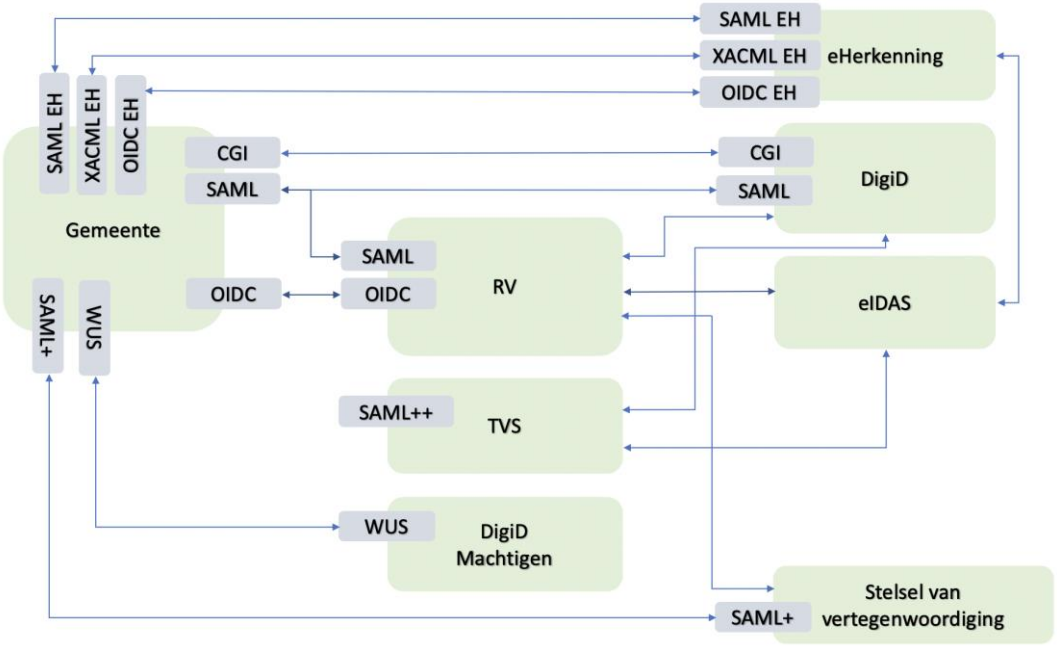
Hoe verloopt de authenticatie van een digitale identiteit van de BRP: qua proces en qua techniek?

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.

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.

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?

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.

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.

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.

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.

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).

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.

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

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 identificatie nader beschreven.

https://www.rvig.nl/binaries/rvig/documenten/richtlijnen/2019/01/30/handleiding-uitvoeringsprocedures---hup---versie-3.2/HUP+BRP+3.2.pdf
EB: In par 1.4 zijn de voor het document relevante stukken opgesomd.

De lijken allen gericht op het Identiteitenbeheer en niet zo zeer op verifiëren van identiteiten (=authenticatie).

De WID staat er niet tussen, maar lijkt de meest -en mogelijk ook enig- relevante: https://wetten.overheid.nl/BWBR0006297/2017-03-01#HoofdstukI_Artikel1.

Echter, het gaat telkens om authenticatie van de persoon tbv juiste registratie in de BRP, dan wel voor niet-digitale aspecten. Daar staat niets over digitale authenticatie irt de BRP, dus authenticatie op basis van een digitale identiteit.

De hele beschrijving is opgezet rondom de identiteit in de analoge/reële wereld en niet rondom de digitale identiteit. In de gesprekken rondom de toekomst van de BRP komt dit aspect ook naar boven.

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/

Pas op blz 11 in de handleiding voor de medewerkers, wordt gesproken over het “zich digitaal melden van de burger bij de overheid”. En daarna gaat alles over documenten en niet over digitale authenticatie. Ook hier dus dezelfde opmerking als hierboven ☹.

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

Interessant zijn met name 2.1.2 Bewijs en verificatie van Identiteit (natuurlijk persoon).

En voor Identificatie / authenticatie van bedrijven is dan interessant: 2.1.3 Bewijs en verificatie van identiteit (rechtspersoon).

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

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 een overzicht opgesteld (hier een link naar het Excel-bestand van Bob) in welke wet gebruik wordt gemaakt van welke voorgeschreven identificatiemiddelen. Van de 115 geïnventariseerde 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.

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 eIdas verordening.

Binnen de eIdas verordening worden de volgende betrouwbaarheidsniveaus onderkend:
- 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.

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

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.

Maar een bedrijf B met authenticatiemiddel A kan niet zomaar de BRP gaan gebruiken. Gecontroleerd wordt of een middel voldoet en wordt toegelaten. Het geheel van processen (inschrijving, middelen aanvraag etc) is gedocumenteerd en gevisualiseerd door RvIG. Die stukken worden momenteel opgevraagd. Voor de toelating is niet de middelenuitgever maar de authenticatiedienst (Logius DigiD) verantwoordelijk geworden. Dat lijkt een beetje een 'kromme' situatie, aangezien de digitale authenticatiemiddelen ALTIJD afgeleid moeten worden van de 'moederkaart' c.q. identiteitskaart/paspoort van RvIG.

Den Haag, 27 augustus 2019

Menno Stigter

Bob te Riele

Anne Schrijer