Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programmeringsraad GDI
www.pgdi.nl
www.noraonline.nl/wiki/GDI-Architectuur_(GA)
Postbus.pgdi@minbzk.nl

GDI-Architectuur

Identificatie & authenticatie

Onderdeel van het domein Toegang

Datum : 26 augustus 2022
Versie : 1.0
Status : Definitief

Projectnaam GDI-Architectuur
Organisatie Bureau MIDO
Contact postbus.pgdi@minbzk.nl

Versiehistorie

Datum	Versie	Auteur	Opmerkingen
11 oktober 2021	0.1	Wim Bakkeren	Versie voor review kerngroep GA
2 november 2021	0.2	Wim Bakkeren	Eerste review kerngroep verwerkt
6 december 2021	0.3	Wim Bakkeren Bob te Riele	Tweede review kerngroep en programma Toegang verwerkt
24 december 2021	0.4	Wim Bakkeren Bob te Riele Tom Peelen	Derde review kerngroep en programma Toegang verwerkt Versie voor review door klankbordgroep GA
21 februari 2022	0.8	Wim Bakkeren Bob te Riele Tom Peelen	Review klankbordgroep en behandeling in sponsorgroep verwerkt
26 augustus 2022	1.0	Wim Bakkeren Bob te Riele Tom Peelen	Tweede review klankbordgroep, behandeling sponsorgroep en akkoord PGDI verwerkt.

Inhoud

1 Inleiding

Dit document bevat de uitwerking van de GDI-Architectuur (GA)[1] voor het subdomein Identificatie en authenticatie, onderdeel van het domein Toegang. Het document bouwt voort op het resultaat van de werkgroep Identificatie en authenticatie van de pressurecooker. In deze pressurecooker is medio 2020 in opdracht van het ministerie van Binnenlandse zaken en Koninkrijksrelaties een versnelling aangebracht in de uitwerking van de strategie voor de Generieke Digitale Infrastructuur (GDI).[2] De resultaten van de pressurecooker zijn overgedragen aan het project GA om verder door te ontwikkelen tot onderdelen van de GDI-Architectuur.[3] Dit document verwerkt het pressurecooker-rapport in de voor de GA gehanteerde architectuurmethode en documentstructuur met kaders, generieke functies, principes en keuzes voor afspraken, standaarden en generieke voorzieningen.[4]

Het document heeft de volgende indeling, zoals ook weergegeven in de afbeelding hieronder:

- Hoofdstuk 1 is deze inleiding.
- Hoofdstuk 2 is een algemene inleiding tot de GDI-Architectuur. Het beschrijft de context voor het onderdeel van de GDI-Architectuur dat is uitgewerkt in dit document.
- Hoofdstukken 3 en 4 beschrijven de kaders voor identificatie en authenticatie. Hoofdstuk 3 beschrijft wat we verstaan onder identificatie en authenticatie. Hoofdstuk 4 beschrijft de wettelijke en beleidskaders, de relevante maatschappelijke en technische ontwikkelingen en de scope.
- Hoofdstuk 5 beschrijft de generieke functies voor identificatie en authenticatie.
- Hoofdstuk 6 beschrijft de principes: de algemene regels en richtlijnen die richting geven aan de keuzes voor afspraken, standaarden en voorzieningen.
- Hoofdstuk 7 beschrijft de keuzes en de afspraken, standaarden en generieke voorzieningen die daaruit volgen en die invulling geven aan de generieke functies.
- Bijlage 8 bevat de lijst met begrippen.
- Bijlage 9 beschrijft de belangrijkste verschillen met het pressurecooker-rapport voor het subdomein identificatie en authenticatie.

De in dit document gebruikte begrippen die GDI-Architectuur-breed van toepassing zijn, zijn opgenomen in het GA-begrippenkader. Dit begrippenkader is ten behoeve van de lezer in zijn volledigheid opgenomen in de bijlage en bevat ook begrippen die in dit document niet worden gebruikt. In die bijlage zijn aan de GDI-brede begrippen de begrippen die specifiek zijn voor identificatie en authenticatie.

[1] GA werd voorheen GO (Gemeenschappelijke Overheidsarchitectuur) genoemd. Met de wijzigingen in de besturing van de GDI en de overgang van de Programmeringsraad Logius naar de Programmeringsraad GDI is GO hernoemd naar GA.

[2] De pressurecooker-rapporten zijn beschikbaar op NORA online.

[3] De GDI-Architectuur (GA) vormt de doelarchitectuur van de Generieke Digitale Infrastructuur (GDI) die het Meerjarenprogramma Infrastructuur Digitale Overheid (MIDO) helpt om te sturen op de ontwikkeling van de GDI.

[4] De beschrijving van de GA-architectuurmethode is beschikbaar op NORA online.

2 Inleiding GA

De GDI-Architectuur (GA)[5] vormt de doelarchitectuur voor de Generieke Digitale Infrastructuur (GDI) die het Meerjarenprogramma Infrastructuur Digitale Overheid (MIDO) helpt om te sturen op de ontwikkeling van de GDI.

2.1 Wat is de GDI?

De bouwstenen van de GDI, zoals DigiD, MijnOverheid, Digipoort en ook gegevensuitwisseling met de basisregistraties zijn onmisbaar voor de digitale publieke dienstverlening aan burgers en bedrijven.[6] Samen met andere gezamenlijke bouwstenen vormen zij de ruggengraat van de digitale overheid. Deze bouwstenen (afspraken, standaarden en voorzieningen) ondersteunen dienstverleners met een publieke taak bij de inrichting van hun digitale dienstverlening aan burgers en bedrijven en waar nodig bij hun onderlinge digitale samenwerking. We noemen deze ruggengraat de "Generieke Digitale Infrastructuur" (GDI).

2.2 Hoe vindt sturing op de GDI plaats?

Voor gemeenschappelijke sturing op de digitale overheid heeft de staatssecretaris Koninkrijksrelaties en Digitalisering het Meerjarenprogramma Infrastructuur Digitale Overheid (MIDO) ingesteld:[7]

- Het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) dat tot taak heeft de staatssecretaris van BZK te adviseren over het beleid voor de digitale overheid.
- De Programmeringsraad GDI (PGDI) die het OBDO adviseert over de gewenste prioritering en programmering van de doorontwikkeling van de afspraken, standaarden en voorzieningen van de GDI.
- De Programmeringstafels voor de domeinen Toegang, Interactie, Gegevensuitwisseling en Infrastructuur die de PGDI adviseren met betrekking tot de functionaliteiten in het domein.

5 De GDI-Architectuur (GA) werd voorheen Gemeenschappelijke Overheidsarchitectuur (GO) genoemd.
6 Zie De 'WHY' van de Generieke Digitale Infrastructuur (noraonline.nl)
7 Besluit Sturing Digitale Overheid

- De Architectuurraad ter ondersteuning van OBDO, PGDI en programmeringstafels, die de hoeder is van de architectuur(producten) van de GDI en een toetsende en adviserende rol heeft binnen de vastgestelde architectuurkaders voor de GDI.

2.3 Wat is GA?

De GDI-Architectuur (GA), bestaande uit o.a. een aantal domeinarchitecturen, biedt, als ware het een bestemmingsplan, inzicht in de beoogde ontwikkeling van de GDI. Het doel daarvan is voor MIDO een referentie te hebben bij besluitvorming over programma's en projecten en bij de bepaling van de impact op de GDI van nieuwe beleidsvoornemens. Aan beheerorganisaties van GDI-bouwstenen geeft het richting bij het aanpassen of ontwikkelen van deze GDI-bouwstenen. Uitvoeringsorganisaties e.a. die de GDI gebruiken, kunnen ermee anticiperen op het inzetten van GDI-bouwstenen.

De GA is opgedeeld in de volgende vier domeinen, aansluitend bij de programmeringstafels van MIDO.

Domein: Toegang
Het domein Toegang bestaat uit twee subdomeinen. Het subdomein Identificatie & authenticatie omvat de bouwstenen vanuit de GDI om burger, bedrijf, instelling, intermediair uniek te identificeren en authenticeren ten behoeve het verlenen van toegang tot publieke diensten. Het subdomein Machtigen & vertegenwoordigen omvat de bouwstenen om de bevoegdheid tot het digitaal handelen namens een ander vast te stellen.

Domein: Interactie
Het domein Interactie omvat de bouwstenen van de GDI ten behoeve van elektronische informatie-uitwisseling met burgers, bedrijven, instellingen, intermediairs en hun gemachtigden. Uitwisseling ten behoeve van Toegang is hiervan uitgezonderd.

Domein: Gegevensuitwisseling
Het domein Gegevensuitwisseling omvat de bouwstenen van de GDI voor uitwisseling van gegevens tussen informatiesystemen van overheidsorganisaties onderling en met informatiesystemen van andere organisaties.

Domein: Infrastructuur
Het domein Infrastructuur omvat de bouwstenen van de GDI die van algemeen belang (ofwel: infrastructureel) zijn voor de GDI en die veelal een basis vormen voor de bouwstenen van de andere drie domeinen.

De GA omvat de volgende architectuurproducten. Zodra producten gereed zijn worden ze gepubliceerd op NORA-online:[8]

GA productgroep	Toelichting
Opdracht en aanpak	• Het Besluit Sturing Digitale Overheid en het document "Architectuurfunctie GDI" beschrijven de opdracht van de Architectuurraad GDI. • Het jaarplan bevat de planning voor de activiteiten in het lopende jaar.
Visie	• De "WHY van de GDI" beschrijft waarom overheidsorganisaties samen een GDI nodig hebben voor de digitale overheid. • De architectuurvisie beschrijft de principes voor inrichting van de GDI die voortkomen uit maatschappelijke en technologische ontwikkelingen.
Werkwijze & kaders	• De architectuurmethode beschrijft een aantal afspraken over de manier waarop de GA wordt vormgegeven. • De GA-basisprincipes zijn een aanvulling op de NORA-principes die samen de onderbouwing zijn voor keuzen die de GA maakt. • De GA-begrippen zijn algemene begrippen die gebruikt worden in de GA.
Uitwerking domeinen	• De uitwerking van de domeinen bevat de richtinggevende keuzen van de GA ten aanzien van de generieke functies en bijbehorende afspraken, standaarden en voorzieningen. Deze keuzen zijn per

[8] Zie https://www.noraonline.nl/wiki/GDI-Architectuur_(GA)

	domein en soms sub-domein in afzonderlijke documenten opgenomen. • De pressurecooker-documenten bevatten de generieke functies per domein of sub-domein die in de GA verder worden uitgewerkt tot richtinggevende keuzen.

Bovenstaande producten dienen als referentie bij toetsen van en adviezen over nieuwe ontwikkelingen in de GDI.

2.4 Hoe komt GA tot stand en wordt GA geïmplementeerd?

De GDI-Architectuur (GA) wordt binnen MIDO continu onderhouden, zodat de architectuur blijft aansluiten bij ontwikkelingen in de maatschappij en de (digitale) overheid. De uitwerkingen baseren zich daarbij zowel op (wettelijke) kaders, beleidskaders en architectuurprincipes van NORA als op de visie en architectuurprincipes van GA zelf. GA heeft een architectuur-backlog waaruit uitbreidingen en verandering op prioriteit worden opgepakt.[9] De Architectuurraad is verantwoordelijk voor ontwikkeling en onderhoud van de GA en wordt daarin ondersteund door werkgroepen met architecten, een klankbordgroep en het bureau MIDO. De Architectuurraad en haar taken en verantwoordelijkheden in de totstandkoming van GA worden beschreven in de architectuurparagraaf van het MIDO-kader[10]. De werkwijze van de Architectuurraad, werkgroepen, klankbordgroep e.a. is eind 2021 uitgewerkt en vastgesteld.

De GA is een bestemmingsplan dat de op lange termijn beoogde doelarchitectuur van de GDI beschrijft. Om de benodigde transitie naar de doelarchitectuur in goede banen te leiden, kent MIDO een GDI-programmeringsplan. Om dit tot stand te brengen moet een roadmap opgesteld worden met belanghebbenden waarin vanuit de huidige architectuur in stappen naar de doelarchitectuur toegewerkt wordt. Het GDI-programmeringsplan weegt belangen van burgers, bedrijven, overheidsbeleid, uitvoering, beheer e.a. om tot een juiste planning te komen. Dit programmeringsplan maakt geen deel uit van de GA.

Het GDI-programmeringsplan is input voor beheerders die GDI-bouwstenen realiseren en voor gebruikers die GDI-bouwstenen toepassen. Op basis van de roadmap worden plannen voor ontwikkeling respectievelijk aansluiting uitgewerkt om de binnen MIDO gemaakte afspraken in te vullen.

2.5 Meer informatie

Meer informatie over MIDO en de GDI-Architectuur is te vinden op:

- https://pgdi.nl/
- http://www.noraonline.nl/wiki/GDI-Architectuur_(GA)
- https://pgdi.nl/ga/
- mailto:postbus.pgdi@minbzk.nl

[9] De GA-backlog is beschikbaar op de website pgdi.nl.
[10] Zie conceptuitwerking van de Architectuurraad (toen nog 'Architectuurboard'), is behandeld in de PGDI van 25-11-2021.

3 Wat is identificatie en authenticatie?

3.1 Wat verstaan we onder identificatie en authenticatie?

Identificatie is het uniek duiden van een entiteit[11] in een bepaalde context. Het geeft antwoord op de vraag: welke entiteit is het? Authenticatie is het bevestigen van de door de entiteit geclaimde identiteit. Het geeft antwoord op de vraag: is het inderdaad de entiteit die het claimt te zijn?

'Identificatie en authenticatie' kent meerdere toepassingen. Deze versie van de architectuur gaat in op digitale identificatie en authenticatie van natuurlijke personen voor het verlenen van toegang tot digitale publieke diensten, zowel in het burger- als in het bedrijven- en organisatiedomein. We spreken daarom in deze versie van de architectuur over identificatie en authenticatie van personen en niet van entiteiten. Identificatie en authenticatie van andere entiteiten dan natuurlijke personen komt in volgende versies van de architectuur aan bod.

We noemen de natuurlijke persoon die toegang vraagt tot een digitale dienst de handelend persoon. De handelend persoon wordt in dit document ook wel persoon of gebruiker (van een identificatiemiddel) genoemd. De handelend persoon kan namens zichzelf handelen, maar ook namens een ander natuurlijk of niet-natuurlijk persoon. Bij het handelen namens een ander spreken we over vertegenwoordiging. Vertegenwoordiging is geen onderwerp van deze architectuur, maar van de GDI-Architectuur voor 'Machtigen en vertegenwoordigen'.[12]

Bij digitale dienstverlening, waarbij er geen fysiek contact is tussen dienstverlener en handelend persoon, moet identificatie en authenticatie digitaal plaats kunnen vinden. Zowel om te kunnen bepalen of de persoon toegang tot de dienst mag krijgen, als om op de persoon afgestemde dienstverlening te kunnen bieden. Zowel voor het verlenen van toegang als voor het afstemmen van de dienstverlening op de persoon zijn vaak meer gegevens nodig dan alleen de vastgestelde identiteit. Zo kan het van belang zijn of de persoon meerderjarig is of over de juiste beroepsregistratie beschikt. Het verkrijgen en beoordelen van deze aanvullende gegevens is niet in scope van deze architectuur.

Onder digitale identificatie verstaan we het proces van het gebruiken van identificatiegegevens in digitale vorm die op unieke wijze een persoon aanduiden.[13] Onder identificatiegegevens verstaan we een verzameling gegevens aan de hand waarvan de identiteit van een persoon kan worden vastgesteld.[14] Onder digitale authenticatie verstaan we een digitaal proces dat de bevestiging van de digitale identificatie van een persoon in digitale vorm mogelijk maakt.[15] Als we hierna spreken over identificatie en authenticatie dan bedoelen we steeds de digitale vorm ervan.

Voor authenticatie wordt gebruik gemaakt van een identificatiemiddel: een materiële en/of immateriële eenheid die identificatiegegevens bevat waarmee de identiteit van een persoon is aan te tonen.[16] Bij een identificatiemiddel horen authenticatiefactoren waarover alleen de te authenticeren persoon beschikt en waarmee hij kan aantonen de identiteit te hebben die hij claimt te hebben. Voorbeelden van authenticatiefactoren zijn wachtwoorden, codes van een authenticator-app of uit een SMS-bericht op een telefoon in bezit van de persoon en biometrische kenmerken.

Andere onderdelen en toepassingen van identificatie en authenticatie komen in volgende versies of in andere onderdelen van de GDI-Architectuur aan bod. Zie voor de precieze scope van deze versie van de architectuur paragraaf 4.4. Onder andere het volgende komt niet aan bod in deze versie van de architectuur:

- identificatie en authenticatie van andere soorten zelfstandig handelende (ook wel: autonome) entiteiten, zoals informatiesystemen, apparaten en objecten;[17]
- identificatie en authenticatie voor andere doeleinden dan toegang tot digitale diensten, zoals ondertekening en wilsuiting;
- identificatie en authenticatie van de dienstverlener, zowel richting de handelend persoon als bij de samenwerking met andere overheidsorganisaties. Identificatie en authenticatie

11 Een natuurlijk of niet-natuurlijk persoon, informatiesysteem, apparaat of object.
12 Deze architectuur is beschikbaar op NORA online.
13 Deze definitie is gebaseerd op het begrip 'elektronische identificatie' uit de eIDAS-verordening
14 Deze definitie is gebaseerd op het begrip 'persoonsidentificatiegegevens' uit de eIDAS-verordening
15 Deze definitie is gebaseerd op het begrip 'authenticatie' uit de eIDAS-verordening
16 Deze definitie is gebaseerd op het begrip 'elektronisch identificatiemiddel' uit de eIDAS-verordening
17 Het gebruik van apparaten door natuurlijke personen bij identificatie en authenticatie is wel in scope.

van de dienstverlener richting de handelend persoon is een essentieel onderdeel van de interactie tussen beide. Het gaat vooraf aan het vaststellen van de identiteit van de handelend persoon. De handelend persoon moet eerst kunnen vaststellen met welke dienstverlener en authenticatiedienst hij heeft te maken. Onder andere het 'slotje' in webbrowsers geeft hier invulling aan. Deze identificatie en authenticatie van de dienstverlener is, zoals gezegd, niet beschreven in deze versie van de architectuur.

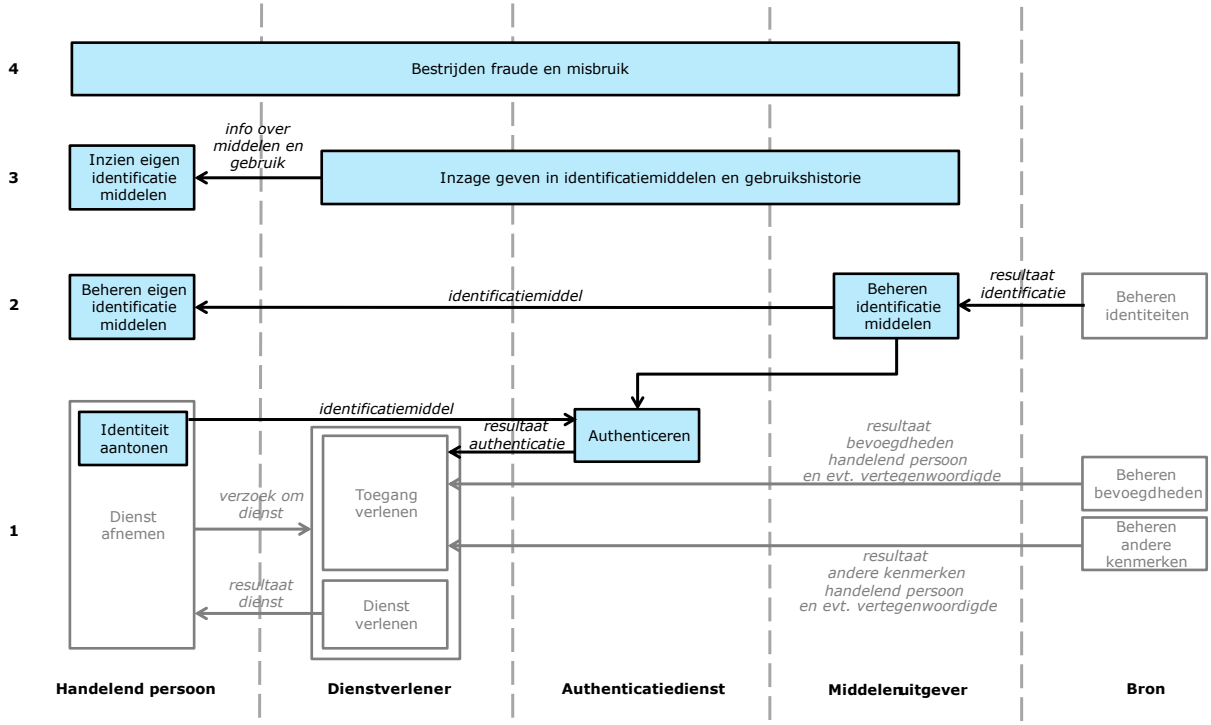
3.2 Identificatie en authenticatie bij toegang verlenen

De afbeelding hieronder geeft de verantwoordelijkheden en rollen weer die van belang zijn bij identificatie en authenticatie voor het verlenen van toegang tot een digitale dienst. De rechthoeken geven verantwoordelijkheden weer en de kolommen geven weer bij welke rollen deze verantwoordelijkheden horen. De pijlen geven informatieproducten weer die vanuit de verantwoordelijkheden worden geleverd. De rechthoeken en pijlen met zwarte lijnen zijn in scope van deze architectuur en die met grijze lijnen niet. De afbeelding toont de situatie waarin een handelend persoon toegang vraagt tot een dienst van één dienstverlener.

De rol 'Middelenuitgever' verstrekt identificatiemiddelen waarmee personen hun identiteit kunnen aantonen.[18] De rol 'Authenticatiedienst' controleert en bevestigt de door de persoon geclaimde identiteit aan de hand van het identificatiemiddel en geeft daarvoor een authenticatieresultaat (ook wel: authenticatieverklaring) af. De rol 'Bron' beschikt over (persoonsgebonden) gegevens die relevant zijn voor het verlenen van toegang en stelt deze beschikbaar. In de afbeelding zijn drie verschillende soorten bronnen weergegeven. Deze zijn verderop toegelicht.

De afbeelding is een functionele weergave die geen uitspraken doet over de vorm waarin de informatieproducten (de pijlen in de afbeelding) worden geleverd. Zo is bijvoorbeeld niet weergegeven of bevoegdheden rechtstreeks bij een bevoegdhedenbron worden opgevraagd of dat de bevoegdheid eerst wordt opgeslagen in de digitale wallet van de handelend persoon en door de persoon vanuit zijn wallet wordt verstrekt. De afbeelding doet ook geen uitspraken over hoe verantwoordelijkheden (de rechthoeken in de afbeelding) organisatorisch en technisch zijn ingericht; bijvoorbeeld over het al dan niet beleggen van verschillende rollen bij dezelfde organisatie. Zo kan dezelfde organisatie zowel de rol 'Authenticatiedienst' als de rol 'Middelenuitgever' vervullen. De afbeelding laat ook in het midden hoe het vaststellen van de bevoegdheden en andere kenmerken van een persoon is ingericht. Deze inrichting, die meer omvat dan de directe pijlen naar de betreffende bronnen in de afbeelding suggereren, is niet in scope van deze deelarchitectuur.

[18] Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties kiest er in de uitwerking van de Wet digitale overheid (Wdo) voor om in het bedrijvendomein de rol Authenticatiedienst te activeren en de rol Middelenuitgever niet. Dit om de complexiteit van de regelgeving te beperken. Dat betekent dat een partij die de rol van Authenticatiedienst vervult ook de rol van Middelenuitgever vervult. In deze GA-deelarchitectuur onderkennen we beide rollen apart.
In de uitwerking van de Wdo wordt in het bedrijvendomein ook de rol Machtigingsdienst geactiveerd. Deze rol is niet in scope van GA Identificatie en authenticatie, maar van GA Machtigen en vertegenwoordigen.



In de afbeelding zijn van onderen naar boven vier 'lagen' te onderkennen, namelijk:

1. authenticeren van de handelend persoon ten behoeve van het verlenen van toegang tot een digitale dienst;
2. beheren (verkrijgen, wijzigen en beëindigen en intrekken of blokkeren) van identificatiemiddelen;
3. inzage geven aan de bezitter in zijn identificatiemiddelen en de gebruikshistorie;
4. bestrijden van fraude en misbruik: het voorkomen, detecteren, opvolgen en herstellen van authenticatiefraude en misbruik van identificatiemiddelen.

Deze 'lagen' zijn hieronder toegelicht.

Op alle vier de 'lagen' moet de handelend persoon ondersteuning kunnen krijgen. Zowel bij het gebruiken van zijn identificatiemiddelen op 'laag 1', als bij het verkrijgen en beheren ervan op 'laag 2', als bij het inzien van zijn middelen en de gebruikshistorie op 'laag 3', als bij het bestrijden van fraude en misbruik en het herstel na geconstateerde fraude op 'laag 4'. De rollen dienstverlener, authenticatiedienst, middelenuitgever en bron hebben hier allemaal een verantwoordelijkheid in. Deze verantwoordelijkheden zijn niet weergegeven in de afbeelding. Ook verantwoordelijkheden m.b.t. besturing (ook wel: governance) en toezicht op en handhaving van naleving van de gemaakte afspraken zijn niet weergegeven in de afbeelding.

3.2.1 Laag 1: Authenticeren van de handelend persoon bij het verlenen van toegang

De handelend persoon wil een dienst afnemen en dient daarvoor toegang tot de dienst te krijgen. De dienstverlener beslist op basis van zijn toegangsbeleid[19] of de handelend persoon toegang krijgt. Daarvoor dient te worden vastgesteld:

1. Wie de handelend persoon is (identificatie en authenticatie). Hiervoor wordt gebruikt gemaakt van een identificatiemiddel. Een authenticatiedienst voert de authenticatie uit. Daarbij wordt naast de identiteit van de persoon ook de echtheid, en geldigheid en het betrouwbaarheidsniveau van het middel getoetst.
2. Of de handelend persoon de juiste bevoegdheden heeft om toegang te krijgen, waaronder de juiste vertegenwoordigingsbevoegdheden als hij handelt namens een ander. Als sprake is van vertegenwoordiging kan het ook nodig zijn om van de vertegenwoordigde vast te stellen of deze de juiste bevoegdheden heeft.
   Voor het toetsen van de bevoegdheden wordt (direct of indirect) gebruik gemaakt van een

[19] Onder toegangsbeleid verstaan we de regels die een dienstverlener hanteert bij het verlenen van toegang tot diensten.

bevoegdhedenbron waar bevoegdheden worden beheerd. Een machtigingenregister is een voorbeeld van zo'n bevoegdhedenbron.[20]
De toets op bevoegdheden is niet in scope van deze architectuur, maar van de GDI-architectuur voor Machtigen en vertegenwoordigen.

3. Of is voldaan aan de overige regels in het toegangsbeleid van de dienstverlener. Onderdeel daarvan kan de toets zijn of de handelend persoon de overige kenmerken of kwalificaties heeft die voorwaarde zijn voor toegang (zoals in bezit van de benodigde beroepsregistratie). Als sprake is van vertegenwoordiging kan het ook nodig zijn om van de vertegenwoordigde vast te stellen of deze de juiste kenmerken heeft.
Onder 'overige kenmerken of kwalificaties' verstaan we hier zowel expliciet vastgelegde toestemmingen (bijvoorbeeld in een autorisatieregister) als kenmerken die medebepalend zijn voor het verlenen van toegang (bijvoorbeeld de woonplaats van de handelend persoon of de vertegenwoordigde). Hiervoor wordt gebruik gemaakt van wat we hier een kenmerkenbron noemen. Dat kan een persoonsregistratie zijn, maar de gegevens kunnen ook aan de handelende persoon zelf worden gevraagd.
De toets op overige kwalificaties en de inrichting ervan is niet in scope van deze architectuur. Het is de verantwoordelijkheid van de dienstverlener hiervoor zorg te dragen. De GDI bevat hiervoor op het moment van schrijven geen generieke bouwstenen, anders dan de basisregistraties waarin een deel van de mogelijk relevante kenmerken zijn vastgelegd en bouwstenen voor het benaderen van deze basisregistraties of andere registraties.

Op basis van de uitkomsten van deze drie toetsen bepaalt de dienstverlener of de handelend persoon toegang krijgt tot de digitale dienst.

3.2.2 Laag 2: Beheren van identificatiemiddelen

Om toegang te kunnen krijgen dient de handelend persoon te beschikken over een identificatiemiddel. Dergelijke middelen worden uitgegeven en beheerd door een partij met de rol middelenuitgever. Om middelen uit te kunnen geven zijn identificatiegegevens nodig. Deze worden beheerd door een identiteitenbeheerder.

De handelend persoon beheert zijn eigen identificatiemiddelen. Hij moet middelen kunnen verkrijgen, wijzigen en beëindigen. Ook de middelenuitgever heeft hierin een rol en kan zo nodig ingrijpen, bijvoorbeeld door een middel in te trekken als het gecompromitteerd is. Ook andere gebeurtenissen, zoals het overlijden van de bezitter van het middel, kunnen leiden tot wijziging of beëindiging van een middel.

Het hebben van betrouwbare identificatiegegevens is een voorwaarde voor het betrouwbaar kunnen vaststellen van de identiteit van een persoon: het beheren van identiteiten is randvoorwaardelijk voor identificatie en authenticatie. Identiteitenbeheer is niet in scope van deze architectuur.[21] Identiteitenbeheer is een op zichzelf staande functie die voor meer doeleinden bestaat dan alleen identificatie en authenticatie en daarmee breder is dan de scope van deze architectuur. Denk bijvoorbeeld aan de BRP met persoonsgegevens van inwoners van Nederland en van personen die Nederland hebben verlaten of aan een klantenregistratie van een bedrijf. De relatie tussen identificatiemiddelenbeheer en identiteitenbeheer is wel in scope vanwege de afhankelijkheid van identificatiemiddelenbeheer van betrouwbaar identiteitenbeheer. Nederland kent diverse gezaghebbende of authentieke bronnen[22] waar persoonsgegevens (ook wel: attributen[23]) worden beheerd, waaronder de BRP en het Handelsregister (voor ondernemingen en rechtspersonen die inschrijvingsplichtig zijn in Nederland).

[20] In de GDI-architectuur voor Machtigen en vertegenwoordigen noemen we een machtigingenregister meer algemeen een vertegenwoordigingsbevoegdhedenbron.

[21] Onder het beheren van identiteiten verstaan we hier het vaststellen, registreren, wijzigen en beëindigen van administratieve identiteiten van personen.

[22] Het voorstel voor wijziging van de eIDAS-verordening definieert authentieke bron als: 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.

[23] Het voorstel voor wijziging van de eIDAS-verordening definieert attribuut als: een eigenschap, kenmerk of kwaliteit van een natuurlijke of rechtspersoon of een entiteit, in elektronisch formaat.

3.2.3 Laag 3: Inzage geven in identificatiemiddelen en gebruikshistorie

Middelenuitgevers, authenticatiediensten en dienstverleners hebben allemaal een verantwoordelijkheid in het geven van inzage aan de bezitter van middelen in welke identificatiemiddelen hij bezit en wanneer en waarvoor deze zijn gebruikt. Deze verantwoordelijkheid is weergegeven met één rechthoek die zich uitstrekt over alle drie de rollen, wat niet betekent dat er ook per se één gezamenlijke oplossing voor moet worden gecreëerd. Er zijn op z'n minst afspraken nodig over de verdeling van deze taken en verantwoordelijkheden.

3.2.4 Laag 4: Bestrijden van fraude en misbruik

Middelenuitgevers, authenticatiediensten, dienstverleners en ook de bezitter van middelen zelf hebben allemaal een verantwoordelijkheid in het voorkomen, detecteren, opvolgen en herstellen van authenticatiefraude en misbruik van identificatiemiddelen. Deze verantwoordelijkheid is weergegeven met één rechthoek die zich uitstrekt over alle vier de rollen, wat niet betekent dat er ook per se één gezamenlijke oplossing voor moet worden gecreëerd. Er zijn op z'n minst afspraken nodig over de verdeling van deze taken en verantwoordelijkheden. O.a. over wanneer identificatiemiddelen geblokkeerd of ingetrokken moeten worden en hoe de gevolgen van fraude worden hersteld.

4 Kaders voor identificatie en authenticatie

Dit hoofdstuk beschrijft de relevante kaders voor identificatie en authenticatie.

4.1 Kaders uit wet- en regelgeving

Voor identificatie en authenticatie zijn de volgende kaders uit wet- en regelgeving van belang:

A. De **EU-verordening eIDAS**[24] bevat regels en eisen waaraan identificatiemiddelen in lidstaten moeten voldoen om een bepaald betrouwbaarheidsniveau te bereiken. Er worden drie betrouwbaarheidsniveaus onderkend: Laag, Substantieel en Hoog.[25] Alleen middelen die via de procedure van eIDAS worden goedgekeurd mogen met betrouwbaarheidsniveaus substantieel of hoog worden aangemerkt.

   De verordening bevat ook afspraken over de erkenning van identificatiemiddelen uit lidstaten en het onderlinge gebruik van digitale infrastructuren om binnen Europa grensoverschrijdend zaken te kunnen doen.

   De eIDAS-verordening legt ook een relatie tussen authenticatie en gekwalificeerde ondertekening.[26] Dit is niet in scope van deze versie van de architectuur, maar van een volgende versie.
   Nauw hiermee verbonden is wilsuiting. Wilsuiting is een inherent onderdeel van het gebruik van identificatiemiddelen bij het inloggen. Door gebruik te maken van zijn identificatiemiddel geeft de handelend persoon aan de intentie te hebben om in te loggen bij de dienstverlener. Daarmee geeft de handelend persoon ook toestemming aan de authenticatiedienst om persoonsgegevens te verstrekken aan de dienstverlener. Dit is dan de rechtsgrond voor de verwerking van die persoonsgegevens, zoals vereist in AVG Artikel 6. Bij publieke dienstverleners zal de rechtsgrond overigens vaak ook een wettelijke basis hebben.

B. **Single Digital Gateway verordening** – Deze regelt dat alle EU-burgers en bedrijven makkelijk toegang moeten krijgen tot in de verordening gespecificeerde digitale dienstverlening in andere EU-lidstaten. Dit vraagt dat iedere persoon die gebruik wil maken van deze digitale dienstverlening moet kunnen beschikken over een conform de eIDAS-verordening erkend identificatiemiddel (en/of andere onder de SDG-verordening erkende oplossingen voor identificatie en authenticatie).

C. Er is een voorstel voor een **revisie van de eIDAS-verordening** die moet leiden tot een **European Digital Identity Framework**. Dit raamwerk maakt het gebruik van een Europese Digitale Identiteit (ook wel: eID of EDI) binnen de interne markt mogelijk. Binnen dit raamwerk kunnen digitale identiteiten én attributen met 'wallets', en met gebruik van biometrie op mobiele apparaten, bij overheden én bedrijven tot op het hoogste betrouwbaarheidsniveau worden gebruikt, online en offline. Het idee van de revisie is dat nationale overheden hiervoor (zelf of in de markt) één of meer gecertificeerde wallets realiseren, waarmee burgers en bedrijven hun digitale identiteiten en attributen zelf kunnen delen. De wallet-opzet maakt het mogelijk om attributen te verkrijgen van verschillende 'attribute providers' (een nieuwe vertrouwensdienst in het voorstel). Met deze wallets dienen personen ook gekwalificeerd te kunnen ondertekenen.

   De **digitale bronidentiteit (DBI)** is een concept dat aan de Tweede Kamer is aangekondigd en momenteel wordt uitgewerkt. Deze DBI geeft invulling aan de 'core identity' die nodig is voor de implementatie van het European Digital Identity Framework. Het idee is dat de DBI een door de overheid uitgegeven, erkende en in wet- en regelgeving verankerde, digitale identiteit[27] is voor gebruik in de publieke en private sector. De DBI

[24] electronic IDentification Authentication and trust Services
[25] De onderliggende eIDAS-uitvoeringsverordening 1502 geeft een nadere invulling aan deze niveaus.
[26] Deze relatie bestaat eruit dat eIDAS toe laat dat de signeersleutel van de gebruiker zich 'op afstand' in een Hardware Security Module (HSM) bevindt bij een trusted partij en dat de gebruiker deze HSM kan instrueren om te tekenen middels een authenticatie van eIDAS betrouwbaarheidsniveau Substantieel of Hoog. Dit is nader uitgewerkt in Europese normen EN 419241-2 (SAM) en EN 419221-5 (HSM)
[27] Een digitale identiteit is in de beschrijving van DBI gedefinieerd als een verzameling van betrouwbare gegevens die een entiteit (persoon, organisatie, object of apparaat) representeren in het digitale

bevat een minimale set van identificatiegegevens die nodig zijn in het maatschappelijk verkeer. De overheid creëert met de DBI een 'gezaghebbende bron' van betrouwbare identificatiegegevens. De DBI maakt als 'gezaghebbende bron' afgeleide identificatiemiddelen mogelijk. Deze afgeleide identificatiemiddelen zullen zowel publiek als privaat gebruikt kunnen worden.

D. Het voorstel voor de eerste tranche van de **Wet digitale overheid (Wdo)** (die de eIDAS-verordening als basis heeft) heeft als doel 1) veilige identificatiemiddelen voor burgers en bedrijven voor digitale publieke dienstverlening en later ook voor private dienstverlening en 2) open toelating van identificatiemiddelen, zowel publieke als private middelen.

   De Wdo schrijft voor dat publieke dienstverleners de digitale diensten die zij leveren moeten classificeren op het juiste betrouwbaarheidsniveau en dat toegang tot die diensten alleen mogelijk is met een toegelaten identificatiemiddel op minimaal dat niveau. Hiervoor schept de Wdo de benodigde kaders en spelregels.

   De Wdo schept ook kaders en afspraken voor erkenning en toelating van private middelen voor burgers en vertegenwoordigers van organisaties en bedrijven. De Wdo schrijft ook voor dat alle dienstverleners met een publieke taak aangesloten moeten zijn op alle huidige en nieuwe uitgevers van toegelaten identificatiemiddelen.

   In de memorie van toelichting bij het voorstel voor de Wdo is beschreven dat de regering wil dat burgers niet afhankelijk zijn van de beschikbaarheid van private middelen voor het verkrijgen van toegang tot digitale dienstverlening in het publieke domein.[28] Burgers kunnen daarvoor DigiD Hoog en Substantieel gebruiken via de eID-applicatie op de wettelijke identificatiedocumenten. Ook voor DigiD geldt de acceptatieplicht.

   Volgens het wetsvoorstel is de Minister van BZK verantwoordelijk voor de inrichting en werking van:
   - een routeringsvoorziening, waarmee bestuursorganen en aangewezen organisaties eenvoudig kunnen aansluiten op diverse identificatiemiddelen voor burgers die zij moeten accepteren;
   - het BSNk dat een rol speelt bij het activeren van een middel en bij de authenticatie van een persoon;
   - het eIDAS-knooppunt voor de routering van de authenticatie met het Nederlandse middel naar een andere lidstaat en vice versa;
   - de publieke machtigingenvoorziening (deze is niet in scope van deze architectuur, maar van de architectuur voor machtigen en vertegenwoordigen).

   Volgens het wetsvoorstel is de Minister van Infrastructuur en Waterstaat verantwoordelijk voor opname van data ten behoeve van elektronische authenticatie in een chip op het rijbewijs.

   Onder de Wdo zijn vijf regelingen van belang[29]:
   - Besluit identificatiemiddelen voor natuurlijke personen Wdo;
   - Besluit bedrijfs- en organisatiemiddel Wdo;
   - Besluit Digitale Overheid;
   - Regeling nadere eisen toelating identificatiemiddelen Wdo. Deze regeling specificeert nadere interpretaties van de eIDAS-uitvoeringsverordening 1502 ten behoeve van erkende authenticatie- en machtigingsdiensten;.
   - Regeling betrouwbaarheidsniveaus authenticatie. Deze regeling bevat een classificatiemodel aan de hand waarvan publieke dienstverleners bepalen wat het

domein, zoals: 1) de combinatie naam, geboortedatum, adres, 2) 'identifiers' zoals BSN en telefoonnummer of 3) biometrische gegevens zoals vingerafdruk.

[28] De motie van Van der Molen over een geïntegreerd burger-, bedrijfs- en organisatiemiddel "verzoekt de regering, te onderzoeken op welke wijze een publiek middel kan worden verschaft als bedrijfs- en organisatiemiddel, dan wel hoe de eID-ontwikkeling aangegrepen kan worden om een geïntegreerd burger- en bedrijfs- en organisatiemiddel tot stand te brengen". In de Aanpak uitvoering publiek middel in het bedrijvendomein zegt de staatsecretaris "De motie wil ik kort samengevat uitvoeren met de ontwikkeling van een publiek middel. Dat middel kan op korte termijn gebruikt worden om de compensatieregeling te vervangen en de uitvoeringsproblemen bij de Belastingdienst op te lossen. Op de lange termijn kan het worden opgeschaald naar het geïntegreerd middel waarom de motie verzoekt."

[29] Deze regelingen zijn op het moment van schrijven nog concept.

vereiste betrouwbaarheidsniveau van authenticatie is voor de verlening van elektronische diensten.

E. **Algemene verordening gegevensbescherming (AVG)** – De AVG is de Nederlandse vertaling van de GDPR. De AVG verplicht om persoonsgegevens op een passende manier te beveiligen. Art. 32 AVG stelt: "Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten (…)"

   Deze open norm omschrijft niet aan welke eisen moet worden voldaan om op het gebied van identificatie en authenticatie om het niveau van adequate beveiliging te bereiken. De (uitvoeringsregelgeving van de) Wdo zal concretiseren in welke mate van beveiliging van toegang tot publieke dienstverlening passend is in relatie tot de gegevens die worden getoond/verwerkt bij deze dienstverlening.

   Vooruitlopend op de inwerkingtreding van de Wdo bieden de Handreiking Betrouwbaarheidsniveaus van Forum Standaardisatie en de door de Autoriteit Persoonsgegevens gegeven uitleg van de AVG concrete richtsnoeren. Zo worden aan de beveiliging van gezondheidsgegevens die online worden verwerkt extra hoge eisen gesteld; de verwerking van gezondheidsgegevens via internet mag alleen met behulp van (minimaal) meerfactorauthenticatie.[30]

F. Nederland kent een gecentraliseerd identiteitenstelsel met als **gezaghebbende of authentieke bron**[31] de Basisregistratie Personen (BRP) voor inwoners van Nederland en personen die Nederland hebben verlaten en het Handelsregister (HR) voor ondernemingen en rechtspersonen.

   1) De **Wet basisregistratie personen** reguleert de verplichting van specifiek aangewezen overheidsorganisaties om bepaalde persoonsgegevens van de inwoners en niet-ingezetenen van Nederland te verzamelen en te registreren in de BRP. De Wet BRP regelt ook het gebruik van die gegevens.
   2) De **Handelsregisterwet** reguleert het basisregister van ondernemingen en rechtspersonen, dat wil zeggen de registratie en het gebruik van gegevens over ondernemingen en rechtspersonen.

   In deze basisregistraties zijn voor natuurlijke personen en niet natuurlijke personen identificerende nummers vastgelegd. Voor burgers is dat het BSN en voor bedrijven het KvK-nummer en het RSIN (voor een niet-natuurlijk persoon) en het BSN voor een natuurlijk persoon. Deze nummers worden ook gebruikt in de digitale identificatiemiddelen in het publieke domein, als identificatie van de bezitter van het middel.

   Voor beide bronnen geldt dat de ze niet alle personen registreren die op basis van hun rechten en plichten toegang moeten hebben tot publieke dienstverlening. Ook geldt dat niet alle personen die zijn geregistreerd in de BRP kunnen beschikken over een wettelijk identificatiedocument. Deze personen kunnen daardoor geen identificatiemiddel met betrouwbaarheidsniveau Hoog gebruiken. Om al deze personen te kunnen bedienen is het daarom randvoorwaardelijk om ook personen te kunnen identificeren die buiten het BSN- of KvK/RSIN-domein vallen. Ook zijn er diverse andere (soms afgeleide) sectorspecifieke identificerende nummers in gebruik, o.a. om privacy redenen, zoals UZI in de zorg, voor de rijkspas en in het onderwijs en Probas voor ambassades en andere internationale

[30] De Autoriteit Persoonsgegevens heeft in oktober 2018 aangegeven dat het betrouwbaarheidsniveau Hoog verplicht is in de zorg waar toegang tot "gegevens over gezondheid" worden ontsloten. De AP geeft impliciet aan dat het betrouwbaarheidsniveau substantieel wordt gedoogd zolang hoog nog onvoldoende beschikbaar is. Betrouwbaarheidsniveau laag wordt niet geaccepteerd voor toegang tot gegevens over gezondheid.

[31] Het voorstel voor wijziging van de eIDAS-verordening definieert authentieke bron als: 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.

organisaties. Er is daarom een breder stelsel van identiteitenbronnen nodig dan alleen de BRP en het Handelsregister.

Voor de BRP geldt ook dat niet alle dienstverleners de persoonsgegevens uit deze bron mogen gebruiken. Een oplossing hiervoor is om de gegevens te versleutelen zodat ze wel bruikbaar zijn zonder dat ze beschikbaar komen voor de dientverlener, zoals met de introductie van pseudoniemen. Deze pseudoniemen hebben als voornaamste doel dat ook private partijen met afgeleide gegevens uit deze bronnen personen kunnen identificeren, met in achtneming van de privacy van gebruikers. De Wdo en het BSNk bieden hier de basis voor.

G. (Digitale) Identiteiten zijn nodig voor alle persoonsgebonden diensten. In de **Wet hergebruik overheidsinformatie** en in de Wet BRP is het verplichte hergebruik van de persoonsgegevens in de BRP aangegeven.

H. **Wet algemene bepalingen burgerservicenummer (Wabb)** - Dit betreft de toekenning van het identificerend gegeven BSN aan de personen (mensen) over wie gegevens in de BRP zijn opgenomen. De Wabb regelt ook op hoofdlijnen het gebruik van het BSN door overheidsorganisaties. Er zijn aanverwante wetten over het gebruik van het BSN in o.a. de zorg en de financiële sector. Zie ook wat de overheid aan burgers zegt over Wat is het BSN? De Wabb wordt herzien, omdat kaders over gebruik nu nog sectoraal worden bepaald en de behoefte er ligt om dit centraal vast te leggen.

I. **Wet op de identificatieplicht (Wid)** - Deze regelt welke fysieke documenten officieel aangewezen zijn om iemands identiteit vast te stellen. De Wid reguleert ook het gebruik van de NFC-chip op de aangewezen fysieke documenten. Zie ook wat de overheid aan burgers zegt over de identificatieplicht.

J. **Vreemdelingenwet 2000** - Deze regelt de toelating en uitzetting van vreemdelingen, het toezicht op vreemdelingen die in Nederland verblijf houden, en de grensbewaking. De wet definieert een vreemdeling als iemand die de Nederlandse nationaliteit niet bezit en niet op grond van een wettelijke bepaling als Nederlander moet worden behandeld. Zie ook wat de overheid aan burgers zegt over vreemdelingen/immigranten.

K. **Algemene wet bestuursrecht** – Deze bevat een open norm die noopt tot adequate toegangsbeveiliging van berichten: Artikel 2:14 lid 3. ‘Indien een bestuursorgaan een bericht elektronisch verzendt, geschiedt dit op een voldoende betrouwbare en vertrouwelijke manier, gelet op de aard en de inhoud van het bericht en het doel waarvoor het wordt gebruikt.’

Sectorspecifiek zijn er ook eisen met betrekking tot de veiligheid van elektronische gegevensuitwisseling, zoals de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, het Besluit elektronische gegevensuitwisseling verplicht om de NEN7510, NEN7512 en NEN7513 na te leven.

L. **Wet Elektronisch Berichtenverkeer (WEBV)** – Deze schept het wettelijk kader voor het verplichten van elektronisch berichtenverkeer in het contact met de Belastingdienst. In artikel X van deze wet is bovendien een grondslag opgenomen voor voorzieningen voor elektronisch berichtenverkeer, elektronische authenticatie en elektronische registratie van machtigingen en het raadplegen ervan en voor de in dat verband noodzakelijke verwerking van persoonsgegevens. De zorg voor deze voorzieningen wordt aan de Minister van BZK opgedragen. Ook is bepaald dat hij persoonsgegevens verwerkt, waaronder het BSN, voor zover dit noodzakelijk is voor de goede vervulling van zijn taken.

Met de Wet EBV, in werking getreden op 1 november 2015, is een eerste fundament gelegd onder de GDI, met het oog op de in de praktijk functionerende voorzieningen MijnOverheid, DigiD en DigiD Machtigen. Ook het BSNk, essentieel voor het functioneren van identificatiemiddelen in het publieke domein, is nader gereguleerd.

Overeenkomstig hetgeen in de memorie van toelichting bij de Wet EBV is vermeld, zal

artikel X komen te vervallen wanneer een specifieke wet in werking treedt. Hiervan is sprake met het voorstel voor de Wdo. Voor wat betreft de onder de Wet EBV tot stand gekomen uitvoeringsregelgeving geldt dat het Besluit verwerking persoonsgegevens GDI zal worden gebaseerd op dit wetsvoorstel. Ook de Regeling voorzieningen GDI, waarin onder meer gebruik(ers)voorschriften terzake van authenticatie en machtigen zijn opgenomen zal worden aangevuld en gewijzigd naar aanleiding van dit wetsvoorstel.

M. **Overige regelgeving en juridica**
Naast de hiervoor genoemde wet- en regelgeving is meer regelgeving van toepassing op het verlenen van toegang tot publieke diensten en de identificatie van personen. Voorbeelden zijn de Regeling elektronisch berichtenverkeer Belastingdienst, de DigiD-aansluitvoorwaarden (civielrechtelijke overeenkomst) en de deelnemersovereenkomsten en gebruiksvoorwaarden van het afsprakenstelsel Elektronische Toegangsdiensten. De laatste twee vervallen bij inwerkingtreding van de Wdo. Om het vertrouwen te garanderen geldt er een auditverplichting voor dienstverleners. Dit zijn nu de DigiD-assessments en worden bij inwerkingstreding van de Wdo de eID-assessments.

4.2 Beleidskaders

Voor identificatie en authenticatie zijn de volgende beleidskaders van belang:

N. **NL Digibeter** (Agenda Digitale Overheid) benoemt de doelen en actielijnen die passen bij de kaders uit wet- en regelgeving die hiervoor zijn beschreven.

De uitgangspunten voor de digitale basisinfrastructuur zoals beschreven in het ‘Beleidskader digitale basisinfrastructuur’ zijn verwerkt in de GA-basisprincipes en zijn daarmee ook van toepassing op identificatie en authenticatie. Omdat deze uitgangspunten in de basisprincipes zijn verwerkt, zijn ze niet in dit hoofdstuk opgenomen.

4.3 Maatschappelijke en technische ontwikkelingen

Voor identificatie en authenticatie zijn de volgende maatschappelijke en technische ontwikkelingen van belang:

O. De digitale transformatie van de samenleving vraagt om vertrouwen in de digitale wereld. **De overheid moet voorwaarden scheppen** zodat burgers en bedrijven veilig, persoonlijk en gebruiksvriendelijk digitale diensten af kunnen nemen. De digitale dienstverlening neemt toe, zowel in het al bestaande aanbod als in nieuwe vormen. Om de positie van de gebruiker te versterken en te beschermen, is er veel aandacht voor inclusie, privacy en het voorkomen en aanpakken van identiteitsfraude. Uit de Monitor Identiteit 2019 (ministerie van BZK) blijkt dat 4,1% van de onderzochte populatie dat jaar te maken heeft gehad met een vorm van identiteitsfraude. Dat is bijna een verdubbeling t.o.v. 2014 (2,1%). Dit vraagt om maatregelen om misbruik van identificatiemiddelen te voorkomen en detecteren en afspraken over de taken en verantwoordelijkheden van betrokken partijen bij (vermeende) fraude, waaronder afspraken over blokkeren of intrekken van middelen.

P. Het bewustzijn rond het gebruik van persoonsgegevens en identificatiemiddelen neemt toe. **De gebruiker verwacht inzage, privacy en de beveiliging van zijn gegevens bij organisaties met publieke taken**. Niet alleen is er wettelijk door de AVG een grotere druk op de verwerking van persoonsgegevens, ook is er een enorme “data honger”, zowel vanuit de publieke als in de private sector. Bij de laatste vaak gevoed vanuit het businessmodel. Ook big-data-ontwikkelingen dragen hieraan bij. Het gevolg en tegenwicht is een grotere maatschappelijke discussie over gegevensverwerking. Daarbij groeit de roep om meer regie op eigen gegevens (in de zin van transparantie en hergebruik binnen zowel het publieke als private domein) en de eis om niet onnodig gegevens meerdere keren uit te wisselen. Het programma Regie op Gegevens moet ervoor zorgen dat mensen (persoonlijke) data kunnen gebruiken om hun leven, werk of bedrijf te organiseren, terwijl belangrijke waarden als veiligheid en privacy geborgd zijn. Regie op gegevens vraagt o.a. om betrouwbare identificatie en authenticatie. In Europees verband wordt geëxperimenteerd volgens het Self Sovereign Identity (ESSIF) concept. SSI is niet in scope van deze versie van de architectuur, maar wordt in een volgende versie uitgewerkt.

Q. **Er zijn meer personen die beschikken over middelen op de niveaus substantieel en hoog.** Steeds meer DigiD-gebruikers stappen over van gebruikersnaam en wachtwoord naar 2-factorauthenticatie. De DigiD-app kent eind 2021 ongeveer 10,8 miljoen gebruikers, waarvan ongeveer 6,3 miljoen accounts op substantieel niveau. Sinds 2021 is het mogelijk om in combinatie met de eNIK (de identiteitskaart met chip en applet) en het eRijbewijs (met chip en applet) via een smartphone op eIDAS-betrouwbaarheidsniveau hoog in te loggen. Er zijn ook private middelen beschikbaar met deze betrouwbaarheidsniveaus. Om namens niet-natuurlijke personen in te loggen is er al geruime tijd de mogelijkheid om op alle eIDAS-betrouwbaarheidsniveaus (laag, midden en hoog) in te loggen met behulp van eHerkenning.

R. Er is **meer behoefte aan betrouwbare identificatiemiddelen die in verschillende contexten en via verschillende kanalen** (apps, telefonisch, virtueel, videocalls) gebruikt kunnen worden. Ook wordt in de samenleving steeds vaker geopperd om het anoniem handelen op het internet, met name op sociale media, terug te dringen. Hier kunnen de oplossingen voor identificatie en authenticatie van de overheid in de toekomst mogelijk een bijdrage aan leveren. Een aandachtspunt daarbij is de spanning tussen enerzijds betrouwbaar kunnen identificeren en anderzijds het vanuit privacyoverwegingen niet willen koppelen van handelingen van personen in verschillende publieke en private contexten.[32]

S. **Verschuiving van gegevensuitwisseling naar verifieerbare beweringen** (ook wel: 'claims'). Een belangrijke ontwikkeling is dat ook voor de identiteitsvaststelling, een beweging ontstaat van gegevensuitwisseling in de 'back-office' naar het uitgeven van verifieerbare beweringen (zoals: ik ben ouder dan 18 jaar) over een identiteit. Ook bestaat de wens, in het kader van privacy en gegevensminimalisatie, om een minimale set van rechtsgeldige, tot de bron herleidbare attributen uit te wisselen die bijdragen aan vaststelling van identiteit en de bevoegdheid van de bezitter van het middel. Dit alles leidt tot de situatie waarbij we de identificerende gegevens minimaliseren en de rest van de identificatiegegevens of daarvan afgeleide gegevens als verifieerbare bewering willen uitwisselen. De gebruiker krijgt zo meer regie over zijn gegevens en gebruikt in verschillende elementen van dienstverlening telkens alleen de gegevens die in dat proces nodig zijn. Voor het domein van identificatie en authenticatie betekent dit, dat ook daar minder gegevens uitgewisseld zullen worden en er meer bewijsbare claims over gegevens uitgewisseld zullen worden via vertrouwensdiensten.
Het uitgeven van verifieerbare beweringen is niet in scope van deze versie van deze architectuur, maar wordt in een volgende versie uitgewerkt in samenhang met de onderwerpen SSI en wallets.

T. **Het domein van digitale vertrouwensdiensten, identificatiemiddelen en attributendiensten ontwikkelt zich snel**, zoals de internationale en Europese ontwikkelingen op gebied van zowel technologie als ook publieksgebruik en wetgeving. Deze snelle ontwikkeling vraagt om een infrastructuur met zo min mogelijk afhankelijkheid van specifieke middelen die een bepaalde functie vervullen. De infrastructuur moet ook geschikt zijn voor privaat gebruik van publieke identificatiemiddelen en publiek gebruik van private middelen. Daarnaast gaat het er in de infrastructuur steeds vaker over om cryptografie toe te passen, zodat er onafhankelijk van de infrastructuur een hoog vertrouwen wordt gerealiseerd. Afsprakenstelsels en standaarden kunnen hier zorgen voor

[32] Het Nederlandse eID-stelsel biedt hiervoor nu al oplossingen, maar die worden beperkt of niet gebruikt. Het eID-stelsel voorziet erin dat personen niet alleen kunnen inloggen onder verstrekking van hun BSN (zoals nu bij DigiD), maar ook onder verstrekking van een pseudoniem (gebaseerd op het BSN). Omdat verschillende dienstverleners verschillende pseudoniemen krijgen voor dezelfde persoon, kan niet gekoppeld worden op basis van deze pseudoniemen. De pseudoniemen zijn verder onafhankelijk van het identificatiemiddel en worden ook door de Nederlandse eID-applicatie op eNIK en eRijbewijs ondersteund. Bij deze opzet zal een persoon maar één account kunnen hebben bij een dienstverlener op basis van pseudonieme authenticatie met een door de overheid erkend identificatiemiddel. Een persoon kan bovendien middelen van meerdere middelenuitgevers hebben, welke wel volledig interoperabel zijn richting dienstverleners. Dit maakt het bijvoorbeeld mogelijk dat burgers met hun identificatiemiddel inloggen bij hun werkgever zonder hun BSN prijs te geven. Het maakt het ook mogelijk om 'trol'-accounts te voorkomen. Andere gebruikers zouden bijvoorbeeld op social media kunnen instellen alleen berichten te willen zien van accounts die gebruik maken van erkende identificatiemiddelen. Eventueel kan gerealiseerd worden dat de identiteit van de gebruiker kan worden achterhaald (onder de juiste waarborgen) in het geval deze strafbare activiteiten uitvoert (zoals het uiten van bedreigingen).

interoperabiliteit van verschillende oplossingen.

U. Er is steeds **meer uitwisseling en samenwerking tussen de publieke en de private sector**. Hierbij is een gedeelde oplossing voor identificatie en authenticatie nodig om te weten dat het over dezelfde persoon gaat, zonder dat bijvoorbeeld het BSN worden gebruikt bij private diensten terwijl dit bij publieke diensten is vereist. Ook hier kunnen afsprakenstelsels en standaarden zorgen voor interoperabiliteit van verschillende oplossingen.

4.4 De scope van identificatie en authenticatie

M.b.t. de scope zijn de volgende opmerkingen van toepassing:

- Dat zaken in scope zijn betekent dat ze uitgewerkt worden in de architectuur voor identificatie en authenticatie. Zaken die wel in scope zijn, maar niet in deze versie worden uitgewerkt, zijn opgenomen onder de kop 'In scope, maar niet in deze versie'.
- Dat zaken in scope zijn, betekent niet per se dat er bouwstenen binnen de GDI voor worden gerealiseerd. Dat is afhankelijk van de in de architectuur gemaakte keuzes die worden bepaald door wet- en regelgeving, beleid en de architectuurprincipes voor de GDI.
- Dat zaken in scope zijn zegt niets over per wanneer er bouwstenen voor worden gerealiseerd. De architectuur doet daar geen uitspraken over, de roadmap GDI wel, zoals is beschreven in paragraaf 2.4.

We hebben ervoor gekozen de scope van deze eerste versie beperkt te houden en te focussen op de identificatie en authenticatie van natuurlijke personen die toegang tot digitale diensten vragen. In volgende versies zullen we de scope uitbreiden en onder andere in meer detail kijken naar impact van ontwikkelingen zoals de SSI, wallets en de eIDAS-revisie.

4.4.1 In scope en in deze versie uitgewerkt.

Het volgende is in scope en is in deze versie uitgewerkt:

1. Identificatie en authenticatie van natuurlijke personen ten behoeve van het verlenen van toegang tot digitale publieke diensten, zowel in het burger- als in het bedrijven- en organisatiedomein. Natuurlijke personen kunnen namens zichzelf of namens een ander natuurlijk of niet-natuurlijk persoon digitale diensten afnemen.
   De WHY van de GDI stelt dat de GDI open staat voor samenwerking van overheid en bedrijfsleven, zodat ook partijen buiten de overheid de GDI kunnen gebruiken. We houden daarom rekening met gebruik van de GDI-bouwstenen voor identificatie en authenticatie voor toegang tot diensten buiten het publieke domein.[33]
   De architectuur voor identificatie en authenticatie moet het mogelijk maken dat personen hun middelen in verschillende contexten en voor verschillende doeleinden kunnen gebruiken.

4.4.2 In scope, maar niet in deze versie uitgewerkt

Het volgende is in scope van GA Identificatie en authenticatie, maar is niet uitgewerkt in deze versie:

1. Identificatie en authenticatie van andere soorten zelfstandig handelende (ook wel: autonome) entiteiten dan natuurlijke personen, zoals informatiesystemen, autonome apparaten en objecten. Het gebruik van apparaten bij de identificatie en authenticatie van natuurlijke personen is wel in scope van deze versie.
2. Identificatie en authenticatie van dienstverleners, zowel richting de handelend persoon (de persoon die dienst afneemt namens zichzelf of een ander) als bij de samenwerking met andere (overheids)organisaties ten behoeve van de dienstverlening.[34]

[33] Zie ook de GA-basisprincipes onder de kop 'Documentatie' op de webpagina over de GDI-Architectuur op NORA online.

[34] De overheid moet voor de gebruiker ook identificeerbaar en authenticeerbaar zijn, zodat deze weet dat hij met de overheid te maken heeft en bijvoorbeeld niet met een frauderende tussenpersoon. Deze stap komt nog voordat de gebruiker moet worden geauthenticeerd. Zoals blijkt uit het wegvallen van de publieke PKIoverheid-certificaten en de discussie over wat daarvoor in de plaats dient te komen, is een gezamenlijke uitwerking hiervan voor de digitale overheid wenselijk.

3. Identificatie en authenticatie voor andere doeleinden dan toegang tot digitale diensten, zoals ondertekening en wilsuiting. De eIDAS-verordening legt een relatie tussen authenticatie en gekwalificeerde ondertekening. Nauw hiermee verbonden is wilsuiting.
4. Verstrekken van persoons(identificatie)gegevens voor andere doelen dan identificatie en authenticatie.
   Dit wordt in een volgende versie uitgewerkt in samenhang met de onderwerpen SSI, wallets en de eIDAS-revisie die op het moment van schrijven in ontwikkeling is.

4.4.3 Niet in scope

Het volgende is niet in scope:

1. Identiteitenbeheer
   Het registreren en beheren van digitale identiteiten, identificatiegegevens en andere persoonsgegevens is niet in scope. Het beheren van persoonsgegevens is een op zichzelf staande functie die voor meer doeleinden bestaat dan alleen digitale identificatie en authenticatie en daarmee breder is dan de scope van deze architectuur.
   De beschikbaarheid van digitale identiteiten met een voldoende hoog betrouwbaarheidsniveau is echter wel een noodzakelijke voorwaarde voor het digitaal kunnen identificeren en authenticeren. Vanuit de (betrouwbaarheids-)eisen aan identificatie en authenticatie volgen er eisen aan de betrouwbaarheid van identificatiegegevens.
   Ook van belang is dat de levenscyclus van identificatiemiddelen afhankelijk is van de levenscyclus van digitale identiteiten: een middel kan niet bestaan zonder een geldige en 'actieve' digitale identiteit. Deze digitale identiteit is weer afhankelijk is van het bestaan van de fysieke entiteit waar de digitale identiteit naar verwijst.
   Om alle personen die op basis van hun rechten en plichten toegang moeten hebben tot publieke dienstverlening te kunnen bedienen is het randvoorwaardelijk om ook personen te kunnen identificeren die buiten het BSN- of KvK/RSIN-domein en de Europese lidstaten vallen.
2. Uitgeven van fysieke identiteitsbewijzen, zoals paspoort en rijbewijs. Dit is belegd bij respectievelijk het ministerie van BZK met de RvIG en met ministerie van IenW en de RDW.
   Dit onderwerp is niet in scope, maar er zijn wel raakvlakken, omdat deze fysieke documenten ook een rol spelen bij digitale identificatie en authenticatie, o.a. door middel van gebruik van NFC-chips, zoals hiervoor in paragraaf 4.1 is beschreven. Ook is het steeds meer mogelijk om van oorsprong fysieke documenten in een digitale 'wallet' op te nemen, zoals dat al een tijd kan met bijvoorbeeld vliegtuigtickets en bankpassen. Dit is relevant voor als de onderwerpen SSI en wallets worden uitgewerkt.
3. Toetsen van bevoegdheden en overige kenmerken en kwalificaties.
   De toets of de handelend persoon en eventueel de vertegenwoordigde over de juiste bevoegdheden en overige kenmerken en kwalificaties beschikken is niet in scope. De toets op overige kwalificaties en de inrichting ervan is de verantwoordelijkheid van de dienstverlener. De GDI bevat hiervoor op het moment van schrijven geen generieke bouwstenen anders dan de basisregistraties waarin een deel van de mogelijk relevante kenmerken zijn vastgelegd.
   Het verstrekken en gebruiken van vertegenwoordigingsbevoegdheden is beschreven in de GDI-Architectuur voor 'Machtigen en vertegenwoordigen'.[35] Het toekennen en raadplegen van andere soorten bevoegdheden is op moment van schrijven niet in scope van de GDI-Architectuur.
   Er zijn wel raakvlakken. Het is zowel voor de handelend persoon als de dienstverlener wenselijk dat deze toetsen op een vergelijkbare manier verlopen als de authenticatie. Dat geldt zowel voor de gebruikerservaring als voor de gebruikte standaarden en technologieën, zoals Oauth 2.0, en de gebruikte voorzieningen. Dit is een aandachtspunt voor de fases die volgen op deze architectuur.
4. Toegang zonder identificatie en authenticatie
   Een gebruiker kan een niet-persoonsgebonden 'toegangsbewijs' hebben waarmee hij toegang tot een dienst kan krijgen. Identificatie en authenticatie is voor de dienstverlener dan niet nodig. Een voorbeeld hiervan is het door middel van een uitnodiging in een mail eenmalig toegang geven tot een enquête of video-conferentie.

[35] Zie onder de koppen Documentatie en Generieke functies op de webpagina over de GDI-Architectuur op NORA online.

Dit onderwerp is niet in scope. Het is de verantwoordelijkheid van de dienstverlener. De GDI bevat hiervoor op het moment van schrijven geen generieke bouwstenen.
Er zijn wel raakvlakken. Het is zowel voor de handelend persoon als de dienstverlener wenselijk dat deze manier van toegang verlenen op een vergelijkbare manier verloopt als wanneer wel authenticatie nodig is. Dat geldt zowel voor de gebruikerservaring als voor de gebruikte standaarden, technologieën en voorzieningen. Dit is een aandachtspunt voor de fases die volgen op deze architectuur.

5 Generieke functies voor identificatie en authenticatie

Dit hoofdstuk beschrijft de generieke functies voor identificatie en authenticatie. Volgens NORA is een generieke functie "iets wat meerdere overheidsorganisaties moeten kunnen voor het uitvoeren van hun taken. […] Het gaat daarbij over capaciteiten waarover overheidsorganisaties in relatie tot de buitenwereld moeten beschikken, die zodanig generiek zijn dat ze op een vergelijkbare manier zijn in te richten. Vaak met behulp van informatietechnologie."

De generieke functies in de GDI-Architectuur zijn geformuleerd vanuit het perspectief van de overheid: het benoemt wat de overheid moet kunnen, waar de overheid voor moet zorgen dat mogelijk is.

Voor identificatie en authenticatie onderkennen we de volgende generieke functies.[36] We onderkennen voor het domein één hoofdfunctie met een aantal onderliggende generieke functies.

Kunnen digitaal identificeren en authenticeren
Het betrouwbaar digitaal kunnen vaststellen van de identiteit van een persoon.[37]

Deze hoofdfunctie kent de volgende onderliggende generieke functies:

1. ***Kunnen laten beschikken over digitale identificatiemiddelen***
   Het ervoor kunnen zorgen dat personen kunnen beschikken over digitale identificatiemiddelen waarmee ze hun identiteit kunnen aantonen. Hieronder valt het uitgeven, wijzigen en beëindigen of intrekken van digitale identificatiemiddelen.
2. ***Kunnen laten gebruiken van digitale identificatiemiddelen***
   Het ervoor kunnen zorgen dat personen hun digitale identificatiemiddelen kunnen gebruiken om hun identiteit digitaal op een passend betrouwbaarheidsniveau aan te tonen.
3. ***Kunnen inzage geven in identificatiemiddelen en gebruik***
   Het ervoor kunnen zorgen dat bezitters van identificatiemiddelen inzage hebben in de middelen die ze bezitten en de gebruikshistorie ervan.
4. ***Kunnen instaan voor betrouwbaarheid en veiligheid van authenticatie***
   Het ervoor kunnen zorgen dat identificatie en authenticatie veilig en betrouwbaar kan plaatsvinden, waaronder het voorkomen, detecteren, opvolgen en herstellen van fraude met identificatiemiddelen.

Deze generieke functies zijn hieronder uitgewerkt. De afspraken, standaarden en voorzieningen die de generieke functies realiseren, zijn uitgewerkt in hoofdstuk 7.

In bijlage 9 is beschreven wat de verschillen zijn met de generieke functies uit het pressurecooker-rapport.

5.1 Kunnen digitaal identificeren en authenticeren

GA-GF-IA00 – Kunnen digitaal identificeren en authenticeren
ID: GA-GF-IA00 ***Naam*** Korte naam: Identificeren en authenticeren Lange naam: Kunnen digitaal identificeren en authenticeren

[36] In de GA benoemen we geen generieke functies voor het kunnen geven van ondersteuning en het kunnen besturen en beheren van de afspraken, standaarden en voorzieningen voor het domein.

[37] Omdat deze versie van de architectuur zich richt op identificatie en authenticatie van natuurlijke personen gebruiken we in de formulering van de generieke functies de term 'persoon' en niet 'entiteit'. Ook de beschrijving van de functie en de implicaties richt zich op personen. Dit doen we omdat we op dit moment nog onvoldoende kunnen bepalen of alle uitspraken ook zondermeer van toepassing zijn voor de andere soorten zelfstandig handelende entiteiten zoals apparaten, objecten en informatiesystemen.

GA-GF-IA00 – Kunnen digitaal identificeren en authenticeren

Beschrijving
Het betrouwbaar digitaal kunnen vaststellen van de identiteit van een persoon.
Dit is de hoofdfunctie.

Rationale
Dienstverlening wordt steeds digitaler en vraagt om digitale oplossingen. Bij digitale dienstverlening, waarbij er geen fysiek contact is tussen dienstverlener en handelend persoon, moet de identiteit van de handelend persoon betrouwbaar digitaal kunnen worden vastgesteld. Zowel om te kunnen bepalen of deze de bevoegdheden heeft om toegang tot de dienst en de informatie te krijgen, als om op de persoon afgestemde dienstverlening te kunnen bieden. De overheid moet voorwaarden scheppen zodat handelende personen veilig, persoonlijk en gebruiksvriendelijk digitale diensten af kunnen nemen.

Verdere rationale voor deze generieke functie is te vinden in:
- Wettelijk kaders A, B, C, D, E, G, H, K, L
- Beleidskader N

Wettelijke en beleidskaders die van invloed zijn op deze generieke functie zijn: F, I, J.

Maatschappelijke en technische ontwikkelingen die van invloed zijn op deze generieke functie zijn: O, P, Q, R, S, T, U.

Implicaties
Zie voor de implicaties de onderliggende generieke functies:
1. Kunnen laten beschikken over digitale identificatiemiddelen
2. Kunnen laten gebruiken van digitale identificatiemiddelen
3. Kunnen inzage geven in identificatiemiddelen en gebruik
4. Kunnen instaan voor betrouwbaarheid en veiligheid van authenticatie

Voorbeelden
Zie de voorbeelden bij de onderliggende generieke functies.

5.2 Kunnen laten beschikken over digitale identificatiemiddelen

GA-GF-IA01 – Kunnen laten beschikken over digitale identificatiemiddelen

ID: GA-GF-IA01

Naam
Korte naam: Voorzien in identificatiemiddelen
Lange naam: Kunnen laten beschikken over digitale identificatiemiddelen

Beschrijving
Het ervoor kunnen zorgen dat personen kunnen beschikken over digitale identificatiemiddelen waarmee ze hun identiteit kunnen aantonen. Hieronder valt het uitgeven, wijzigen en beëindigen of intrekken van digitale identificatiemiddelen.

Rationale
De overheid moet voorwaarden scheppen zodat personen veilig, persoonlijk en gebruiksvriendelijk digitale diensten af kunnen nemen. Een noodzakelijke voorwaarde daarvoor is zorgen dat ze kunnen beschikken over digitale identificatiemiddelen van een voldoende betrouwbaarheidsniveau.

Verdere rationale voor deze generieke functie is te vinden in:
- Wettelijk kaders A, B, C, D, E, G, H, K, L, M
- Beleidskader N

Wettelijke en beleidskaders die van invloed zijn op deze generieke functie zijn: F, I, J.

Maatschappelijke en technische ontwikkelingen die van invloed zijn op deze generieke functie zijn: O, P, Q, R, S, T, U.

GA-GF-IA01 – Kunnen laten beschikken over digitale identificatiemiddelen

Implicaties

a. Personen moeten identificatiemiddelen kunnen verkrijgen, wijzigen en beëindigen.

b. Er moeten kaders en eisen zijn voor het verstrekken, wijzigen, beëindigen en gebruiken van identificatiemiddelen, die gelden ongeacht door wie de middelen worden uitgegeven.

c. Er moeten voorzieningen (o.a. organisaties) zijn om identificatiemiddelen uit te geven, beheren en beëindigen.

d. Er moet voorlichting zijn over beschikbare middelen en veilig en verantwoord gebruik ervan. En ondersteuning voor personen bij het verkrijgen en beheren van identificatiemiddelen. Hierbij moet goed worden afgewogen hoe met het dilemma maximale privacy moet worden omgegaan. Het is niet voldoende om mensen inlogmiddelen te geven. Er moet ook zijn nagedacht over bijvoorbeeld herstel bij verlies van het middel.

e. Als de overheid publieke identificatiemiddelen uitgeeft dient ze over de hiervoor genoemde voorzieningen te beschikken of deze taak uit te besteden.
In de memorie van toelichting bij het voorstel voor de Wdo is beschreven dat de regering wil dat burgers niet afhankelijk zijn van de beschikbaarheid van private middelen voor het verkrijgen van toegang tot digitale dienstverlening in het publieke domein. Burgers kunnen sinds 1 januari 2021 DigiD Hoog gebruiken via de eID-applicatie op de wettelijke identificatiedocumenten. Bovendien kan de overheid, ten behoeve van inclusie, eenvoudiger zorgen voor identificatiemiddelen die ook bruikbaar zijn voor specifieke doelgroepen die private aanbieders niet of minder snel zullen aanbieden.

f. Interoperabiliteit voor digitale identiteiten en betrouwbaarheidsniveau's moeten gewaarborgd worden, zowel nationaal als internationaal.

g. Om identificatiemiddelen uit te kunnen geven zijn betrouwbare identiteiten en identificerende gegevens nodig waar middelenuitgevers gebruik van moeten kunnen maken om in de middelen op te nemen. Het Nederlandse stelsel bevat daarvoor de BRP en het Handelsregister als gezaghebbende bronnen. Er zijn echter ook groepen van personen die niet in deze bronnen zijn geregistreerd. Ook zijn er ingezetenen die niet beschikken over een Nederlands identiteitsdocument.[38] Voor deze groepen moeten andere bronnen worden bepaald die aan de (betrouwbaarheids-)eisen voor gezaghebbende bronnen voldoen. Tot deze groepen behoren personen op de BES-eilanden, Nederlanders die naar het buitenland zijn verhuisd (en daardoor niet zijn geregistreerd in RNI) en buitenlanders en organisaties buiten Europa. Ook zijn er groepen die wel in een gezaghebbende bron zijn geregistreerd, maar geen identificatiedocument zoals een paspoort hebben en daarom niet een identificatiemiddel met een hoog betrouwbaarheidsniveau kunnen gebruiken.

Voorbeelden

Voorbeelden van bestaande oplossingen voor het uitgeven van middelen (niet alleen voor natuurlijke personen) zijn DigiD, eHerkenning, iDIN, PKIoverheid en de UZI-pas.

5.3 Kunnen laten gebruiken van digitale identificatiemiddelen

GA-GF-IA02 – Kunnen laten gebruiken van digitale identificatiemiddelen

ID: GA-GF-IA02

Naam

Korte naam: Authenticeren
Lange naam: Kunnen laten gebruiken van digitale identificatiemiddelen

[38] Dit zijn in Nederland ingezetenen, die afkomstig zijn van buiten Europa, en die niet beschikken over een Nederlands identiteitsdocument. Zij wonen in Nederland, staan ingeschreven in de BRP en hebben ook een BSN, maar omdat het Nederlandse identiteitsdocument aan de basis staat van betrouwbaarheidsniveau Substantieel en Hoger, kunnen zij nog niet aan een inlogmiddel op dat hogere betrouwbaarheidsniveau komen.

GA-GF-IA02 – Kunnen laten gebruiken van digitale identificatiemiddelen

Beschrijving
Het ervoor kunnen zorgen dat personen hun digitale identificatiemiddelen kunnen gebruiken om hun identiteit digitaal op een passend betrouwbaarheidsniveau aan te tonen.

Rationale
De overheid moet voorwaarden scheppen zodat burgers en bedrijven veilig, persoonlijk en gebruiksvriendelijk digitale diensten af kunnen nemen. Een noodzakelijke voorwaarde daarvoor is zorgen dat ze hun digitale identificatiemiddelen kunnen gebruiken om toegang te krijgen tot publieke diensten en ook tot diensten buiten het publieke domein.

Verdere rationale voor deze generieke functie is te vinden in:
- Wettelijk kaders A, B, C, D, E, G, H, K, L, M
- Beleidskader N

Maatschappelijke en technische ontwikkelingen die van invloed zijn op deze generieke functie zijn: O, P, Q, R, S, T, U.

Implicaties

a. De dienstverlener moet de handelend persoon in staat stellen zijn toegelaten identificatiemiddelen te gebruiken en moet deze ook accepteren.

b. De dienstverlener moet in staat worden gesteld om het identificatiemiddel te (laten) verifiëren. Deze verificatie kent de volgende stappen: verificatie van de echtheid van het middel, de geldigheid van het middel, het betrouwbaarheidsniveau van het middel en de identiteit van de gebruiker. Dit zijn generiek ook de stappen die bij cryptografie gedaan worden.

c. Dienstverleners moeten het voor hun dienstverlening benodigde betrouwbaarheidsniveau van authenticatie vaststellen en aangeven/toepassen bij het verlenen van toegang.

d. Authenticatie gaat gepaard met identificatie; er moeten duidelijke afspraken komen welke gegevens -- onder voorwaarden -- voor identificatie beschikbaar (kunnen) worden gesteld bij een authenticatie.

e. Authenticatie dient als basis geschikt te zijn en gebruikt te worden voor de overige beoordelingen bij het verlenen van toegang, zoals het beoordelen van de bevoegdheden van de handelend persoon.

Voorbeelden
Voorbeelden van bestaande oplossingen voor authenticatie zijn de authenticatievoorzieningen van DigiD, eHerkenning, iDIN, en de UZI-pas.

5.4 Kunnen inzage geven in identificatiemiddelen en gebruik

GA-GF-IA03 – Kunnen inzage geven in identificatiemiddelen en gebruik

ID: GA-GF-IA03

Naam
Korte naam: Inzage geven
Lange naam: Kunnen inzage geven in identificatiemiddelen en gebruik

Beschrijving
Het ervoor kunnen zorgen dat bezitters van identificatiemiddelen inzage hebben in de middelen waarover ze beschikken en de gebruikshistorie ervan.

Rationale
Personen dienen regie te kunnen voeren op alle door hen in het stelsel geactiveerde identificatiemiddelen en zicht te hebben op het gebruik daarvan.

Verdere rationale voor deze generieke functie is te vinden in:
- Wettelijk kaders E
- Maatschappelijke en technische ontwikkelingen P.

Verdere rationale voor deze generieke functie is ook te vinden in de GA-basisprincipes:

GA-GF-IA03 – Kunnen inzage geven in identificatiemiddelen en gebruik

- Denken vanuit behoeften van burgers en bedrijven (GA-BP-1)
- Overheidsdiensten zijn veilig en betrouwbaar (GA-BP-6)

Implicaties

a. De verschillende rollen (dienstverlener, authenticatiedienst, middelenuitgever en indien nodig identiteitenbeheerder) moeten gegevens beschikbaar maken om de bezitter van identificatiemiddelen inzage te kunnen geven in zijn middelen en de gebruikshistorie.

Voorbeelden
Een voorbeeld van een overzicht voor de middelenbezitter is het Inzageregister BSNk dat in ontwikkeling is.

5.5 Kunnen instaan voor betrouwbaarheid en veiligheid van authenticatie

GA-GF-IA04 – Kunnen instaan voor betrouwbaarheid en veiligheid van authenticatie

ID: GA-GF-IA04

Naam
Korte naam: Instaan voor betrouwbaarheid en veiligheid
Lange naam: Kunnen instaan voor betrouwbaarheid en veiligheid van authenticatie

Beschrijving
Het ervoor kunnen zorgen dat identificatie en authenticatie veilig en betrouwbaar kan plaatsvinden, waaronder het voorkomen, detecteren, opvolgen en herstellen van fraude met identificatiemiddelen.

Rationale
De overheid moet voorwaarden scheppen zodat personen veilig, persoonlijk en gebruiksvriendelijk digitale diensten af kunnen nemen en maatregelen nemen zodat ze in kan staan voor de betrouwbaarheid en veiligheid ervan.

Verdere rationale voor deze generieke functie is te vinden in:

- Wettelijk kaders D, E
- Maatschappelijke en technische ontwikkelingen O, R.

Verdere rationale voor deze generieke functie is ook te vinden in de GA-basisprincipes:

- Denken vanuit behoeften van burgers en bedrijven (GA-BP-1)
- Overheidsdiensten zijn veilig en betrouwbaar (GA-BP-6)

Implicaties

a. Er dient toezicht en handhaving te zijn m.b.t. authenticatiefraude, zodat dit wordt voorkomen, gedetecteerd en opgevolgd. Het moet mogelijk zijn identificatiemiddelen te blokkeren en in te trekken en om de gevolgen van authenticatiefraude te herstellen.

Voorbeelden
Het Meldpunt Fouten in Overheidsregistraties is een voorbeeld van een meldpunt dat burgers en bedrijven helpt bij het herstellen van fouten en de gevolgen ervan, in dit geval bij fouten in overheidsregistraties.

5.6 Generieke functies versus kaders

Onderstaande tabel geeft de relatie weer tussen de rationale van de generieke functies en de kaders.

Kaders / **Generieke functies**	1. Voorzien in authenticatie-middelen	2. Authenticeren	3. Inzage geven	4. Instaan voor betrouw-baarheid
A. eIDAS	X	X		
B. DSG	X	X		
C. eIDAS-revisie en DBI	X	X		
D. Wdo	X	X	X	X
E. AVG	X	X	X	X
F. BRP en HR	X	X	X	
G. Wet hergebruik overheidsinfo	X	X		
H. Wabb	X	X		
I. Wid	X	X		
J. Vreemdelingenwet	X	X		
K. Awb	X	X		
L. WEBV	X	X		
M. Overige juridica	X	X		
N. NL Digibeter	X	X		
O. Voorwaarden door de overheid	X	X		X
P. Inzage, privacy en beveiliging	X	X	X	
Q. Middelen hoog en substantieel	X	X		
R. Verschillende contexten	X	X		X
S. Verifieerbare beweringen	X	X		
T. Snelle ontwikkeling	X	X		
U. Samenwerking publiek privaat	X	X		

5.7 Raakvlakken met andere domeinen

Voor de generieke functies van identificatie en authenticatie bestaan de volgende raakvlakken met andere (sub-)domeinen binnen en buiten de scope van de GA:

1. Machtigen en vertegenwoordigen
   Identificatie en authenticatie is noodzakelijk voor het domein Machtigen en vertegenwoordigen (zie GDI-Architectuur Machtigen & vertegenwoordigen). De personen betrokken bij een vertegenwoordigingsrelatie moeten uniek geduid kunnen worden. Als de vertegenwoordiger toegang tot een digitale dienst vraagt moet zijn digitale identiteit worden bepaald, zodat kan worden vastgesteld of hij de benodigde vertegenwoordigingsbevoegdheid heeft om de dienst namens een ander af te nemen.
2. Interactie
   Identificatie en authenticatie van personen bij digitale dienstverlening vormt in het domein Interactie een basis voor veilige en betrouwbare informatie-uitwisseling met burgers en bedrijven.
3. Gegevensuitwisseling
   Identificatie en authenticatie van organisaties en hun informatiesystemen bij uitwisseling van gegevens tussen overheidsorganisaties onderling en met bedrijven is noodzakelijk voor het domein Gegevensuitwisseling. Deze vorm van identificatie en authenticatie is niet in scope van deze versie van de architectuur.
   Identificatiegegevens worden ook gedeeld voor andere doeleinden dan identificatie en authenticatie, bijvoorbeeld bij het delen van attributen (kenmerken van een entiteit in digitale vorm, zoals een geboortejaar) vanuit een wallet.
4. Identiteitenbeheer
   Om identificatiemiddelen uit te kunnen geven zijn betrouwbare digitale identiteiten en identificerende gegevens nodig waar middelenuitgevers gebruik van moeten kunnen maken om in de middelen op te nemen. Het Nederlandse stelsel kent de BRP en het Handelsregister als gezaghebbende of authentieke bronnen. Er zijn echter ook groepen van personen die momenteel niet in deze bronnen zijn geregistreerd. Voor deze groepen moet worden bepaald welke identiteitenbronnen gebruikt kunnen worden als basis voor het uitgeven van identificatiemiddelen.

6 Principes voor identificatie en authenticatie

Dit hoofdstuk beschrijft de principes voor identificatie en authenticatie. Een principe is een stelling over een gewenste, generieke, kwalitatieve eigenschap waar architectuur invulling aan moet geven in de publieke sector. De GA-principes vullen de NORA-principes aan met principes die specifiek zijn voor gerichte doorontwikkeling van de GDI.

We onderscheiden binnen de GA twee soorten principes:

- Basisprincipes: voor de hele GA geldende principes.
- Domeinprincipes: principes voor een specifiek domein of subdomein binnen de GA.

Identificatie en authenticatie kent geen principes die specifiek voor het subdomein zijn. Dit hoofdstuk beschrijft daarom alleen de implicaties van de GA-basisprincipes.

De GA-basisprincipes zijn:[39]

1. Denken vanuit behoeften van burgers en bedrijven (GA-BP-1)
2. Rekening houden met diversiteit bij burgers en bedrijven (GA-BP-2)
3. Rekening houden met diversiteit bij dienstverleners (GA-BP-3)
4. Gebruik van flexibele en ontkoppelde functies (GA-BP-4)
5. Afspraken voor standaarden voor generieke voorzieningen (GA-BP-5)
6. Overheidsdiensten zijn veilig en betrouwbaar (GA-BP-6)

De grijs gearceerde tekst bij de principes hieronder is ter informatie steeds overgenomen uit de beschrijving van de GA-basisprincipes.

6.1 Denken vanuit behoeften van burgers en bedrijven (GA-BP-1)

GA-BP-1 - Denken vanuit behoeften van burgers en bedrijven

De beschrijving en rationale van dit GA-basisprincipe zijn als volgt:

Beschrijving

We nemen de NORA-basisprincipes over als vertaling van denken vanuit de behoeften van "burgers en bedrijven" bij het realiseren van diensten (N.B.: NORA gebruikt de term "afnemers" waar GA de term burgers en bedrijven gebruikt):

- *BP01 Proactief: Afnemers krijgen de dienstverlening waar ze behoefte aan hebben*
- *BP02 Vindbaar: afnemers kunnen de dienst eenvoudig vinden.*
- *BP03 Toegankelijk: afnemers hebben eenvoudig toegang tot de dienst.*
- *BP04 Standaard: afnemers ervaren uniformiteit in de dienstverlening door het gebruik van standaardoplossingen.*
- *BP05 Gebundeld: afnemers krijgen gerelateerde diensten gebundeld aangeboden.*
- *BP06 Transparant: afnemers hebben inzage in voor hen relevante informatie.*
- *BP07 Noodzakelijk: afnemers worden niet geconfronteerd met overbodige vragen.*
- *BP08 Vertrouwelijk: afnemers kunnen erop vertrouwen dat informatie niet wordt misbruikt.*
- *BP09 Betrouwbaar: afnemers kunnen erop vertrouwen dat de dienstverlener zich aan afspraken houdt.*
- *BP10 Ontvankelijk: afnemers kunnen input leveren over de dienstverlening.*

Rationale

De overheid wil, voor zover dit mogelijk is binnen haar beleidsuitvoeringstaken, aansluiten bij behoeftes van burgers en bedrijven.

De GDI gaat over de generieke infrastructuur die nodig is om de (digitale) overheid te faciliteren. Met de GDI los je geen maatschappelijk vraagstuk op. Dat is de taak van de betreffende uitvoeringsorganisatie of overheid en gebaseerd op de politieke keuzes die

[39] De GA-basisprincipes zijn beschreven in het document 'GA Basisprincipes' op NORA online.

GA-BP-1 - Denken vanuit behoeften van burgers en bedrijven
worden gemaakt. De GDI moet wel in staat zijn om hen daarbij te faciliteren. Daarbij blijft de behoefte van burgers en bedrijven centraal. *Bundeling van deze tien NORA basisprincipes vergemakkelijkt het gebruik binnen GA doordat hier integraal aan gerefereerd kan worden.*

De implicaties van dit principe zijn:

1. Burgers en bedrijven kunnen beschikken over de identificatiemiddelen met betrouwbaarheidsniveaus die nodig zijn om toegang te krijgen tot digitale diensten.
2. Burgers en bedrijven kunnen op eenvoudige wijze gebruik maken van hun identificatiemiddelen om toegang te krijgen.
3. Burgers en bedrijven kunnen hun identificatiemiddelen op dezelfde manier gebruiken voor verschillende publieke en private diensten.
4. Burgers en bedrijven hebben inzage in hun identificatiemiddelen en het gebruik ervan.
5. Burgers en bedrijven hoeven zich alleen te authenticeren voor diensten waarvoor dat nodig is en alleen op het betrouwbaarheidsniveau dat nodig is voor de dienst.
6. Burgers en bedrijven moeten zich, o.a. bij het wisselen van dienstverlener, alleen opnieuw authenticeren als dat vanuit beveiligingsoptiek nodig is. De wijze van herauthenticatie sluit aan bij het betrouwbaarheidsniveau van de dienst. Dit wordt ook wel aangeduid als een single-sign-on-achtige gebruikerservaring.
7. Publieke diensten worden niet uitsluitend in een overheidsomgeving aangeboden, maar meer en meer in de door de burger en bedrijven zelf gekozen digitale omgeving. Burgers en bedrijven kunnen daarom de digitale diensten in een zelf gekozen digitale omgeving afnemen en daar gebruik maken van hun toegelaten identificatiemiddelen.

6.2 Rekening houden met diversiteit bij burgers en bedrijven (GA-BP-2)

GA-BP-2 - Rekening houden met diversiteit bij burgers en bedrijven
De beschrijving en rationale voor dit GA-basisprincipe zijn als volgt: *Beschrijving* *We houden rekening met diversiteit bij burgers en bedrijven.* *Rationale* *Zowel "burgers als bedrijven" kunnen in meerdere opzichten sterk van elkaar verschillen. Dit kan voortkomen uit het door de verschillende rollen die een gebruiker vervult (burger, ondernemer, professional, andere overheden) in de context waarbinnen hij met de overheid te maken heeft. Maar verschillende personen in dezelfde rol en context zijn ook niet identiek (digitale vaardigheid, persoonlijke aard, persoonlijke omstandigheden). Bovendien heeft de Nederlandse overheid niet alleen met Nederlandse burgers en bedrijven maar ook met EU-burgers en –bedrijven en daarbuiten van doen.* De implicaties van dit principe zijn: 1. Authenticatie is mogelijk voor alle burgers en bedrijven die vanuit hun rechten en plichten toegang moeten hebben tot digitale publieke diensten, ongeacht nationaliteit en verblijfplaats.

6.3 Rekening houden met diversiteit bij dienstverleners (GA-BP-3)

GA-BP-3 - Rekening houden met diversiteit bij dienstverleners

De beschrijving en rationale voor dit GA-basisprincipe zijn als volgt:

Beschrijving

We houden rekening met diversiteit bij dienstverleners.

Rationale

De GDI bestaat uit generieke functies die voor vrijwel alle partijen binnen de (digitale) overheid van toepassing zijn. Maar dienstverleners kunnen in meerdere opzichten sterk van elkaar verschillen.

Voor onderstaande implicaties is dit GA-basisprincipe geïnterpreteerd als 'Denken vanuit behoeften van dienstverleners'.

De implicaties van dit principe zijn:

1. Dienstverleners kunnen alle soorten identificatiemiddelen op vergelijkbare wijze verwerken.
2. De oplossingen voor authenticatie zijn door dienstverleners eenvoudig in te passen in hun proces voor het verlenen van toegang tot hun digitale diensten.
3. Dienstverleners kunnen gebruik maken van 'ontzorgende functies' (ook wel: intermediaire functies, routeringsvoorzieningen of knooppunten) bij het accepteren van identificatiemiddelen.
4. Dienstverleners hebben de ruimte om zelf voorzieningen te maken, zoals een routeringsvoorziening om aan te sluiten op de verschillende authenticatiediensten.

6.4 Gebruik van flexibele en ontkoppelde functies (GA-BP-4)

GA-BP-4 - Gebruik van flexibele en ontkoppelde functies

De beschrijving en rationale voor dit GA-basisprincipe zijn als volgt:

Beschrijving

We gebruiken functies die los van elkaar kunnen werken en samenwerken via gestandaardiseerde diensten.

Rationale

Ontkoppeling draagt bij aan wendbaarheid en robuustheid.

We willen rekening houden met veranderende politieke en beleidswensen. Het is daarom nodig om bij de ontwerpkeuzen voldoende flexibiliteit en vrijheidsgraden in te bouwen. Dit is vergelijkbaar met rekening houden met ontwikkelingen in IT: je weet dat die er zullen komen, je weet alleen niet wanneer en in welke vorm ze komen.

Vanuit Europa en ook daarbuiten hebben wetten, richtlijnen en wensen invloed op het handelen van onze (digitale) overheid. Dat vraagt om flexibiliteit om op nieuwe ontwikkelingen in te spelen. Dit vraagt ook om het realiseren van gestandaardiseerde koppelvlakken die eenduidig gebruik mogelijk maken om waar mogelijk invloeden te beperken. Deze koppelvlakken met Europa als generieke functies zien, maakt het mogelijk hiervoor een generieke oplossing in de vorm van een standaard of 'gateway'-voorziening in te richten. Zo staan afzonderlijke organisaties niet voor het verbindingsprobleem en helpen we de burger buiten Nederland met een meer uniforme behandeling.

De ervaring leert dat technologie en beleid zich snel ontwikkelen. Architectuur moet dat mogelijk maken. We mogen bij de inrichting dus niet alleen uit gaan van het huidige situatie, maar moeten ook toekomstige beleidsontwikkelingen maximaal mogelijk maken en technologische ontwikkelingen kunnen volgen.

GA-BP-4 - Gebruik van flexibele en ontkoppelde functies
De implicaties van dit principe zijn: 1. Oplossingen voor authenticatie zijn flexibel opgezet zodat ze aangepast kunnen worden aan toekomstige ontwikkelingen in wetgeving, beleid en technologie. Ze zijn daarvoor o.a. gebaseerd op open standaarden. 2. Oplossingen voor authenticatie kunnen worden gecombineerd met oplossingen voor de andere onderdelen van toegang verlenen, zoals vertegenwoordiging, om dienstverleners te ontzorgen met 'totaaloplossingen'.

6.5 Afspraken voor standaarden voor generieke voorzieningen (GA-BP-5)

GA-BP-5 - Afspraken voor standaarden voor generieke voorzieningen
De beschrijving en rationale voor dit basisprincipe zijn als volgt: *Beschrijving* *De generieke functies in de digitale basisinfrastructuur worden ingevuld door afspraken, standaarden en voorzieningen. Daarbij gaan afspraken boven standaarden en gaan standaarden boven voorzieningen.* *Rationale* *Uitvoeringsorganisaties hebben vaak een andere populatie van burgers en bedrijven en andere wetgeving waarbinnen zij hun taken uitvoeren. Het maken van afspraken is een flexibele manier om binnen een diverse overheid tot resultaten te komen. Het biedt dienstverleners maximale vrijheid om in hun dienstverlening de optimale invulling voor burgers en bedrijven te realiseren.* *Verder is er een tendens waarbij burgers en bedrijven steeds vaker autonomie vragen om eigen middelen (bijvoorbeeld voor authenticatie of beheer van persoonlijke gegevens) te kunnen toepassen. Dat vraagt om een overheid die middelen accepteert die de burger al heeft en voorwaarden stelt waaronder dat mogelijk is. Dat betekent dus minder overheids-voorzieningen maken en meer afsprakenstelsels om aan te sluiten.* *In het belang van burgers en bedrijven en uitvoering van de wet kan het noodzakelijk zijn naast afspraken ook standaarden of ook generieke voorzieningen toe te passen.* *Gebruik van generieke voorzieningen door (deels) autonome organisaties kan binnen het Nederlandse bestuurlijk bestel in de praktijk leiden tot grote uitdagingen. De functies van de GDI worden daarom bij voorkeur gerealiseerd via generieke afspraken en standaarden. Als de beoogde doelen hiermee niet worden bereikt, worden voorzieningen geïntroduceerd. Een voorziening die juist vrijheden geeft (door ontkoppeling volgens GA-BP-4) helpt wel bij deze uitdagingen.* De implicaties van dit principe zijn: 1. Geen andere implicaties dan beschreven in het document GA-basisprincipes.

6.6 Overheidsdiensten zijn veilig en betrouwbaar (GA-BP-6)

GA-BP-6 - Overheidsdiensten zijn veilig en betrouwbaar
De beschrijving en rationale voor dit basisprincipe zijn als volgt: *Beschrijving* *De overheid moet ervoor zorgen dat hun diensten aan burgers en bedrijven veilig en betrouwbaar zijn.* *Rationale* *Burgers en bedrijven moeten er vanuit kunnen gaan dat hun contact met de overheid veilig en betrouwbaar verloopt, zodat ze zonder risico's gebruik kunnen maken van hun rechten en kunnen voldoen aan hun plichten.*

GA-BP-6 - Overheidsdiensten zijn veilig en betrouwbaar
'Vertrouwelijk' en 'Betrouwbaar' is ook onderdeel van het GA-basisprincipe GA-BP-1. Dit wordt hier (ook) als zelfstandig architectuurprincipe opgenomen vanwege het belang om expliciet aandacht te geven aan een veilige en betrouwbare werking van alle domeinen van de GDI.

De implicaties van dit principe zijn:

1. De uitgifte van identificatiemiddelen is betrouwbaar, bijvoorbeeld door het inbouwen van fysieke contactmomenten waar nodig en maatregelen die betrouwbare uitgifte op afstand, zonder fysiek contact, mogelijk maken.
2. Er zijn maatregelen om fraude met identificatiemiddelen te voorkomen, detecteren en op te lossen. Bezitters van identificatiemiddelen worden in staat gesteld om fouten en misbruik en de gevolgen ervan te (laten) herstellen. Ook zijn er mogelijkheden om middelen in te trekken als daar een aanleiding voor is.
3. Er zijn maatregelen om de privacy van bezitters van identificatiemiddelen te waarborgen. Persoonsgegevens worden alleen verstrekt voor zover nodig voor authenticatie en onder de juiste voorwaarden.
4. Er zijn maatregelen om veranderingen in identificatiemiddelen te signaleren aan de bezitter.

7 Keuzes voor identificatie en authenticatie

Dit hoofdstuk beschrijft de keuzes voor identificatie en authenticatie; keuzes die resulteren in afspraken, standaarden en voorzieningen die invulling geven aan de generieke functies in het domein.

Op NORA online is beschreven wat we in de GDI-Architectuur verstaan onder generieke functies, afspraken, standaarden en voorzieningen:
*"[Een] **generieke functie**: "iets wat meerdere overheidsorganisaties moeten kunnen voor het uitvoeren van hun taken". Het gaat daarbij over capaciteiten waarover overheidsorganisaties in relatie tot de buitenwereld moeten beschikken die zodanig generiek zijn dat ze op een vergelijkbare manier zijn in te richten. Vaak met behulp van informatietechnologie. Een voorbeeld van een generieke functie is het digitaal kunnen identificeren en authenticeren van burgers en bedrijven.*

*Om generieke functies binnen de overheid op een vergelijkbare manier in te richten maken we afspraken. Een **afspraak** is een "overeenkomst binnen de overheid of een deel (domein of sector) over de inrichting en het toepassen van generieke functies". Afspraken kunnen een verschillend karakter hebben en gaan over hoe we samenwerken (proces, taken, verantwoordelijkheden), over het toepassen van standaarden en/of voorzieningen. Afspraken zijn vastgelegd in een wet (bijv. de Wet Digitale Overheid) of in bijvoorbeeld AMVB's, regelingen, beleidsregels of convenanten.*

*Bij de realisatie van een generieke functie kan gebruik worden gemaakt van (een) **standaard**(en): "een set van regels die beschrijven hoe mensen materialen, producten, diensten, technologieën, taken, processen en systemen dienen te ontwikkelen en beheren". De lijst open standaarden van het Forum Standaardisatie speelt daarbij een belangrijke rol omdat ze voor alle overheidsorganisaties worden aanbevolen of verplicht zijn om te gebruiken.*

*Voor de realisatie van generieke functies kan gebruik worden gemaakt van (een) **voorziening**(en): een "groepering van services die aan afnemers worden aangeboden, met als doel het bevorderen van uniformiteit en efficiëntie binnen de overheid". Een voorziening kan bedrijfs- en/of applicatie- en/of technologische services leveren. In de praktijk is het meestal een combinatie van services. Bij een voorziening hoort ook een 'leveringsproduct': "op schrift gestelde voorwaarden op basis waarvan de levering van diensten plaatsvindt".*

Samenvattend geldt dat voor het inrichten van generieke functies afspraken, standaarden en voorzieningen nodig zijn. Het bereik van afspraken, standaarden en voorzieningen kan verschillen. In de meest brede zin gelden ze voor alle overheidsorganisaties zodat een generieke functie door alle organisaties op een vergelijkbare manier wordt ingericht. Ze vallen dan binnen het domein van de Generieke Digitale Infrastructuur (GDI) en de daarbij behorende GDI-Architectuur (GA). Ze kunnen echter ook gelden voor een deelverzameling van overheidsorganisaties. Bijvoorbeeld voor alle organisaties binnen een sector of keten."

Voor identificatie en authenticatie gelden per generieke functie (zie hoofdstuk 5) onderstaande keuzes. Deze zijn in de paragrafen die volgen nader beschreven.

Generieke functie 1: Kunnen laten beschikken over digitale identificatiemiddelen

A. ***Toelating van middelen van meerdere middelenuitgevers***
Overeenkomstig de eIDAS-verordening en de Wdo zijn er afspraken voor toelating van identificatiemiddelen van meerdere middelenuitgevers.[40] De middelen zijn zowel voor toegang tot diensten ten behoeve van de bezitter zelf als voor gebruik bij vertegenwoordiging van andere personen en van organisaties.[41] De middelen zijn voor toegang tot publieke en private dienstverlening en in een privé en een zakelijke context te gebruiken.[42] Ook zijn er afspraken over het blokkeren en intrekken van uitgegeven

[40] Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties kiest er in de uitwerking van de Wet digitale overheid (Wdo) voor om in het bedrijvendomein de rol Authenticatiedienst te activeren en de rol Middelenuitgever niet. Dit om de complexiteit van de regelgeving te beperken. Dat betekent dat een partij die de rol van Authenticatiedienst vervult ook de rol van Middelenuitgever vervult. In de uitwerking van de Wdo wordt in het bedrijvendomein ook de rol Machtigingsdienst geactiveerd. Deze rol is niet in scope van deze architectuur, maar van de GDI-architectuur voor Machtigen en vertegenwoordigen.

[41] Het verstrekken en gebruiken van vertegenwoordigingsbevoegdheden is niet in scope van deze architectuur maar van de GDI-architectuur voor Machtigen en vertegenwoordigen.

[42] In de eerste tranche van de Wdo wordt onderscheid gemaakt tussen middelen in het burgerdomein en in het bedrijven- en organisatiedomein. Burgermiddelen zijn niet bestemd voor gebruik in het bedrijven- en

middelen. Overeenkomstig de Wdo zorgt de overheid voor aangewezen publieke middelen voor Nederlandse burgers, zodat ze voor toegang tot publieke diensten niet afhankelijk zijn van private middelen.[43]

Generieke functie 2: Kunnen laten gebruiken van digitale identificatiemiddelen

B. ***Verplichte acceptatie van toegelaten middelen door publieke dienstverleners***
Overeenkomstig de eIDAS-verordening en de Wdo zijn er afspraken voor acceptatie door dienstverleners van toegelaten identificatiemiddelen. Publieke dienstverleners zijn verplicht de toegelaten middelen te accepteren. Private dienstverleners kunnen ervoor kiezen deze te accepteren.

Generieke functie 3: Kunnen inzage geven in identificatiemiddelen en gebruik

C. ***Centraal overzicht van eigen identificatiemiddelen en inzage in gebruikshistorie***
Bezitters van toegelaten middelen kunnen beschikken over een overzicht van hun middelen. Het overzicht verwijst per middel naar de uitgever ervan, zodat de bezitter daar zijn middel kan beheren. Het overzicht verwijst ook per middel naar een overzicht van de gebruikshistorie.[44] Het overzicht van middelen en de overzichten van gebruikshistorie dragen bij aan transparantie richting de bezitter, aan regie door de bezitter op zijn middelen en aan detectie door de bezitter van eventueel misbruik van zijn middelen.

D. ***Notificatie bij wijziging en gebruik van eigen identificatiemiddelen***
Bezitters van identificatiemiddelen kunnen notificaties krijgen bij wijziging en gebruik ervan.[45] De gebruiker kan bepalen waarover, wanneer en hoe hij wordt genotificeerd. Ook dit draagt bij aan transparantie richting de bezitter, aan regie door de bezitter op zijn middelen en aan detectie door de bezitter van eventueel misbruik van zijn middelen.

Generieke functie 4: Kunnen instaan voor betrouwbaarheid en veiligheid van authenticatie

E. ***Afspraken voor toezicht en handhaving m.b.t. authenticatiefraude***
Er zijn afspraken over de verdeling van taken, verantwoordelijkheden en bevoegdheden over de partijen die deelnemen aan het stelsel voor identificatie en authenticatie i.h.k.v. het voorkomen, detecteren en opvolgen van authenticatiefraude.[46] Deze afspraken zijn nauw verweven met het afsprakenstelsel voor toezicht en handhaving m.b.t. identiteitsfraude.

Deze keuzes voor identificatie en authenticatie resulteren in de afspraken, standaarden en voorzieningen zoals weergegeven in de tabellen in de hiernavolgende paragrafen. Daarbij maken we onderscheid tussen:

- **Generieke centrale bouwstenen**: bouwstenen die voor alle gevallen gelden en die centraal (ook wel: landelijk) worden gerealiseerd. De afspraken, standaarden en centrale of landelijke voorzieningen behoren tot deze categorie.

organisatiedomein en bedrijfsmiddelen niet voor gebruik in het burgerdomein. In de tweede tranche van de Wdo wordt beoogd om dit onderscheid te laten vervallen. In deze architectuur maken we dit onderscheid daarom niet.

43 Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties kiest er in de eerste tranche van de Wdo voor om het gebruik van publieke middelen voor toegang tot private diensten uit te sluiten, omdat de regering het onwenselijk acht dat de rijksoverheid zich zou mengen in de markt van identificatiemiddelen voor diensten buiten het publieke domein. In deze architectuur hanteren we deze beperking niet, zodat de architectuur is voorbereid op het eventueel vervallen ervan.

44 Het Ministerie van Binnenlandse Zeken en Koninkrijksrelaties kiest er in de uitwerking van de Wdo voor dat bezitters inzage in hun geactiveerde middelen kunnen krijgen. Het bieden van inzage in de gebruikshistorie is onder de Wdo geen verplichting voor deelnemers aan het stelsel. Daar is voor gekozen om de verplichtingen voor deelnemers beperkt te houden. Inzage in de gebruikshistorie is wel wenselijk en daarom in de architectuur opgenomen.

45 Het Ministerie van Binnenlandse Zeken en Koninkrijksrelaties kiest er in de uitwerking van de Wdo voor dat bezitters genotificeerd worden over het activeren en intrekken van hun middelen. Het bieden van notificatie over gebruik is onder de Wdo geen verplichting voor deelnemers aan het stelsel. Daar is voor gekozen om de verplichtingen voor deelnemers beperkt te houden. Notificatie van gebruik is wel wenselijk en daarom in de architectuur opgenomen.

46 Onder authenticatiefraude verstaan we op basis van de 'concept regeling nadere eisen toelating identificatiemiddelen WDO' het volgende: authenticatie namens een persoon zonder diens toestemming. Authenticatiefraude is onderdeel van het bredere begrip 'identiteitsfraude'. Deze architectuur kijkt alleen naar authenticatiefraude en niet naar identiteitsfraude in brede zin.

- **Decentrale stelselvoorzieningen**: Voorzieningen die onderdeel zijn van een landelijke stelsel (met afspraken, standaarden en voorzieningen) en waar meerdere (decentrale) voorkomens van zijn. Al deze decentrale voorkomens voldoen aan de landelijke afspraken en standaarden
- **Oplossingen bij afnemers**: oplossingen die afnemers (de dienstverleners) moeten realiseren om aan te sluiten op en gebruik te maken van de bouwstenen van het stelsel. Deze oplossingen realiseren afnemers zelf of, indien gewenst, gezamenlijk (door een aantal partijen die ervoor kiezen om dat samen te doen). Het ontbreken van een generieke of dezentrale stelselvoorziening sluit niet uit dat een aantal afnemers een gezamenlijke voorziening inricht of laat inrichten en dat deze voorziening om bestuurlijke redenen onder de governance en/of financiering van de GDI valt.

Deze architectuur benoemt waarvoor afspraken, standaarden en voorzieningen nodig zijn. De nadere uitwerking van deze bouwstenen vindt plaats in de fases die volgen op deze architectuur.

De keuzes en bouwstenen zijn beschreven per generieke functie. De generieke functies zelf zijn beschreven in hoofdstuk 5.

In bijlage 9 is beschreven wat de verschillen zijn met de capability's die zijn beschreven in het pressurecooker-rapport.

7.1 Generieke functie 1: Kunnen laten beschikken over digitale identificatiemiddelen

7.1.1 Keuze A: Toelating van middelen van meerdere middelenuitgevers

Keuze
Toelating van identificatiemiddelen van meerdere middelenuitgevers

Toelichting bij de keuze
Overeenkomstig de eIDAS-verordening en de Wdo zijn er afspraken voor toelating van identificatiemiddelen van meerdere middelenuitgevers.[47] De middelen zijn zowel voor toegang tot diensten ten behoeve van de bezitter zelf als voor gebruik bij vertegenwoordiging van andere personen en van organisaties. [48] De middelen zijn voor toegang tot publieke en private dienstverlening en in een privé en een zakelijke context te gebruiken.[49] Ook zijn er afspraken over het blokkeren en intrekken van uitgegeven middelen. Overeenkomstig de Wdo zorgt de overheid voor aangewezen publieke middelen voor Nederlandse burgers, zodat ze voor toegang tot publieke diensten niet afhankelijk zijn van private middelen.[50]

Voor het uitgeven van betrouwbare identificatiemiddelen zijn authentieke of gezaghebbende bronnen met digitale identiteiten nodig. Het afsprakenstelsel maakt het mogelijk om middelen uit te geven op basis van meerdere erkende authentieke digitale-identiteitenbronnen. Hierdoor kunnen middelen worden uitgegeven op basis van andere bronnen dan de BRP en het Handelsregister. Dit is nodig, omdat de dekking van deze twee bronnen niet voldoende is voor iedereen die op basis van zijn rechten en plichten toegang moet kunnen hebben tot digitale publieke dienstverlening. Hiervoor moet een oplossing komen, bijvoorbeeld door de populatie van de BRP en het

47 Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties kiest er in de uitwerking van de Wet digitale overheid (Wdo) voor om in het bedrijvendomein de rol Authenticatiedienst te activeren en de rol Middelenuitgever niet. Dit om de complexiteit van de regelgeving te beperken. Dat betekent dat een partij die de rol van Authenticatiedienst vervult ook de rol van Middelenuitgever vervult. In de uitwerking van de Wdo wordt in het bedrijvendomein ook de rol Machtigingsdienst geactiveerd. Deze rol is niet in scope van deze architectuur, maar van de GDI-architectuur voor Machtigen en vertegenwoordigen.

48 Het verstrekken en gebruiken van vertegenwoordigingsbevoegdheden is niet in scope van deze architectuur maar van de GDI-architectuur voor Machtigen en vertegenwoordigen.

49 In de eerste tranche van de Wdo wordt onderscheid gemaakt tussen middelen in het burgerdomein en in het bedrijven- en organisatiedomein. Burgermiddelen zijn niet bestemd voor gebruik in het bedrijven- en organisatiedomein en bedrijfsmiddelen niet voor gebruik in het burgerdomein. In de tweede tranche van de Wdo wordt beoogd om dit onderscheid te laten vervallen. In deze architectuur maken we dit onderscheid daarom niet.

50 Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties kiest er in de eerste tranche van de Wdo voor om het gebruik van publieke middelen voor toegang tot private diensten uit te sluiten, omdat de regering het onwenselijk acht dat de rijksoverheid zich zou mengen in de markt van identificatiemiddelen voor diensten buiten het publieke domein. In deze architectuur hanteren we deze beperking niet, zodat de architectuur is voorbereid op het eventueel vervallen ervan.

Handelsregister uit te breiden of door aanvullende gezaghebbende bronnen aan te wijzen, bijvoorbeeld bij organisaties die contact hebben met personen die buiten de populatie van de BRP en het Handelsregister vallen, zoals de Belastingdienst, DUO en SVB. Een voorbeeld van zo'n aanvullende gezaghebbende bron is Probas als bron voor ambassades en consulaten.

Aan de digitale-identiteitenbronnen die worden gebruikt voor het uitgeven van middelen worden eisen gesteld om de betrouwbaarheidsniveaus van middelen te garanderen. Die eisen zijn onderdeel van het afsprakenstelsel voor identificatie en authenticatie.

De afspraken voor het toelaten van middelen maken het gebruik van verschillende soorten 'dragers' voor identificatiemiddelen mogelijk, zoals de in de eIDAS-revisie aangekondigde, in lidstaten erkende wallets.

In het afsprakenstelsel zijn ook afspraken opgenomen over het blokkeren en intrekken van uitgegeven middelen, waaronder afspraken over welke aanleidingen er daarvoor kunnen zijn, wie kan blokkeren of intrekken, wat de gevolgen ervan zijn en hoe de bezitter op de hoogte wordt gesteld en wordt geholpen.

Samen met de afspraken bij de andere in dit hoofdstuk beschreven keuzes ontstaat een afsprakenstelsel voor identificatie en authenticatie voor digitale diensten in het publieke en ook het private domein.

Bouwstenen
De volgende bouwstenen geven invulling aan deze keuze.

	Generieke centrale stelselbouwstenen	**Decentrale stelselvoorzieningen**	**Oplossingen bij stelselafnemers**
Afspraken	- Afspraken voor toelating van middelenuitgevers en middelen		
Standaarden	- Standaarden (normen) voor toegelaten middelen		
Voorzieningen	- Stelselregie-organisatie voor het beheren van de afspraken, het toelaten van middelen en het toezien op en handhaven van de afspraken	- Functionaliteiten van middelenuitgevers voor uitgeven van middelen, o.a. voor publieke middelen - Functionaliteiten van identiteiten-beheerders ten behoeve van het uitgeven van middelen	- Geen voor het toelaten en uitgeven van middelen

Rationale
De keuze is gebaseerd op de eIDAS-verordening en de Wdo. Betrouwbare identificatie en authenticatie zijn belangrijke voorwaarden voor betrouwbaar digitaal zakendoen. De afspraken maken een verschuiving mogelijk van het uitgeven van identificatiemiddelen voor mensen alleen door de overheid naar een stelsel waarin meer keuze voor burgers en bedrijven ontstaat voor de middelen die ze kunnen gebruiken en meer duidelijkheid voor private partijen voor het aanbieden van middelen die passen binnen de gestelde kaders. Het stelsel zorgt voor meer robuustheid, doordat het niet afhankelijk is van één identificatiemiddel uitgegeven door één partij met één authenticatiedienst.

De overheid geeft identificatiemiddelen uit als daarmee de werking, betrouwbaarheid en veiligheid van het digitaal zaken doen wordt bevorderd, of wanneer dit gedreven wordt door relevante Europese en/of internationale ontwikkelingen en standaarden. De overheid wil echter ook private partijen toelaten om de markt voor identificatiemiddelen te betreden, zoals dat al mogelijk is in het afsprakenstelsel eHerkenning.

De afspraken betekenen niet dat personen meer identificatiemiddelen *moeten* gebruiken. Het betekent dat ze uit meer middelen kunnen kiezen dan bijvoorbeeld alleen DigiD en dat ze hun toegelaten middelen voor meer doeleinden kunnen gebruiken, ook buiten publieke dienstverlening en zowel in een particuliere als in een zakelijke context.

De afspraken en het bijbehorende toezicht en handhaving hierop moet vertrouwen geven, vergelijkbaar met hoe het paspoort vertrouwen geeft.

Verdere rationale voor deze keuze is te vinden in:
- eIDAS en eIDAS-revisie
- Wdo
- Denken vanuit behoeften van burgers en bedrijven (GA-BP-1)
- Rekening houden met diversiteit bij burgers en bedrijven (GA-BP-2)
- Gebruik van flexibele en ontkoppelde functies (GA-BP-4)
- Afspraken voor standaarden voor generieke voorzieningen (GA-BP-5)

Nadere toelichting bouwstenen
Generieke centrale stelselbouwstenen
Afspraken:
- Afspraken voor toelating van middelenuitgevers en middelen:
    - Rollen, taken en verantwoordelijkheden van middelenuitgevers.
    - Toezicht op en handhaving van de afspraken voor toelating van middelenuitgevers en middelen.
    - Toelating van middelenuitgevers en middelen.
    - Betrouwbaarheidsniveaus van middelen.
    - Eisen aan bronnen voor digitale identiteiten op basis waarvan middelen worden uitgegeven.
    - Ondersteuning van gebruikers bij het verkrijgen en beheren van middelen. Een belangrijk aandachtspunt hierbij is het spanningsveld tussen ondersteuning enerzijds en privacy anderzijds. Het is niet voldoende om mensen inlogmiddelen te geven, er moet ook zijn nagedacht over herstel bij verlies van het middel.
    - Privacy-beschermende maatregelen voor het uitgeven van middelen en het ondersteunen van bezitters.
    - Afspraken over blokkeren en intrekken van uitgegeven middelen, waaronder afspraken over welke aanleidingen er daarvoor kunnen zijn, wie kan blokkeren of intrekken, wat de gevolgen ervan zijn en hoe de bezitter op de hoogte wordt gesteld en wordt geholpen.

Standaarden:
- Standaarden (normen) voor toegelaten middelen, waaronder de betrouwbaarheidsniveaus en beveiligingsmaatregelen.

Generieke centrale voorzieningen:
- Stelselregie-organisatie voor besturing en beheer van het afsprakenstelsel, voor het toelaten van middelenuitgevers en het toelaten van middelen en goedkeuring van digitale-identiteitenbronnen en het toezien op en handhaven van de stelselafspraken.

Decentrale stelselvoorzieningen
- Functionaliteiten van middelenuitgevers voor het uitgeven van middelen en het beheren en intrekken ervan, o.a. voor publieke middelen.
- Functionaliteiten van identiteitenbeheerders (als authentieke of gezaghebbende bronnen) t.b.v. het uitgeven van middelen. Zoals het BSNk als voorziening voor het activeren van identiteiten gebaseerd op het BSN en de bijbehorende faciliteiten zoals verstrekken van de hiervoor benodigde cryptografische sleutels. Zoals geregeld in de Wdo heeft het BSNk een rol in versterken van beveiliging, privacy en interoperabiliteit van het eIDAS-stelsel.

Oplossingen bij stelselafnemers
- Geen voor toelaten en uitgeven van identificatiemiddelen.

Voorbeelden
Een voorbeeld van een bestaand afsprakenstelsel voor het toelaten en uitgeven van middelen is eHerkenning. Een voorbeeld van een bestaand publiek middel voor burgers is DigiD, in combinatie met eNIK en eID op het rijbewijs.

Voorbeelden van kaders voor middelen zijn opgenomen in o.a. eIDAS, Wdo, AVG, BIO en Wabb. Aanvullend zijn de ISO norm 24760 en de W3C norm DID.

7.2 Generieke functie 2: Kunnen laten gebruiken van digitale identificatiemiddelen

7.2.1 Keuze B: Verplichte acceptatie van toegelaten middelen door publieke dienstverleners

Keuze
Verplichte acceptatie van toegelaten middelen door publieke dienstverleners

Toelichting bij de keuze
Overeenkomstig de eIDAS-verordening en de Wdo zijn er afspraken voor acceptatie door dienstverleners van toegelaten identificatiemiddelen. publieke dienstverleners zijn verplicht de toegelaten middelen te accepteren. Private dienstverleners kunnen ervoor kiezen deze te accepteren.

Samen met de afspraken bij de andere keuzes ontstaat een afsprakenstelsel voor identificatie en authenticatie voor digitale diensten in het publieke en ook het private domein.

Bouwstenen
De volgende bouwstenen geven invulling aan deze keuze.

	Generieke centrale stelselbouwstenen	**Decentrale stelselvoorzieningen**	**Oplossingen bij stelselafnemers**
Afspraken	- Afspraken voor acceptatie van toegelaten middelen - Aansluitvoorwaarden voor dienstverleners en eisen voor inschaling van diensten naar betrouwbaarheids-niveau's		
Standaarden	- Standaarden voor authenticatie o.b.v. toegelaten middelen		
Voorzieningen	- Ontsluiten van metadata over toegelaten middelen - Aansluiting op het Europese stelsel (eIDAS-node) - Aansluitingen op andere (nog te erkennen) internationale stelsels voor authenticatie	- Functionaliteiten van authenticatiediensten t.b.v. dienstverleners voor authenticatie o.b.v. toegelaten middelen - Functionaliteiten van identiteiten-beheerders t.b.v. authenticatie-diensten - Functionaliteiten van middelenuitgevers t.b.v. authenticatiediensten - Routeringsfunctionaliteiten voor aansluiting van dienstverleners op authenticatiediensten	- Aansluitingen van dienstverleners op het stelsel voor authenticatie

Rationale
De keuze is gebaseerd op de eIDAS-verordening en de Wdo. Betrouwbare identificatie en authenticatie zijn belangrijke voorwaarden voor betrouwbaar digitaal zakendoen. De afspraken zorgen ervoor dat dienstverleners toegelaten middelen van meerdere middelenuitgevers

accepteren. Dit maakt een verschuiving mogelijk van het uitgeven van toegelaten identificatiemiddelen alleen door de overheid naar een stelsel waarin meer keuze voor burgers en bedrijven ontstaat voor de middelen die ze kunnen gebruiken, vergelijkbaar met het eHerkenningsstelsel nu.

Verdere rationale voor deze keuze is te vinden in:
- eIDAS en eIDAS-revisie
- Wdo
- Denken vanuit behoeften van burgers en bedrijven (GA-BP-1)
- Gebruik van flexibele en ontkoppelde functies (GA-BP-4)
- Afspraken voor standaarden voor generieke voorzieningen (GA-BP-5)

Nadere toelichting van de bouwstenen
Generieke centrale stelselbouwstenen
Afspraken:
- Afspraken voor acceptatie en gebruik van toegelaten middelen:
    - Rollen, taken en verantwoordelijkheden van identiteitenbeheerders, middelenuitgevers, authenticatiediensten en dienstverleners.
    - Acceptatie van toegelaten middelen door dienstverleners.
    - Aansluitvoorwaarden voor dienstverleners, waaronder beveiligingsassessment en technische conformiteitseisen.
    - Ondersteuning van dienstverleners bij het aansluiten op het stelsel.
    - Inschaling van diensten in betrouwbaarheidsniveaus.
    - Ondersteuning van gebruikers bij het gebruiken van middelen.
    - Privacy-beschermende maatregelen, zoals het gebruik van pseudoniemen
      De privacy wordt geborgd bij het gebruik van identificatiemiddelen. De richtlijnen uit de AVG en BIO worden gevolgd bij het verzamelen van metadata (IP-adres, tijdstip authenticatie, afgenomen dienst) tijdens het gebruik van een identificatiemiddel. Zo min mogelijk (meta-)gegevens over de identiteiten worden geregistreerd en bovendien met beperkte bewaartermijnen. Dat geld ook voor registraties waar gegevens in gekopieerd worden, zoals audit- en loggingsregistraties, authenticatiefraude-preventie-registraties e.d. Vanuit de AVG is ook inzage voor burgers vereist.
      De privacy wordt geborgd bij het gebruik van identificatiemiddelen. Daarom worden persoonsgebonden, middelonafhankelijke pseudoniemen verstrekt die per dienstverlener uniek zijn en niet aan elkaar te relateren zijn.

Standaarden:
- Standaarden voor authenticatie o.b.v. toegelaten middelen, waaronder voor authenticatieverzoeken en -resultaten (authenticatieverklaringen), pseudoniemen (op basis van BSN en identificaties uit andere authentieke bronnen), vereiste betrouwbaarheidsniveaus voor diensten en specificaties voor decryptie.

Generieke centrale voorzieningen:
- Ontsluiten van metadata over toegelaten middelen.
  Het gaat hier om de partijen, hun diensten en de toegelaten authenticatiediensten. Hiermee wordt een mogelijkheid geboden om de centrale verantwoordelijkheid van de minister m.b.t. de erkenning en toelating onder de Wdo (artikel 9, lid 1,2,3 en artikel 11, lid 1,2) invulling te geven. Middels het beheer op de metadata kunnen op eenvoudige wijze partijen worden af-/uitgesloten van het stelsel.
- Aansluiting op het Europese stelsel voor gebruik van middelen uit andere lidstaten (eIDAS-node).
- Aansluiting op andere (nog te erkennen) internationale stelsels voor acceptatie van middelen uit die stelsels, bijvoorbeeld voor burgers van buiten Europese lidstaten.

Decentrale stelselvoorzieningen
- Functionaliteiten van authenticatiediensten t.b.v. dienstverleners voor authenticatie op basis van toegelaten middelen.
- Functionaliteiten van identiteitenbeheerders t.b.v. authenticatiediensten voor het verstrekken van identiteiten en pseudoniemen bij een authenticatie. Zoals, het BSNk als centrale bron voor het gebruiken van identiteiten en de bijbehorende faciliteiten zoals verstrekken van de hiervoor benodigde cryptografische sleutels.

- Routeringsfunctionaliteiten, voor aansluiting van dienstverleners en het efficiënt om gaan met meerdere authenticatiediensten en middelenuitgevers. Routeringsfunctionaliteiten moeten (vergelijkbaar met eHerkenningsmakelaars) het voor dienstverleners makkelijker maken om aan te sluiten op het stelsel.
  Deze routeringsfunctionaliteit kan onderdeel zijn van voorzieningen die voor dienstverleners een groter deel van de toegangscontrole uitvoeren dan alleen authenticatie en ook de controle op vertegenwoordigingsbevoegdheden uitvoeren. Het gecombineerd aanbieden van authenticatiediensten en diensten m.b.t. vertegenwoordiging kan een versnelling geven aan het ondersteunen van vertegenwoordiging door dienstverleners. De achterliggende bouwstenen voor enerzijds authenticatie en anderzijds vertegenwoordiging moeten wel onafhankelijk kunnen blijven functioneren (zie ook GA-basisprincipes 4 'Flexibele en ontkoppelde functies'). De combinatie van beide onderdelen van toegang verlenen is een onderwerp dat nader uitgewerkt moet worden, samen met het beantwoorden van de vraag of het een GDI-bouwsteen is.

Oplossingen bij stelselafnemers

- Aansluitingen van dienstverleners op het stelsel voor authenticatie

Voorbeelden
Een voorbeeld van een bestaand afsprakenstelsel voor acceptatie van middelen is eHerkenning. Een voorbeeld van bestaande afspraken over acceptatie van een publiek middel zijn de afspraken rond DigiD.

7.3 Generieke functie 3: Kunnen inzage geven in identificatiemiddelen en gebruik

7.3.1 Keuze C: Centraal overzicht van eigen identificatiemiddelen en inzage in gebruikshistorie

Keuze
Centraal overzicht van eigen identificatiemiddelen en inzage in gebruikshistorie

Toelichting bij de keuze
Bezitters van toegelaten middelen kunnen beschikken over een overzicht van hun middelen. Het overzicht verwijst per middel naar de uitgever ervan, zodat de bezitter daar zijn middel kan beheren. Het overzicht verwijst ook per middel naar een overzicht van de gebruikshistorie.[51] Het overzicht van middelen en de overzichten van gebruikshistorie dragen bij aan transparantie richting de bezitter, aan regie door de bezitter op zijn middelen en aan detectie door de bezitter van eventueel misbruik van zijn middelen.

Hier ligt een relatie met andere centrale persoonlijke overzichten die de overheid nu en in de toekomst aan burgers (zoals op MijnOverheid) en bedrijven biedt.

De wijze waarop de bezitter inzicht krijgt in zijn middelen en de gebruikshistorie vraagt een afweging tussen gebruiksgemak (alles in 1 overzicht ontsluiten) en privacybescherming (niet alles op 1 plek ontsluiten). Deze afweging moet plaatsvinden bij de verdere uitwerking van het stelsel. Deze uitwerking zal ook bepalen hoe de verdeling van taken en verantwoordelijkheden is over identiteitenbronnen, middelenuitgevers, authenticatiediensten en dienstverleners. Dienstverleners en authenticatiediensten zullen geen rol hebben in het overzicht van eigen middelen, maar wel in het beschikbaar maken van de gebruikshistorie. Het ontsluiten van (logging-)gegevens die om auditredenen worden vastgelegd is een mogelijke manier om de middelenbezitter inzage in de gebruikshistorie te geven.

Een ander aandachtspunt bij de verdere uitwerking van het overzicht van eigen middelen is: wat is de invloed van wie het middel heeft verkregen of aangeschaft? Mensen kunnen zelf middelen 'aanschaffen' voor gebruik in zowel privé als zakelijke contexten. Mensen kunnen (in zakelijke contexten) ook middelen gebruiken die bijvoorbeeld door hun werkgever zijn aangeschaft. Dit kan

[51] Het Ministerie van Binnenlandse Zeken en Koninkrijksrelaties kiest er in de uitwerking van de Wdo voor dat bezitters inzage in hun geactiveerde middelen kunnen krijgen. Het bieden van inzage in de gebruikshistorie is onder de Wdo geen verplichting voor deelnemers aan het stelsel. Daar is voor gekozen om de verplichtingen voor deelnemers beperkt te houden. Inzage in de gebruikshistorie is wel wenselijk en daarom in de architectuur opgenomen.

van belang zijn voor het overzicht en ook voor de notificaties die zijn beschreven bij de volgende keuze.

Een centraal overzicht van middelen introduceert ook informatiebeveiligingsrisico's die om passende maatregelen vragen.

Samen met de afspraken bij de andere keuzes ontstaat een afsprakenstelsel voor identificatie en authenticatie voor digitale diensten in het publieke en ook het private domein.

Bouwstenen
De volgende bouwstenen geven invulling aan deze keuze.

	Generieke centrale stelselbouwstenen	**Decentrale stelselvoorzieningen**	**Oplossingen bij stelselafnemers**
Afspraken	- Afspraken over middelenoverzicht en gebruikshistorie - Afspraken over logging door middelenuitgevers, authenticatiediensten en dienstverleners		
Standaarden	- Standaarden voor gegevens over middelen en gebruikshistorie		
Voorzieningen	- Centraal overzicht van eigen middelen - Verder afhankelijk van de nadere uitwerking	- Afhankelijk van de nadere uitwerking	- Afhankelijk van de nadere uitwerking

Rationale
Personen dienen regie te kunnen voeren op alle door hen in het stelsel geactiveerde identificatiemiddelen en zicht te hebben op het gebruik daarvan. Dit draagt zowel bij aan transparantie als aan fraudedetectie en aan het vermogen van de gebruiker om fouten en fraude en de gevolgen daarvan te (laten) herstellen.

Verdere rationale voor deze keuze is te vinden in:
- Denken vanuit behoeften van burgers en bedrijven (GA-BP-1)
- Overheidsdiensten zijn veilig en betrouwbaar (GA-BP-6)

Nadere toelichting bouwstenen
Generieke centrale stelselbouwstenen
Afspraken:
- Afspraken over het bieden van een middelenoverzicht en van gebruikshistorie:
  - Taken en verantwoordelijkheden van middelenuitgevers t.b.v. het middelenoverzicht.
  - Taken en verantwoordelijkheden van middelenuitgevers, authenticatiediensten en dienstverleners t.b.v. inzicht in gebruikshistorie.
- Afspraken over logging door middelenuitgevers, authenticatiediensten en dienstverleners
  - Logging van middelenuitgevers bij wijziging van middelen.
  - Logging van authenticatiediensten bij authenticatie o.b.v. een middel.
  - Logging van dienstverleners bij toegang tot een dienst o.b.v. een authenticatie.

Standaarden:
- Standaarden voor het ontsluiten van gegevens over middelen en gebruikshistorie.

Generieke centrale voorzieningen:
- Centraal overzicht van eigen middelen met verwijzingen naar mogelijkheden voor beheer en naar gebruikshistorie.
- Verder afhankelijk van de nadere uitwerking.

Decentrale stelselvoorzieningen
- Afhankelijk van de nadere uitwerking.

Oplossingen bij stelselafnemers
- Afhankelijk van de nadere uitwerking.

Voorbeelden
Een voorbeeld van een inzageregister is het BSNk Inzageregister dat in ontwikkeling is.
Andere voorbeelden van inzage zijn de overzichten bij banken van middelen en apps die klanten kunnen gebruik voor betaling of inloggen.

7.3.2 Keuze D: Notificatie bij wijziging en gebruik van eigen identificatiemiddelen

Keuze
Notificatie bij wijziging en gebruik van eigen identificatiemiddelen.

Toelichting bij de keuze
Bezitters van identificatiemiddelen kunnen notificaties krijgen bij wijziging en gebruik ervan.[52] De gebruiker kan bepalen waarover, wanneer en hoe hij wordt genotificeerd. Ook dit draagt bij aan transparantie richting de bezitter, aan regie door de bezitter op zijn middelen en aan detectie door de bezitter van eventueel misbruik van zijn middelen.

Samen met de afspraken bij de andere keuzes ontstaat een afsprakenstelsel voor identificatie en authenticatie voor digitale diensten in het publieke en ook het private domein.

Bouwstenen
De volgende bouwstenen geven invulling aan deze keuze.

	Generieke centrale stelselbouwstenen	**Decentrale stelselvoorzieningen**	**Oplossingen bij stelselafnemers**
Afspraken	- Afspraken over notificatie door middelenuitgevers en authenticatiediensten		
Standaarden	- We volgen de afspraken voor het GA-domein Interactie / Berichtenstelsel		
Voorzieningen	- We volgen de afspraken voor het GA-domein Interactie / Berichtenstelsel		

Rationale
Personen dienen regie te kunnen voeren op alle door hen in het stelsel geactiveerde identificatiemiddelen en zicht te hebben op het gebruik daarvan. Dit draagt zowel bij aan transparantie als aan fraudedetectie en aan het vermogen van de gebruiker om fouten en fraude en de gevolgen daarvan te (laten) herstellen.

Verdere rationale voor deze keuze is te vinden in:
- Denken vanuit behoeften van burgers en bedrijven (GA-BP-1)
- Overheidsdiensten zijn veilig en betrouwbaar (GA-BP-6)

Nadere toelichting bouwstenen
Generieke centrale stelselbouwstenen
Afspraken:
- Afspraken over notificatie door middelenuitgevers en authenticatiediensten
  - Notificatie door middelenuitgevers bij wijziging van een middel.
  - Notificatie door authenticatiediensten bij gebruik van een middel.

[52] Het Ministerie van Binnenlandse Zeken en Koninkrijksrelaties kiest er in de uitwerking van de Wdo voor dat bezitters genotificeerd worden over het activeren en intrekken van hun middelen. Het bieden van notificatie over gebruik is onder de Wdo geen verplichting voor deelnemers aan het stelsel. Daar is voor gekozen om de verplichtingen voor deelnemers beperkt te houden. Notificatie van gebruik is wel wenselijk en daarom in de architectuur opgenomen.

Voor de overige bouwstenen bij deze keuze volgen we de afspraken, standaarden en voorzieningen zoals beschreven in het GA-domein Interactie / Berichtenstelsel.

Voorbeelden
Diverse online diensten sturen een melding als een inlogmiddel is gewijzigd of is gebruikt om in te loggen bij de dienst zelf of bij een andere online dienst. Diverse online diensten leggen vast wanneer en met welk middel vanaf welk apparaat toegang is verkregen tot online diensten.

7.4 Generieke functie 4: Kunnen instaan voor betrouwbaarheid en veiligheid van authenticatie

7.4.1 Keuze E: Afspraken voor toezicht en handhaving m.b.t. authenticatiefraude

Keuze
Afspraken voor toezicht en handhaving m.b.t. authenticatiefraude.

Toelichting bij de keuze
Er zijn afspraken over de verdeling van taken, verantwoordelijkheden en bevoegdheden over de partijen die deelnemen aan het stelsel voor identificatie en authenticatie i.h.k.v. het voorkomen, detecteren en opvolgen van authenticatiefraude.[53] Deze afspraken zijn nauw verweven met het afsprakenstelsel voor toezicht en handhaving m.b.t. identiteitsfraude.

De overheid neemt maatregelen om authenticatiefraude met identificatiemiddelen te voorkomen en om de gevolgen van authenticatiefraude te herstellen. Om authenticatiefraude te kunnen detecteren zijn gegevens nodig van verschillende partijen in het stelsel, omdat iedere partij beschikt over slechts een gedeelte van de gegevens.

Het uitgangspunt is dat de stelselpartijen en dienstverleners zelf verantwoordelijk zijn. Centraal fraudemanagement heeft betrekking op partij-overstijgende authenticatiefraude waarbij een centrale organisatie een coördinerende rol heeft richting de stelselpartijen. De organisatie vergaart informatie om proactief fraudepatronen of signalen te onderzoeken en eventueel te genereren. De coördinerende rol kan een gerichte uitvraag omvatten van bepaalde monitoringinformatie bij de erkende partijen. Die uitvraag is dan verbonden aan een actuele, urgente authenticatiefraude. Deze opzet is gebruikelijke in bijvoorbeeld de bancaire sector en volgt ook uit de proportionaliteit en subsidiariteit beginselen van de AVG.

Samen met de afspraken bij de andere keuzes ontstaat een afsprakenstelsel voor identificatie en authenticatie voor digitale diensten in het publieke en ook het private domein.

Bouwstenen
De volgende bouwstenen geven invulling aan deze keuze.

	Generieke centrale stelselbouwstenen	**Decentrale stelselvoorzieningen**	**Oplossingen bij stelselafnemers**
Afspraken	- Afspraken voor toezicht en handhaving m.b.t. authenticatiefraude		
Standaarden	- Standaarden voor delen van gegevens m.b.t. detectie en opvolgen van fraude		
Voorzieningen	- Centrale authenticatie-fraude-preventie-organisatie	- Functionaliteiten van middelenuitgevers en authenticatiediensten voor voorkoming, detectie en opvolging	- Functionaliteiten van dienstverleners voor voorkoming, detectie en opvolging van authenticatie-fraude

[53] Onder authenticatiefraude verstaan we op basis van de 'concept regeling nadere eisen toelating identificatiemiddelen WDO' het volgende: authenticatie namens een persoon zonder diens toestemming. Authenticatiefraude is onderdeel van het bredere begrip 'identiteitsfraude'. Deze architectuur kijkt alleen naar authenticatiefraude en niet naar identiteitsfraude in brede zin.

	Generieke centrale stelselbouwstenen	Decentrale stelselvoorzieningen	Oplossingen bij stelselafnemers
		van authenticatie-fraude en delen van gegevens	en delen van gegevens

Rationale
De overheid heeft een zorgplicht in het voorkomen van authenticatiefraude en om de gevolgen ervan te herstellen. Toezicht op en handhaving bij authenticatiefraude draagt bij aan de betrouwbaarheid van de middelen. Het draagt ook bij aan de kwaliteit en betrouwbaarheid van het stelsel en aan het vermogen van de gebruiker om fouten en fraude en de gevolgen daarvan te (laten) herstellen. Op nationaal niveau, kan preventie gewaarborgd worden in de vorm van wettelijk verplichte maatregelen, certificeringen e.d., zoals het nu door BIO wordt vereist t.a.v. beveiliging.

Verdere rationale voor deze generieke functie is te vinden in:
- Denken vanuit behoeften van burgers en bedrijven (GA-BP-1)
- Rekening houden met de diversiteit bij burgers en bedrijven (GA-BP-2)
- Overheidsdiensten zijn veilig en betrouwbaar (GA-BP-6)

Nadere toelichting bouwstenen
Generieke centrale stelselbouwstenen
Afspraken:
- Afspraken voor toezicht en handhaving m.b.t. authenticatiefraude:
  - De relatie met het stelsel voor toezicht en handhaving op identiteitsfraude.
  - Beveiliging in het stelsel ter voorkoming en detectie van authenticatiefraude, waaronder afspraken over het verzamelen van gegevens om authenticatiefraude te kunnen detecteren.
  - Meldingsplicht bij de detectie van (mogelijke) authenticatiefraude
    De stelselpartijen monitoren het gebruik van identificatiemiddelen en speuren actief naar misbruik daarvan. Daar waar partijen het vermoeden hebben van authenticatiefraude, bestaat al een signalerings- en meldingsplicht bij de door overheid aangestelde opsporingsinstanties.
  - Opvolging en herstel bij geconstateerde authenticatiefraude, voor zowel stelselpartijen als dienstverleners.
  - De mogelijkheid om per direct een identificatiemiddel te kunnen blokkeren of intrekken bij geconstateerde fraude, inclusief afspraken over signalering naar en ondersteuning van de bezitter van het middel.
  - Grondslagen voor gegevensuitwisseling.

Standaarden:
- Standaarden voor delen van gegevens mb.t. detectie van authenticatiefraude en het onderling relateren van die gegevens. In de regelgeving onder de Wdo is een minimale dataset van gebruiksgegevens benoemd die elke authenticatiedienst (en ook machtigingsdienst) moet doorgeven aan het centrale fraude en misbruik systeem'

Generieke centrale voorzieningen:
- Centrale authenticatiefraude-preventie-organisatie met een centraal meldpunt voor gebruikers en dienstverleners.
  De overheid realiseert een centrale authenticatiefraude-preventie-organisatie waarmee alle betrokken organisaties tot een meer gezamenlijke aanpak kunnen komen, onder meer door relevante informatie gezamenlijk te delen en stelselbrede authenticatiefraude te detecteren. De overheid zorgt ook voor een landelijk centraal meldpunt, dat zorgt voor het herstel van de gevolgen.

Decentrale stelselvoorzieningen
- Functionaliteiten van middelenuitgevers en authenticatiediensten voor voorkoming, detectie en opvolging en herstel van authenticatie-fraude en delen van gegevens met de centrale authenticatiefraude-preventie-organisatie.

Oplossingen bij stelselafnemers
- Functionaliteiten van dienstverleners voor voorkoming, detectie en opvolging en herstel van authenticatie-fraude en delen van gegevens met de centrale authenticatiefraude-preventie-organisatie.

Voorbeelden
Geen

7.5 Raakvlakken met andere domeinen

Zie voor de raakvlakken met andere domeinen paragraaf 5.7

8 Bijlage: Begrippen

In deze bijlage zijn de begrippen in dit document beschreven. Een deel van de begrippen is GA-breed en afkomstig uit de GA-begrippenlijst. De GA-begrippenlijst is volledig overgenomen en bevat ook begrippen die in deze architectuur niet worden gebruikt. Een ander deel is specifiek voor identificatie en authenticatie en maakt geen onderdeel uit van de GA-brede begrippenlijst.[54] Dit is aangegeven met (I&A) achter het begrip.

Begrip	**Definitie**
Afspraak	Regels die voor de inrichting van een generieke functie door partijen zijn overeengekomen, vastgelegd en gepubliceerd. Toelichting: Het kan nodig zijn om afspraken vast te leggen in een wettelijk kader, zoals de Wet Digitale Overheid. Maar dit kan ook in AMVB's, regelingen, beleidsregels, convenanten etc. Binnen architectuurdiagrammen gebruiken we het Archimate-element 'contract'.
Architectuur	Een beschrijving van een (complex) geheel, en van de principes die van toepassing zijn op de ontwikkeling van het geheel en zijn onderdelen. Bron: NORA Toelichting: in de context van de GA is het een stuurinstrument voor de doorontwikkeling van de GDI. Voor formele architectuurbeschrijvingen gebruiken we de architectuurbeschrijvingstaal Archimate.
Architectuurprincipe	Een stelling over een gewenste, generieke, kwalitatieve eigenschap waar architectuur invulling aan moet geven in de publieke sector. Bron: NORA Synoniem: principe. Toelichting: Uitspraak, geldend voor langere termijn, die betrekking heeft op de inrichting van organisatie, processen en informatievoorziening. Richtinggevend voor overheidsorganisaties bij het inzetten van veranderingen en het uitvoeren van projecten. Binnen architectuurdiagrammen gebruiken we het Archimate-element 'principle'.
Attribuut (I&A)	Een eigenschap, kenmerk of kwaliteit van een natuurlijke of rechtspersoon of een entiteit, in elektronisch formaat. Bron: eIDAS-revisie
Authenticatie, authenticeren (I&A)	Een digitaal proces dat de bevestiging van de digitale identificatie van een persoon in digitale vorm mogelijk maakt. Bron: gebaseerd op eIDAS: Authenticatie - een elektronisch proces dat de bevestiging van de elektronische identificatie van een natuurlijke persoon of rechtspersoon, of van de oorsprong en integriteit van gegevens in elektronische vorm mogelijk maakt
Authenticatiedienst (I&A)	Partij die op basis van een identificatiemiddel een authenticatieverklaring afgeeft. Bron: Wdo
Authenticatiefactor (I&A)	Een factor waarvan is bevestigd dat deze gebonden is aan een bepaalde persoon en die onder een van de drie volgende categorieën valt: • Op bezit gebaseerde authenticatiefactor: een authenticatiefactor waarvan de betrokkene moet aantonen dat deze in zijn bezit is. • Op kennis gebaseerde authenticatiefactor: een authenticatiefactor waarvan de betrokkene moet aantonen dat hij ervan kennis draagt. • Inherente authenticatiefactor: een authenticatiefactor die op een fysiek kenmerk van een natuurlijke persoon is gebaseerd en waarbij de betrokkene moet aantonen dat hij dat fysieke kenmerk bezit.

[54] De GA-brede begrippen zijn overgenomen uit versie 0.29 van GA Begrippen.

	Bron: NORA
Authenticatiefraude (I&A)	Authenticatie namens een persoon zonder diens toestemming. Bron: Gebaseerd op de concept regeling nadere eisen toelating identificatiemiddelen WDO, versie 18 september 2021
Authenticatieverklaring (I&A)	Een Verklaring waaruit het bestaan en de juistheid kan worden opgemaakt van een authenticatie die heeft plaatsgevonden in de context van een bepaalde handeling of dienst. Bron: Afsprakenstelsel.etoegang.nl
Authentieke bron (I&A)	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 Bron: eIDAS-revisie Synoniem: Gezaghebbende bron
Autorisatie (I&A)	Het verlenen van toestemming (een bevoegdheid) aan een geauthenticeerde partij om toegang te krijgen tot een bepaalde dienst of toestemming om een bepaalde actie uit te voeren. Een autorisatie kan worden vastgelegd in toegangsrechten. Het verlenen van toegang kan (mede) gebaseerd zijn op die in toegangsrechten vastgelegde autorisatie. Bron: Afsprakenstelsel.etoegang.nl
Bestuursorgaan	Orgaan van een rechtspersoon krachtens publiekrecht ingesteld" (a-orgaan), of "een persoon of college, met enig openbaar gezag bekleed" (b-orgaan). Bron: Algemene wet bestuursrecht, Awb artikel 1:1 lid 1 Toelichting: Uitzonderingen staan vermeld in art. 1:1 lid 2 Awb. Zie ook overheidsorganisatie.
Betrouwbaarheidsniveau (I&A)	Mate waarin vertrouwen kan worden gesteld in een identificatiemiddel, gebaseerd op de mate van zekerheid waarmee attributen, identiteiten, identificatiemiddelen en/of bevoegdheden zijn vastgesteld. Bron: gebaseerd op Wdo en NORA.
Burgers en bedrijven	Verkorte schrijfwijze voor: burgers, bedrijven, instellingen, intermediairs en hun gemachtigden. Synoniemen: NP en NNP; Natuurlijke personen en Niet Natuurlijke Personen. Toelichting: Dit begrip is opgevolgd, maar kan in oudere documenten nog voorkomen. Er worden verschillende termen gebruikt om de 'klanten' van de overheidsorganisaties aan te duiden zoals afnemers, burgers, bedrijven e.a. Vaak geven deze geen eenduidige volledig dekkende aanduiding van de bedoelde groep. GA hanteert daarom (inmiddels) meestal de termen "persoon" of "NP en NNP" of "Natuurlijk persoon en Niet Natuurlijk Persoon" om hen aan te duiden. Deze termen kunnen ook los van elkaar voorkomen om een deel van de populatie aan te duiden. Zie ook: Persoon.
Decentrale stelselvoorziening	Voorziening die onderdeel is van een landelijk stelsel (met afspraken, standaarden en voorzieningen) en waar meerdere (decentrale) voorkomens van zijn. Al deze decentrale voorkomens voldoen aan de landelijke afspraken en standaarden van het stelsel. Bron: GA

Dienst	Een afgebakende prestatie van een persoon of organisatie (de dienstverlener), die voorziet in een behoefte van haar omgeving (de dienstafnemers). Bron: NORA Toelichting: Diensten zijn zowel het leveren van informatie als het uitvoeren van andere handelingen. De dienstafnemer kan dit positief ervaren maar ook negatief (bijvoorbeeld een belastingaanslag) waarbij de behoefte meestal een bredere maatschappelijke behoefte is.
Dienstafnemer	De persoon of organisatie die een dienst in ontvangst neemt. Bron: NORA Synoniem: afnemer (niet gebruiken), klant Toelichting: Dit kan een burger, een (medewerker van een) bedrijf of instelling dan wel een collega binnen de eigen of een andere organisatie zijn. In andere contexten wordt de term afnemer gebruikt om een overheidsorganisatie aan te duiden die een generieke voorziening gebruikt om een dienst aan te bieden. Om verwarring hiermee te voorkomen gebruiken we bij voorkeur de term 'dienstafnemer'.
Dienstverlener	De persoon of organisatie die voorziet in het leveren van een afgebakende prestatie (dienst) aan haar omgeving (de afnemers). Bron: NORA Synoniemen: Dienstaanbieder
Digitale bronidentiteit (I&A)	Een verzameling van betrouwbare gegevens die een entiteit (persoon, organisatie, object of apparaat) representeren in het digitale domein. Voorbeelden zijn: 1) de combinatie naam, geboortedatum adres, 2) 'identifiers' zoals BSN en telefoonnummer of 3) biometrische gegevens zoals vingerafdruk. Bron: Kamerbrief over visie digitale identiteit
Digitale identiteit (I&A)	Een identiteit die een digitale representatie is van een persoon.
Domein	Een inhoudelijk verwante verzameling van publieke dienstverlening. Binnen de context van de GDI zijn dit: Toegang, Interactie, Gegevensuitwisseling en Infrastructuur. Bron: NORA, Besluit Sturing Digitale Overheid 202255 Toelichting: Zie de begrippen Toegang, Interactie, Gegevensuitwisseling en Infrastructuur.
GDI	Afkorting van Generieke Digitale Infrastructuur
GDI-Architectuur	Het deel van de Overheidsarchitectuur dat de inrichting van de GDI beschrijft en hiervoor richtinggevende afspraken, standaarden en generieke voorzieningen beschrijft (afgekort: GA). Synoniemen: Architectuur GDI Toelichting: Er is meer overheidsarchitectuur (NORA familie o.a.). De GA gaat alleen over de GDI.
Gegevensuitwisseling (domein)	Het domein Gegevensuitwisseling omvat de bouwstenen van de GDI voor uitwisseling van gegevens tussen informatiesystemen van overheidsorganisaties onderling en met informatiesystemen van andere organisaties. Bron: GA.
Gemeenschappelijk	Voor 'gemeenschappelijke functies' en 'gemeenschappelijke voorzieningen' geldt dat ze door meerdere (minimaal 2) organisaties toegepast worden. Daarmee omvat dit behalve generieke functies/voorzieningen met name ook functies/voorzieningen die door een deel van de organisaties samen (gemeenschappelijk) ingericht is.

[55] https://wetten.overheid.nl/BWBR0046935/

	Bron: De toelichting is afkomstig uit het Beleidskader Digitale Infrastructuur Synoniem: gedeeld Toelichting: De GDI is beperkt tot generieke functies. Daarnaast zijn er niet-generieke functies die voortkomen uit andere – gemeenschappelijke of individuele - behoeften van beleid en dienstaanbieders. Voor de invulling van die niet-generieke functies zijn zij zelf verantwoordelijk, al dan niet in een coalitie van partijen. De intentie bij de inrichting van deze functies is dat hergebruik in bredere zin mogelijk moet zijn, waarbij (vanzelfsprekend) tegemoetgekomen wordt aan architectuurprincipes en geldende standaarden. Gemeenschappelijk impliceert vaak dat iets niet-generiek is. Aangezien dit impliciet is, wordt de voorkeur gegeven aan 'niet generiek' waar dit onderscheid wezenlijk is.
Gemeenschappelijke Overheidsarchitectuur	Oude naamgeving van de GDI-Architectuur (afgekort GO) (vervallen).
Generiek	Voor alle gevallen geldend, niet specifiek. Bron: Van Dale woordenboek
Generieke Digitale Infrastructuur	De verzameling aan afspraken, standaarden en voorzieningen die overheidsorganisaties en dienstverleners met een publieke taak ondersteunt bij de inrichting van hun digitale dienstverlening aan burgers en bedrijven en ook bij hun onderlinge digitale samenwerking (afgekort GDI). Bron: Besluit Sturing Digitale Overheid 202255 Synoniemen: Basisinfrastructuur, Digitale basisinfrastructuur Toelichting: De GDI bestaat uit de kern van de digitale overheid die niet organisatie-, sector- of domein specifiek is en die wordt begrensd door de Generieke functies. De GDI omvat tevens de functies van de in de Wet Digitale Overheid genoemde voorzieningen. Het wetsvoorstel hiervoor (de eerste tranche van de wet digitale overheid) regelt nu het voor authenticatie relevante deel van de infrastructuur bij bestuursorganen en aangewezen organisaties, zodat burgers met een toegelaten identificatiemiddel van het juiste betrouwbaarheidsniveau toegang hebben tot de digitale dienstverlening van alle bestuursorganen en aangewezen organisaties.
Generieke functie	Iets wat meerdere overheidsorganisaties moeten kunnen voor het uitvoeren van hun taken. Bron: NORA Toelichting: Binnen de GDI wordt gebruik gemaakt van generieke functies om de doelen van de GDI te bereiken. De GA werkt die generieke functies uit in afspraken, standaarden en voorzieningen die in alle gevallen van toepassing zijn en gebruikt worden.
Gezaghebbende bron (I&A)	Synoniem van authentieke bron
Handelend persoon (I&A)	Natuurlijke persoon die toegang vraagt tot digitale diensten. Synoniem: gebruiker (van een identificatiemiddel) Bron: GA Identificatie en authenticatie
Identificatie & autorisatie (domein)	Zie "Toegang". Toelichting: Deze term is vervangen.

Identificatie, identificeren (I&A)	Het proces van het gebruiken van persoonsidentificatiegegevens in digitale vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden. Bron: gebaseerd op eIDAS: elektronische identificatie - het proces van het gebruiken van persoonsidentificatiegegevens in elektronische vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden.
Identificatiegegevens (I&A)	Een verzameling gegevens aan de hand waarvan de identiteit van een persoon kan worden vastgesteld Bron: gebaseerd op eIDAS: persoonsidentificatiegegevens - een reeks gegevens aan de hand waarvan de identiteit van een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, kan worden vastgesteld
Identificatiemiddel (I&A)	Een materiële en/of immateriële eenheid die identificatiegegevens bevat waarmee de identiteit van een persoon is aan te tonen. Bron: gebaseerd op eIDAS: elektronisch identificatiemiddel - een materiële en/of immateriële eenheid die persoonsidentificatiegegevens bevat en die gebruikt wordt voor authenticatie bij een onlinedienst. Synoniem: authenticatiemiddel
Identiteit (I&A)	Een verzameling unieke kenmerken of gegevens (attributen) die een persoon uniek beschrijven in een gegeven context. Bron: gebaseerd op Practicioner's Guide van The World Bank
Infrastructuur (domein)	Het domein Infrastructuur omvat de bouwstenen van de GDI die van algemeen belang (ofwel: infrastructureel) zijn voor de GDI en die veelal een basis vormen voor de bouwstenen van de andere drie domeinen. Bron: GA.
Interactie (domein)	Het domein Interactie omvat de bouwstenen van de GDI ten behoeve van elektronische informatie-uitwisseling met burgers, bedrijven, instellingen, intermediairs en hun gemachtigden. Uitwisseling ten behoeve van Toegang is hiervan uitgezonderd.. Bron: GA.
Middelenuitgever (I&A)	Partij die zorgdraagt voor de uitgifte van toegelaten identificatiemiddelen aan natuurlijke personen, rechtspersonen of ondernemingen. Bron: Wdo
Natuurlijk persoon (NP)	Een mens (individu) die in het recht als rechtssubject is erkend en daarmee drager is van wettelijke rechten en plichten. Bron: CBS. Toelichting: Een natuurlijk persoon kan zelfstandig in het rechtsverkeer optreden, en vormt daarmee, net als zijn juridische tegenhanger, de rechtspersoon (een abstracte juridische entiteit, bijvoorbeeld een vereniging), een rechtssubject. Het zijn van een natuurlijk persoon vangt algemeen aan met het levend en levensvatbaar geboren zijn van een individu. Het zijn van een natuurlijk persoon eindigt met het overlijden.
Niet-natuurlijk persoon (NNP)	Een rechtspersoon of een samenwerkingsverband zonder rechtspersoonlijkheid. Bron: CBS. Toelichting: Een samenwerkingsverband zonder rechtspersoonlijkheid is een rechtsvorm behorend bij een georganiseerde groep van natuurlijke personen en/of rechtspersonen die zelf niet in het recht is erkend als drager van wettelijke rechten en plichten. Voorbeelden: Privaatrechtelijke rechtspersonen zijn besloten vennootschap, naamloze vennootschap, vereniging en stichting. Publiekrechtelijke rechtspersonen zijn ministerie, provincie, gemeente,

	waterschap, Sociaal-Economische Raad, Publiekrechtelijke bedrijfsorganisatie, Zelfstandig bestuursorgaan. Ook kerkgenootschappen zijn rechtspersonen. Samenwerkingsverbanden zonder rechtspersoonlijkheid zijn de maatschap, de vennootschap onder firma (vof) en de commanditaire vennootschap (cv).
Overheid(s-organisaties)	In de context van GA: alle, op basis van het Koninklijk Besluit van 16 juli 1859, in de staatsalmanak opgenomen organisaties (zie https://almanak.overheid.nl/). Uitgezonderd hiervan zijn: • ZBO's met een privaatrechtelijke rechtsvorm, • Caribisch Nederland (BES-eilanden), • Aruba, Curaçao en Sint Maarten. Synoniemen: bestuursorgaan GA geeft geen duiding van mogelijk facultatieve deelname aan (onderdelen van) de GDI door niet-overheidsorganisaties. Aanvullend aan Overheid(s-organisaties) kan gedacht worden aan organisaties (niet-overheid) met een publieke taak zoals: • alle ZBO's met een privaatrechtelijke rechtsvorm, • pensioenfondsen aangesloten bij de pensioenfederatie.
Overheidsarchitectuur	Een Architectuur gericht op het functioneren van de overheid (overkoepelend, sectoraal gericht of organisatiegericht).
Persoon	Natuurlijk persoon of niet-natuurlijk persoon.
Persoonsidentificatie-gegevens (I&A)	Zie identificatiegegevens
Principe	Zie architectuurprincipe.
Privaat identificatie-middel (I&A)	Niet van rijkswege uitgegeven identificatiemiddel. Bron: gebaseerd op Wdo
Publiek identificatie-middel (I&A)	Van rijkswege uitgegeven identificatiemiddel. Bron: gebaseerd op Wdo
Publieke digitale dienstverlening	Verlening van elektronische diensten aan natuurlijke personen, ondernemingen of rechtspersonen ter uitoefening van een publieke taak. Bron: GA
Publieke taak	Een taak waarvoor de overheid de eindverantwoordelijkheid op zich neemt en die wordt uitgevoerd voor de behartiging van een publiek of algemeen belang. Bron: GA
Self Sovereign Identity (SSI) (I&A)	Het concept Self Sovereign Identity legt de controle en de macht over een digitale identiteit volledig bij de entiteit die deze digitale identiteit representeert. Dit vereist volledige onafhankelijkheid van een centraal register of centrale autoriteit. Bron: pressurecooker identificatie en authenticatie
Standaard	Een set van regels die beschrijven hoe mensen materialen, producten, diensten, technologieën, taken, processen en systemen dienen te ontwikkelen en beheren. Bron: NORA Toelichting: Binnen architectuurdiagrammen gebruiken we het Archimate-element 'requirement'.
Stelsel	Een systeem waarbinnen organisaties via afspraken, standaarden en/of voorzieningen samenwerken om bepaalde functionaliteit te realiseren. Bron: NORA

	Toelichting: Een stelsel is een implementatie voor een of meerdere generieke functies (of delen daarvan). Voorbeelden: Federatief Berichten Stelsel (FBS), eHerkenning-stelsel, stelsel van basisregistraties.
Toegang (domein)	Het domein Toegang bestaat uit twee subdomeinen. Het subdomein Identificatie & authenticatie omvat de bouwstenen vanuit de GDI om burger, bedrijf, instelling, intermediair uniek te identificeren en authenticeren ten behoeve het verlenen van toegang tot publieke diensten. Het subdomein Machtigen & vertegenwoordigen omvat de bouwstenen om de bevoegdheid tot het digitaal handelen namens een ander vast te stellen. Bron: GA. Synoniemen: Het domein werd voorheen "Identificatie & autorisatie" genoemd.
Voorziening	Groepering van services die aan afnemers worden aangeboden, met als doel het bevorderen van uniformiteit en efficiëntie binnen de overheid. Bron: NORA . Toelichting: Voorzieningen zullen binnen de context van de GA vaak (ook) geautomatiseerde informatiesystemen omvatten, maar kunnen zich ook beperken tot een bedrijfsproces voor het leveren van een dienst. Binnen architectuurdiagrammen gebruiken we het Archimate-element 'product' ('A product represents a coherent collection of services and/or passive structure elements, accompanied by a contract/set of agreements, which is offered as a whole to (internal or external) customers').
Wallet (I&A)	Een apparaat (ook wel: device), online service of softwareprogramma dat vertrouwelijke gegevens kan bevatten, zoals persoonlijke attributen, identificatiegegevens, inloggegevens en bankpassen, en dat de bezitter in staat stelt digitale transacties uit te voeren, zoals aantonen van zijn identiteit, attributen verstrekken en betalingen te doen. Bron: GA Identificatie en authenticatie

9 Bijlage: Verantwoording pressurecooker

Deze bijlage beschrijft de belangrijkste verschillen met het pressurecooker-rapport voor het subdomein Identificatie & authenticatie en de redenen daarvoor.

De tabel hieronder toont voor de generieke functies de belangrijkste verschillen met het pressurecooker-rapport.

Capability's pressurecooker	**Generieke functies GDI-Architectuur**

Het pressurecooker-rapport benoemt de volgende basisfuncties:
- Identificatie
- Authenticatie
- Autorisatie
 	
Het plaatst de functie 'autorisatie' buiten scope.
	In de GDI-Architectuur onderscheiden we de functies:
	- Identificeren en authenticeren
	  o Voorzien in identificatiemiddelen
	  o Authenticeren
	  o Inzage geven in middelen en gebruik
	  o Instaan voor betrouwbaarheid en veiligheid
	
	De functie 'autorisatie' verruimen we in hoofdstuk 3 naar 'toetsen op bevoegdheden en overige kenmerken'. We plaatsen deze functie net als in de pressurecooker buiten scope.
	Ook het beheren van identiteiten is niet in scope van het subdomein Identificatie & authenticatie, omdat identiteitenbeheer, zoals in de Basisregistratie Personen, een breder toepassingsgebied heeft dan alleen identificatie en authenticatie. Identiteitenbeheer is wel aangeduid als een noodzakelijke voorwaarden voor betrouwbare identificatie en authenticatie.
	De generieke functie 'Inzage geven' die we hier onderkennen vertoont overlap met de capability 'Regie op eigen identiteitsgegevens' zoals onderkend in het pressurecooker-rapport (zie de tabelrij hieronder)

Het pressurecooker-rapport benoemt onderstaande 7 capability's voor identificatie en authenticatie: 1. Duidelijk kaders stellen vanuit de overheid voor Identificatie en Authenticatie én vertrouwen geven aan burgers en ondernemers. 2. Uitgeven en beheren van unieke en betrouwbare digitale bronidentiteiten. 3. Afsprakenstelsel digitaal vertrouwen ten behoeve van uitgifte en beheer van betrouwbare identificatie- en authenticatiemiddelen. 4. Single-Sign-On by default 5. Regie op de eigen identiteitsgegevens. 6. Toezicht en Handhaving bij ID-fraude. 7. IAM-functies binnen de overheid	Capability is in de architectuurmethode voor de GDI-Architectuur een synoniem voor 'generieke functie'. De zeven capability's uit het pressurecooker-rapport hebben we niet overgenomen als generieke functies. Ze zijn grotendeels verwerkt in de keuzes voor afspraken, standaarden en voorzieningen in hoofdstuk 7. Zie daarvoor de tabel hierna.

De tabel hieronder toont de releatie tussen de capability's in het pressurecooker-rapport en de keuzes zoals beschreven in deze architectuur.

Capability's pressurecooker	Keuzes GDI-Architectuur
1. Duidelijk kaders stellen vanuit de overheid voor Identificatie en Authenticatie én vertrouwen geven aan burgers en ondernemers.	Deze capability hebben we verdeeld over de vijf keuzes (A t/m E). Iedere keuze resulteert in een combinatie van afspraken, standaarden en voorzieningen. De afspraken die invulling geven aan de vijf keuzes vormen samen het afsprakenstelsel dat de kaders stelt die vertrouwen geven aan burgers en bedrijven.
2. Uitgeven en beheren van unieke en betrouwbare digitale bronidentiteiten.	Het uitgeven van digitale (bron)identiteiten is geen onderwerp van deze architectuur. De beschikbaarheid van betrouwbare digitale identiteiten is wel aangeduid als een noodzakelijke voorwaarde voor het afsprakenstelsel voor identificatie en authenticatie. Het onderwerp digitale bronidentiteit zal samen met de onderwerpen SSI, wallets en de eIDAS-revisie op een ander moment worden uitgewerkt.
3. Afsprakenstelsel digitaal vertrouwen ten behoeve van uitgifte en beheer van betrouwbare identificatie- en authenticatiemiddelen.	Deze capability hebben we niet opgenomen als aparte keuze, maar is net als capability 1 verdeeld over de afspraken bij de vijf keuzes.
4. Single-Sign-On by default	Deze capability is niet opgenomen als keuze, maar als een implicatie van het basisprincipe 'Denken vanuit behoeften van burgers en bedrijven' en daarmee als een eis aan het nader uit te werken afsprakenstelsel voor identificatie en authenticatie. De implicatie is verwoord als 'een gebruikerservaring vergelijkbaar met single-sign-on', omdat de eis is dat de gebruiker niet vaker moet inloggen dan dat vanuit betrouwbaarheid en veiligheid noodzakelijk is. Hoe aan deze eis invulling wordt gegeven dient te worden uitgewerkt bij de nadere uitwerking van het domein.
5. Regie op de eigen identiteitsgegevens.	Deze capability is vertaald naar keuzes C (Overzicht van eigen identificatiemiddelen) en D (Notificatie bij wijzing en gebruik van eigen identificatiemiddelen). Regie op identiteitsgegevens is breder dan de scope van deze architectuur. Regie op identificatiemiddelen is wel in scope en is daarom opgenomen in de vorm van keuze C. Keuze D is een nadere invulling van regie op eigen identificatiemiddelen.
6. Toezicht en Handhaving bij ID-fraude.	Deze capability is vertaald naar keuze E (Stelsel voor toezicht en handhaving m.b.t. authenticatiefraude) Toezicht en handhaving bij identiteitsfraude is breder dan de scope van deze architectuur. Fraude en handhaving bij authenticatiefraude is wel in scope en opgenomen in de vorm van deze keuze. Daarbij is benoemd dat er een sterke relatie is tussen identiteitsfraude en

Capability's pressurecooker	Keuzes GDI-Architectuur
	fraude met identificatiemiddelen en dat bij de nadere uitwerking van het stelsel voor identificatie & authenticatie invulling moet worden gegeven aan deze relatie.
7. IAM-functies binnen de overheid	Deze capability is niet opgenomen als keuze, omdat identificatie en authenticatie van overheidsmedewerkers op het moment van schrijven geen functie van de GDI is. De beleidsvraag of het stelsel ook daarvoor ingezet wordt is opgenomen in de backlog. Overheidsmedewerkers kunnen op het moment van schrijven met gebruik van eHerkenning diensten van andere organisaties afnemen. Die mogelijkheid blijft bestaan binnen het stelsel voor identificatie en authenticatie.