Authenticatie van Natuurlijke Personen

Auteurs: Menno Stigter, Bob ter Riele, Harro Kremer, Anne Schrijer
Versie: 0.21 dd 29 augustus 2019

1 Voorwoord

Binnen de NORA expertgroep "Digitale identificatie en authenticatie" is de behoefte geuit aan een verbetering van de teksten op het gebied van Authenticatie van Natuurlijke Personen[1]. Dit document bevat een eerste, nog onvolledige, uitwerking daarvan door de hierboven genoemde auteurs.

Het streven is om een structuur neer te zetten die inzichtelijk maakt welke aspecten beschreven moeten worden en om deze structuur te vullen met teksten die bruikbaar zijn voor mensen met weinig kennis en ervaring met het onderwerp Authenticatie.

2 Inhoudsopgave

[1] www.noraonline.nl/wiki/Authenticatie_in_de_praktijk
www.noraonline.nl/wiki/Identiteitenbeheer

3 Inleiding

3.1 Wat is authenticatie?

In de praktijk betekent authenticatie dat de handelende identiteit (bijv. een natuurlijke persoon), tijdens het afnemen van een (digitale) dienst bij een dienstaanbieder, moet kunnen aantonen dat wat zijn identiteit is. Dit wordt vaak gedaan met een authenticatiemiddel dat in het bezit is van de handelende identiteit en dat door de dienstverlener vertrouwd wordt omdat het is uitgegeven door een vertrouwde (zich zelf of een derde) partij.

Als voorbeeld:

> Ik kan als burger met een BSN (*identiteit*) berichten lezen in de door Logius (*dienstverlener*) gefaciliteerde berichtenbox op MijnOverheid.nl (*dienst*) door mij te authenticeren met mijn DigID (*authenticatiemiddel*) die door Nederlandse staat (*vertrouwde partij*) is uitgeven.

3.2 Scope

De scope van dit document omvat de authenticatie van natuurlijke personen bij digitale interactie[2] met de Nederlande Overheid[3]. Hieronder vallen:

- Nederlandse ingezetenen met Nederlandse nationaliteit
- Geregistreerde niet ingezeten (Nederlande of andere nationaliteit)
- Overige personen die contact hebben met NL overheid.

De huidige versie van dit document beantwoord de vragen alleen voor Nederlandse staatsburgers; de andere groepen personen worden in een latere versie toegevoegd.

3.3 Doelstelling

Dit document geeft antwoord op de volgende vragen:

1. In welke (wettelijke) regels is beschreven hoe de authenticatie van een natuurlijke persoon plaats dient te vinden? (kaders)
2. Welke architectuurkaders zijn van toepassing en waar zijn die vastgelegd? (kaders)
3. Welke authenticatiemiddelen kunnen gebruikt worden en wat zijn de bijbehorende authenticatie niveau's? (wat)
4. Welke processen zijn uitgewerkt voor het beheren en gebruiken van authenticatiemiddelen? (hoe)?

[2] De kaders en processen rond het beheer en gebruik van fysieke authenticatiemiddelen (waaronder Nederlandse en Buitenlandse paspoorten) en de visuele controle ervan worden als gegeven beschouwd.
[3] De beperking tot Nederlandse Overheid hangt samen met de scope van de NORA.

4 Authenticatie Nederlandse ingezetenen

Dit hoofdstuk betreft de ingezetenen van Nederland. De digitale identiteit van deze personen wordt vastgelegd in de BRP (onderdeel persoonsgegevens).

Met opmerkingen [HKr1]: TODO: tekst nalopen en verwarring tussen BRP (zowel als geheel als alleen het deel voor de ingezeten) en RNI (als specifiek onderdeel van het BRP) vermijden.

4.1.1 Wettelijke kaders Fysieke authenticatiemiddelen

Binnen de NL wetgeving zijn op vele plaatsen eisen gesteld aan het identificeren van personen, het gebruikte authenticatiemiddel en de controle daarop. Alle WID's zoals beschreven in de wet: https://wetten.overheid.nl/BWBR0006297/2017-03-01#HoofdstukI_Artikel1 .

Door het RvIG is een overzicht opgesteld (hier een link naar het bestand van Bob) in welke wet gebruik wordt gemaakt van welke voorgeschreven fysieke authenticatiemiddelen. Van de 115 geïnventariseerde wetten, zijn er 75 welke over de volle breedte van de beschreven WID's gebruik maken.

Als documenten waarmee in bij de wet aangewezen gevallen de identiteit van personen kan worden vastgesteld, worden aangewezen:

1°.een geldig reisdocument als bedoeld in artikel 2, eerste lid, onder a, b, c, d, e en g, of een Nederlandse identiteitskaart en vervangende Nederlandse identiteitskaart als bedoeld in artikel 2, tweede lid, van de Paspoortwet;
2°.de documenten waarover een vreemdeling ingevolge de Vreemdelingenwet 2000 moet beschikken ter vaststelling van zijn identiteit, nationaliteit en verblijfsrechtelijke positie;
3°.een geldig nationaal, diplomatiek of dienstpaspoort dat is afgegeven door het daartoe bevoegde gezag in een andere lidstaat van de Europese Gemeenschappen of in een andere staat die partij is bij de Overeenkomst betreffende de Europese Economische Ruimte, voor zover de houder de nationaliteit van die andere lidstaat bezit;
4°.een geldig rijbewijs dat is afgegeven op basis van de Wegenverkeerswet, een geldig rijbewijs als bedoeld in artikel 107 van de Wegenverkeerswet 1994 of een rijbewijs dat is afgegeven door het daartoe bevoegde gezag in een andere lidstaat van de Europese Gemeenschappen of in een andere staat die partij is bij de Overeenkomst betreffende de Europese Economische Ruimte, waarvan de houder in Nederland woonachtig is, zolang de bij de Wegenverkeerswet 1994 vastgestelde termijn van geldigheid in Nederland niet is verstreken, aan de houder geen administratieve maatregel bedoeld in paragraaf 9 van hoofdstuk VI van de Wegenverkeerswet 1994 is opgelegd of aan hem niet de bijkomende straf bedoeld in artikel 179 van die wet is opgelegd en mits het rijbewijs is voorzien van een pasfoto van de houder.
1°.een geldig reisdocument als bedoeld in artikel 2, eerste lid, onder a, b, c, d, e en g, of een Nederlandse identiteitskaart en vervangende Nederlandse identiteitskaart als bedoeld in artikel 2, tweede lid, van de Paspoortwet;

In 13 verschillende wetten wordt gesproken van een kopie van een geldig identiteitsbewijs, op basis hiervan mag geconcludeerd worden dat deze identificatie slechts tot doel heeft de administratieve verantwoording op orde te houden, en geen feitelijke identificatie bevat. Van de overige referenties aan identificatie wordt in 22 gevallen het gebruik van een rijbewijs uitgesloten, In de overige gevallen zijn er beperkingen op het gebied van buitenlandse identiteitsbewijzen, of zijn er aanvullende eisen gesteld zoals een leveranciersmiddel.

Binnen deze lijst lijkt er een tweedeling te zijn: daar waar een rijbewijs is toegestaan of niet.

Met opmerkingen [HKr2]: Waar komt dit onderscheid vandaan? Komt dit door ofwel ontbrekende informatie (bijv. geen nationaliteit), een minder betrouwbaar uitgifte proces of door iets anders

In de praktijk zijn er vele situaties waarin er de wet geen expliciete eis stelt, of waar de betrokken personen een lagere betrouwbaarheid accepteren (bijvoorbeeld in de vorm van een kopie van een

rijbewijs) of waarbij diensten gebruikt worden die eigen authenticatie niveau's definieren (al dan niet met 2-factor authenticatie). Denk hierbij bijvoorbeeld aan de bestandenpostbus.nl die claimt te voldoen aan de eisen uit de BIO.

4.1.2 Introductie logische authenticatiemiddelen

De hierboven genoemde documenten hebben een fysiek karakter en kunnen over het algemeen niet direct gebruikt worden voor authenticatie van de persooon. Een voorbeeld buiten de overheid waarin het wel direct gebruikt wordt zijn de incheck systemen op schiphol waarbij het gepresenteerde paspoort wordt uitgelezen en de gebruiker op basis daarvan geauthenticeerd wordt.

Bij digitale systemen / diensten van de overheid wordt vaak bij processen waarbij de identiteit van de persoon bevestigd moet worden, dit gedaan op basis van andere authenticatie middelen dan de genoemde fysieke authenticatie middelen. Enkele voorbeelden hiervan zijn een DigID, een wachtwoord wat behoord bij een gebruikersnaam of een certificaat.

De impliciete aanname is dat bij het afnemen van een dienst via een digitaal kanaal de digitale authenticatie gebruik maakt van een digitaal authenticatiemiddel met eenzelfde betrouwbaarheid als het authenticatie middel dat nodig is om de dienst via een niet digitale weg af te nemen.

Voor de wettelijk benoemde authenticaties geldt dat een gebruiker zich zal moeten identificeren met een middel dat een gelijk of hoger betrouwbaarheidsniveau heeft als het minimale betrouwbaarheidniveau van de af te nemen dienst. Het principe hierbij is dat een dienst afgenomen mag worden met een authenticatie middel dat tenminste het zelfde betrouwbaarheidsniveau heeft.

De belangrijkste authenticatie middelen voor natuurlijke personen bij de interactie met de overheid zijn DigID en het afsprakenstelsen Electronische toegangsdiensten (AET). Wettelijke Kaders DigID[4]

<<inleidende zin over wat DigID>>

<<Bijzoeken wat wordt er in de wetgeving vermeld over gebruik van DigID>>
• Waar mag het gebruikt worden • Kaders voor uitgifte • Kaders voor gebruik

4.1.3 Wettelijke Kaders idensys en eHerkenning

<<inleidende zin over wat het Afsprakenstelsen Electronische Toegangsdiensten is>> Deze kan als opvolger van DigID kan worden gezien en bevat zowel idensys als eHerkenning. Het AET is de Nederlandse invulling van het eIDAS stelsel.

Voor de authenticatie van natuurlijke personen is alleen idensys van belang; eHerkenning is voor (zakelijke) afnemers[5].In de loop van 2018 lijkt de ontwikkeling van idensys gestopt en is de aandacht verschoven naar het uitrollen van DigID op levels 3 en 4.

Met opmerkingen [HKr3]: Dit klinkt als dat ik als burger mij ook met een eHerkenningsmiddel zou kunnen authenticeren bij een overheidsinstantie. Mits de dienst dit ondersteund en de dienst mijn identificatie (het BSN dus) via het middel binnenkrijg.

<<Bijzoeken wat wordt er in de wetgeving vermeld over gebruik van AET >>

4.1.4 Wettelijke Kaders iDIN

<<inleidende zin over wat iDINs>>

<<Bijzoeken wat wordt er in de wetgeving vermeld over gebruik van DigID>>

[4] Omdat DigID op dit moment voor burgers nog de effectief vigerende standaard is
[5] https://www.noraonline.nl/wiki/Bouwstenen/alfabetisch

4.1.5 Overige middelen

Daarnaast zijn er de volgende specifieke kaders bekend <<waarvan de impact op dit stuk nader moet worden uitgewerkt>>

- Afsprakenstelsel Electronische toegangsdiensten (eHerkenning en idensys)
- Normenkader Rijkspas (inclusief widscan)
- KEI wetgeving voor toegang KEI systeem

Technologische ontwikkelingen hebben het gebruik van Google+ ID en Facebook ID's mogelijk gemaakt. Er is op dit moment nog geen wettelijk kader dat gebruik hiervan mogelijk maakt.

4.2 Relevante architectuur

4.3 Authenticatie middelen en –niveau's

De wetgeving legt op een aantal punten expliciet het authenticatiemiddel vast; waarbij het altijd middelen zijn met een hoger betrouwbaarheidsniveau. In de praktijk zijn er ook situatie waarbij er (nog) geen wetgeving is en de behoefte van de overheidsorganisatie niet deze zware middelen rechtvaardigd. Dit betreft vaak aanvullende informatie met een juridisch niet bindende status. Er is behoefte aan authenticatie kaders voor dit soort contacten met de overheid.

Het meest recente en breedst werkende stelsel voor authenticatie van natuurlijke personen in de hoedanigheid van burger zijn eIDAS en iDIN.

Er is een breed geaccepteerde exceptie m.b.t. het gebruik van DigID: diensten staan authenticatie met DigID niveau 2+ toe zolang niveau 3+4 middelen nog niet wijd verspreid zijn onder de Nederlandse bevolking.

<<korte uitleg wat eIDAS zegt over middelen>>

Binnen de eIDAS verordening worden de volgende betrouwbaarheidsniveaus onderkend. <<hoe verhouden deze zich tot het

Laag	Het betrouwbaarheidsniveau 'Laag' is in de basis 'Self-declared'. Concreet betekend dit dat de middelaanvrager zelf zijn identiteit invuld, zonder dat daar een validatie middels een identiteitsbewijs aan gekoppeld is.
Substantieel	Het betrouwbaarheidsniveau 'Substantieel' is ook 'Self Declared' met het verschil dat een verplichte validatie op basis van een WID onderdeel uit maakt van de identiteits vaststelling.
Hoog	Het betrouwbaarheidsniveau 'Hoog' tenslotte wordt gebaseerd op een Face-2-Face validatie van de houder van een WID en het WID. Hiermee wordt het hoogste niveau geborgd.

Voor authenticatie van natuurlijke personen in een beroepsmatige functie zijn er meerdere stelsels; eHerkenning kan door iedereen worden gebruikt.

Opgemerkt moet worden dat de eHerkenning cq. eIDAS middelen beschouwd moeten worden als afgeleide middelen, immers zijn zijn te allen tijde gebaseerd op een validatie / verificatie van de door het Bevoegd gezag vastgestelde identiteit.

Binnen diverse sectoren zijn er specifieke stelsels die zich veelal richten op digitale authenticatie voor private organisaties. Er is een behoefte om authenticatiemiddelen uit deze sectoren ook te gebruiken voor contact met de overheid (bijv. AdvocatenPas bij contact met de Rechtspraak) zodat de betrokken professional zich overal met éénzelfde middel kan authenticeren. Dit impliceert dat de

Met opmerkingen [HKr4]: Wat is op dit moment de status van dit stelsel?

Met opmerkingen [HKr5]: TODO: nalopen op consistent zijn met de handreiking betrouwbaarheidsniveau's van het forum standaardisatie.

Met opmerkingen [as6]:

De keren dat ik ben tegngekomen dat er voor een lager betrouwbaarheidsniveau toch een hogere authenticatie werd gevraagd had dat vaak te maken met de beperkte technische mogelijkheden op dat moment.

Vaker heb ik gezien dat een dienst lager geclassificeerd werd omdat er anders geen authenenticatie kon plaatsvinden. Dit werd dan tegengegaan doro extra maatregelen te treffen. (meer controles achteraf)

Met opmerkingen [HKr7]: Staat in de handleiding van het forum standaardisatie niet iets over verschillende mate's van verficatie tegen een basisregister (in dit geval dus de BRP).

Met opmerkingen [HKr8]: Worden hiermee alle WID's op één niveau geschaard? De tabel eerder kent in elk geval een tweedeling (mag rijbewijs wel of niet).

Met opmerkingen [as9]: Dit zegt alleen wat over de betrouwbaar heid van de **registratie** van het middel.
Volgens mij nog niks over de **uitgifte** en het **gebruik**.
Voor de uitgifte zijn er volgens mij wel al processen/procedures/compliancy checks. (geen idee waar)
Voor het gebruik wordt inmijn mening vaak met security testen aangetoond dat de gerukte connecties,protocollen etc veilig genoeg zijn.

Met opmerkingen [as10]: Wordt heir bedoeld: eHerkenning is als middel eidas geaccrediteerd en kan daarmee door iedereen (binnen de huidige scope) beroepsmatig gebruikt worden om diensten af te nemen bij overheidspartijen?

Met opmerkingen [as11]: Vraag: is het de bedoeling dat al dieauthenticatiemiddelen naar dezelfde natuurlijk persoon verwijzen? Of zijn ze juist bedoeld om wel te authentiseren (bij de beheerder van de identiteit) maar juist niet de natuurlijk persoon te weten?

Mogelijke issues
Wat als je bent overleden en je partner gebruikt jouw advocatenpas nog?

vertrouwensniveau's op elkaar af te beelden zijn en dat er vertrouwensafspraken gemaakt worden. NB: De rijksoverheid kan voor de Rijkspas ook worden gezien als een specifieke sector.

Daarnaast zijn er allehande bestandenpostbussen die soms een eigen authenticatie gebruiken die vaak gebaseerd is op een 2-factor authenticatie waarbij zender en ontvanger afspraken maken via een onafhankelijk kanaal.

Nog te bespreken zijn de volgende randgebieden:

- <<Authenticatie van gastgebruikers van wifi binnen overheidsonderdelen>>
- <<Authenticatie binnen onderwijs (denk aan Surfnet waar studenten toegang toe hebben) Vallen onderwijs instellingen onder de Nederlandse Overheid of niet? De NORA kent de HORA en ROSA dochters. >>

4.4 Processen gebruik authenticatie middelen

<<wat zijn de afspraken over eIDAS middelen bij gebruik door de overheid>>

<<wat zijn de afspraken over iDIN middelen bij gebruik door de overheid>>

<<wat zijn de afspraken over personen die nog geen eIDAS middel hebben, zoals bijvoorbeeld een DigID niveau 2/2+>>

4.5 Techniek gebruik authenticatie middelen

<<Misschien hier de oude tekst (die nu achterin het document staan).

4.6 Processen beheer authenticatie middelen

De processen voor het beheer van authenticatie middelen worden grotendeels beschreven in de wettelijke kaders voor het betreffende middel en worden daarom hier niet herhaald of samengevat.

4.7 Overige informatie

RiVG	https://www.rvig.nl/brp/brp-als-basisregistratie https://www.rvig.nl/brp/rni
	DigID

Identificatie van natuurlijke personen is beschreven in de "Handleiding Uitvoeringsprocedures (HUP)" Hierin staan de procedures beschreven om personen in te schrijven als ingezetene in de Basisregistratie Personen (BRP). De HUP beschrijft verder hoe gegevens in de BRP moeten worden gewijzigd en gecorrigeerd. Als onderdeel van de HUP is de indentificatie nader beschreven.
https://www.rvig.nl/binaries/rvig/documenten/richtlijnen/2019/01/30/handleiding-uitvoeringsprocedures---hup---versie-3.2/HUP+BRP+3.2.pdf

In het ID-protocol van de NvvB (Nederlandse vereniging van Burgerzaken) is beschreven welke handelingen een medewerker Burgerzaken kan uitvoeren om met meer zekerheid te komen tot een validatie van de identiteit van een Burger, dan wel de initiële vaststelling van een identiteit voor een Burger.
https://nvvb.nl/nl/producten/handreikingen/id-management/

Met opmerkingen [as12]: Ik heb geprobeerd hier een plaatje van te maken (nog niet echt duidelijk maar wil ik het graag eens over hebben)

Iedereen kan binnen zijn eigen context(identiteiten die daar in beheer zijn) beslutien zelf middelen uitgeven en te accepteren. Zodra je buiten je eigen context komt dien je de middelen te gebruiken die overkoepelend zijn.
Vb:
Als rijksambtenaar kan ik prima rijksambtenaar diensten afnemen warbij ik gebruik maak van de rijkspas.Als advocaat kan ik prima advocaatdiensten afnemen met de advocatenpas. Zodra ik als ambtenaar een advocaat dienst wil afnemen moet ik een gezamelijk middel gebruiken → digid , eH etc.

Dit betekend dat iedereen in nederland tenminste de landelijke middelen moet accepteren en eventuele eigen middelen.

Met opmerkingen [as13]: Wat wordt hier bedoeld? Zoiets als een ftp oplossing met sms token?

Met opmerkingen [as14]: Onderwijs heeft veel studenten die niet een nederlands ingezetene zijn.

Met opmerkingen [HKr15]: Link naar informatie over DigID toevoegen

Voor uitgifte WID is geen betrouwbaarheidsniveau vast gesteld, immers het betreft hier een initiële identiteitsvaststelling op basis waarvan opname in de BRP geschied. Indien je daar een betrouwbaarheidsniveau aan zou willen koppelen, is dit altijd een hoger niveau dan het "niveau hoog' zoals dit beschreven is in de eIdas verordening.

5 Authenticatie geregistreerde niet-ingezetenen

Dit hoofdstuk gaat over alle personen die niet behoren tot de ingezeten van Nederland die langdurig in Nederland verblijven en daarom opgenomen zijn in het Register Niet Ingezetenen (RNI).

Met opmerkingen [HKr16]: Tekst uitlijnen op de beschrijving van de

NB: Dit hoofdstuk wordt ingevuld in een latere versie van dit document en zal de volgende onderwerpen adresseren:

1. Wettelijke kaders
2. Relevante architectuur
3. Authenticatie middelen en –niveau's
4. Processen gebruik authenticatie middelen
5. Processen beheer authenticatie middelen
6. Overige informatie

RiVG	https://www.rvig.nl/brp/brp-als-basisregistratie https://www.rvig.nl/brp/rni

6 Authenticatie overige personen

Dit hoofdstuk gaat over alle personen die niet vallen onder de vorige 2 hoofdstukken. Kenmerkend voor deze personen is dat ze dus niet zijn opgenomen in de BPR of het RNI. Deze groep personen wordt beschouwd in dit document omdat deze personen ook de noodzaak kunnen hebben om met de NL overheid digitaal in contact te treden, bijvoorbeeld om bezwaar te kunnen maken tegen een verkeersboete.

NB: Dit hoofdstuk wordt ingevuld in een latere versie van dit document en zal de volgende onderwerpen adresseren:

1. Wettelijke kaders
2. Relevante architectuur
3. Authenticatie middelen en –niveau's
4. Processen gebruik authenticatie middelen
5. Processen beheer authenticatie middelen

Het eIDAS stelsel is europese regelgeving en addresseert 2 aspecten. Hiervan is het eerste relevant voor dit document; het tweede valt buiten de scope van de authenticatie van natuurlijke personen bij de Nederlandse overheid.

- Inkomend verkeer (verplicht): Europese burgers en bedrijven die met een door Europa erkend inlogmiddel inloggen bij Nederlandse dienstverleners.
- Uitgaand verkeer (niet verplicht): Nederlandse burgers en bedrijven die met een door Europa erkend Nederlands inlogmiddel bij andere Europese dienstverleners inloggen.

7 Nog te herplaatsen teksten

8 Hoe verloopt de authenticatie van een digitale identiteit van de BRP: qua proces en qua techniek?

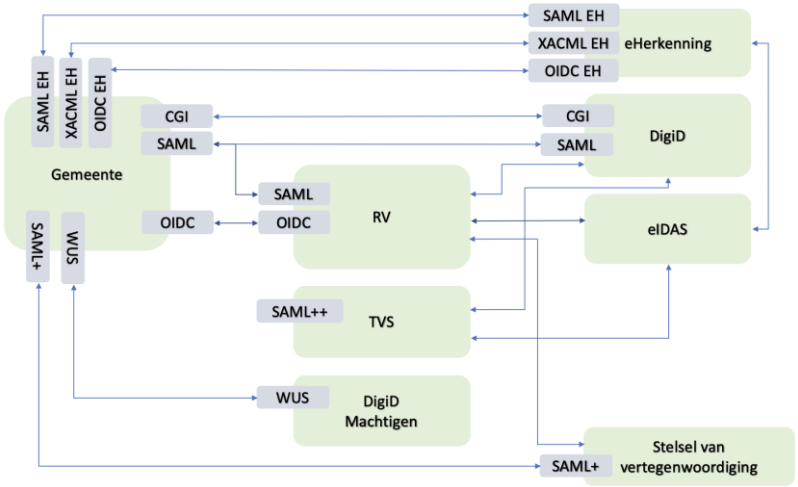
Er is geen eenduidig proces voor de authenticatie (verificatie) van een door RvIG uitgegeven digitale identiteit. De authenticatie vindt in de praktijk decentraal plaats en is ook afhankelijk van het middel dat daarbij wordt gebuikt. Authenticatie wordt doorgaans mogelijk gemaakt via herbruikbare bouwstenen of via diensten. Zo zijn er bijvoorbeeld diensten als DigiD, eHerkenning, Toegangsverleningsservice (TVS), die een autorisatie hebben op de BRP ihkv verificatie (authenticatie). Middels de identity providers worden dienstverleners wel voor een deel ontzorgd. Specifiek toegang tot de authenticatiemiddelen (chip op paspoort, eNIK e.d.) hebben maar een paar partijen. Verificatie van de attributen op de chip(s) gebeurt via autorisaties. Vaak zijn die authenticatiemiddelen technisch gestandaardiseerd (bij DigiD bijvoorbeeld gebaseerd SAML). Door standaardisatie op Informatie-/Applicatielaag wordt gestimuleerd de authenticaties te uniformeren. Vanuit deeloplossingen (rijbewijs, PKIO, Zorgpas, overheidspas, etc) treed ook enige standaardisatie op. Er is echter nog geen eenduidige architectuur voor de overheid waarin deze authenticatie is uitgewerkt.

Met opmerkingen [as17]: wordt hier bedoelt dat je geautoriseerd moet zijn als dienstverlener om de chip te mogen lezen?
Zolas het heir staat lijkt het alsof je de attributen op de chip nog moet verifieren bij een andere bron.

Met opmerkingen [as18]: Is verificatie een onderdeel van authenticatie?

Ik zou juist verificatie laten staan en de authenticatie weghalen. Zie 1e regel en ook de 5e.

Door VNG-Realisatie is het volgende overzicht opgesteld waarbij de verschillende koppelvlakken in beeld zijn gebracht inclusief de status van dat koppelvlak.



De SAML + en SAML ++ koppelvlakken uit bovenstaand figuur zijn niet gestandaardiseerd. Het zijn ‘eigen’ invullingen van de SAML Metadata Extensions. Interoperabiliteit van deze implementaties is een vraagstuk.

8.1 Koppelvlak DigiD CGI

Nog flink aantal gemeenten zijn aangesloten op dit oorspronkelijke DigiD koppelvlak, gebaseerd op een oude standaard. Dit koppelvlak is ‘end of life’. Het is de bedoeling dat gemeenten overstappen naar een nieuw koppelvlak. De vraag is welke keuze deze gemeenten moeten maken. Aansluiten op het DigiD SAML-koppelvlak of wachten op de routeringsvoorziening? En welk koppelvlak van de routeringsvoorziening moet men dan implementeren? Aansluiten op het huidige DigiD SAML-koppelvlak of wachten op de beschikbaarheid van het OIDC-koppelvlak, omdat dan pas andere toegangsdiensten via de routeringsvoorziening worden ontsloten?

Met opmerkingen [as19]:
Dit is een standaardisatie,koppelvlak discussie.
Veel van deze problemen zouden opgelost kunnen worden door de TVS-en,RV-en etc.

Ervaring leert ook dat als alle partijen dezelfde voorziening gebruiken , die voorziening steeds meer problemen gaat krijgen om mee te gaan in de nieuwe ontwikkelingen.

Zou het mogelijk zijn om hieruit een aantal uitgangspunten te definieren voor authenticatie?

Ik merk zelf dat de grote commercieele leveranciers van authenticatie afhandeling ook nog niet heel flexibel zijn in de geboden dienstverlening.

8.2 Koppelvlak DigiD SAML

Het huidige DigiD SAML koppelvlak is substantieel en hoog bestendig en als dusdanig ook beproeft in de DigiD-Hoog pilot van 2017. Het DigiD SAML koppelvlak biedt geen ondersteuning voor machtigingen.

Met opmerkingen [as20]: Authenticate is ook geen machtigingen.

Ik probeer deze altijd uit elkaar te houden.

➔eerst identificatie
➔dan authenticatie indien nodig
➔daarna pas de autorisaties en/of machtiging.

Het feit dat je geauthentiseerd bent wil niet zeggen dat je geautoriseerd bent. Er is altijd nog een autorisatie stap (al zou dat alleen maar een pass-thru zijn. 😊)

Ik zie in de praktijk nu vaak dat er geprobeerd wordt om met een handeling alle drie af te vangen.
Dat is bij machtigingen niet mogelijk aangezien er altijd meerdere partijen bij betrokken zijn.

8.3 Koppelvlak routeringsvoorziening Logius (Identity Bridge van de Belastingdienst in 'plus versie')

De routeringsvoorziening start met het DigiD SAML-koppelvlak. Hierop komen DigiD en eIDAS (met alleen BSN, dus zonder attributen) beschikbaar. Er wordt gewerkt aan de definitie van een OIDC-koppelvlak waarmee aanvullende attributen, machtigen en aanvullend middel(en) kunnen worden ontsloten. De planning hiervan is niet duidelijk. Er is een globale fasering weergegeven over de komende jaren.

8.4 Koppelvlak routeringsvoorziening TVS

Het zorgveld beproefd een eigen routeringsvoorziening, de TVS. De TVS maakt gebruik van een SAML-'plus' koppelvlak. Een specifiek voor de TVS ontwikkeld koppelvlak op basis van SAML. Dit koppelvlak maakt het mogelijk om naast DigiD, ook andere middelen en machtigen te ontsluiten.

Met opmerkingen [as21]: Vendor lock-in? 😊

8.5 Koppelvlak DigiD Machtigen

Het huidige DigiD Machtigen bestaat al een tijd en kent een eigen koppelvlak gebaseerd op SAML. Hiervan is aangegeven dat dit koppelvlak 'end of life' is. Bij de introductie van de nieuwe machtigingsvoorziening (het stelsel van vertegenwoordiging, met een nieuw koppelvlak) wordt dit bestaande koppelvlak op termijn uitgefaseerd. Het bestaande koppelvlak is namelijk niet geschikt om de nieuwe functionele toepassingen van het nieuwe stelsel te ontsluiten richting de gemeente. Het advies is derhalve hier nu al niet meer op aan te sluiten, tenzij zeer weloverwogen en met urgent belang. Waar moet een gemeente dan wel op aansluiten om snel aan de slag te kunnen met machtigen? Direct op het nieuwe koppelvlak voor machtigen, of wachten op de routeringsvoorziening? Wanneer ontsluit die routeringsvoorziening machtigen? Hierover is al aangegeven dat dit alleen wordt ontsloten via het nieuwe koppelvlak op de routeringsvoorziening gebaseerd op de OIDC-standaard. Vooralsnog is er voor machtigen geen alternatief voor handen anders dan het terug vallen op een papieren proces.

8.6 Koppelvlak 'stelsel van vertegenwoordiging' (de nieuwe machtigingsvoorziening)

Aansluiten op het stelsel van vertegenwoordiging kan op termijn op de zogenoemde 'Bevoegdheidsverklaringsdienst'. Hiervoor wordt een eigen SAML-koppelvlak ontwikkeld. Voor pilotdoeleinden komt een eerste versie in 2019 beschikbaar. Later volgen ook de specificaties voor een OIDC-koppelvlak is de planning. Partijen kunnen dan mogelijk kiezen welk koppelvlak men toepast.

Onbekend is of beide koppelvlakken straks volledig dezelfde functionaliteit ondersteunen en hoe lang het SAML-koppelvlak wordt ondersteund. De beide routeringsvoorzieningen kunnen ook

aansluiten op dit koppelvlak (SAML en later ook OIDC), waardoor aangesloten partijen op de routeringsvoorziening alleen het koppelvlak van de routeringsvoorziening hoeven te implementeren (en zich niet meer druk hoeven te maken om het koppelvlak van de bevoegdheidsverklaringsdienst). Alleen: wanneer is dit beschikbaar en kan/wil men hierop wachten? (met het risico dat het OIDC-koppelvlak op de routeringsvoorziening veel langer op zich laat wachten dan voorspelt).

8.7 Koppelvlak ETD

Het afsprakenstelsel Elektronische Toegangsdiensten kent een eigen, op SAML gebaseerd, koppelvlak. Het zou goed zijn om te onderzoeken of hergebruik kan worden gemaakt van deze koppelvlakdefinities. Is het logisch om de makelaars binnen het ETD een ander koppelvlak te laten ondersteunen dan de routeringsvoorziening(en) en de machtigingsregisters een ander koppelvlak dan de machtigingsvoorziening (stelsel van vertegenwoordiging)? Over de ETD-koppelvlakken is al goed nagedacht en zijn bovendien breed geïmplementeerd (ook bij gemeenten). Alleen kent ETD nog geen concrete plannen om over te stappen op de OIDC-standaard, wat wel weer de strategie is bij de andere genoemde voorzieningen.

8.8 Hoe is de identificatie van natuurlijke personen in de diverse wetten verankerd?

8.9

Voor de afgifte van eHerkenning cq. eIDAS middelen is het geheel vastgelegd in deze specificaties per betrouwbaarheidsniveau:

https://afsprakenstelsel.etoegang.nl/display/as/Technische+specificaties+en+procedures+voor+uitgifte+van+authenticatiemiddelen

Opgemerkt moet worden dat de eHerkenning cq. eIDAS middelen beschouwd moeten worden als afgeleide middelen, immers zijn zijn te allen tijde gebaseerd op een validatie / verificatie van de door het Bevoegd gezag vastgestelde identiteit.

8.10 Welke identificatiemiddelen zijn toepasbaar?

Alle WID's zoals beschreven in de wet: https://wetten.overheid.nl/BWBR0006297/2017-03-01#HoofdstukI_Artikel1.
Door het RvIG is en overzicht opgesteld (hier een link naar het bestand van Bob) in welke wet gebruik wordt gemaakt van welke voorgeschreven indentificatiemiddelen. Van de 115 geinventariseerde wetten, zijn er 75 welke over de volle breedte van de beschreven WID's gebruik maken. Dit zijn de volgende documenten:

1Als documenten waarmee in bij de wet aangewezen gevallen de identiteit van personen kan worden vastgesteld, worden aangewezen:

- **1°.**een geldig reisdocument als bedoeld in artikel 2, eerste lid, onder a, b, c, d, e en g, of een Nederlandse identiteitskaart en vervangende Nederlandse identiteitskaart als bedoeld in artikel 2, tweede lid, van de Paspoortwet;

- **2°.**de documenten waarover een vreemdeling ingevolge de Vreemdelingenwet 2000 moet beschikken ter vaststelling van zijn identiteit, nationaliteit en verblijfsrechtelijke positie;

- **3°.**een geldig nationaal, diplomatiek of dienstpaspoort dat is afgegeven door het daartoe bevoegde gezag in een andere lidstaat van de Europese Gemeenschappen of in een andere staat die partij is bij de Overeenkomst betreffende de Europese Economische Ruimte, voor zover de houder de nationaliteit van die andere lidstaat bezit;

- **4°.**een geldig rijbewijs dat is afgegeven op basis van de Wegenverkeerswet, een geldig rijbewijs als bedoeld in artikel 107 van de Wegenverkeerswet 1994 of een rijbewijs dat is afgegeven door het daartoe bevoegde gezag in een andere lidstaat van de Europese Gemeenschappen of in een andere staat die partij is bij de Overeenkomst betreffende de Europese Economische Ruimte, waarvan de houder in Nederland woonachtig is, zolang de bij de Wegenverkeerswet 1994 vastgestelde termijn van geldigheid in Nederland niet is verstreken, aan de houder geen administratieve maatregel bedoeld in paragraaf 9 van hoofdstuk VI van de Wegenverkeerswet 1994 is opgelegd of aan hem niet de bijkomende straf bedoeld in artikel 179 van die wet is opgelegd en mits het rijbewijs is voorzien van een pasfoto van de houder.

In 13 verschillende wetten wordt gesproken van een kopie van een geldig identiteitsbewijs, op basis hiervan mag geconcludeerd worden dat deze identificatie slechts tot doel heeft de administratieve verantwoording op orde te houden, en geen feitelijke identificatie bevat.

Van de overige referenties aan identificatie wordt in 22 gevallen het gebruik van een rijbewijs uitgesloten,

In de overige gevallen zijn er beperkingen op het gebeid van buitenlandse identiteitsbewijzen, of zijn er aanvullende eisen gesteld zoals een leveranciersmiddel.

8.11 En welke niveau's van authenticatie zijn mogelijk voor die authenticatiemiddelen?

Voor uitgifte WID is geen betrouwbaarheidsniveau vast gesteld, immers het betreft hier een initiële identiteitsvaststelling op basis waarvan opname in de BRP geschied. Indien je daar een betrouwbaarheidsniveau aan zou willen koppelen, is dit altijd een hoger niveau dan het "niveau hoog' zoals dit beschreven is in de eldas verordening.
Binnen de eldas verordening worden de volgende betrouwbaarheidsniveaus ondekend:
Laag
Substantieel
Hoog

Het betrouwbaarheidsniveau 'Laag' is in de basis 'Self-declared'. Concreet betekend dit dat de middelaanvrager zelf zijn identiteit invuld, zonder dat daar een vaidatie middels een identiteitsbewijs aan gekoppeld is.

Het betrouwbaarheidsniveau 'Substantieel' is ook 'Self Declared' met het verschil dat een verplichte validatie op basis van een WID onderdeel uit maakt van de identiteits vaststelling.

Het betrouwbaarheidsniveau 'Hoog' tenslotte wordt gebaseerd op een Face-2-Face validatie van de houder van een WID en het WID. Hiermee wordt het hoogste niveau geborgd.

8.12 Is een proces (document) beschikbaar voor het opzetten / aanvragen van authenticatie bij de BRP? (wat moet je bij wie regelen ed)

Wat bedoelen we hier mee? Dat je specialisten kan inhuren om voor jou een identificatie uit te voeren conform de BRP standaard?

Op basis van de instructies uit de HUP en het ID-Protocol zijn er diverse partijen (AMP, GWK Travelex, notariaat?) die identiteitsvaststelling als dienstverlening aanbieden.