VNG Realisatie

GEMMA Gegevenslandschap

Authenticatie en Autorisatie

Leeswijzer

Dit document beschrijft de visie van VNG Realisatie ten aanzien van authenticatie en autorisatie. Dit document behoort tot de architectuurdocumenten van de ontwikkeling van de gemeentelijke informatievoorziening: het GEMMA Gegevenslandschap. In deze visie worden de gemeentelijke bewegingen op het gebied van de informatievoorziening geschetst, en wordt aan de hand van deze bewegingen een nieuwe, flexibele en meer generieke en gezamenlijke gemeentelijke informatievoorziening geschetst.

Dit document is bestemd voor informatiemanagers, adviseurs, architecten en productmanagers van gemeenten en gemeentelijke leveranciers.

Het document is als volgt opgebouwd:

- Hoofdstuk 1 beschrijft de inleiding;
- Hoofdstuk 2 beschrijft het beleid en de kaders rondom authenticatie en autorisatie;
- Hoofdstuk 3 beschrijft de NORA patronen;
- Hoofdstuk 4 beschrijft de authenticatiemiddelen van personen en bedrijven;
- Hoofdstuk 5 beschrijft de huidige en toekomstige inrichting van IAM bij gemeenten;
- Hoofdstuk 6 beschrijft eisen die aan dienstenafnemers en -aanbieders worden gesteld;
- Hoofdstuk 7 geeft een overzicht en beschrijving van de belangrijkste begrippen.

Dit document is in beheer bij VNG-Realisatie.

Versie	Toelichting	Datum	Opsteller(s)
1.0	Eerste versie	April 2020	VNG Realisatie

VNG Realisatie
Nassaulaan 12 Den Haag | Postbus 30435, 2500 GK Den Haag
070 373 8008 | realisatie@vng.nl

Inhoudsopgave

1. Inleiding

Door VNG Realisatie is de vanuit de informatiekundige visie Common Ground gewenste gelaagde inrichting en opbouw van gemeentelijke applicaties beschreven in het '*GEMMA Gegevenslandschap*'[1]. In deze gelaagde inrichting worden processen gescheiden van gegevens en onderling verbonden via een integratiefaciliteit. Een belangrijk onderdeel van deze inrichting is het identificeren, authenticeren en autoriseren van personen en systemen binnen de verschillende lagen van de architectuur. In de beveiligingswereld heet dit het IAA concept: **I**dentificatie, **A**uthenticatie en **A**utorisatie. Via de functies van het IAA-concept kan een gebruiker (burger, bedrijf of systeem) aantonen wie hij is en wordt bepaald wat die gebruiker mag.

In het GEMMA Gegevenslandschap is op verschillende punten identificatie, authenticatie en autorisatie een vereiste. Denk hierbij aan de identificatie en authenticatie van burgers en bedrijven die gepersonaliseerde diensten van de gemeente willen afnemen. Het is met het oog op onder andere privacywetgeving en regels ten aanzien van informatiebeveiliging een vereiste dat die gepersonaliseerde diensten enkel aan de juiste (lees: geautoriseerde) personen en bedrijven worden geleverd. Een ander voorbeeld is de identificatie, authenticatie en autorisatie van de gemeentelijke medewerkers. Het is van belang dat enkel geauthenticeerde en geautoriseerde medewerkers toegang krijgen tot gegevens en administratieve functies.

In dit document worden de verschillende plaatsten in het GEMMA Gegevenslandschap waar sprake is van authenticatie en autorisatie van personen, bedrijven en systemen beschreven. De onderstaande use-cases worden behandeld:

- burgers en bedrijven voor gemeentelijke diensten en producten;
- medewerkers voor administratieve processen;
- medewerkers voor specifieke (subsets van) gegevens;
- gemeentelijke informatiesystemen voor gebruik van interne diensten;
- gemeentelijke informatiesystemen voor gebruik van externe diensten;
- keten- en netwerkpartijen voor gemeentelijke diensten;

In dit document worden de bovenstaande soorten van autorisatie en de wijze waarop mensen en systemen worden geauthenticeerd nader uitgewerkt. De wijze waarop burgers en bedrijven zich kunnen laten vertegenwoordigen (machtigen) is buiten beschouwing gelaten.

[1] https://www.gemmaonline.nl/index.php/Gegevenslandschap

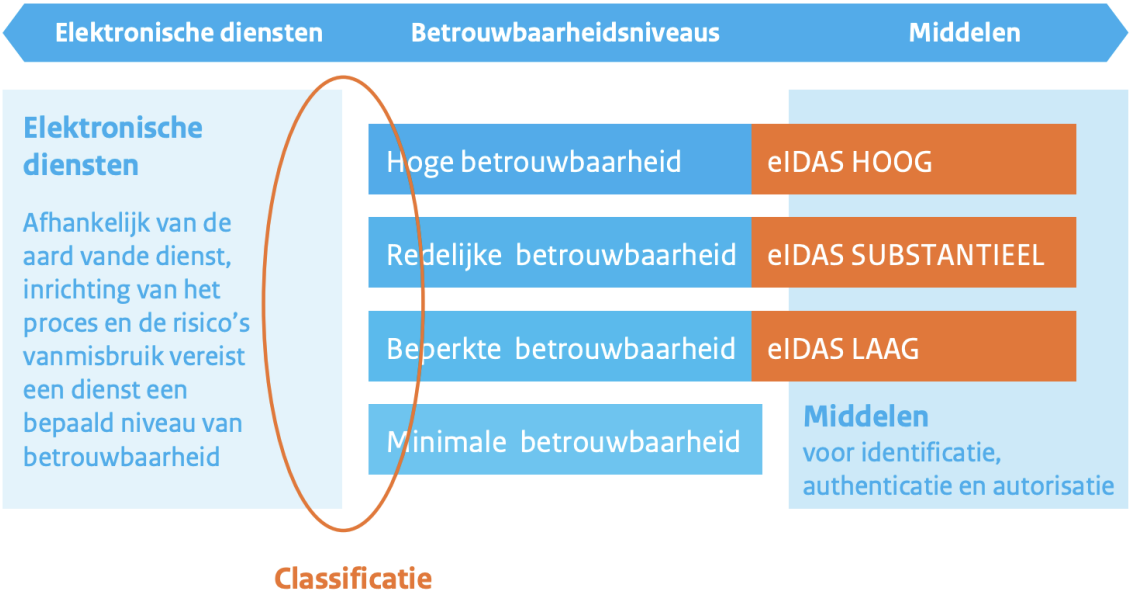
2. Beleid en kaders

Ten aanzien van het identificeren, autoriseren en authenticeren van mensen en systemen zijn verschillende landelijke regels en afspraken van kracht. In onderstaande paragrafen worden deze regels kort toegelicht.

2.1. eIDAS-verordening

eIDAS staat voor 'Electronic Identities And Trust Services'. Met eIDAS hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. Een onderdeel van de verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen. De Europese eIDAS-verordening stelt dat het vanaf september 2018 voor burgers en organisaties mogelijk moet zijn om met de nationale, genotificeerde (door Europa erkende) middelen in te loggen bij alle overheidsorganisaties binnen de Europese Unie. De (Nederlandse) overheidsdiensten moeten ervoor zorgen dat alle EU-ingezetenen zo toegang hebben tot hun dienstverlening. Deze verplichting geldt o.a. voor organisaties die gebruik maken van DigiD en eHerkenning en diensten bieden op niveau substantieel.

In de eIDAS-verordening zijn de mogelijke beveiligingsniveaus voor authenticatiemiddelen vastgelegd. Binnen dit wettelijke kader zijn drie verschillende niveaus te onderscheiden: laag, substantieel en hoog.



De eIDAS-verordening verplicht organisaties om een authenticatiemiddel te hanteren voor toegang tot een elektronische dienst wat past bij het betrouwbaarheidsniveau van die dienst. Bovenstaand schema geeft aan welke middelen passen bij de verschillende betrouwbaarheidsniveaus.

Door het Forum Standaardisatie is een handreiking[2] opgesteld die helpt bij het maken van een heldere en transparante keuze voor het betrouwbaarheidsniveau van een digitale dienst. Deze handreiking is gebaseerd op de inhoud van de eIDAS-verordening voor digitale identificatie- en vertrouwensdiensten, de bijbehorende uitvoeringsbesluiten en de nationale wet- en regelgeving. Organisaties zijn verplicht om bij de elektronische diensten die ze ter beschikking stellen het betrouwbaarheidsniveau te bepalen.

2.2. Algemene wet bestuursrecht (Awb)

De Algemene wet bestuursrecht (Awb) vereist dat elektronisch verkeer tussen burger en bestuursorgaan 'voldoende betrouwbaar en vertrouwelijk' verloopt. In de Awb staan de eisen aan die maatregelen echter niet concreet gedefinieerd. Het Rijk en andere overheden hebben daarom zogenoemde normen vastgesteld: de Baseline Informatiebeveiliging Overheid (BIO)[3].

In de Awb staan de eisen zoals gezegd niet concreet gedefinieerd. Er is wel behoefte aan helderheid nu e-diensten binnen de overheid steeds meer worden gebruikt. Zo is het belangrijk dat overheidsorganisaties in vergelijkbare situaties hetzelfde niveau van betrouwbaarheid en authenticatie vereisen (en borgen) voor hun digitale diensten. Belangrijk is ook dat hun keuzes helder en transparant zijn. Dat draagt bij aan een transparante, toegankelijke, geloofwaardige en zorgvuldig opererende overheid en aan de rechtszekerheid van burgers en bedrijven.

2.3. Wet Digitale Overheid

De Wet Digitale Overheid (WDO) heeft onder andere als doel het regelen van het veilig en betrouwbaar kunnen inloggen voor Nederlandse burgers en bedrijven bij de (semi-)overheid. Met veilig en betrouwbaar inloggen wordt bedoeld dat burgers elektronische identificatiemiddelen krijgen met een hogere mate van betrouwbaarheid dan het huidige DigiD kan bieden. Deze nieuwe middelen geven publieke dienstverleners meer zekerheid over iemands identiteit. De WDO legt de basis voor verdere digitalisering, waaronder regulering van de digitale overheid en meer in het bijzonder de generieke digitale voorzieningen in een gemeenschappelijke infrastructuur van de overheid. Dit wetsvoorstel vormt een eerste tranche van regelgeving ten behoeve van de verdere digitalisering van de overheid op de verschillende niveaus en bevat de meest urgente onderwerpen van regelgeving, te weten:

- de bevoegdheid om bepaalde standaarden te verplichten in het elektronisch verkeer van de overheid;
- het stellen van regels over informatieveiligheid;
- de verantwoordelijkheid voor het beheer van de voorzieningen en diensten binnen de generieke digitale overheidsinfrastructuur (GDI);
- de digitale toegang tot publieke dienstverlening voor burgers (natuurlijke personen) en bedrijven (rechtspersonen en ondernemingen).

[2] https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus
[3] In paragraaf 2.4 is een samenvatting van de BIO opgenomen

Het wetsvoorstel biedt ook grondslagen voor de verwerking van persoonsgegevens in het authenticatieproces, waaronder het Burgerservicenummer (BSN), bij het geven van de digitale toegang tot publieke dienstverlening voor burgers en bedrijven.

De WDO schrijft voor dat alle binnen het burgerdomein toegelaten authenticatiediensten dienen te worden ontsloten bij alle dienstverleners met interactie met burgers. Om aan de WDO te kunnen voldoen zullen alle dienstverleners de toegelaten authenticatiediensten dienen te ontsluiten binnen het eigen ICT-landschap.

2.4. Baseline Informatiebeveiliging Overheid (BIO)

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Van BIG, BIR, BIR2017, IBI en BIWA naar BIO. Hiermee is één gezamenlijk normenkader ontstaan voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek (ISO 27001/2).

De BIO legt de nadruk op risicomanagement. De bestuurder is verantwoordelijk voor een veilige informatievoorziening. Het is daarom aan de bestuurder om de risicobereidheid te bepalen en daarmee ook te controleren of de maatregelen binnen de organisatie de risico's terugbrengen tot een voor de bestuurder acceptabel niveau. Overschrijding van dat niveau vereist expliciete besluitvorming. Risicomanagement staat daarmee aan de basis van informatiebeveiliging. Er dient een continu proces van identificatie en beoordeling van risico's plaats te vinden om te bepalen wat nodig is om informatie adequaat te beschermen. Hierbij moet worden opgemerkt dat het risico nul niet bestaat en dat het aan het bestuur is om te bepalen hoeveel of welk risico acceptabel is. En de risico's zijn talrijk: privacy schendingen door een datalek, economische schade door het uitlekken van vertrouwelijke plannen, fysieke schade door storingen in systemen in de openbare ruimte en als laatste niet te onderschatten afbreukrisico en niet als vertrouwde overheid gezien worden.

Vanuit de BIO worden eisen gesteld aan de inrichting van de toegang van gebruikers tot informatie en informatie verwerkende faciliteiten. Gemeenten dienen in hun autorisatie en authenticatie van gebruikers en systemen te voldoen aan de in de BIO gestelde eisen.

2.5. Landelijke API strategie

Bij het implementeren van een API kunnen veel keuzes gemaakt worden ten aanzien van technische implementatie, beveiliging en autorisatie. Ook zijn veel best practices beschikbaar. Het API Kennisplatform beschrijft in opdracht van het Forum Standaardisatie een eenduidige set van keuzes (de landelijke API-strategie) waardoor er in Nederland een uitgangspunt ontstaat hoe API's moeten werken. Zo wordt het voor afnemers van API's makkelijker om aan te sluiten op koppelvlakken van de Nederlandse Overheid. Organisatorisch werkingsgebied voor deze uitgangspunten zijn Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

In de landelijke API-strategie is beschreven dat authenticatie en autorisatie van een verzoek niet mag afhangen van cookies of sessies. In plaats daarvan wordt elk verzoek voorzien van een token. Binnen het Kennisplatform APIs is gekozen voor OAuth 2.0[4] als de standaard voor het autorisatiemechanisme waar dit nodig is[5]. Het gebruik van OAuth 2.0 wordt verplicht voor applicaties waarbij gebruikers (resource eigenaar) toestemming geven (impliciet of expliciet) aan een dienst (van een derde) om namens hem toegang te krijgen tot specifieke gegevens via een RESTful API. Het gaat dan om een RESTful API waar de resource eigenaar (een burger, medewerker, ketenpartner of systeem) recht tot toegang heeft. Voor RESTful APIs waarvoor niet geldt dat de resource eigenaar toestemming hoeft te geven voor het gebruik geldt de verplichting om OAuth 2.0 te gebruiken niet.

In het geval van APIs met toegangsbeperking (bijvoorbeeld bij verwerking van gesloten gegevens) of doelbinding is er in de API-strategie voor gekozen om aanvullend sprake gebruik te maken van PKIoverheid certificaten en tweezijdig TLS. Door toepassing van tweezijdig TLS wordt geborgd dat beide partijen (zender en ontvanger) bij op het niveau van de verbinding bij een uitwisseling van gegevens 100% zekerheid hebben over elkaars identiteit. TLS wordt voornamelijk gebruikt in situaties waarin het nodig is te verifiëren of men inderdaad verbonden is met de gewenste server. Met name in communicatie met of tussen de overheid is dit van groot belang, aangezien vaak persoonlijke of anderszins vertrouwelijke informatie wordt uitgewisseld.

[4] https://docs.geostandaarden.nl/api/API-Strategie/#nederlands-profiel-oauth
[5] https://docs.geostandaarden.nl/api/API-Strategie/#authenticatie-en-autorisatie

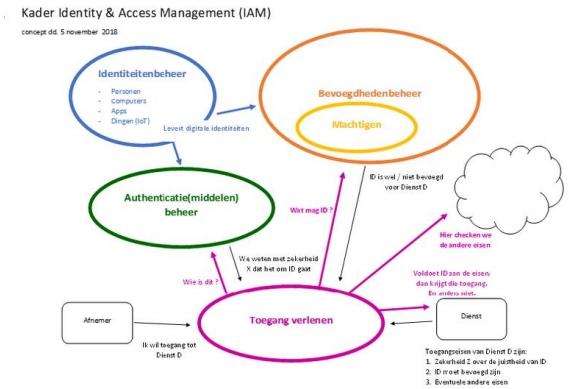
3. Identity en Access Management (IAM) concepten

Identity en Access Management (IAM) is vrij vertaald het beheer om er voor te zorgen dat de juiste "identiteiten" (denk daarbij aan personen of systemen), voor de juiste redenen en op het juiste moment toegang krijgen tot de juiste faciliteiten. IAM regelt drie belangrijke voorwaarden voor digitale dienstverlening:

1. Identificatie zorgt er voor dat bekend is wie je bent (of in elk geval wat een digitale identiteit van je is);
2. Authenticatie zorgt er voor dat met een bepaalde zekerheid bekend is dat je ook echt degene bent die je zegt te zijn;
3. Autorisatie zorgt er voor je alleen toegang krijgt (al dan niet door een ander gemachtigd) tot de diensten waartoe dat toegestaan is.

Als iemand een digitale dienst wil afnemen, dan zal de elektronische identificatie, authenticatie en autorisatie goed geregeld moeten worden om de belangen van zowel de dienstaanbieder als de afnemer te borgen. Om binnen de overheid c.q. samenleving te komen tot een meer eenduidig en gedeeld beeld van IAM is in de Nederlandse Overheid Referentie Architectuur (NORA) daarop een gezamenlijke visie[6] geformuleerd. In deze visie worden de relevante aspecten en begrippen beschreven en wordt een visualisatie en beschrijving van hun samenhang gegeven. Onderstaand figuur uit de NORA schetst deze onderdelen en hun samenhang.

[6] https://www.noraonline.nl/wiki/Identity_%26_Access_Management_(IAM)



Bovenstaand figuur geeft inzicht in de verschillende processen die nodig zijn om subjecten op gecontroleerde wijze toegang te geven tot de middelen (objecten) die zij nodig hebben om hun taak uit te kunnen voeren. In de NORA worden de verschillende onderdelen van IAM uitgebreid beschreven. De NORA beschrijvingen[7] zijn ook geldig voor gemeenten. Voor de volledigheid worden de verschillende begrippen hieronder kort toegelicht.

Identiteitenbeheer - betreft de relatie van een natuurlijk persoon met digitale identiteiten, inclusief het creëren, registreren, wijzigen, verstrekken en verwijderen van die digitale identiteiten.

Bevoegdhedenbeheer - de “levenscyclus” van bevoegdheden, waar vooraf wordt bepaald wat een identiteit mag (of niet mag). Dat kan ook zijn, dat de identiteit door een andere identiteit is gemachtigd om iets te doen.

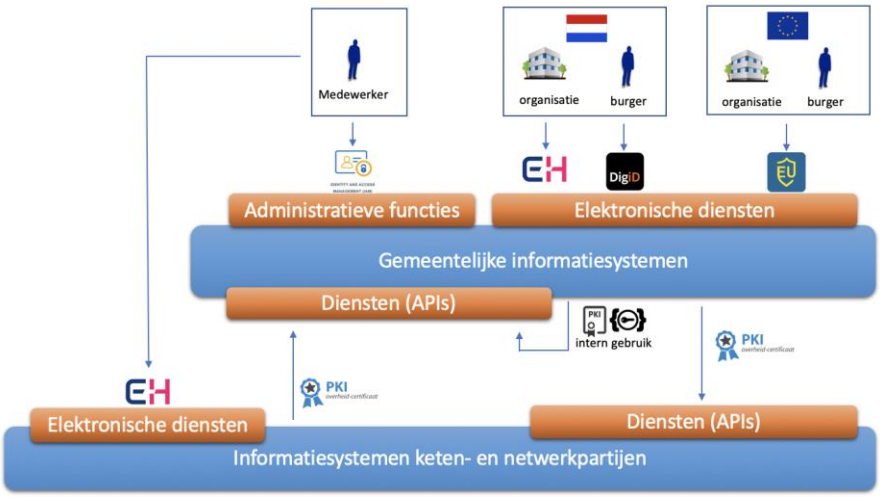
Toegang verlenen - het feitelijk wel of niet toegang verlenen (door de dienstverlener) c.q. verkrijgen (door de gebruiker) tot diensten en voorzieningen, nadat is vastgesteld dat dat wel, respectievelijk niet, mag volgens de bevoegdheden die aan de betreffende digitale identiteit zijn toegekend.

Authenticatiemiddel - Een set van attributen (bijvoorbeeld een certificaat) op grond waarvan authenticatie van een partij kan plaatsvinden.

[7] https://www.noraonline.nl/wiki/Identity_%26_Access_Management_(IAM)

4. Authenticatiemiddelen

Vanuit wet- en regelgeving is bepaald dat elektronische diensten enkel toegankelijk mogen zijn voor personen, organisaties of systemen die op het juiste niveau zijn geauthenticeerd en voor de betreffende dienst zijn geautoriseerd. Onderstaand figuur geeft de authenticatiemiddelen weer die met de huidige stand van zaken[8] voor de verschillende doelgroepen beschikbaar zijn per dienst die geleverd wordt. Hierbij wordt onderscheid gemaakt in diensten aan burgers en bedrijven, interne medewerkers en informatiesystemen.



Figuur 1 - Authenticatiemiddelen per doelgroep

In dit hoofdstuk worden de authenticatiemiddelen beschreven die per doelgroep beschikbaar zijn.

[8] Stand per april 2020

4.1. Burgers en bedrijven

Burgers en bedrijven kunnen via websites van overheidsorganisaties diensten afnemen. Hierbij valt te denken aan elektronische formulieren waarmee diensten of producten aangevraagd kunnen worden en een gemeentelijke persoonlijke internet pagina (PIP). Deze diensten worden in dit document “elektronische diensten” genoemd. Indien deze elektronische diensten een toegangsbeperking kennen (bijvoorbeeld bij verwerking van gesloten data) zal de burger of bedrijf verzocht worden om in te loggen. Hiertoe moeten burgers en bedrijven gebruik maken van een elektronisch identificatiemiddel met een bepaald betrouwbaarheidsniveau. Het vereiste niveau van het authenticatiemiddel hangt af van de aard van de transactie en de gevolgen van die elektronische dienst (zoals financiële of juridische gevolgen). Het authenticatiemiddel wat door een burger of bedrijf wordt gebruikt, moet conform wet- en regelgeving aan sluiten bij het betrouwbaarheidsniveau van de dienst. Bij een dienst die het betrouwbaarheidsniveau '*Substantieel'* heeft, moet dus een authenticatiemiddel gebruikt worden wat ten minst van het niveau Substantieel is. Voorbeelden daarvan zijn DigiD Substantieel en eHerkenning EH3.

In de onderstaande paragrafen is beschreven welke middelen voor de verschillende groepen van burgers en bedrijven beschikbaar zijn op de verschillende betrouwbaarheidsniveaus.

4.1.1. Nederlandse burgers, bedrijven en vertegenwoordigers

In Nederland zijn voor burgers en bedrijven verschillende elektronisch identificatiemiddelen beschikbaar: DigiD voor burgers en eHerkenning voor organisaties en vertegenwoordigers[9].

DigiD - DigiD staat voor Digitale Identiteit. DigiD is een veilig en betrouwbaar authenticatiemiddel wat door de Nederlandse overheid wordt uitgegeven. Burgers kunnen zich met DigiD authenticeren (inloggen) bij overheidsorganisaties, of organisaties met een publieke taak zoals belastingsamenwerkingen, pensioenverzekeraars en zorginstellingen. DigiD is beschikbaar in de betrouwbaarheidsniveau *Basis*, *Midden* en *Substantieel.* Een DigiD-middel op betrouwbaarheidsniveau *Hoog* is in ontwikkeling.

eHerkenning - is een gestandaardiseerd inlogsysteem, waarmee organisaties hun diensten veilig online toegankelijk kunnen maken. eHerkenning regelt de authenticatie en controleert de autorisatie van iemand die online een dienst wil afnemen. Ondernemers en ambtenaren loggen met hun eHerkenningsmiddel, het inlogmiddel, in op een online diensten van een aangesloten organisatie en kunnen zo online hun zaken regelen. eHerkenning is één van de voorzieningen die samen de generieke digitale infrastructuur voor de e-overheid vormen. eHerkenning valt onder het Afsprakenstelsel elektronische toegangsdiensten (ETD-stelsel), welke op haar beurt onderdeel is van het eID-stelsel. eHerkenningsmiddelen worden op verschillende betrouwbaarheidsniveaus uitgegeven. Deze niveaus zijn *EH1*, *EH2*, *EH2+, EH3* en *EH4*.

[9] In de toekomst zullen ook één of meerdere private middelen die voldoen aan de eisen die de overheid aan authenticatiemiddelen stelt worden toegelaten.

De overheid heeft het voornemen om naast DigiD en eHerkenning in de toekomst ook private middelen toe te staan als authenticatiemiddel. Hiervoor zal een verwervingsstrategie worden opgestart door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

In onderstaande tabel is weergegeven hoe de betrouwbaarheidsniveaus van de DigiD en eHerkenningsmiddelen zich verhouden tot de eIDAS betrouwbaarheidsniveaus.

Tabel 1 – eIDAS betrouwbaarheidsniveaus authenticatiemiddelen

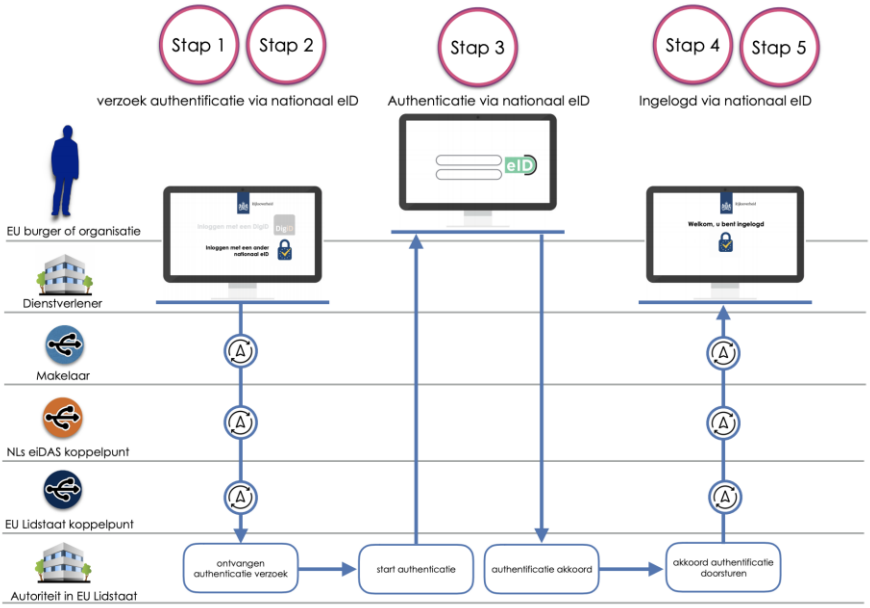
eIDAS	DigiD	eHerkenning[10]
Laag	DigiD Laag, DigiD Midden	EH1, EH2, EH2+[11]
Substantieel	DigiD Substantieel	EH3
Hoog	DigiD Hoog	EH4

Na authenticatie van een burger via een DigiD-middel ontvangt de dienstverlener het BSN van de burger. Bij het gebruik van eHerkenning ontvangt de dienstverlener een pseudoniem en optioneel een aantal overige attributen.

4.1.2. Europese burgers en bedrijven

Europese burgers kunnen voor het afnemen van elektronische diensten waarvoor het betrouwbaarheidsniveau ‘substantieel’ of ‘hoog’ vereist is conform de eIDAS verordening gebruik maken van hun erkende nationale authenticatiemiddel. Onderstaand schema schetst hoe een aanmelding met een dergelijk middel bij een organisatie verloopt.

[10] Zie ook https://afsprakenstelsel.etoegang.nl/display/as/Normenkader+betrouwbaarheidsniveaus
[11] Met de invoering van de Wet DO is de minimale vereiste aan inloggen tweefactor authenticatie. Hierdoor is EH1 niet meer toegestaan en wordt EH2 mogelijk uitgefaseerd uit de categorie eIDAS laag.



Figuur 2 - Authenticatie via een eIDAS-middel

In bovenstaand schema worden de volgende stappen doorlopen:

1. EU-burger of organisatie kiest een dienst en wordt vanuit de aanmelding voor de dienst doorverwezen naar een aanmeldportaal.
2. EU-burger of organisatie kiest de eigen nationale eID uit het keuzemenu.
3. Achter de schermen wordt (via de Nederlandse makelaar en het knooppunt) een identiteitscontrole gedaan op het eigen eID-systeem.
4. Na een positieve identificatie en authenticatie krijgt de EU-burger / organisatie toegang tot het portaal.
5. EU-burger of organisatie kan een of meer diensten afnemen (optioneel).

Elke EU-burger krijgt van het land waar hij woont een pseudoniem op basis van zijn identiteit toegewezen. De eIDAS berichtenservice ontvangt dit pseudoniem. Zodra een bezoeker een dienst afneemt waarvoor BSN vereist is, koppelt de RvIG (Rijksdienst voor Identiteitsgegevens) dit pseudoniem aan het BSN. Hierdoor ontstaat een pseudoniem binnen het Register voor Niet Ingezetenen (RNI) waarmee de persoon altijd juist geïdentificeerd kan worden. Na authenticatie van een burger via een eIDAS-middel ontvangt de gemeente de versleutelde identiteit. Gemeenten kunnen deze versleutelde identiteit decoderen naar een BSN. Mocht de Europese burger geen BSN hebben en de elektronische dienst vereist geen BSN dan ontvangt de gemeente een Persistent Pseudoniem. Dit Persistent Pseudoniem zal voor de burger die met een eIDAS-middel aanmeldt bij elke dienstverleningsvraag met dat middel gelijk zijn. Als de burger een ander eIDAS-middel krijgt, bijvoorbeeld een nieuw rijbewijs, dan krijgt de burger ook een nieuw Persistent Pseudoniem wat niet te herleiden of koppelen is naar voorgaande Persistente Pseudoniemen van die burger.

4.2. Gemeentelijke medewerkers

Medewerkers van de gemeente maken zowel gebruik van diensten die binnen de gemeente worden geboden als van diensten die door keten- en netwerkpartijen worden aangeboden. Onderstaande paragrafen beschrijven de wijze van afhandeling van authenticatie en autorisatie van de medewerkers voor deze diensten.

4.2.1. Afnemer van interne eindgebruikersdiensten

Interne eindgebruikersdiensten van de gemeente zijn administratieve diensten die door informatiesystemen worden geboden. Voorbeelden hiervan zijn functies van het Burgerzaken- of HR-systeem van de gemeente. Om deze diensten te kunnen gebruiken moeten medewerkers zich authenticeren (wie ben ik) en moeten medewerkers ook zijn geautoriseerd (wat mag ik). Het inrichten van een manier waarop medewerkers zich kunnen authenticeren, bijvoorbeeld via een gebruiksnaam en wachtwoord combinatie of een smartcard en het toekennen van autorisaties aan medewerkers is de verantwoordelijkheid van de gemeente.

Voor de authenticatie van medewerkers wordt door organisaties veelal een Identity en Access Management (IAM) systeem gebruikt voor het inrichten en uitvoeren van de processen die zich focussen op het administreren en beheren van gebruikers (in-, door- en uitstroomprocessen) en resources in het netwerk. Deze systemen kunnen zowel gebruikers authenticeren als de toegangscontrole van de gebruikers op applicaties en systemen (de autorisatie) regelen. Veelal gebeurt dit op basis van bedrijfsregels, waardoor rechten worden toegekend op basis van de functie en rol. Vaak wordt het HR-systeem als bronsysteem voor gebruikers gebruikt, maar dit kan ook bijvoorbeeld een Active Directory systeem zijn.

Het gebruik van een IAM-systeem heeft als voordeel dat binnen de gemeente rollen, gebruikersaccounts en hun rechten centraal beheerd worden. Hierdoor wordt het eenvoudiger om bijvoorbeeld aan de eisen op het gebied van de inrichting van de toegang van gebruikers tot informatie en informatie verwerkende faciliteiten uit de BIO te implementeren. De informatiesystemen van de gemeente moeten echter wel de mogelijkheid bieden om aan te sluiten op een dergelijk IAM-systeem.

4.2.2. Afnemer van externe elektronische (web)diensten

Gemeentelijke medewerkers kunnen voor de uitvoering van hun taak gebruik maken van elektronische (web)diensten van andere organisaties. Op het moment dat een gemeentelijke medewerker een dergelijke dienst van een andere organisatie wil gebruiken, bijvoorbeeld een inzage portaal van een keten- of netwerkpartij, is de afspraak binnen de overheid dat deze medewerker daarvoor een eHerkenningsmiddel[12] gebruikt. Het betrouwbaarheidsniveau van het eHerkenningsmiddel dat gebruikt wordt voor het afnemen van de dienst is afhankelijk van het betrouwbaarheidsniveau wat door de dienstverlener aan de dienst is toegekend[13].

4.3. Informatiesystemen

Gemeentelijke informatiesystemen kunnen diensten aanbieden aan andere systemen of organisaties en kunnen diensten gebruiken van andere informatiesystemen of organisaties. Bij het gebruik en aanbieden van

[12] https://www.eherkenning.nl/
[13] Zie paragraaf 4.1.1

deze diensten moet worden geborgd dat alleen geauthenticeerde en geautoriseerde systemen en organisaties gebruik kunnen maken van de diensten. Het niveau van maatregelen wat ter bescherming van de diensten door de aanbieder van de diensten wordt genomen is afhankelijk van de wettelijke eisen aan de dienst, de gevoeligheid van de gegevens die worden verwerkt en de potentiele schade die optreedt bij misbruik van de dienst. De maatregelen kunnen bijvoorbeeld invloed hebben op het niveau van de beveiliging van de uitwisseling van gegevens (eenzijdig of tweezijdig TLS) en het vereiste betrouwbaarheidsniveau van het authenticatiemiddel.

4.3.1. Gebruik van certificaten voor authenticatie

De manier waarop het transport van gegevens wordt beveiligd is via encryptie met digitale certificaten. Digitale certificaten zijn gebonden aan één organisatie, worden uitgegeven aan apparaten of servers, of groepen individuen en worden gebruikt om de communicatie te beveiligen tussen elektronische overheidsapplicaties en diensten. Afhankelijk van het feit of er open- of gesloten gegevens worden verwerkt, wordt gebruik gemaakt van alleen een certificaat van de aanbieder (een-weg TLS) of ook een certificaat van de afnemer van de dienst (tweeweg TLS).

4.3.2. Eenzijdig versus tweezijdig TLS

Open gegevens kunnen uiteraard ook worden uitgewisseld over een tweezijdige TLS-verbinding maar gezien de gevoeligheid van de gegevens is dat niet noodzakelijk. Het opzetten van een tweezijdige TLS-verbinding is technisch ingewikkelder dan het opzetten van een enkelzijdige TLS-verbinding. Toepassing van tweezijdig TLS bij open gegevens diensten zou ertoe kunnen leiden dat partijen door de technische complexiteit afzien van het gebruik van de open gegevens.

4.3.3. Gebruik van systeem-, proces en gemaksdiensten over organisatiegrenzen heen

Binnen de overheid, en de Baseline Informatiebeveiliging Overheid (BIO), geldt de afspraak dat gebruik wordt gemaakt van PKIoverheid-certificaten bij het transport van gesloten gegevens. Het PKIoverheid-certificaat is een computerbestand dat fungeert als een digitaal paspoort. Er zijn twee soorten PKIoverheid-certificaten. Een PKIoverheid persoonsgebonden certificaat wat gebruikt wordt om een bepaalde persoon de mogelijkheid te geven elektronische (internet-)transacties te beveiligen. De andere soort is een PKIoverheid-servicescertificaat[14] wat is gebonden aan een organisatie en wordt uitgegeven aan apparaten of servers, of groepen individuen. Het PKIoverheid-servicescertificaat wordt gebruikt om de communicatie te beveiligen tussen dienstenaanbieders en dienstenafnemers.

Het gebruik van PKIoverheid-servicescertificaten door zowel de aanbieder- als de afnemer van een dienst is verplicht indien:

- Een gemeente een dienst aan externe partijen biedt die gesloten gegevens verwerkt, of
- Een gemeente gebruik maakt van een dienst van andere overheidsorganisaties of organisaties met een publieke taak die gesloten gegevens verwerkt.

Het vertrouwensniveau van PKIoverheid-servicescertificaat komt overeen met eIDAS niveau *Hoog.* PKIoverheid-servicescertificaat zijn daarmee geschikt voor alle diensten van eIDAS betrouwbaarheidsniveaus *Geen*, *Laag*, *Substantieel* en *Hoog*.

4.3.4. Gebruik van systeem-, proces en gemaksdiensten binnen de organisatie

Diensten die binnen de organisatie worden afgenomen dienen te borgen dat deze enkel kunnen worden aangeroepen door geauthenticeerde en geautoriseerde systemen en gebruikers. Voor het authenticeren van systemen kunnen verschillende methoden worden toegepast. Er kan bijvoorbeeld gebruik worden gemaakt van PKIoverheid-servicescertificaten of API-sleutels[15].

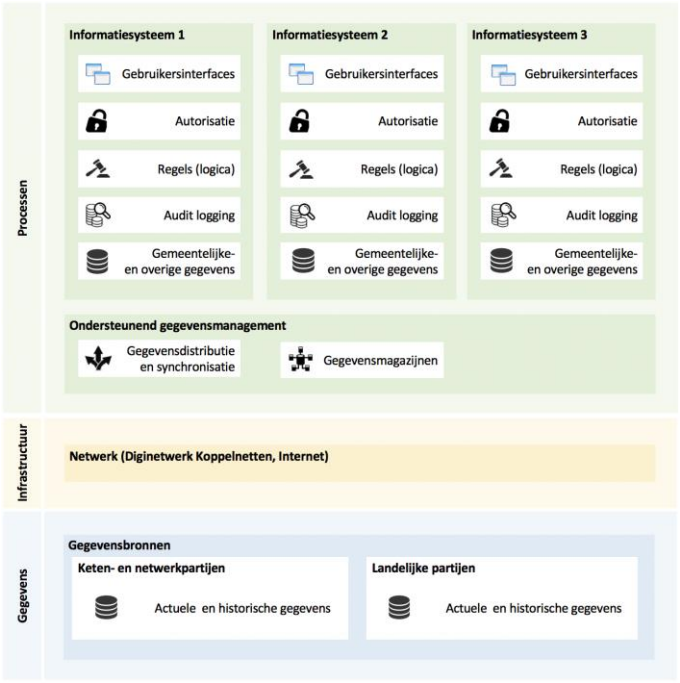
[14] https://www.logius.nl/diensten/pkioverheid
[15] https://en.wikipedia.org/wiki/Application_programming_interface_key

5. Inrichting

5.1. Huidige inrichting authenticatie en autorisatie

Gemeenten maken voor de uitvoering van hun taken gebruik van een groot aantal gegevensverwerkende informatiesystemen. Deze informatiesystemen zijn veelal gericht op de ondersteuning van een specifiek gemeentelijk domein. Voorbeelden van dergelijke domeinen zijn sociale zaken, belastingen en burgerzaken. Daarnaast wordt door gemeenten gebruik gemaakt van informatiesystemen die een meer generieke taak hebben. Voorbeelden hiervan zijn documentsystemen en gegevensmagazijnen. Al deze informatiesystemen worden zowel qua functionaliteit als gebruikte gegevens door leveranciers afgebakend. Daar waar mogelijk wordt door leveranciers gebruik gemaakt van nationale- en internationale standaarden, bijvoorbeeld op het gebied van gegevensmodellering (denk aan het Suwi-Gegevensregister[16] en INSPIRE[17]). De informatiesystemen bieden zelfstandig gebruikersinterfaces, autorisatie, bedrijfsregels, audit logging en gegevensopslag.

[16] https://www.bkwi.nl/producten/suwinet-services/suwinet-standaarden/suwi-gegevensregister-sgr
[17] https://www.geonovum.nl/onderwerpen/inspire



Figuur 3 - Gemeentelijke informatiesilo's

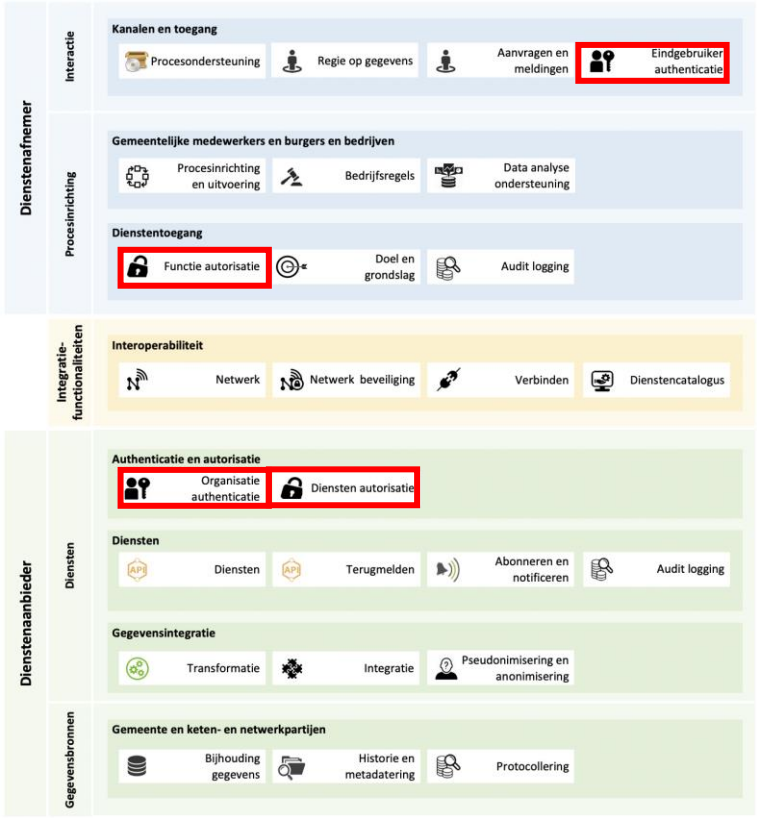
De wijze waarop informatiesystemen omgaan met authenticatie van eindgebruikers wisselt. Sommige informatiesystemen sluiten hiervoor aan bij IAM-systemen en andere, veelal oudere, informatiesystemen maken gebruik van een eigen systeem voor authenticatie en autorisatie. Toegang tot administratieve functies van informatiesystemen wordt over het algemeen verleend via een op autorisatierollen gebaseerde methodiek (RBAC). Eindgebruikers worden hetzij in een IAM-systeem hetzij in het informatiesysteem zelf gekoppeld aan rollen en de rollen worden geautoriseerd voor bepaalde administratieve functies. In de praktijk worden eindgebruikers binnen de infrastructuur van de gemeente geautoriseerd voor het mogen gebruiken van een informatiesysteem waarna de verdere identificatie, authenticatie en autorisatie door het informatiesysteem zelf wordt afgehandeld. Dit betekent dus dat er op vele plaatsen aan authenticatie en autorisatie wordt gedaan.

Nadeel van de RBAC-methode is dat bij meestal rollen ontworpen worden vanuit functies en autorisaties. Autorisaties worden daardoor meestal gekoppeld aan de functies van personen. Beveiligingseisen zijn echter niet alleen afhankelijk van functies van medewerkers. Sommige taken mogen bijvoorbeeld niet op bepaalde systemen worden uitgevoerd, omdat ze op minder veilige plaatsen staan. Denk daarbij aan balie PC's en thuiswerkplekken, maar ook aan meer en minder beveiligde zones en panden. Daarnaast is het zo dat door het gebruik van rollen medewerkers vaak te ruim worden geautoriseerd. Rollen worden immers meestal gedefinieerd op basis van de rechten die een groep van medewerkers nodig heeft. Alle medewerkers krijgt daardoor alle rechten die een andere medewerker nodig heeft. Het is bijna onvermijdelijk dat medewerkers meer rechten krijgen dan waar ze op basis van hun taak recht op hebben. Daarnaast worden binnen organisaties functiewijzigingsprocessen niet goed uitgevoerd. Hierdoor ontstaat ook de situatie dat er medewerkers zijn die voor te veel systemen zijn geautoriseerd. Binnen die systemen zijn de medewerkers voor te veel functies geautoriseerd omdat alleen rechten worden toegevoegd en bijna nooit worden afgenomen. Strikt gezien verhoogt dit de kans op ongeautoriseerde verwerking en kan dus een datalek ontstaan.

Voor gemeenten die informatiesystemen van (veel) verschillende leveranciers gebruiken die elk op hun eigen manier autorisatie, en in sommige gevallen ook authenticatie vormgeven is het een complexe uitdaging om toegangsrechten en identiteiten te beheren.

5.2. Toekomstige inrichting authenticatie en autorisatie

Onderstaand figuur geeft het architectuurmodel van het GEMMA Gegevenslandschap[18] weer. Uitgangspunten in dit model zijn dat processen en gebruikersinterfaces gescheiden zijn van de gegevens die gebruikt worden en autorisatie van (eind)gebruikers zowel plaatsvindt op de processen- en interactielaag als op de gegevenslaag.



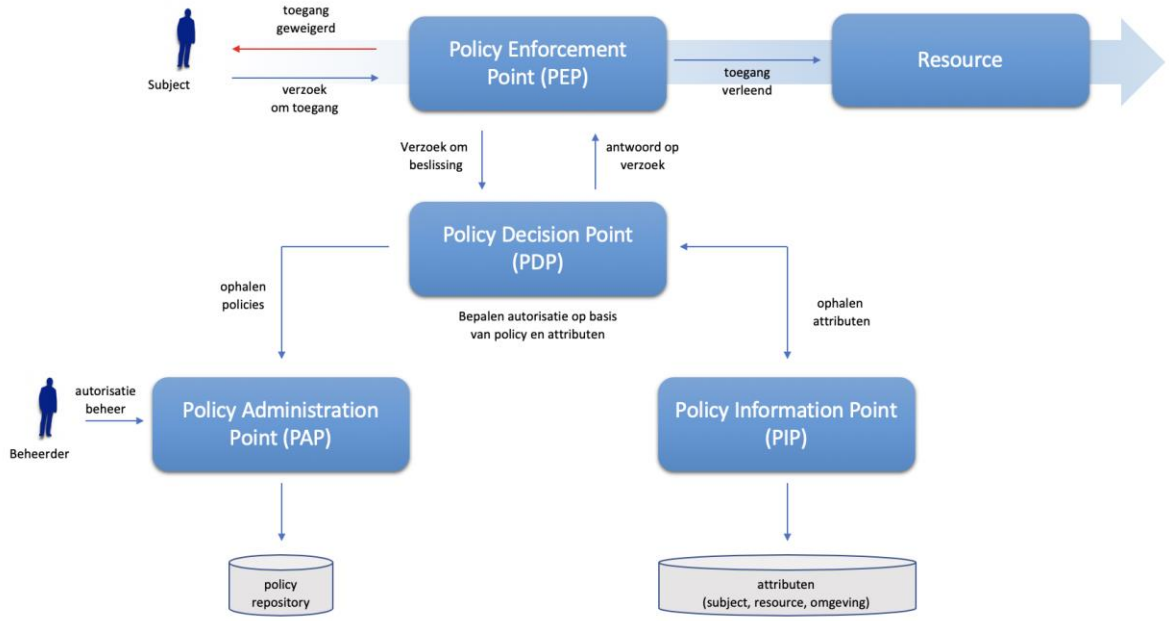
Figuur 4 - GEMMA Gegevenslandschap

Voor de authenticatie van externe eindgebruikers wordt gebruik gemaakt van de in hoofdstuk 4 beschreven authenticatiemiddelen. Dit houdt in dat voor Nederlandse- en EU-burgers en bedrijven op dit moment gebruik gemaakt kan worden van DigiD, eHerkenning en eIDAS-middelen als IdP. Voor interne medewerkers wordt gebruik gemaakt van een IAM-systeem waarbij identiteiten en autorisaties van medewerkers centraal worden beheerd. Er is dus geen sprake meer van de vastlegging van specifieke identiteiten en autorisaties per gemeentelijk informatiesysteem.

[18] https://www.gemmaonline.nl/index.php/Gegevenslandschap

In het GEMMA Gegevenslandschap wordt voor autorisatie voor het applicatiefuncties en de afname van diensten bij voorkeur gebruik gemaakt van autorisatie op basis van attributen (ABAC). De reden hiervoor is dat deze autorisatiemethode ruimte biedt voor het invullen van lokale wensen en invulling kan geven aan de eisen die vanuit de privacywetgeving aan autorisatie worden gesteld. Bij deze methode van autoriseren worden toegangsrechten geassocieerd met een set van regels, die zijn uitgedrukt in meetbare parameters of attributen; vervolgens worden die toegekend aan subjecten die kunnen bewijzen dat zij voldoen aan de regels. ABAC geeft dus toegang tot IT-diensten op basis van een bewering over de eigenschappen (attributen) van de dienstaanvrager (subject). De attributen kunnen allerlei formaten of gedaantes hebben: groepen, rollen, clearance levels, context etc. ABAC past in een omgeving, waar de eigenaar van het object de identiteit van het subject niet exact kent, zoals het internet of een gefedereerde omgeving. Bepaalde kenmerken worden gebruikt om te bepalen of iemand toegang krijgt zonder de identiteit eerst vast te stellen. Die kenmerken kunnen geborgd zijn in certificaten of tokens die zijn uitgegeven door een derde partij.

Voor het inrichten van de toegang tot informatie en systemen via ABAC kan gebruik worden gemaakt van eXtensible Access Control Markup Language (XACML)[19] model. Het gebruik van het XACML-model geeft een grote mate van flexibiliteit ten aanzien van het inregelen en beheren van gebruikersidentiteiten en toegangsrechten.



Figuur 5 - XACML-model

In bovenstaand model verzoekt een subject toegang tot een bepaalde bron, bijvoorbeeld een functie van een toepassing. Het policy Enforcement Point (PEP) ontvangt het toegangsverzoek van de gebruiker en doet een

[19] https://en.wikipedia.org/wiki/XACML

beslissingsverzoek aan de Policy Decision Point (PDP) om het toegangsbesluit te verkrijgen (d.w.z. toegang tot de bron is goedgekeurd of afgewezen) en handelt naar aanleiding van de ontvangen beslissing. Het PDP beoordeelt het toegangsverzoek op basis van vigerend autorisatiebeleid (policies) en de attributen van het subject alvorens een toegangsbesluiten te nemen. De geldende policies worden door het Policy Administration Point (PAP) aan het PDP geleverd. De attributen die van belang zijn voor het toegangsbesluit worden door het PDP opgehaald via het Policy Information Point (PIP). Het PDP komt tot een toegangsbesluit door de ontvangen policy en attributen met elkaar te combineren. Deze afweging kan leiden tot een besluit om toegang toe te staan of te verbieden.

5.2.1. Waarom de keuze voor ABAC

In veel access control systemen wordt toegang bepaald op basis van de identiteit van het subject dat een actie wil uitvoeren op een object. Toegang wordt lokaal bepaald en toegekend op basis van identiteit en/of rollen waar het subject lid van is. Rol-gebaseerde toegangverlening (RBAC) is hier een voorbeeld van. Op termijn is deze vorm van toegangsverlening lastig te beheersen, helemaal als de gebruikers geen deel uitmaken van de organisatie zelf. In dat geval moet er op de een of andere manier de identiteit van de gebruiker ook bekend zijn bij de bronhouder van de objecten en er moet een toegangslijst van worden bijgehouden.

Daarnaast zijn de subject eigenschappen zoals naam en rol niet voldoende om te bepalen wat mag en niet mag als het systeem organisatie overstijgend gebruikt wordt. RBAC neemt een besluit op rol van het subject en is niet makkelijk in staat om met andere parameters om te gaan. Denk bij deze parameters aan organisatie, locatie, soort verwerking die het subject mag uitvoeren etc. RBAC is statisch en gebaseerd op plaats in de organisatie terwijl eigenlijk een meer dynamische vorm van toegangsverlening nodig is.

Het is dus nodig om te zoeken naar een methode om toegang te verlenen zonder dat de object eigenaar kennis heeft van de subjects / gebruikers. Door gebruik te gaan maken van subject en object attributen die consistent binnen en over organisaties heen worden gebruikt is het niet nodig om expliciet toegang te verlenen op basis van gebruikersidentificatie of rol gegevens. ABAC maakt het mogelijk om flexibel om te gaan met autorisaties in grote en meerdere organisaties waar het bijhouden van access control lijsten (ACL) en rollen en groepen over organisaties heen een steeds grotere uitdaging wordt. Met ABAC hoeft men geen autorisaties direct toe te kennen aan een persoon of rol. Door gebruik te maken van de juiste en afgesproken attributen die gelden voor zowel subjecten als objecten kan authenticatie en autorisatie worden beheerd en uitgevoerd in dezelfde of verschillende infrastructuren, zelfs over organisaties heen en blijft beveiligde en gecontroleerde toegang gewaarborgd.

5.2.2. ABAC voor de gemeenten

Gemeenten hebben meestal al een vorm van identiteit- en rechtenbeheer waarbij subject attributen worden gebruikt zoals : Naam, personeelsnummer, rol, specifieke rechten en dergelijke. Gemeenten kunnen ook al beleid hebben aangaande toegang tot gemeentelijke bronnen en informatiesystemen. Bijvoorbeeld of bepaalde functionaliteit alleen vanuit een locatie van de gemeente mag worden gebruikt of ook vanuit een thuiswerkplek. Deze beschrijving van identiteiten en rechten zijn vaak niet goed opgeschreven in een vorm van policies die voor ABAC geschikt zijn en machine leesbaar zijn voor toegangsbeheersing mechanismes. Het consistent vastleggen van autorisaties en rechten die geconsumeerd kunnen worden door ABAC toegangsbeheersingsmechanismen binnen de organisatie en over organisaties heen is een uitdaging waarvoor attribuut management noodzakelijk is. Dit geldt ook voor object attributen die doormiddel van een object attribuut management functie moeten worden beheerst. Pas als subject eigenschappen en object eigenschappen goed zijn vastgelegd in een machine leesbaar formaat kan ABAC worden ingevoerd.

6. Eisen aan dienstenafnemers en -aanbieders

6.1. Dienstenafnemers

Dienstenafnemers nemen, zoals de naam het al zegt, diensten af van dienstenaanbieders. Een dienstenaanbieder heeft de verplichting om een aantal processen op het gebied van identiteiten en autorisaties in te regelen waarmee geborgd wordt dat diensten enkel afgenomen kunnen worden door geautoriseerde personen.

- Interne medewerkers
    - Beheer van identiteiten (instroom, doorstroom, uitstroom)
    - Beheren van autorisaties van medewerkers
    - Beheer van toegangsmiddelen en persoonsgebonden certificaten
    - Beheer van IT-accounts

- Externe gebruikers
    - Authenticatie van gebruiker op correcte niveau voor de dienst

- Transparantie
    - Logging van authenticatieverzoeken
    - Logging van verwerkingen

6.2. Dienstenaanbieder

Organisaties die diensten aanbieden moeten een aantal zaken regelen ten aanzien van het aanbieden van diensten en de afname daarvan door dienstenafnemers.

- Vaststellen van betrouwbaarheidsniveau van diensten;
- Authenticeren van dienstenafnemers met een middel van een niveau wat past bij het betrouwbaarheidsniveau van de dienst;
- Beheren van autorisaties van dienstenafnemers;
- Bieden van transparantie over het gebruik van diensten;
- Vaststellen beleidsregels voor toegang tot de diensten.

De dienstaanbieder bepaalt de policy waartegen attributen worden gehouden om te bepalen of een subject iets mag met een object. De dienstaanbieder hoeft het subject niet te kennen, hij hoeft alleen de policy te definiëren op basis waarvan toegang verleend wordt.

6.2.1. Vaststellen van betrouwbaarheidsniveaus van diensten

Diensten die door een dienstenaanbieder worden aangeboden moeten conform de eIDAS-verordening en de Wet Digitale Overheid (WDO) enkel toegankelijk zijn voor afnemers die op een niveau geauthenticeerd zijn wat past bij het betrouwbaarheidsniveau van de aangeroepen dienst. Dienstenaanbieders zijn daarom verantwoordelijk voor het:

- Vaststellen van het betrouwbaarheidsniveau van een dienst;
- Borgen dat gehanteerde authenticatiemiddelen passend zijn bij het betrouwbaarheidsniveau van de dienst.

Hiervoor is door het Forum Standaardisatie de handreiking "*Betrouwbaarheidsniveaus voor digitale dienstverlening*"[20] opgesteld. Deze handreiking helpt organisaties bij het maken van een heldere en transparante afweging ten aanzien van het betrouwbaarheidsniveau van een digitale dienst. De handreiking doet dit op basis van de eIDAS-verordening voor digitale identificatie- en vertrouwensdiensten, die van kracht is sinds 1 juli 2016. Daarnaast worden de bijbehorende uitvoeringsbesluiten en de nationale wet- en regelgeving meegenomen. Door het vaststellen van een betrouwbaarheidsniveau van een dienst wordt het minimale niveau van het voor de dienst vereist authenticatiemiddel vastgesteld.

6.2.2. Authenticeren van dienstenafnemers

Dienstafnemers (subjects) worden geauthentiseerd op basis van door de dienstenaanbieder te definiëren attributen.

6.2.3. Beheren van autorisaties van dienstenafnemers

Van de diensten die ter beschikking worden gesteld moet van tevoren bepaald worden welke attributen de dienstafnemer moet hebben om de dienst te kunnen gebruiken. Dit vereist dat er binnen de gemeente een attribuut administrator is maar ook dat er voor alle gemeenten vergelijkbare attributen worden afgesproken om op die manier eenduidigheid te krijgen in het beschrijven van attributen van de bron en de afnemer. De autorisatie attributen moeten dan binnen de gemeente worden omgezet in policies (beleidsregels) die beschrijven wat op basis van deze attributen wel of niet is toegestaan

Naast het autoriseren op het niveau van een dienst is het soms ook gewenst om te autoriseren op het niveau van attributen. Het is bijvoorbeeld mogelijk dat een dienst tien attributen kan retourneren maar de eindgebruiker maar voor vijf van die attributen geautoriseerd is. De gegevens die door de dienst worden geretourneerd moeten zich in dat geval, mede vanuit doelbindingseisen vanuit de AVG, beperken tot de attributen waarvoor de eindgebruiker geautoriseerd is.

[20] https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus

7. Begrippen

Access Management (AM) - Het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om de toegang tot en het gebruik van objecten (systemen en informatie) te faciliteren, te beheren en te controleren.

Access Control Mechanisme (ACM) - Binnen ABAC wordt het object beschermd door ACM. Bij een verzoek tot toegang verzameld ACM de attributen en beoordeeld de beleidsregels waarna toegang al of niet verleend wordt.

Authenticatie - De controle (het staven) van de (een) geclaimde identiteit van een partij en de set van zijn geclaimde attributen op een bepaald betrouwbaarheidsniveau[21] (wie ben je).

Autorisatie - 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[22] (wat mag je doen).

Environment of omgeving - is de beschrijving van de context waaronder toegang mogelijk is, hierbij kun je denken aan: locatie van het subject of user, datum en tijd, netwerk gegevens, apparaat gegevens etc. De omgeving is niet puur gerelateerd aan het subject of object het is gerelateerd aan de policy (toegangsbeleid).

Identificatie - Het kenbaar maken van de identiteit van een subject (een gebruiker of een proces). De identiteit wordt gebruikt om de toegang van het subject tot een object te beheersen (autorisatie). Vanuit de optiek van informatiebeveiliging is identificatie van een subject de eerste stap in het autorisatieproces. De tweede stap is de authenticatie, het vaststellen van de juistheid van de opgegeven identiteit. De derde stap in dit proces is autorisatie, het vaststellen of het subject toegang tot het object mag verkrijgen.

Identity Management (IdM) - Het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om de identificatie en authenticatie van subjecten te faciliteren, te beheren en te controleren.

Object - Het object is een bron die beveiligd wordt door ABAC, dit kunnen bestanden, tabellen, programma's en bijvoorbeeld apparaten zijn. Objecten zijn dingen die door subjecten kunnen worden gebruikt en waarvoor

[21] Analoog aan "Forum Standaardisatie, Verkenning Authenticatie, KPMG R.2007.ISC.18 (2007)" en "PKIoverheid, Programma van Eisen deel 4: Definities en Afkortingen, versie 2.1, 11 januari 2010"
[22] Analoog aan Modinis / PKI overheid begrippenlijst (2005) waarbij autorisatie overeenkomt met betekenis 1 en toegang verlenen met betekenis 2 / Van Dale Groot woordenboek van de Nederlandse taal 14, maar specifiek gemaakt voor de context van Elektronische Toegangsdiensten.

toegangsregels gemaakt kunnen worden. Net zoals subjecten hebben objecten ook attributen zoals: eigenaar, datum, toegangsattributen enz.

Policy Administration Point (PAP) - Administreert beleidsregels zoals wachtwoord policy, de authenticatiemethode voor toegang tot specifieke objecten (resources), een kenmerk die een subject (gebruiker) moet hebben voor autorisatie tot een object etc.

Policy Decision Point (PDP) - Neemt real-time besluiten op basis van resource-, identiteit- en policy-informatie. De PDP maakt daarbij gebruik van de Identity Repository (PIP) en de Policy Repository.

Policy Enforcement Point (PEP) - Dwingt real-time in de infrastructuur af dat de juiste policy wordt nageleefd. Dat kan betekenen dat voor een bepaalde URL de gebruiker zich moet authenticeren door middel van één of twee factor authenticatie (Wachtwoord of Token met PIN etc.)

Policy Information Point (PIP) - Bevat alle identiteitsinformatie voor toegang tot IT-systemen zowel persoonsgebonden als functioneel. Vanuit verschillende directories vindt provisioning plaats naar het PIP, dat vervolgens relevante account- en persoonsinformatie real-time kan doorgeven aan authenticatieservices, zoals Kerberos.

Subject - Binnen ABAC is het subject en persoon of systeem dat gebruik wil maken van een dienst / product. De identiteit van het subject wordt bepaald door attributen, bijvoorbeeld: naam, alias, organisatie, afdeling, functie, locatie etc. In een ABAC omgeving is het subject doorgaans een gebruiker.

Bijlage 1: Bronnen

- Handleiding eIDAS, Inzicht in de gehele keten voor het inrichten van grensoverschrijdende dienstverlening, VNG Realisatie, 25 oktober 2018
  https://www.vngrealisatie.nl/sites/default/files/2018-11/Handleiding_eIDAS1.01.pdf

- Afsprakenstelsel elektronische toegangsdiensten, 19 april 2019
  https://afsprakenstelsel.etoegang.nl/

- Betrouwbaarheidsniveaus voor digitale dienstverlening versie 4.0, Forum Standaardisatie, april 2017
  https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus

- eIDAS verordening Nr. 910/2014 van het Europees parlement en de Raad, 23 juli 2014
  https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32014R0910&from=NL

- Identity & Access Management (IAM), Nederlandse Overheid Referentie Architectuur (NORA)
  https://www.noraonline.nl/wiki/Identity_%26_Access_Management_(IAM)

- Patronen Informatiebeveiliging, Platform voor Informatiebeveiliging, januari 2013,
  https://www.pvib.nl/kenniscentrum/documenten/patronen-informtiebeveiliging/downloaden

- Digikoppeling Identificatie en authenticatie v1.4, november 2017, Logius
  https://www.logius.nl/sites/default/files/public/bestanden/diensten/DigiKoppeling/Standaarden/Digikoppeling-Identificatie-en-Authenticatie.pdf

- Guide to Attribute Based Access Control (ABAC), National Institute of Standards and Technology (NIST), januari 2014
  https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-162.pdf