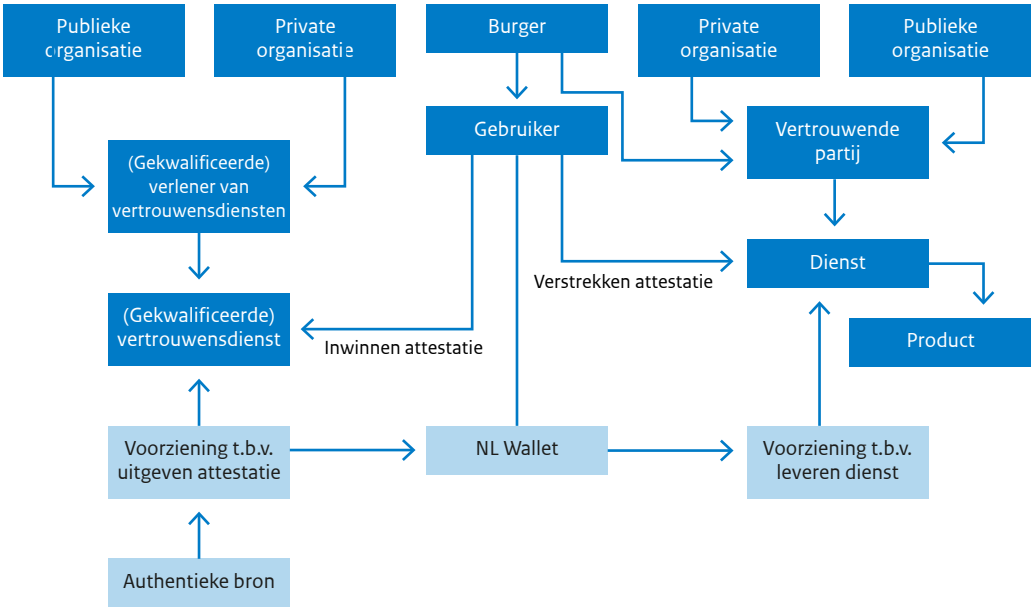
| Actor | Rol | Opmerking |
|---|---|---|
| Private organisatie | Dienstaanbieder<br>• (Gekwalificeerde) verlener van vertrouwensdienst; en<br>• Vertrouwende partij. | Dit betreft het bedrijfsleven; zowel Nederlandse als uit andere lidstaten. Ook 'zeer grote online platformen vallen hieronder. |
| ? | Toezichthouder | |
| ? | Certificerende partij: NL Wallet. | Certificeert de NL Wallet(s). |
| ? | Conformiteitsbeoordelings-orgaan. | Voert audits uit op gekwalificeerde verleners van vertrouwensdiensten. |
| ? | Helpdesk. | Deze rol kan worden toegekend aan meerdere organisaties. |
| Bibliotheek/ informatiepunt digitale overheid. | In-persoon helpdesk voor burgers. | |

## 4.4 Een verdieping: soorten dienstaanbieders

Conform de concept-verordening zijn twee soorten dienstaanbieders te onderscheiden:

- (Gekwalificeerde) verleners van vertrouwensdiensten. Bij deze organisaties kan een gebruiker één of meerdere attestaties[28] aanvragen.
  - Bijvoorbeeld een diploma van opleiding *x*.
- Vertrouwende partijen. Van deze organisaties wil de gebruiker een dienst afnemen.
  - Bijvoorbeeld een aanbieder van opleidingen. De gebruiker wil opleiding *y* volgen en moet aantonen dat hij over diploma *x* beschikt.

***Afbeelding 7*** *Soorten dienstaanbieders*




[28] Het verschil tussen gekwalificeerde attestaties en niet-gekwalificeerde attestaties is hier niet relevant.

Een organisatie kan een (gekwalificeerde) verlener van vertrouwensdiensten zijn maar ook een vertrouwende partij. In het verlengde van bovenstaande voorbeelden: de aanbieder van opleiding y is een:

- Vertrouwende partij in de situatie waarin hij van de gebruiker het diploma van opleiding x ontvangt.
- (Gekwalificeerde) verlener van vertrouwensdiensten in de situatie waarin hij aan de gebruiker het diploma van opleiding y verstrekt.

Een burger kan ook handelen vanuit twee hoedanigheden, namelijk als:
- Dienstafnemer, oftewel: gebruiker. In dat geval neemt hij diensten af van (gekwalificeerde) verleners van vertrouwensdiensten en van vertrouwende partijen.
- Dienstaanbieder, oftewel vertrouwende partij. In dit geval biedt de burger diensten aan aan gebruikers.

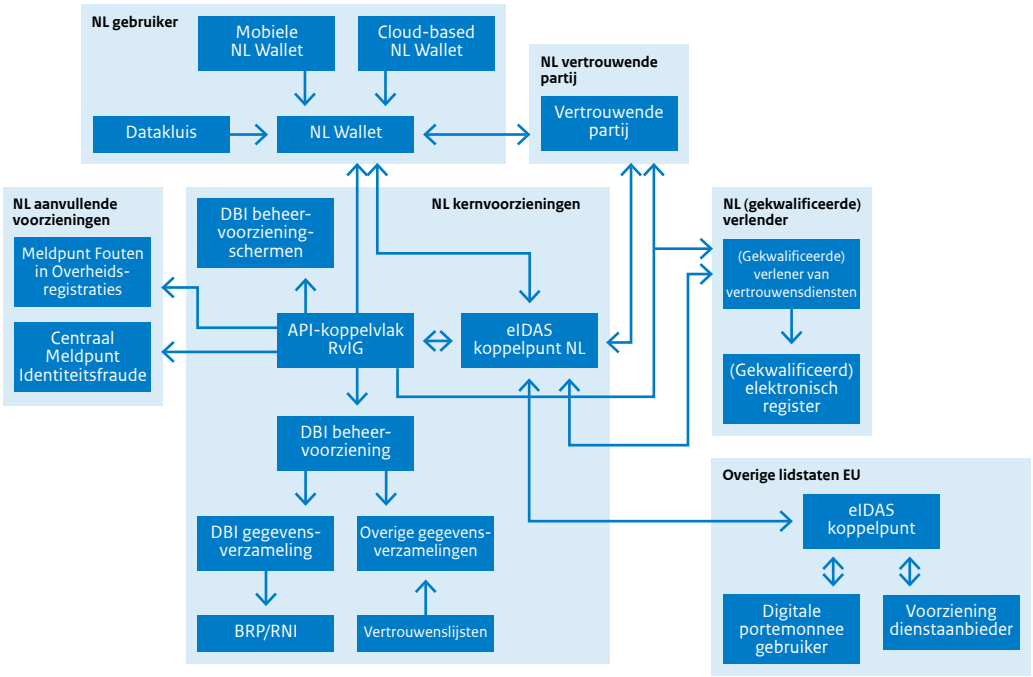
## 4.5 Noodzakelijke voorzieningen

Welke technische voorzieningen een (gekwalificeerde) verlener van vertrouwensdiensten of een vertrouwende partij nodig heeft om een dienst/product te kunnen leveren (lees: om – delen van - een proces te kunnen uitvoeren) is voor het identiteitsecosysteem niet van belang.

Syntactische en technische interoperabiliteit is daarentegen wel van belang om geautomatiseerde gegevensuitwisseling tussen de technische voorzieningen uit het ecosysteem mogelijk te maken. Denk bijvoorbeeld aan de gegevensuitwisseling tussen de NL Wallet die een gebruiker op zijn mobiele telefoon heeft geïnstalleerd en de voorziening van DUO om een attestatie van een diploma aan te vragen resp. te leveren.

Naast specifieke voorzieningen van de (gekwalificeerde) verleners van vertrouwensdiensten en vertrouwende partijen, kent het ecosysteem een aantal generieke voorzieningen.

***Afbeelding 8*** *Het applicatielandschap binnen het identiteitsecosysteem*



Afbeelding 8 toont een logisch applicatielandschap. Dat betekent dat geen uitspraak wordt gedaan door hoeveel, en welke, technische componenten (software) een applicatiecomponent wordt gerealiseerd. Zo is de 'DBI-beheervoorziening' weergegeven als één applicatiecomponent maar kan in de 'werkelijke wereld' uit meerdere - al dan niet losstaande - softwarepakketten bestaan. Bijvoorbeeld één voor de aanvraag en uitgifte van een DBI, één voor het beheer van uitgegeven DBI's en één voor de ondersteuning van gebruikers (denk hierbij aan een website met informatie over DBI).

Het applicatielandschap is onderverdeeld in een zestal 'blokken':

- NL gebruiker. Hier zijn de applicatiecomponenten opgenomen die de gebruiker gebruikt om een DBI te activeren/beheren en om diensten/producten af te nemen. Van het applicatiecomponent 'NL Wallet' zijn twee mogelijke verschijningsvormen opgenomen:
  - Eén die kan worden geïnstalleerd op een mobiele telefoon; en
  - Eén die in een cloud-oplossing is opgenomen. Denk bijvoorbeeld aan MijnOverheid.nl.
  - Een variant hierop is een datakluis. Deze heeft geen wallet-functionaliteit en kan alleen worden gebruikt om gegevens op te slaan en beschikbaar te stellen aan de NL Wallet.
- NL kernvoorzieningen. Dit betreft de overheidsvoorzieningen die nodig zijn om onder andere:
  - DBI-beheervoorziening.
    - DBI's te kunnen uitgeven en beheren.
    - Attestaties die zijn gebaseerd op een DBI uit te geven, beheren en valideren.
    - Het overzicht van geautoriseerde dienstaanbieders te beheren en validatieverzoeken uit te voeren
  - eIDAS knooppunt NL.
    - Diensten af te nemen af te nemen van dienstaanbieder uit andere lidstaten.
    - Diensten aan te bieden aan ingezetenen uit andere lidstaten.
- NL aanvullende voorzieningen. Dit zijn:
  - (bestaande) overheidsvoorzieningen die ondersteunende functionaliteit bieden.
- NL vertrouwende partijen.
  - Hiermee worden de applicatiecomponenten bedoeld van Nederlandse publieke en private vertrouwende partijen.
- NL (gekwalificeerde) verleners van vertrouwensdiensten.
  - Dit betreft de applicatiecomponenten en gegevensverzamelingen van (gekwalificeerde) verleners van vertrouwensdiensten.
- Overige lidstaten EU.
  - Dit zijn enerzijds de applicatiecomponenten van publieke en private gekwalificeerde) verleners van vertrouwensdiensten en vertrouwende partijen en anderzijds de component waarmee gegevens kunnen worden uitgewisseld met Nederlandse applicatiecomponenten.

## 4.6 Verdieping: functionaliteiten DBI-beheervoorziening

De DBI-beheervoorziening stelt minimaal de volgende functionaliteiten beschikbaar.

| Functionaliteit | Opmerking |
|---|---|
| Aanvragen en uitgeven DBI. | |
| Beheren DBI. | |
| Beheren overzicht geautoriseerde NL Wallets. | |
| Beheren overzicht geautoriseerde dienstaanbieders. | |
| Beheren dienstencatalogus. | |
| Uitgeven attestatie. | |
| Verifiëren geldigheid NL Wallet. | |
| Verifiëren geldigheid attestatie. | |
| Verifiëren geldigheid dienstaanbieder. | |
| (Tijdelijk) blokkeren specifieke versie NL Wallet. | |

| Functionaliteit | Opmerking |
|---|---|
| (Tijdelijk) blokkeren DBI/wallet. | |
| (Tijdelijk) blokkeren attestatie. | |
| (Tijdelijk) blokkeren dienstaanbieder. | |
| Revoceren NL Wallet. | |
| Revoceren attestatie. | |
| Verzamelen statistieken. | |

## 4.7 Een verdieping: NL Wallet

Onderstaande beschrijving van de NL Wallet, een verschijningsvorm van de Europese portemonnee voor digitale identiteit, is ontleend aan de concept-verordening. Voor het gemak wordt in het vervolg op de volgende manier verwezen naar het relevante lid van het artikel: '(6 bis 4(a))'.

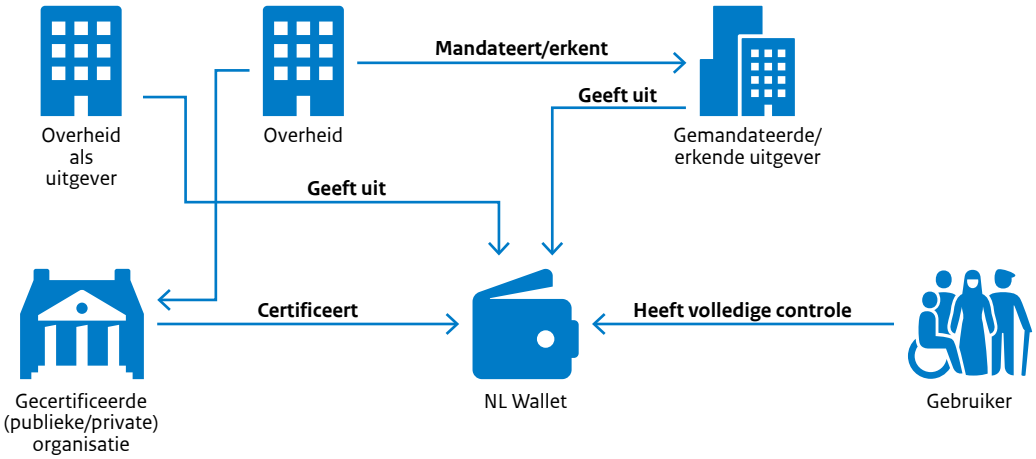
*Enkele algemene kenmerken van de NL Wallet (6 bis 2, 6 bis 4(b), 6 bis 6, 6 bis7, 6 bis 10, 45 septies, 45 bis)*

- De NL Wallet kan worden uitgegeven door de Nederlandse overheid of een, door de overheid, gemandateerde of erkende partij.[29] De laatste twee situaties laten de mogelijkheid om het uitgeven van de NL Wallet over te laten aan private organisaties. Wel is een overheidsorganisatie nodig om partijen te mandateren/erkennen.
- De NL Wallet dient in alle gevallen te voldoen aan eIDAS-betrouwbaarheidssniveau 'Hoog'. Dat heeft ook gevolgen voor de aanvraag-, uitgifte- en activatieprocessen.[30]
- De NL Wallet moet worden gecertificeerd. De certificering wordt uitgevoerd door een door de overheid aangewezen publieke of private organisatie.
- De Nederlandse overheid kan de uitgifte van de NL Wallet opschorten en de geldigheid van (een specifieke versie van) de NL Wallet intrekken. Ook informeert de overheid de Europese Commissie en de overige lidstaten hiervan.
- De overheid kan een opschorting/intrekking herstellen. Ook hiervan worden de Europese Commissie en de overige lidstaten op de hoogte gesteld.
- De NL Wallet moet kosteloos te gebruiken zijn. Dat laatste laat overigens onverlet dat voor de activatie van een DBI wel kosten in rekening zouden kunnen worden gebracht.
- De gebruiker heeft de volledige controle over de NL Wallet.
- De uitgever van de NL Wallet mag geen informatie verzamelen over het gebruik ervan. Uitzondering is informatie over portemonneediensten.
- De NL Wallet moet waarborgen bevatten zodat verleners van gekwalificeerde attesteringen van attributen geen informatie ontvangen over het gebruik van de attributen.
- Een gekwalificeerde elektronische attestering van attributen heeft dezelfde rechtsgevolgen als wettelijk uitgegeven attesteringen op papier.

[29] De beschrijving van de NL Wallet in deze paragraaf is gebaseerd op de concept-verordening, artikel 6 bis

[30] Deze processen dienen te worden ingericht conform UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheids-niveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

*Afbeelding 9*




*Kernfunctionaliteit voor de gebruiker (6 bis 3, 6 bis 4 (a)(3), 6 bis 7, 11 bis 1)*

Een gebruiker kan met de NL Wallet:

- Wettelijke identiteitsgegevens en elektronische attesteringen van attributen inwinnen, verstrekken en opslaan (zie ook de paragraaf over de verschillende verschijningsvormen van de NL Wallet en over de datakluis).
- Wettelijke identiteitsgegevens en elektronische attesteringen van attributen eerst selecteren, eventueel combineren en vervolgens presenteren.[31]
  - Van 'presenteren' onderscheiden wij twee verschijningsvormen:
    - Tonen. Hier laat de gebruiker de gegevens/attesteringen zien aan een vertegenwoordiger van een vertrouwende partij. Er vindt dus geen geautomatiseerde gegevensoverdracht plaats. De vertegenwoordiger leest de gegevens/attesteringen van het scherm van de mobiele telefoon van de gebruiker.
    - Delen. In deze situatie verstuurt de gebruiker de gegevens/ attesteringen op een geautomatiseerde manier vanuit zijn NL Wallet naar de vertrouwende partij.
- Zich, na positieve identificatie, on- en offline authentiseren om publieke en private diensten af te nemen.
- Ondertekenen met gekwalificeerde elektronische handtekeningen.

*Eisen aan gekwalificeerde verleners van vertrouwensdiensten (24 lid 1, 45 decies lid 1)*

Een gekwalificeerde verlener van vertrouwensdiensten moet:

- De identiteit van een gebruiker (of diens specifieke attributen) verifiëren alvorens hij gekwalificeerde elektronische attesteringen van attributen afgeeft aan de betreffende gebruiker.
- Verleners van gekwalificeerde attesteringen van attributen mogen:
  - Geen informatie ontvangen over het gebruik van de door hen verstrekte attributen.
  - De via de NL Wallet ontvangen identiteitsgegevens niet combineren met identiteitsgegevens die zij hebben ontvangen t.b.v. andere vormen van dienstverlening.[32]

[31] De concept-verordening heeft het consequent over 'delen'. Wij zien echter een duidelijk onderscheid tussen tonen en delen vandaar dat hier het containerbegrip 'presenteren' wordt gebruikt. In de uitwerking over mobiele versus cloud-based NL Wallet wordt op de toepasbaarheid van tonen en delen ingegaan.

[32] Ook al staat hier expliciet de NL Wallet genoemd, dit geldt ook voor gegevens die zijn ontvangen via andere verschijningsvormen van de Europese portemonnee voor digitale identiteit. Dus bijv. een in België uitgegeven wallet.

Een gekwalificeerde verlener van vertrouwensdiensten kan:
- Een gekwalificeerd elektronisch register aanmaken.
  - Gebruikers hebben met zo'n register de beschikking over 'bewijs en een vaststaand controlespoor voor de volgorde van transacties en gegevensbestanden.'[33]
    - Dit impliceert dat gebruikers toegang moeten hebben tot gekwalificeerde elektronische registers van diverse gekwalificeerde verleners van vertrouwensdiensten.

### *Eisen aan vertrouwende partijen (6 bis 4 (a)(2), 4 (b), 6 ter 1, 6 ter 2, 12 quater 1)*

Vertrouwende partijen moeten:
- Het voorgenomen gebruik van de NL Wallet bij een overheidsloket melden.
- Identiteitsgegevens en elektronische attesteringen van attributen, die zij ontvangen via een wallet, authentiseren.
- Identiteitsgegevens en elektronische attesteringen van attributen valideren.
- Gebruikers authentiseren.
- Aanvragen voor diensten, gedaan met gecertificeerde wallets uit andere lidstaten, in behandeling nemen.

### *Eisen aan de overheid (6 bis 5, 6 ter 2, 20 lid 1, 45 quinquies lid 1)*

De overheid dient te voorzien in verschillende valideringmechanismen om:
- De authenticiteit en geldigheid van de NL Wallet te kunnen verifiëren.
  - Dat impliceert dat aan elke individuele uitgegeven NL Wallet een status moet kunnen worden toegekend.
- Vertrouwende partijen de mogelijkheid te geven om te controleren of door hen ontvangen elektronische attesteringen van attributen geldig zijn.
- Gekwalificeerde verleners van vertrouwensdiensten en vertrouwende partijen de gelegenheid geven om te controleren of de door hen ontvangen identiteitsgegevens (die zijn opgenomen in de bovengenoemde attestaties) authentiek en geldig zijn.
- Gekwalificeerde verleners van elektronische attesteringen van attributen de mogelijkheid te geven om de authenticiteit van attributen te kunnen verifiëren in een relevante authentieke bron.

Ook dient de overheid:
- Vertrouwenslijsten op te stellen met gekwalificeerde verleners van vertrouwensdiensten en de diensten die elke verlener aanbiedt.
- Een conformiteitsbeoordelingsorgaan in te richten. Dat orgaan voert minimaal eenmaal per 24 maanden een audit uit op de gekwalificeerde verleners van vertrouwensdiensten uit.

Het conformiteitsbeoordelingsorgaan kan de status van een verlener of van (een of meerdere van) zijn diensten intrekken.

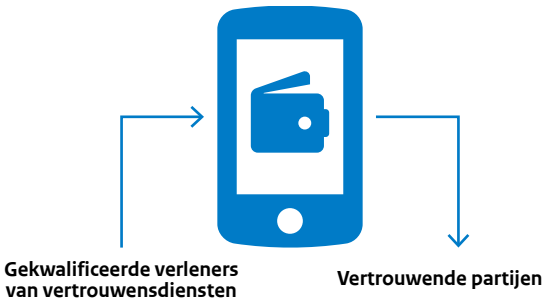
Daarnaast dienen de lidstaten te zorgen voor een gemeenschappelijk mechanisme om de authenticiteit van vertrouwende partijen te kunnen vaststellen.

[33] Voorstel voor een VERORDENING, blz. 9.

## 4.8 Een verdieping: mobiele versus cloud-based NL Wallet en de datakluis

Een wallet kent twee mogelijke verschijningsvormen:
1. Mobiel; en
2. Cloud-based.

***Afbeelding 10*** *mobiele wallet*



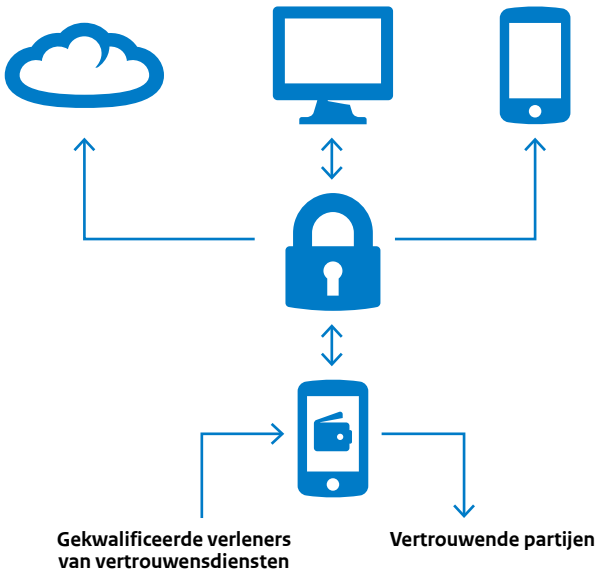

***Afbeelding 11*** *Cloud-based wallet*


Een mobiele wallet kan op zich worden gebruikt naast een cloud-based wallet. Maar het is ook mogelijk dat en gebruiker òf een mobiele òf een cloud-based wallet heeft.

Een datakluis is simpel gezegd een uitgeklede wallet. Het bevat alleen functionaliteit om gegevens op te slaan en te versturen naar de NL Wallet. Daarmee biedt een datakluis ook de mogelijkheid voor back-up & restore.

Met een datakluis kunnen dus geen diensten worden afgenomen van (gekwalificeerde) verleners van vertrouwensdiensten en vertrouwende partijen.

***Afbeelding 12*** *Datakluis*




Een datakluis kan in de cloud staan, op de PC of laptop of op de mobile telefoon van een gebruiker. In afbeelding 8 wordt ervan uitgegaan dat gegevens van de (gekwalificeerde) verleners van vertrouwensdiensten altijd naar de NL Wallet worden gestuurd en vanuit de wallet naar de datakluis. Op zich is het omgekeerde ook mogelijk. Alvorens een beslissing hierover kan worden genomen, zullen eerst de voor- en nadelen van deze twee opties in kaart worden gebracht.

## 4.9 Een verdieping: interactiepatronen

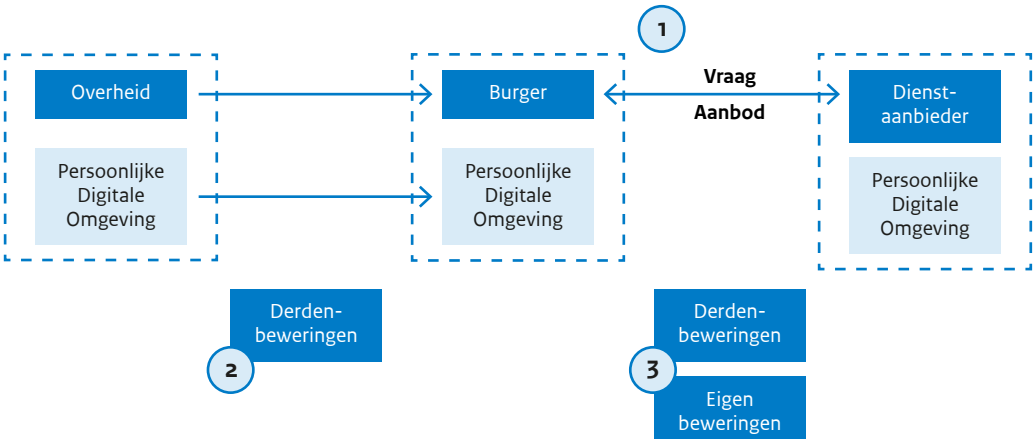
Het delen van gegevens kan op verschillende manieren gebeuren:[34]

1. De burger deelt zelf gegevens met een vertrouwende partij; of
2. De burger geeft (eenmalig?) toestemming aan een vertrouwende partij om bepaalde gegevens op te vragen bij een (gekwalificeerde) verleners van vertrouwensdiensten.

[34] Deze interactiepatronen zijn overgenomen van de Referentiearchitectuur Regie op Gegevens. Daar worden zij 'Burger wint in' resp. 'Dienstaanbieder wint in' genoemd.

In afbeelding 13 is het eerste interactiepatroon weergegeven.

***Afbeelding 13*** *Interactiepatroon 'Burger wint in'*




Onderstaande twee opsommingen zijn gebaseerd op de referentiearchitectuur van Regie op Gegevens en beschrijven het interactiepatroon:

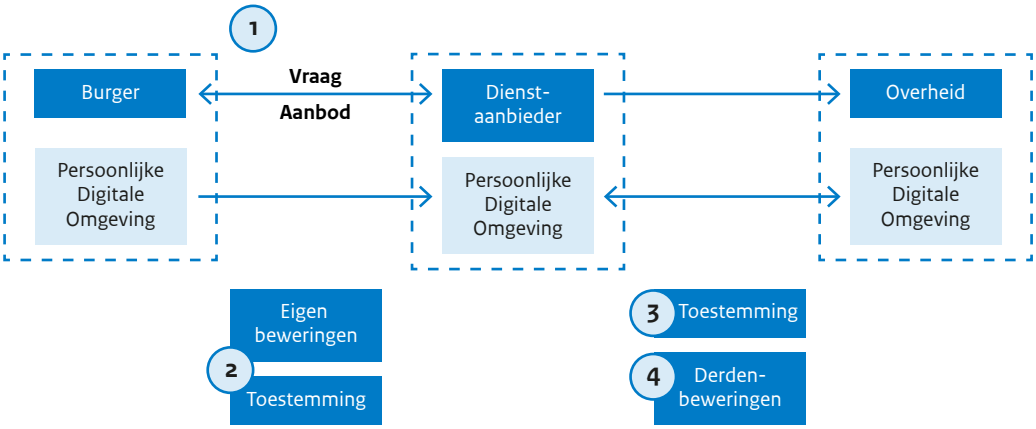
1. De burger wil een product of dienst afnemen van de dienstaanbieder. Om een aanbod te kunnen doen, heeft de dienstaanbieder (persoons)gegevens van/over de burger nodig. Een deel van die informatiepositie zal bestaan uit gegevens die de burger zelf kan/moet invullen (eigen beweringen) en een deel kan bestaan uit gegevens die (op verzoek van de dienstaanbieder) uit een andere bron afkomstig zal zijn, hier gedefinieerd als derdenbeweringen uit de bron van de overheid. Het deel van de informatiepositie dat de burger met eigen beweringen kan invullen, kan de burger direct aan de dienstaanbieder leveren.
2. Voor derdenbeweringen zal de burger dit gegeven eerst uit de bron van de overheid moeten ophalen en in zijn eigen Persoonlijke Digitale Omgeving moeten brengen. Als hij nog over een geldig gegeven uit de overheidsbron in zijn eigen Persoonlijke Digitale Omgeving beschikt, dan kan hij deze natuurlijk direct gebruiken en is ophalen bij de overheid niet nodig.
3. Als de burger de gevraagde gegevens voor de informatiepositie (dus derdenbeweringen en eigen beweringen) compleet heeft, kan hij deze aan de dienstaanbieder leveren zodat deze het aanbod kan doen.

Kenmerken van dit interactiepatroon zijn:

- De positie van de burger. Deze staat letterlijk tussen dienstaanbieder en de bron in en heeft by design volledig zicht en controle op de gegevens die vanuit de overheidsbron met de dienstaanbieder gedeeld worden.
- Geen koppeling tussen uitvraag bij de bron en doel waarvoor het gebruikt wordt: de burger hoeft niet aan de bronhouder te verantwoorden waarom/waarvoor het persoonsgegeven ingewonnen wordt.
- De wens van het waarmerk: de dienstaanbieder wil de garantie dat het gegeven uit de bron (de derdenbewering) ook daadwerkelijk van die bron afkomstig is en overeenkomt met die bron. Hier speelt de vertrouwensservice (trustservices uit eIDAS) een grote rol.
- Het onderwerp toestemming (niet zijnde wettelijke vertegenwoordiging) maakt geen onderdeel uit van dit interactiepatroon.

Onderstaande afbeelding geeft het tweede interactiepatroon weer.

***Afbeelding 14*** *Interactiepatroon 'Dienstaanbieder wint in'*




Onderstaande twee opsommingen zijn gebaseerd op de referentiearchitectuur van Regie op Gegevens en beschrijven het interactiepatroon:

1. Ook dit interactiepatroon start met de relatie tussen dienstaanbieder en de burger. Om een aanbod te kunnen doen heeft de dienstaanbieder (persoons)gegevens van/over de burger nodig. Een deel van die informatiepositie zal bestaan uit eigen beweringen en (mogelijk) een deel uit derdenbeweringen.
2. Het verschil met het vorige interactiepatroon is dat niet de burger de derdenbewering inwint, maar de dienstaanbieder aanbiedt om dat namens deze burger te doen. Het is dus de dienstaanbieder die zich bij de overheid digitaal meldt met het verzoek om een persoonsgegeven uit de bron van de overheid. De bronhouder zal vanwege zijn geheimhoudingsplicht deze gegevens alleen ter beschikking stellen indien de dienstaanbieder als gevolmachtigde van de burger optreedt, m.a.w. de dienstaanbieder toestemming heeft van de burger om namens hem de persoonsgegevens bij de overheid in te winnen.
3. De dienstaanbieder wint met toestemming van de burger zijn persoonsgegevens (derdenbeweringen) in bij de overheid.
4. De overheid deelt - na validatie van het verzoek – de derdenbeweringen met de dienstaanbieder.

Kenmerken van dit interactiepatroon zijn:

- De positie van de burger. In dit interactiepatroon staat de dienstaanbieder tussen de burger en de bron in. Vanuit deze positie heeft de burger by design veel minder zicht en controle op de gegevens die vanuit de overheidsbron met de dienstaanbieder gedeeld worden. Om de burger toch vertrouwen te geven in zowel dienstaanbieder als overheid en hem uit vrij wil te bewegen gebruik te maken van deze dienst, zijn aanvullende maatregelen gericht op dit vertrouwen noodzakelijk.
- Het onderwerp toestemming maakt altijd onderdeel uit van dit interactiepatroon.
- Koppeling tussen uitvraag bij de bron en doel waarvoor het gebruikt wordt: de burger geeft toestemming aan de dienstaanbieder om gegevens namens hem in te winnen. De eis aan de toestemming is dat deze voldoende specifiek en afgebakend is (dus geen toestemming zoals dat nu bij bijv. cookies het geval is). Hierdoor kan de overheid mogelijk afleiden welke gegevens, waarvoor en aan wie geleverd worden.
- De wens van het waarmerk is in dit interactiepatroon minder relevant: de dienstaanbieder haalt namelijk zelf de gegevens rechtstreeks bij de vertrouwde bron en heeft daarmee al de nodige garanties op afzender en integriteit van het gegeven. Hier speelt de vertrouwensservice (trust-services uit eIDAS) dus minder een rol. Natuurlijk staat het de dienstaanbieder vrij om tegen vergoeding extra vertrouwensservices zoals digitale handtekening en/of digitale seal te gebruiken.
- Het moment waarop de burger volmacht (toestemming) verleent en aan wie kan verschillen en leiden tot een variant op bovenstaand interactiepatroon. Het is namelijk ook mogelijk dat de burger zijn wilsuiting (toestemming tot het leveren van vooraf gedefinieerde persoonsgegevens aan vooraf gedefinieerde dienstaanbieders in vooraf gedefinieerde gevallen) aan de overheid kenbaar maakt voordat de dienstaanbieder een verzoek bij de overheid tot het leveren van specifieke persoons-

gegevens voor deze burger doet. De overheid zal dan in haar eigen administratie moeten nagaan of de specifieke toestemming van die burger bestaat om vervolgens dit gegeven met toestemming van die burger aan de dienstaanbieder te kunnen leveren.

Beide interactiepatronen geven uiteindelijk hetzelfde resultaat. De eisen van de interactiepatronen (bijvoorbeeld waarmerken en toestemming) zijn echter anders.

Een belangrijk uitgangspunt van Regie op Gegevens is dat de burger vrij is in zijn keuze voor een interactiepatroon. Dat kan dus per dienstafname anders zijn.

## 4.10 Een verdieping: digitaal rijbewijs

Vooruitlopend op de definitieve versie van de 'use case #3 Mobile Driving License' is in deze paragraaf een mogelijke uitwerking daarvan binnen het identiteitsecosysteem uitgewerkt.

In afbeelding 15 zijn de gegevens benoemd die op het rijbewijs staan vermeld.

***Afbeelding 15*** *Attributen van het rijbewijs*

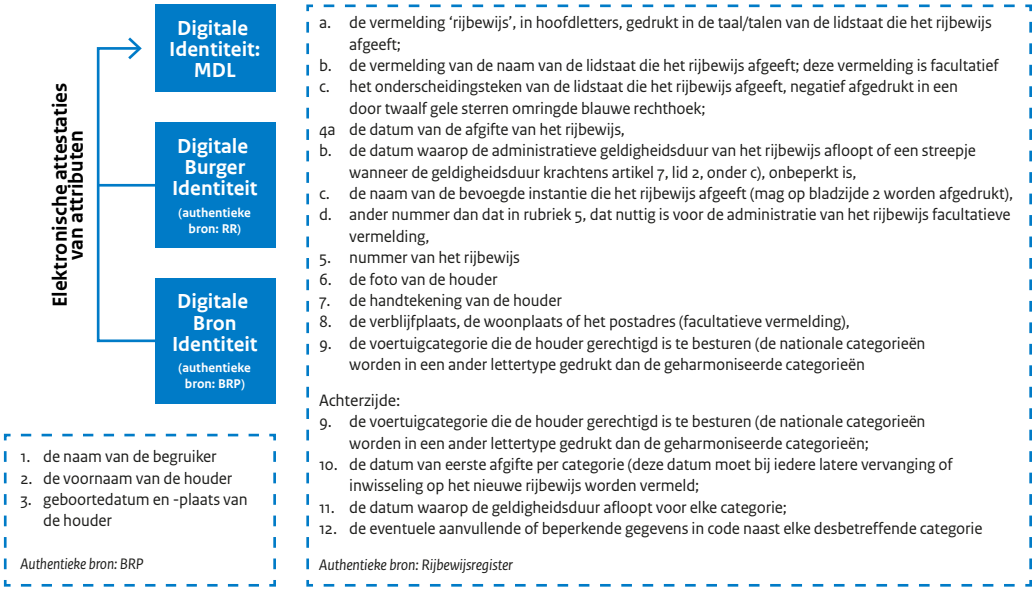

Voorzijde
a) de vermelding „rijbewijs", in hoofdletters, gedrukt in de taal/talen van de lidstaat die het rijbewijs afgeeft;
b) de vermelding van de naam van de lidstaat die het rijbewijs afgeeft; deze vermelding is facultatief;
c) het onderscheidingsteken van de lidstaat die het rijbewijs afgeeft, negatief afgedrukt in een door twaalf gele sterren omringde blauwe rechthoek;
1. de naam van de houder,
2. de voornaam van de houder,
3. geboortedatum en -plaats van de houder,
4. a. de datum van afgifte van het rijbewijs,
b. de datum waarop de administratieve geldigheidsduur van het rijbewijs afloopt of een streepje wanneer de geldigheidsduur krachtens artikel 7, lid 2, onder c), onbeperkt is,
c. de naam van de bevoegde instantie die het rijbewijs afgeeft (mag op bladzijde 2 worden afgedrukt),
d. ander nummer dan dat in rubriek 5, dat nuttig is voor de administratie van het rijbewijs (facultatieve vermelding),
5. nummer van het rijbewijs,
6. de foto van de houder,
7. de handtekening van de houder,
8. de verblijfplaats, de woonplaats of het postadres (facultatieve vermelding),
9. de voertuigcategorie die de houder gerechtigd is te besturen (de nationale categorieën worden in een ander lettertype gedrukt dan de geharmoniseerde categorieën);

Achterzijde:
9. de voertuigcategorie die de houder gerechtigd is te besturen (de nationale categorieën worden in een ander lettertype gedrukt dan de geharmoniseerde categorieën);
10. de datum van eerste afgifte per categorie (deze datum moet bij iedere latere vervanging of inwisseling op het nieuwe rijbewijs worden vermeld);
11. de datum waarop de geldigheidsduur afloopt voor elke categorie;
12. de eventuele aanvullende of beperkende gegevens in code naast elke desbetreffende categorie

Een deel van deze gegevens zijn afkomstig uit het BRP als authentieke bron. De overige gegevens zijn afkomstig uit het Centraal Rijbewijzenregister als authentieke bron van de Dienst Wegverkeer RDW).

In afbeelding 16 zijn de bronnen van de gegevens anders weergegeven, namelijk: de Digitale Bronidentiteit (met BRP als authentieke bron) en de Digitale burgeridentiteit (met voor deze use case het Rijbewijsregister als authentieke bron).

***Afbeelding 16*** *Authentieke bronnen*



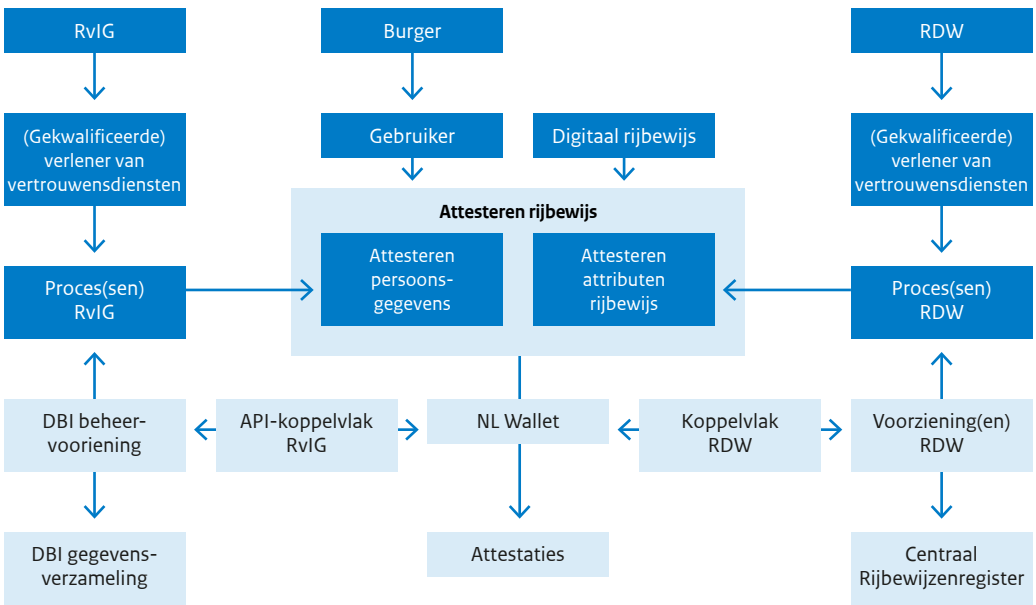

Attributen uit zowel de Digitale Bron- als Burgeridentiteit worden via attestaties beschikbaar gesteld aan de burger en vormen tezamen zo een digitaal rijbewijs.

Hieronder is een tweetal mogelijke uitwerkingen van het identiteitsecosysteem voor het digitale rijbewijs weergegeven en beschreven. Let op: dit zijn slechts voorbeelden; de uiteindelijke uitwerking dient te worden gedaan in samenwerking met o.a. de RDW!

In beide uitwerkingen vraagt een burger om zijn digitale rijbewijs (lees: neemt hij de dienst 'Attesteren rijbewijs' af).

In uitwerking 1 (afbeelding 17) vraagt de burger (lees: de NL Wallet) gegevens over de rijbevoegdheid op bij de RDW en persoonsgegevens (voor- en achternaam, geboortedatum) bij RvIG. In deze uitwerking worden de individuele authentieke bronnen dus direct bevraagd door de burger (lees: NL Wallet).

***Afbeelding 17*** *Ecosysteem digitaal rijbewijs - uitwerking 1*

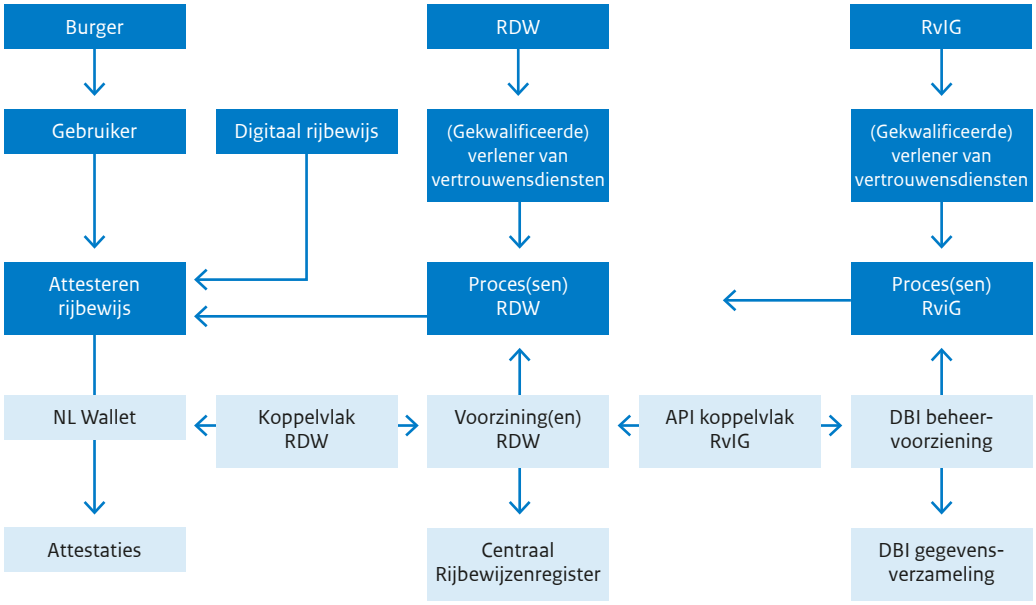


Deze uitwerking impliceert ook dat de dienstaanbieder aan wie de burger zijn digitale rijbewijs (in de vorm van een of meerdere attestaties) toezendt, bij beide authentieke bronnen de geldigheid van de attestaties verifieert.

In uitwerking 2 (afbeelding 18) vraagt de burger (lees: de NL Wallet) alle gegevens op bij de RDW. RDW vraagt vervolgens de relevante persoonsgegevens op bij RvIG. In deze uitwerking is de RDW dus het enige aanspreekpunt voor de burger. Tussen RDW en RvIG bestaan afspraken over onder welke voorwaarden RDW welke gegevens mag opvragen.

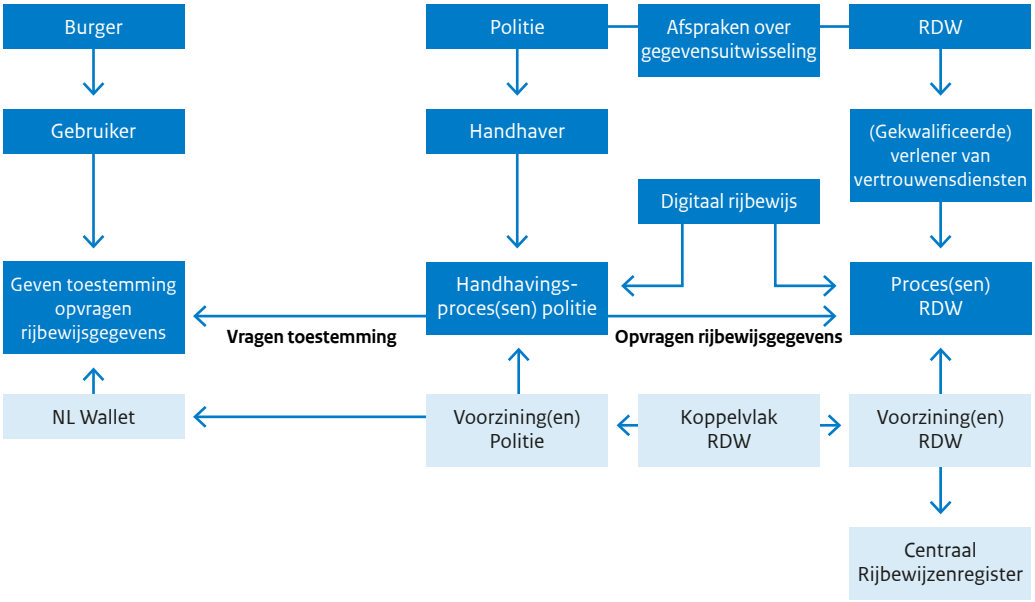
Enkele vragen bij deze uitwerking:
- Vraagt RDW eenmalig de attestaties op bij RvIG en neemt RDW vervolgens een 'abonnement' op wijzigingen in de status van de attestaties? Of vraagt RDW de attestaties op als de burger RDW vraagt om zijn digitale rijbewijs?
- Bevraagt de verifiërende organisatie RDW of RvIG over de geldigheid van de attestaties die uit de DBI-beheervoorziening komen?

***Afbeelding 18*** *Ecosysteem digitaal rijbewijs - uitwerking 2*




Een andere mogelijkheid is dat een vertrouwende partij, analoog aan interactiepatroon 2, de rijbewijsgegevens opvraagt bij de bron. In onderstaande afbeelding is de politie die vertrouwende partij. De politie vraagt eerst toestemming aan de burger. Ervan uitgaande dat de burger die toestemming geeft, vraagt de politie vervolgens de rijbewijsgegevens op bij de RDW.

***Afbeelding 19*** *Ecosysteem digitaal rijbewijs – uitwerking 3*




## 4.11 Niet-functionele vereisten

Voor de 'use case #3 Mobile Driving License' zijn inmiddels veel eisen/wensen op papier gesteld. Een aantal kan wellicht ook gelden voor soortgelijke use cases (lees: dienstverlening):

- Een verificatie van attestaties moet gemiddeld minder dan drie seconden duren, maar mag maximaal tien seconden in beslag nemen.
- De beschikbaarheid van de voorzieningen t.b.v. verificatie is gesteld op 99,9%.

# 5 Aanbevelingen

- RvIG kan niet 'in splendid isolation' het identiteitsecosysteem uitwerken. Alle individuele dienstaanbieders – of vertegenwoordigers daarvan – moeten worden betrokken. Alleen dan kan interoperabiliteit worden gegarandeerd.
- Bepaal aan de hand van een geprioriteerd overzicht van diensten/producten, wanneer een dienstaanbieder, of zijn vertegenwoordiger, (uiterlijk) moet zijn betrokken bij het identiteitsecosysteem.
  - Stel een architectuurberaad in. Deelnemers zijn (enterprise) architecten van alle organisaties die een rol (gaan) spelen in het identiteitsecosysteem. Doel van het beraad zou moeten zijn o.a. het onderling bespreken en afstemmen van het identiteitsecosysteem.
- De conceptverordening kan inhoudelijk nog worden aangepast en moet nog worden aangenomen door het Europees Parlement.[35] Daarnaast staat in de conceptverordening dat de Europese Commissie meerdere uitvoeringshandelingen gaat publiceren. Het is dan ook van belang om de ontwikkelingen over de verordening nauwgezet in de gaten te houden.

[35] https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021PC0281&qid=1638281061733 (30-11-2021).

Dit is een uitgave van:

**Rijksdienst voor Identiteitsgegevens**
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Postbus 10451 | 2501 HL Den Haag

December 2022