



Marktconsultatie

Customer Identity Access Management - Kadaster

ten behoeve van:
Directie DGV

Datum: 9-02-2023
Versie: 1.0

Auteurs : Niek Sombekke, Bart Maessen, Martin Borgman, Erwin Lazet, Rob Müller

Inhoudsopgave

1	ALGEMEEN	3
1.1	AANLEIDING	3
1.2	ACHTERGROND EN DOELSTELLING.....	3
1.3	OPDRACHTGEVER	3
1.3.1	<i>Het Kadaster</i>	<i>3</i>
1.3.2	<i>Unieke positie Kadaster</i>	<i>3</i>
1.4	RANDVOORWAARDEN MARKTCONSULTATIE	4
1.5	LEESWIJZER.....	4
2	DE TE VOLGEN PROCEDURE	5
2.1	ALGEMEEN.....	5
2.2	AANKONDIGING	5
2.3	MARKTCONSULTATIE	5
2.4	AANLEVEREN GEGEVENS MARKTCONSULTATIE	5
2.5	COMMUNICATIE TIJDENS DE MARKTCONSULTATIE	5
2.6	UITERSTE DATUM VOOR AANLEVERING VAN DE BEANTWOORDING	5
2.7	VOORWAARDEN AAN DE BEANTWOORDING	6
2.8	VERTROUWELIJKHEID	6
2.9	PLANNING	6
2.10	VORMVEREISTEN	6
3	VRAGEN AAN DE MARKTPARTIJEN	7
3.1	INLEIDING / CONTEXT	7
3.2	VRAGEN AAN DE MARKTPARTIJEN	10
3.2.1	<i>Algemeen.....</i>	<i>10</i>
3.2.2	<i>Identity management</i>	<i>10</i>
3.2.3	<i>Identity Provider (authenticatiemiddel)</i>	<i>11</i>
3.2.4	<i>Access management, toegangsautorisatie.....</i>	<i>11</i>
3.2.5	<i>Applicatieautorisatie.....</i>	<i>13</i>
3.2.6	<i>Aanpak / transitie</i>	<i>14</i>
3.2.7	<i>Deployment en verdien/financieel model.....</i>	<i>15</i>
3.2.8	<i>Overige vragen</i>	<i>16</i>

1 ALGEMEEN

1.1 Aanleiding

De dienst voor het Kadaster en de openbare registers, hierna te noemen “het Kadaster”, wenst door middel van deze marktconsultatie een duidelijk beeld te krijgen in het marktaanbod van oplossingen en mogelijkheden op het gebied Customer Identity Access Management (CIAM).

1.2 Achtergrond en doelstelling

De bestaande inrichting van CIAM is in 2008 geïntroduceerd en bevat een significant deel aan maatwerk componenten. Kadaster denkt een groot deel van de betreffende functionaliteit als standaard dienst in de markt te kunnen vinden waarbij ook invulling gegeven kan worden aan nieuwe wensen/eisen met betrekking tot autorisatiebeheer (selfservice, machtigen) en standaarden zoals OAuth en OIDC.

Met deze marktconsultatie wordt advies ingewonnen bij meerdere marktpartijen. Het doel van deze marktconsultatie bestaat uit de volgende aspecten:

- bepalen of het Kadaster tot een aanbesteding kan overgaan;
- beste aanbestedingsstrategie kiezen;
- een (modulaire) kostenindicatie verkrijgen als onderbouwing van het vervolgtraject.

De resultaten van de marktconsultatie worden, in voorkomend geval, verwerkt in de aanbestedingsdocumenten, zonder dat deze herleidbaar zijn tot de deelnemers van de marktconsultatie.

1.3 Opdrachtgever

Opdrachtgever is de directie Data Governance en Vernieuwing (DGV) van het Kadaster.

1.3.1 *Het Kadaster*

Het Kadaster verzamelt gegevens over registergoederen in Nederland, houdt deze bij in openbare registers en op kadastrale kaarten en stelt deze gegevens vaak tegen een vergoeding beschikbaar aan particulieren, bedrijven en andere belanghebbenden in de samenleving. Voor nadere informatie over het Kadaster wordt inschrijver verwezen naar de website van het Kadaster www.kadaster.nl.

1.3.2 *Unieke positie Kadaster*

Als het aankomt op vastgoed- en geo-informatie beschikt het Kadaster over een schat aan feiten. De behoefte aan feiten zal in de toekomst niet minder worden. Wat wél verandert, is de manier waarop deze informatie wordt gedistribueerd en gebruikt. En dat betekent dus óók een veranderende rol voor het Kadaster in de maatschappij.

De verspreiding en het gebruik van informatie is met name de afgelopen twintig jaar radicaal veranderd. Het internet maakt data voor iedereen over de hele wereld beschikbaar en de digitale revolutie heeft ervoor gezorgd dat dit gigantische informatienetwerk op elke plaats en op elk tijdstip toegankelijk is. Wil het Kadaster hier effectief op inspelen, dan zal het Kadaster de uitbreiding van ‘verstrekker van data’ naar ‘partner in informatie’ voor de maatschappij moeten versnellen. Betrouwbaar en onafhankelijk, zoals men van het Kadaster gewend is, maar ook proactief en flexibel, zoals de wereld van vandaag én morgen van het Kadaster mag verwachten.

1.4 Randvoorwaarden marktconsultatie

1. Deze marktconsultatie dient uitdrukkelijk niet om een voorselectie te maken van gegadigden in het kader van een eventueel uit te voeren vervolgtraject. Evenmin zullen bij de marktconsultatie betrokken partijen op enige wijze worden uitgesloten van eventuele participatie in een mogelijk vervolgtraject.
2. Marktpartijen komen door deel te nemen aan de marktverkenning niet in een bevooroordeelde of benadeelde positie op het moment van een mogelijk vervolgtraject.
3. Deelnemers aan de marktconsultatie kunnen geen rechten ontleen aan deelname aan de marktconsultatie of aan enige informatie die tijdens de marktconsultatie wordt verstrekt. Marktpartijen kunnen geen rekening sturen of anderszins aanspraak maken op een (geldelijke of andere) vergoeding voor hun bijdrage aan de consultatie.
4. De informatie uit de marktconsultatie wordt gebruikt om een businesscase te vervolmaken en mogelijk om de doelstellingen en eisen aan te scherpen van een mogelijk vervolgtraject.
5. Deelnemende marktpartijen stemmen er mee in dat door hen aangeleverde informatie geanonimiseerd verwerkt kan worden in het eventuele vervolgtraject, zoals bijvoorbeeld een door het Kadaster nader uit te werken programma van eisen;
6. Verstrekte informatie in het kader van de marktconsultatie kan afwijken van in de eventuele aanbestedingsprocedure te verstrekken informatie;
7. De inbreng van deelnemende partijen zal zoveel mogelijk vertrouwelijk behandeld worden, waarbij in ieder geval rekening zal worden gehouden met de gerechtvaardigde (zakelijke) belangen van partijen;
8. Financiële inbreng wordt altijd zeer vertrouwelijk behandeld, niet gedeeld met derden en alleen gebruikt om te budgetteren;
9. Claims over het gebruik van informatie, vertrouwelijkheid, of verzoeken om vergoedingen in verband hiermee worden niet gehonoreerd;
10. De door deelnemende partijen ingezonden documenten worden beschouwd als openbare documenten, vrij van auteursrechten. Indien auteursrechten van toepassing zijn dan wordt het Kadaster hiervan gevrijwaard door de deelnemende partij(en), zie ook paragraaf 2.8;
11. Het Kadaster is op geen enkele wijze gebonden aan de uitkomsten van de marktconsultatie of verplicht tot realisatie en/of aanbesteding van het project waarop de marktconsultatie betrekking heeft;
12. Aan de door u gegeven antwoorden op de gestelde vragen zal door het Kadaster geen waardeoordeel gehangen worden;
13. Het Kadaster behoudt zich het recht voor:
 - a. het voorgenomen aanbestedingsproces qua vorm en inhoud op andere wijze uit te voeren dan het proces dat mogelijk is medegedeeld;
 - b. deze marktconsultatie tijdelijk of definitief te staken.
14. Door deelname aan deze marktconsultatie geven partijen te kennen onvoorwaardelijk akkoord te gaan met de voorwaarden zoals vermeld in dit document.

1.5 Leeswijzer

In hoofdstuk 2 is aangegeven welke procedure gevolgd wordt bij deze marktconsultatie. Hoofdstuk 3 beschrijft de vragen die wij hebben aan de marktpartijen.

2 DE TE VOLGEN PROCEDURE

2.1 Algemeen

De aanvragende dienst is:
Kadaster/Inkoop & contractmanagement

Contactpersoon:
Dhr. N. Stoker (inkoopadviseur IT)
Contact via de berichtenfunctie op TenderNed.

2.2 Aankondiging

Deze marktconsultatie wordt via www.TenderNed.nl gepubliceerd.

2.3 Marktconsultatie

Deze marktconsultatie bestaat uit een vragenlijst die door marktpartijen beantwoord kan worden (hoofdstuk 3).

Indien u vragen heeft over deze marktconsultatie kunt u deze via TenderNed aan ons sturen (zie paragraaf 2.9). Het Kadaster zal deze vragen beantwoorden en geanonimiseerd op TenderNed plaatsen.

Indien er na het indienen van de schriftelijke beantwoording aanvullende vragen zijn, zullen deze worden toegestuurd aan alle partijen die hebben deelgenomen aan de marktconsultatie. Het Kadaster behoudt zich het recht voor een mondelinge toelichting te vragen naar aanleiding van de ingediende beantwoording. Indien dit van toepassing is zal hierover contact met u worden opgenomen.

2.4 Aanleveren gegevens marktconsultatie

Wij verzoeken u de beantwoording in de Nederlandse taal te doen. Tevens verzoeken wij u de vragen kort en bondig te beantwoorden en in uw beantwoording geen gebruik te maken van doorverwijzingen via "link's/ URL's".

2.5 Communicatie tijdens de marktconsultatie

Tijdens de marktconsultatie verloopt alle communicatie met betrekking tot dit onderwerp via de berichtenmodule in TenderNed.

2.6 Uiterste datum voor aanlevering van de beantwoording

Wij verzoeken u de beantwoording uiterlijk, digitaal via TenderNed, aan te leveren volgens de planning zoals vermeld in paragraaf 2.9.

Wijze van aanlevering van de beantwoording
Via berichtenmodule van TenderNed;
Alle documentatie mag als Pdf-bestand worden aangeleverd.

2.7 Voorwaarden aan de beantwoording

Het deelnemen aan de marktconsultatie is voor zowel deelnemers, als het Kadaster vrijblijvend. Partijen (inclusief partijen die niet deelnemen aan de marktconsultatie) kunnen aan deze marktconsultatie geen (wederzijdse) verplichtingen of rechten jegens het Kadaster ontleen.

Voor de beantwoording en de daarvoor uit te voeren werkzaamheden en te verstrekken materialen kunnen aan het Kadaster geen kosten in rekening worden gebracht.

2.8 Vertrouwelijkheid

Conform artikel 5.1, eerste lid, onderdeel c, van de Wet open overheid behandelt het Kadaster alle informatie die in het kader van deze marktconsultatie door marktpartijen wordt verstrekt als vertrouwelijk, tenzij de marktpartij zelf aangeeft dat (een deel van) die informatie openbaar gemaakt kan worden.

2.9 Planning

Activiteit	Datum
Publiceren Marktconsultatie	09-02-2023
Indienen vragen over consultatie door marktpartijen uiterlijk 14.00 uur	23-02-2023
Vragen van marktpartijen beantwoord	02-03-2023
Beantwoording door marktpartijen	09-03-2023

2.10 Vormvereisten

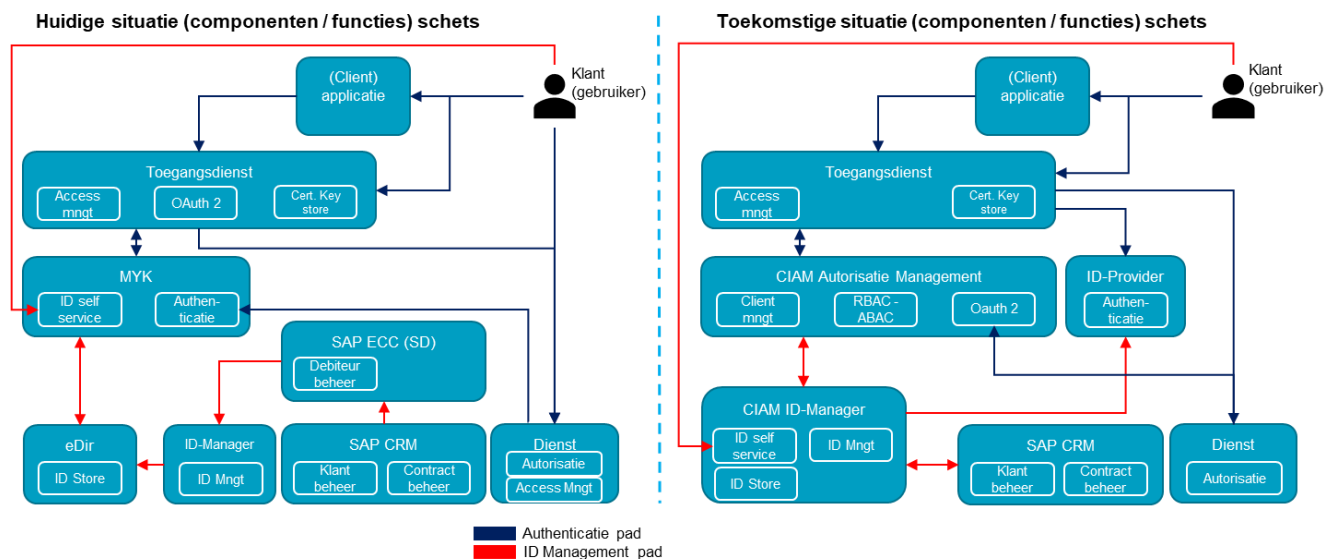
Het is uitdrukkelijk niet de bedoeling offertes in te leveren, wij verzoeken u dringend om u te beperken tot de beantwoording van de gestelde vragen in Hoofdstuk 3.

Beantwoording graag kort en krachtig. Uiteraard bent u niet verplicht tot het verstrekken van antwoorden en u bent eveneens vrij bepaalde vragen over te slaan. De bijdrage aan de marktconsultatie/beantwoording van de vragen ontvangen wij bij voorkeur in MS Word of Excel format, waarbij de volgorde van de vragen aangehouden dient te worden. Aanvullende en overige documentatie mag als pdf-bestand worden aangeleverd. In de begeleidende brief bij de bijdrage aan de marktconsultatie ontvangen wij graag van de contactpersoon aan de kant van de marktpartijen de volgende gegevens; naam, functie, kantooradres, telefoonnummer en e-mailadres.

3 VRAGEN AAN DE MARKTPARTIJEN

3.1 Inleiding / context

De bestaande inrichting van 'CIAM' binnen Kadaster vindt zijn oorsprong in 2008 en kent een aanzienlijk maatwerk deel ('MYK'):



Figuur 1: Globaal logisch applicatiemodel CIAM transitie

MYK is een afkorting van 'Mijn Kadaster' en biedt een centrale landingsplek (portaal) voor geregistreerde en gecontracteerde rechtspersonen. Betreffende klanten kunnen op rekening bestellen. Gelieerde rechten worden eenmalig verstrekt aan de Beheerder Mijn Kadaster (BMK), een gebruiker van een klant. De BMK kan andere gebruikers, werkzaam voor betreffende organisatie, beheren (aanmaken, machtigen, aanpassen en verwijderen).

Mijn Kadaster bevat meerdere componenten waaronder:

- ID self service; gebruikers- en accountbeheer door de klant zelf
- Authenticatie; MYK biedt een ID-Provider functie om gebruikers te authentifieren op basis van gebruikersnaam + wachtwoord.

De 'Toegangsdiens' biedt een primaire functie om de toegangscontrole tot beschermde bronnen van Kadaster af te dwingen (Access mngt), maar biedt in de huidige vorm daarvoor ook ondersteuning voor OAuth 2 en een authenticatievorm op basis van certificaten. In dit document wordt nog verder ingegaan op de rol van de toegangsdiens.



Belangrijkste voorziene veranderingen, CIAM transitie

Een van de doelstellingen van de marktconsultatie is het toetsen van het toekomstbeeld wat Kadaster heeft. Figuur 1 toont de belangrijkste componenten -en hierbinnen de functies- met de veranderingen/uitgangspunten:

- MYK (security) vervalt
- Micro Focus componenten worden vervangen (ID-Mngr en ID Store)
- Introductie centraal Autorisatie Management
- Diensten implementeren OAuth 2
- Toegangsdienst blijft toegang Policy Enforcement Point (PEP)

Klanten en markten (ontwikkeling)

Naast organisaties kent Kadaster ook andere soorten klanten zoals particulieren die afhankelijk van de dienst zich moeten identificeren met bijvoorbeeld DigID en/of direct betalen met iDeal. Hierin speelt MYK dus geen rol.

In de bestaande situatie wordt deze klant niet expliciet geregistreerd, maar alleen gekoppeld aan de transactie. Verschillende ontwikkelingen en wetgeving vereisen van Kadaster wel dat dit type klant ook geregistreerd moet gaan worden, zodat bijvoorbeeld bestellingen gedownload kunnen worden.

Om het gebruik van open producten te kunnen controleren/reguleren is in de toekomst een vrijwillige registratie nodig van natuurlijke (rechts)personen. Zij kunnen interesses opgeven voor actieve berichtgeving n.a.v. ontwikkelingen in de dienstverlening van Kadaster of kunnen API-Client applicaties registreren voor diensten die een authenticatievorm vereisen.

Voor met name zakelijke klanten geldt een expliciete registratie en contractering om op rekening te kunnen bestellen. De markt -of branche- waarbinnen een organisatie actief is, bepaalt ook in belangrijke mate welke producten/diensten van toepassing zijn en waarvoor rechten worden verstrekt op basis van het contract.

Wet Digitale Overheid | WDO

De WDO is nog niet aangenomen, maar vraagt van Kadaster om authenticatiemiddelen te gebruiken van het stelsel elektronische toegangsdiensten voor die diensten waarvan het betrouwbaarheidsniveau geclassificeerd is als substantieel of hoger (niveau 3 van 5). Wanneer de wet ingaat is er geen overgangperiode, dus Kadaster is reeds begonnen met het implementeren van eHerkenning naast het eigen authenticatiemiddel (MYK). Klanten kunnen nu nog kiezen welk middel ze willen gebruiken.

Voor Machine-to-Machine koppelingen wordt gebruik gemaakt van:

1. Mutual-TLS op basis van PKI-Overheid certificaten
2. OAuth 2 Client Credentials flow met (PKI-O) gesigneerd JWT
3. OAuth 2 authorization code grant flow (eHerkenning)

Voor niveau onder substantieel, kan Kadaster zelf het authenticatiemiddel verzorgen. Liefst door gebruik te maken van bestaande ID-P's op basis van federatie.



Autorisatie

Kadaster splitst de autorisatie in twee delen; (1) *toegang* tot producten/diensten en (2) autorisatie *binnen* producten/diensten. Voor de toegangsautorisatie wordt gebruik gemaakt van de zgn. Toegangsdienst waarbij met een gateway een policy enforcement point (PEP) wordt geïmplementeerd voor het gros van de Kadaster diensten. Betreffende diensten “zitten achter de gateway”. De gateway wordt geïnstrueerd op basis van policies waarbij ook de noodzakelijke authenticatie wordt afgedwongen. Nadat authenticatie heeft plaatsgevonden, wordt de digitale identiteit van de gebruiker vastgesteld (deze ligt vast in eDir | Identity store) en betreffende identiteit gepropageerd naar de achterliggende applicaties. Zgn. ‘GAA-token’ bevat feitelijk een kopie van de identiteit inclusief rechten. In de toekomstige situatie is dit onwenselijk en wil Kadaster op basis van OAuth 2 de identiteitsgegevens beperken tot de scope van de doelapplicaties.

“Herinrichten CIAM: de transitie”

In de doel situatie heeft het MYK maatwerk plaatsgemaakt voor (‘best of breed’) CIAM functionaliteit die idealiter als service wordt gebruikt. De Kadaster informatievoorziening is service georiënteerd ingericht met API’s als leidende vorm van ontsluiting. Diensten worden dan ook met een “API First” uitgangspunt beschikbaar gesteld.

In voorgaande uitleg is al gesproken van ontwikkelingen waar Kadaster invulling aan moet gaan geven zoals wetgeving. Kadaster zoekt voor CIAM standaard dienstverlening met minimale inzet van eigen maatwerk. De gateway is nu een centrale on-premise infra component die met de nieuwe multi-cloud policy (SAAS voor PAAS voor IAAS voor on-premise) op een andere manier beslag moet gaan krijgen. Zero trust is hier het basisprincipe.

3.2 Vragen aan de marktpartijen

Kadaster wenst de bestaande CIAM inrichting te vervangen door 'standaard' oplossingen in de markt. Met de marktconsultatie wil Kadaster een beeld krijgen van de aanbieders en hun visie/oplossingen voor CIAM en dan binnen de context van Kadaster in het bijzonder.

Het Kadaster verzoekt u de vragen volgorde te beantwoorden met vermelding van het ID-nummer.

3.2.1 Algemeen

Middels antwoorden op de onderstaande vragen kunt u aangeven hoe uw organisatie aan de gevraagde aspecten inhoud geeft,

ID	Vraag	Toelichting
ALG1	Beschrijf uw oplossing(en) en visie	maximaal 4 pagina's A4
ALG2	Beschrijf uw support- en beheermodel	maximaal 2 pagina's A4
ALG3	Beschrijf uw verdienmodel	maximaal 2 pagina's A4
ALG4	Beschrijf uw implementatie visie en aanpak, en welke rol u hierin voor Kadaster, u en mogelijk uw partners ziet.	maximaal 4 pagina's A4
ALG5	Beschrijf uw visie op privacy/wetgeving, security en kwaliteit	maximaal 2 pagina's A4
ALG6	Beschrijf aandachtspunten en risico's	maximaal 2 pagina's A4

3.2.2 Identity management

Stelling/uitgangspunt Kadaster CIAM: Digitale identiteit

In de basis hanteert Kadaster de regel dat elk subject binnen de informatievoorziening van Kadaster één (unieke) digitale identiteit heeft. Deze digitale identiteit wordt vastgelegd in een Identity Store in een context (organisatie/groep) en bevat identificerende kenmerken en entitlements in de vorm van rollen en attributen.

ID	Vraag	Toelichting
IDM1	Kunt u zich vinden in het uitgangspunt van Kadaster met betrekking tot de digitale identiteit?	Onderbouw s.v.p. uw antwoord
IDM2	Hoe komt het onboarding proces van een klant tot stand?	Welke functionaliteit ziet u hierin als noodzakelijk (visualisatie, operatie/controle, validatie, ..). Geef aan of dit proces binnen scope van de aangeboden oplossing zit en/of dat Kadaster moet denken aan eigen procestooling zoals een BPMS.
IDM3	Welke visie heeft u op het beheer van entitlements? Zie ook paragraaf 3.2.5 over applicatie autorisatie.	Klassieke benaderingen zijn Rol- of Attribuu gebaseerd (RBAC / ABAC). Geef aan welke keuzecriteria er zijn.
IDM4	Wat is in uw visie de bron van een digitale (klant) identiteit?	Welke vormen van onboarding zijn er te onderscheiden en wat is de rol van een contract in deze? In de visie van Kadaster is CRM het 'system of records' van klantdata.
IDM5	Hoe werkt binnen uw oplossing de standaard integration flows richting een CRM systeem (heen en terug)?	Om zo een beeld te krijgen wat de CIAM oplossing aan informatie nodig heeft uit ons SAP CRM systeem. Hiermee zouden we alvast kunnen voorsorteren op de impact op SAP.
IDM6	Wat biedt uw oplossing aan customer selfservice functies?	Het huidige MYK biedt de mogelijkheid om gebruikers en bijbehorende identiteiten te beheren, rechten te koppelen en accountbeheer (ww reset).

IDM7	Welke vormen van machtigen kent uw oplossing?	Kadaster verstaat onder machtigen dat partij A rechten toekent aan partij B.
IDM8	Welke visie heeft u op het beheer van entitlements?	Wat is de bron van een kenmerk/attribuut/groep en een rol en welk beheerproces hoort hier bij.

3.2.3 Identity Provider (authenticatiemiddel)

Stelling/uitgangspunt Kadaster CIAM: ID-Provider

Kadaster heeft een beslisboom opgesteld waarin de WDO leidend is. Indien hieruit voor een casus een WDO plicht naar voren komt, zal gebruik gemaakt worden van de voorgeschreven authenticatiemiddelen van het stelsel elektronische toegangsdiens ten overheid. Voor overige situaties leidt de beslisboom volgorde lijk tot:

1. Federatie met bestaande (externe) ID-P's, SAML-2.0 en OIDC als standaarden
2. Configuratie (externe) ID-P dienst
3. Inzet van een eigen ID-P

Twee factor authenticatie is door de CISO als basis niveau gedefinieerd.

ID	Vraag	Toelichting
IDP1	Kunt u zich vinden in de uitgangspunten van Kadaster en waarom wel/niet?	
IDP2	Welke mogelijkheden biedt uw oplossing voor een eigen Kadaster (klant) ID-P	
IDP3	Hoe kan vanuit identity management (paragraaf 3.2.2) de ID-P aangestuurd worden en welke configuratiemogelijkheden zijn er?	
IDP4	Welke standaarden ondersteunt de ID-P functie in uw oplossing?	Denk aan SAML, OIDC, SCIM

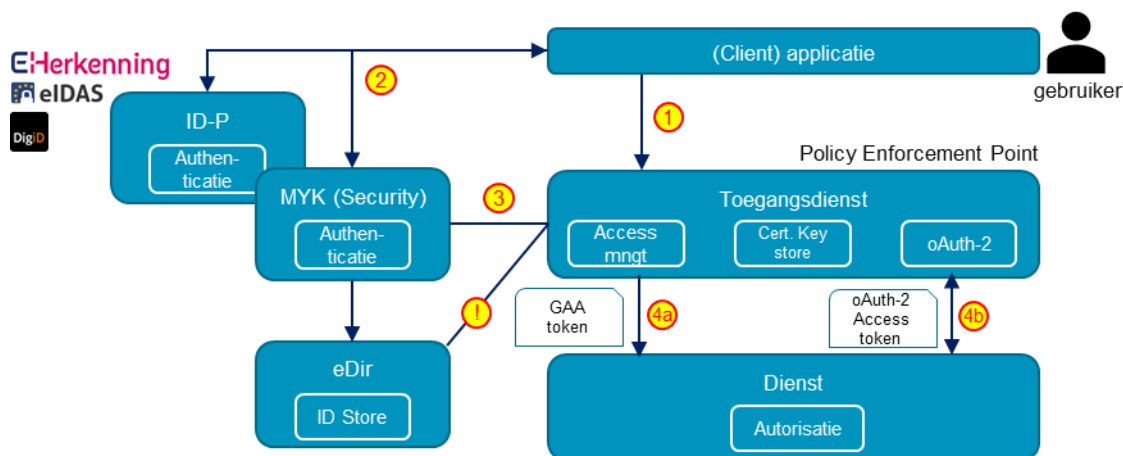
3.2.4 Access management, toegangsautorisatie

Kadaster maakt momenteel gebruik van een gateway als centraal (access)policy enforcement point (PEP). Dat betekent dat de gateway de voorwaarden voor toegang tot protected resources bewaakt op basis van policies die met een Policy Manager worden geconfigureerd.

Op deze manier dwingt de gateway ook de juiste authenticatievorm af wanneer geen passend bewijs van authenticatie getoond kan worden door de gebruiker.

Met de genoemde positie van de gateway biedt deze een consistente vorm van toegangsautorisatie aan als Policy Enforcement Point (PEP).

Naast de gateway en policy management wordt ook OAuth 2.0 support aangeboden.



Figuur 2: globaal logisch applicatiemodel bestaande situatie; access management

Figuur 2 laat globaal de positie en de belangrijkste functie van de gateway zien binnen het CIAM domein:

1. Een client applicatie spreekt een dienst aan ('protected resource'). De gateway controleert of er sprake is van een geldige sessie en/of (OAuth 2 access) token
2. Indien er geen sprake is van een geldig token wordt een web client naar de juiste ID-P gestuurd waarop authenticatie van de (eind)gebruiker kan plaatsvinden. Voor de OAuth 2 Client Credentials flow geldt een andere route om een access token te verkrijgen (niet weergegeven)
3. Stap 2 levert nu een 'ticket-ID' op waarmee de gateway een 'verificatiedocument' kan opvragen met informatie over de (rechten van de) gebruiker
4. Afhankelijk van het beoogde target ('dienst'):
 - a. Vertaald de gateway het verificatiedocument naar een 'GAA' token van de klant identiteit en propageert deze naar de beoogde dienst
 - b. Kan de doelapplicatie (dienst) op basis van een access token en de OAuth 2 scope van de applicatie, het token controleren en benodigde kenmerken van de digitale identiteit opvragen
 - c. Verzorgt de doelapplicatie (dienst) de fijnmazige autorisatie.

(!) Figuur 2 laat ook een "Cert Key store" zien als functie. Kadaster biedt (zakelijke) klanten ook de mogelijkheid om op basis van mutual TLS (mTLS) op basis van een PKI-Overheids certificaat te authenticeren. De certificate (key) store wordt gebruikt om de mTLS verbinding toe te staan en de klant te identificeren op basis van het certificaatnummer (OIN) in eDir op Klant niveau (OU) is vastgelegd. Dit is geen wenselijke route voor de toekomst omdat er geen centrale autoriteit is voor het controleren en uitgeven van tokens.

Met het herinrichten van CIAM wil Kadaster de rol van de gateway terugbrengen naar een (access) policy enforcement point (PEP), zonder de authorization server functie.

ID	Vraag	Toelichting
AM1	Past het voorgenomen plan van Kadaster om een gateway als PEP te behouden in uw visie cq aangeboden oplossing? Zo ja hoe en zo nee, waarom niet?	Kadaster is zich ervan bewust dat een zero-trust multi-cloud (deployment) policy van de gateway vereist dat deze kan worden gedistribueerd
AM2	Past het huidige PEP principe in uw oplossing en/of ziet u andere principes als alternatief?	Aansluitend op AM1; huidige directe toegang van de gateway naar de ID-Store (eDir) zal mogelijk ook vervangen moeten worden door OAuth 2
AM3	Biedt uw oplossing alternatieven voor de gateway? Zo ja, hoe ziet de authenticatie- en autorisatie flow er dan globaal uit?	
AM4	Waar wordt in uw visie het niveau van authenticatie bewaakt zodat eventueel ook een step-up gemaakt kan worden binnen een actieve sessie?	

3.2.5 Applicatieautorisatie

Stelling/uitgangspunt Kadaster CIAM: Applicatie autorisatie

De rechten van klanten binnen klantapplicaties vinden hun oorsprong in de overeenkomst (contract) met de klant waarin de volgende basisgegevens zijn opgenomen:

1. Product – dienst
2. Conditie van gebruik product – dienst (bijvoorbeeld een abonnementsvorm)
3. Start- en einddatum overeenkomst

Rollen (RBAC) worden door proceseigenaren (business) vanuit producten/diensten gedefinieerd en hebben daarmee betekenis binnen die context.

Attributen (ABAC) zijn kenmerken van klanten (organisatie, gebruiker, branche, etc) en kunnen dynamisch zijn (mede ook in het kader van zero trust).

ID	Vraag	Toelichting
AA1	Hoe zou Kadaster het beste de overeenkomsten met klanten kunnen vertalen naar autorisaties binnen applicaties? Welke gelaagdheid / normalisatie zou hier in kunnen zitten (informatiemodel)?	In de bestaande situatie is het zo dat product/dienst artikelnummers impliciet als attribuut aan een digitale entiteit worden gekoppeld. Er is geen expliciete vertaling naar een attribuut of een rol.
AA2	Kunt u hier een basis (informatie) model schetsen waarin de belangrijkste entiteiten zijn opgenomen met hun oorsprong (bron)?	Aansluitend op AA1; hoe verhouden contracten, identiteiten, entitlements, kenmerken, rollen en groepen zich in uw visie
AA3	Welk governance model is van toepassing?	We willen een wildgroei op attributen en rollen voorkomen.

3.2.6 Aanpak / transitie

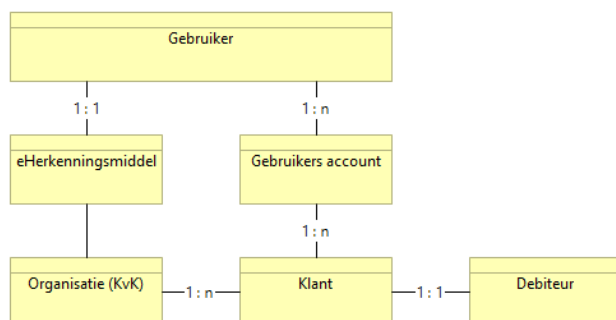
Kadaster ziet het herinrichten van CIAM als een uitdaging. De groep zakelijke klanten (debiteur-relatie) is de grootste groep klanten die Kadaster nu actief registreert. Kenmerken:

1	Klanten (rechtspersonen)	:	43000
2	(Klant)gebruikers	:	160000
3	Gemiddeld aantal logins / dag	:	13000
4	Aantal producten/diensten	:	80

Een klein deel van de klanten (ca. 5 %) maakt al gebruik van eHerkenning.

Momenteel is het zo dat gebruikers hun eHerkenningmiddel kunnen koppelen aan de Kadaster (gebruikers)identiteit. Ook is het zo dat een rechtspersoon (organisatie) *geen* 1:1 relatie heeft met een Kadaster klant welke in SAP CRM is opgevoerd, zie Figuur 3. Zo kunnen bijvoorbeeld grotere organisaties bijvoorbeeld afdelingen registreren als Klant waarbij Kadaster gerichter kan factureren (KvK : klant : debiteur = 1 : n : 1) en de klant de factuur makkelijker kan afletteren. Het nadeel is echter dat de klantadministratie onnodig complex wordt én een medewerker van een organisatie (KvK) namens meerdere klanten bij Kadaster kan inloggen en hiervoor ook verschillende gebruikersaccounts heeft. Met één eHerkenningmiddel betekent dat dat de gebruiker meerdere gebruikersaccounts moet kunnen koppelen en na inloggen met eHerkenning moet kunnen kiezen namens welke klant hij/zij wil gaan werken.

Het voornemen wat Kadaster heeft is om Klant : KvK terug te brengen naar 1:1 en klanten bij een bestelling en eigen kenmerk op te laten geven die gebruikt kan worden om de factuurregels van Kadaster te kunnen afletteren in de boekhouding.



Figuur 3: bestaande basis entiteitenmodel

Het gebruikersaccount wat in Figuur 3 is weergegeven valt onder selfservice gebruikersbeheer van Mijn Kadaster. Bijbehorende authenticatievorm is een single factor; gebruikersnaam en wachtwoord. Deze past niet bij WDO-plichtige diensten en wanneer de WDO in gaat kan dus voor deze diensten niet meer met dit middel worden ingelogd, maar alleen nog maar met eHerkenning.

ID	Vraag	Toelichting
AT1	Vormt de bestaande situatie van de klantadministratie een probleem voor de voorgenomen herinrichting van CIAM?	Kadaster wil weten of de huidige klantadministratie blokkerend is voor herinrichting van CIAM.
AT2	Welke (groe) fasering voor de transitie van bestaand naar nieuwe situatie stelt u voor?	Kadaster is op zoek naar een migratie met zo min mogelijk overlast voor de eindgebruiker en voor onze dienstverlening.
AT3	Welke tijdslijnen zijn gemiddeld genomen van toepassing voor een transitie die Kadaster nu voor ogen heeft?	
AT4	Wat zijn de belangrijkste voorwaarden voor een succesvolle transitie?	Kadaster wil toetsen of ze klaar is voor een succesvolle transitie.

AT5	Zijn er nog andere risico's en mitigerende maatregelen die u in deze transitie voorziet?	
AT6	Hoe gaat u om met een verandering van oplossing, bijvoorbeeld van PAAS naar SAAS, gedurende de contractperiode?	De veranderingen van de IT strategie van het kadaster zullen de komende jaren nopen tot verder aanpassingen in het IT infrastructuur- en applicatie landschap en het beheermodel. Wij vragen ons af, hoe onze leveranciers en partners hierin kunnen meebewegen.

3.2.7 Deployment en verdien/financieel model

Kadaster verkiest 'SAAS voor PAAS voor IAAS voor on-premise' als basis uitgangspunt. De bestaande klantenkring die wordt geregistreerd kent een basis van plm 130K gebruikers/identiteiten. O.a. onder druk van de Wet Modernisering Elektronisch Bestuurlijk Verkeer (WMEBV), verwacht Kadaster ook particulieren als klant te moeten registreren en een portaal te bieden waarmee aanvragen gedaan kunnen worden, de status van een aanvraag ingezien kan worden en producten kunnen worden gedownload. In potentie neemt daarmee het aantal actieve gebruikers van CIAM fors toe (miljoenen woningeigenaren). Vanuit de rol als publieke dienstverlener is daarmee een groot deel van de volwassen Nederlandse bevolking kandidaat klant-gebruiker. De aangeboden oplossing moet hiermee rekening houden qua capaciteit en kosten.

ID	Vraag	Toelichting
DL1	Hoe ziet u de prijsstelling?	Graag modulair voorzien van alle specificaties zoals bijvoorbeeld het afrekenmodel, support, eenmalige configuratie, opleiding gebruikers, specialisten etc. Dit is voor het Kadaster erg van belang. Het Kadaster zal de informatie die u hierover verstrekt zeer vertrouwelijk behandelen.
DL2	Op welke manier(en) wordt de door u voorgestelde oplossing(en) aangeboden?	Cloud, on-premise of hybride.
DL3	Hoe zit het licentiemodel in elkaar van de door u aangeboden oplossing(en)?	Welke staffel mogelijkheden zijn er van toepassing bij een groeiend gebruik? Welke prijsindicaties kunt hier hiervoor geven (CAPEX / OPEX). <i>Het Kadaster zal de informatie die u hierover verstrekt zeer vertrouwelijk behandelen.</i>
DL4	Welke basis support en/of SLA is er op de oplossing van toepassing en welke variaties/uitbreidingen kent u?	Voor de bedrijfskritische diensten die CIAM levert, verwacht Kadaster een oplossing die in de basis een 24*7 uren dienstverlening ondersteunt.
DL5	Aansluitend / verdiepend op DL3; welke operationele- en functionele ondersteuning valt er binnen het basisniveau van de aangeboden oplossing?	Feitelijk wordt hier ook gevraagd naar de belangrijkste beheerprocessen waar zowel Kadaster als de leverancier een rol in hebben.
DL6	Wat is de visie vanuit de aangeboden oplossing op ontwikkeling, testen en kwaliteitsbeheer?	Worden er bijvoorbeeld meerdere omgevingen aangeboden zoals test- en productieomgeving.

3.2.8 Overige vragen

ID	Vraag	Toelichting
OV1	Welke onderwerpen zijn van belang maar niet aan bod gekomen?	Geef per onderwerp aan wat het belang is en hoe het Kadaster daar in een eventuele aanbesteding mee om kan gaan.
OV2	Kunt u op basis van de situatie bij Kadaster en de voorgenomen richting een klant referentie geven die hierbij aansluit?	
OV3	Het Kadaster is gehouden aan de Baseline Informatiebeveiliging Overheid (BIO), gebaseerd op de ISO27001 en 27002. Bent u hiermee bekend en in welke mate kunt u hieraan voldoen?	
OV4	Kadaster zoekt een totaaloplossing met kennis en functionaliteit. Kunt u dat zelf leveren of bent u dat gewend te doen met partners?	Voor Kadaster is het van belang om één aanspreekpunt te hebben.