Bijlage 1a Programma van Eisen en Wensen

Openbare Europese aanbesteding

Customer Identity and Access Management (CIAM)

Kadaster

Auteur	Kadaster
Versie	1.1
Versiedatum	22 juli 2024

Inhoudsopgave

Hoofdstuk 1. Inleiding 4

Hoofdstuk 2. Uitvoeringseisen 5
2.1. Milieu, belastingen en arbeidsvoorwaarden 5
2.2. Gedragsregels leverancier 5
2.3. Overige uitvoeringseisen 5

Hoofdstuk 3. Eisen m.b.t. algemene financiële afspraken 6
3.1. Prijsstelling 6
3.2. Factureren 6

Hoofdstuk 4. Eisen m.b.t. juridische kaders 8

Hoofdstuk 5. Functionele eisen en wensen 9
5.1. Context CIAM 9
5.2. Klanten, gebruikers en accounts 9
5.3. Bestaande CIAM inrichting 14
5.4. Scope en (globale) transitie 15
5.5. Gewenste situatie (‘SOLL’) 19
5.6. Processen en CIAM functionaliteiten 22
5.7. Functioneel- en operationeel beheer CIAM services (voor Kadaster medewerkers) 35
5.8. “Interne” klanten 37
5.9. API Management 37
5.10. Klant ondersteuning 38
5.11. Machtigingen (mandateren) 39
5.12. Fraude detectie en preventie 39
5.13. Service Operation Center (SOC) 39
5.14. Integratie 40
5.15. Rapportages 42

Hoofdstuk 6. Migratie en implementatie 44
6.1. Inleiding / context 44
6.2. Stap 1: introductie ID-P met 2FA 45
6.3. Stap 2: uitfaseren bestaande CIAM componenten 48
6.4. Stap 3: aansluiten diensten op nieuwe access control methoden 50
6.5. Implementatie 51
6.6. Inrichting solution 51
6.7. Pilot nieuwe dienstverlening 51
6.8. Operationaliseren 2FA (MVP) (bij voorkeur nov 2024) 52
6.9. CIAM volledig ingericht (MVP) voorbereid voor migratie (juni 2024) 52
6.10. Bredere Kadaster context 52

6.11. Voorbereiding (eisen) 53

Hoofdstuk 7. Non-functionals 55
7.1. Beschikbaarheid 55
7.2. Performance 55
7.3. Continuiteit 55
7.4. Bewaken van de Oplossing 55
7.5. Privacy en security 55
7.6. Artificial Intelligence (AI) 56
7.7. Voorzieningen en Licenties 57
7.8. Testen van de Oplossing 57
7.9. Migratie kaders (re)transitie en exit 57
7.10. Toegankelijkheid 57

Hoofdstuk 8. Support 58
8.1. Support gerelateerd 58
8.2. Helpdesk (CIAM) 58
8.3. 2de , 3de en 4de lijns support van opdrachtnemer 59
8.4. Upgrades en changes 60

Hoofdstuk 9. Contractmanagement en rapportage 61
9.1. Contractmanagement: 61
9.2. Service Level Rapportage 62

Hoofdstuk 10. Toegevoegde Diensten Inschrijver 63
10.1. CIAM specialisten 63
10.2. Kennispartner 64
10.3. Training niveau en voor wie 64
10.4. Documentatie 64
10.5. Lifecyclemanagement 64

Hoofdstuk 11. Opdracht 66
11.1. Marktconformiteit 66
11.2. Opdrachtverstrekking n.a.v. offertetraject 66
11.3. Acceptatietest 66

Hoofdstuk 1. Inleiding

In deze bijlage staan de eisen en wensen beschreven die Opdrachtgever stelt aan de gevraagde dienstverlening en oplossing. Opdrachtnemer gaat door Inschrijving expliciet akkoord op alle bovenstaande eisen bij inschrijving op deze aanbesteding.

Opdrachtgever geeft geen afnamegarantie of omzetvolumes af, noch neemt hij enige afnameverplichting op zich, noch kan Opdrachtnemer aan de in dit Beschrijvend Document genoemde aantallen rechten ontlenen. Ten aanzien van de prognoses omtrent omvang of waarde van de dienstverlening/leveringen, geldt uitdrukkelijk dat het hier ramingen/schattingen betreft. Opdrachtgever kan voor de juistheid van deze gegevens geen enkele garantie geven.

Indien in dit document merken en/of merknamen worden gebruikt, dan betreft dit een indicatie van de gewenste kwaliteit en dan dient Opdrachtnemer te lezen “of ten minste gelijkwaardig”.

Alle bijlagen maken integraal onderdeel uit van dit bestek en daarvan dient een Opdrachtnemer kennis te hebben genomen.

Opdrachtnemers dienen te voldoen aan alle opgenomen eisen die de Aanbestedende dienst heeft geformuleerd ten aanzien van de te leveren prestatie. Eisen wensen in dit Programma van Eisen en Wensen worden als volgt weergegeven.

- Uitvoeringseisen: Dit zijn voorwaarden waar opdrachtnemer zich bij de uitvoering van de opdracht aan dient te houden. Deze zijn beschreven in Hoofdstuk 2 van dit document met bijbehorende bijlagen.
- Eisen: Dit zijn knock-out criteria en moet dus aan worden voldaan. Deze zijn rood gemarkeerd in dit document en tevens opgesomd in spreadsheet Bijlage 1b “Programma van Eisen en Wensen”
- Wensen: Dit is sub-gunningscriteria 5, waarop de economisch meest voordelige Opdrachtnemer mede op wordt bepaald.

  De gele gemarkeerde wensen zijn ja/nee wensen waarbij de leverancier aangeeft of hij hieraan kan voldoen of niet. Bij een Ja, worden de punten verkregen die verbonden zijn aan de wens. Dit kan aangegeven worden in Bijlage H Programma van Wensen.

  Van de groen gemarkeerde wensen wordt een toelichting verwacht in Bijlage H Programma van Wensen met een maximum aantal woorden. Meer informatie zal niet worden meegenomen in de beoordeling. Eventuele verwijzingen zullen niet worden meegenomen in de beoordeling. Deze groene vragen worden beoordeeld aan de hand van het beoordelingskader, zie paragraaf 7.4 van het Beschrijvend document.

  Alle wensen in dit document zijn ook opgesomd in spreadsheet Bijlage 1b “Programma van Eisen en Wensen”

Hoofdstuk 2. Uitvoeringseisen

2.1. Milieu, belastingen en arbeidsvoorwaarden

1.	*Opdrachtnemers dienen bij het opstellen van hun inschrijving rekening te hebben gehouden met de verplichtingen uit hoofde van de bepalingen inzake de arbeidsbescherming en de arbeidsvoorwaarden die gelden in het land waar de opdracht wordt uitgevoerd, zoals bedoeld in artikel 2.81 lid 2Aw2012. Kennis omtrent die belastingen en milieubescherming, arbeidsvoorwaarden en arbeidsbescherming kunnen Opdrachtnemers, voor zover het gaat om uitvoering in Nederland, verkrijgen bij:* *• het Ministerie van Infrastructuur en Waterstaat,* https://www.rijksoverheid.nl/ministeries/ministerie-van-infrastructuur-en-waterstaat *;* *• het Ministerie van Sociale Zaken en Werkgelegenheid,* www.rijksoverheid.nl/ministeries/szw *.*

2.2. Gedragsregels leverancier

2.	*Opdrachtnemer conformeert zich aan de gedragsregels leverancier, Bijlage 11.*

2.3. Overige uitvoeringseisen

3.	*Opdrachtnemer zorgt dat medewerkers die ingezet worden ten behoeve van de uitvoering van onderhavige Opdracht beschikken over een Verklaring Omtrent Gedrag (VOG) of een soortgelijk document uit andere EU lidstaten van maximaal 6 maanden oud . Op verzoek van Opdrachtgever zal Opdrachtnemer dergelijke verklaringen binnen een week overleggen. Opdrachtgever heeft het recht om aanvullend veiligheidsonderzoek door de AIVD ten aanzien van medewerkers te vragen in geval de vertrouwelijkheid van de verwerkte gegevens daartoe aanleiding geeft.*

Hoofdstuk 3. Eisen m.b.t. algemene financiële afspraken

3.1. Prijsstelling

4.	*Alle kosten/Prijzen/tarieven zijn opgegeven in Euro, exclusief BTW.*
5.	*Alle met de CIAM gemoeide kosten zijn verwerkt in de prijs, tenzij anders vermeld.*
6.	*De opgegeven prijzen en tarieven dienen realistisch en marktconform te zijn*
7.	*De door Opdrachtnemer geoffreerde tarieven mogen jaarlijks, en voor het eerst in 2025 geïndexeerd worden. Voor de dienstverlening is indexering toegestaan op basis van het CBS-indexcijfer Dienstprijzen – Commerciële dienstverlening en transport index 2010=100, tabel 62 computerprogrammering, advisering. Voor de overige tarieven is indexering toegestaan op basis van het algemene CBS-indexcijfer "dienstenprijsindex (DPI)*
8.	*Kosten die niet in de inschrijving genoemd worden en niet verdisconteerd zijn in de prijsstelling, maar toch noodzakelijk blijken te zijn voor een goed functioneren van het product of de dienstverlening, conform de in het beschrijvend document gestelde eisen, zijn voor rekening van Opdrachtnemer.*
9.	*Het is niet toegestaan met de ingediende prijzen de gehanteerde formule te frustreren; en negatieve prijzen zijn in ieder geval niet toegestaan.*
10.	*Een manipulatieve inschrijving is niet toegestaan en zal terzijde worden gelegd. Van een manipulatieve inschrijving kan bijvoorbeeld sprake zijn wanneer, als gevolg van miskenning door Opdrachtnemer van bepaalde aannames van Opdrachtgever, zoals bijvoorbeeld dat er realistische tarieven zullen worden aangeboden, de beoordelingssystematiek zo wordt gemanipuleerd dat het daarmee beoogde doel wordt verstoord. Van een manipulatieve inschrijving kan eveneens sprake zijn als het totaaltarief hoger is dan gemiddeld en kostenposten met een hoge weging een lager dan gemiddeld tarief hebben.*

Indien Opdrachtgever zelfstandig besluit over te gaan tot het gelasten van een nader onderzoek naar een manipulatieve en /of niet-marktconforme inschrijving is de betreffende Opdrachtnemer – kosteloos – gehouden schriftelijk en deugdelijk gemotiveerd te reageren op vragen die Opdrachtgever stelt. Voorts is de betreffende Opdrachtnemer gehouden alle bewijsstukken te overleggen die Opdrachtgever noodzakelijk acht om een eventueel vermoeden van strategisch inschrijfgedrag, een manipulatieve inschrijving, niet-realistische tarieven en/of niet-marktconforme tarieven op passende wijze te kunnen onderzoeken. Opdrachtgever benadrukt dat deze onderzoeksbevoegdheid in het leven is geroepen ter bescherming van haar belangen. Eventuele klagende Opdrachtnemers die menen dat een dergelijke inschrijving is gedaan, kunnen Opdrachtgever dan ook niet dwingen van haar bevoegdheid gebruik te maken.

3.2. Factureren

11.	*Facturatie dient plaats te vinden conform de bepalingen in de Overeenkomst*.

Op de factuur dienen ten minste de volgende gegevens te worden vermeld:

- Factuurdatum;
- Afleveradres;
- Het inkoopordernummer dat door Opdrachtgever wordt verstrekt;

- Omschrijving van de gefactureerde zaken met verwijzing naar het prijsaspect van het prijzenblad.

Facturen worden als Pdf-bestand verstuurd aan: facturen@kadaster.nl.

Indien de opdrachtnemer op zijn facturen een van bovenstaande gegevens niet vermeldt, beschouwt Opdrachtgever het ontvangen stuk niet als een geldige dan wel juiste factuur en is zij niet verplicht tot betaling van de factuur over te gaan.
Eventuele ontvangst- dan wel betalingstermijnen gaan niet lopen. Opdrachtnemer is in een dergelijk geval verplicht op eerste aanzegging van Opdrachtgever met betrekking tot de onderhavige factuur binnen 7 werkdagen de onderhavige factuur te crediteren.
Opdrachtgever heeft het recht na overleg met opdrachtnemer gedurende de looptijd van de Overeenkomst een andere factuurfrequentie af te spreken.

12.	*Gedurende de uitvoering van de Overeenkomst mogen geen prijzen/kosten gefactureerd worden die niet in de offerte opgegeven zijn, tenzij tussen partijen uitdrukkelijk anders wordt overeengekomen.*
13.	*Opdrachtnemer berekent geen additionele kosten door aan Opdrachtgever voor de in scope zijnde diensten die verband houden met de inzet van medewerkers, middelen en/of diensten.*
14.	*Opdrachtnemer gaat akkoord met het meewerken aan de eventuele automatisering van de facturatie aan Opdrachtgever. Opdrachtnemer zal Opdrachtgever geen kosten in rekening brengen voor de uitvoering van het proces.*
15.	*Opdrachtnemer factureert maandelijks achteraf. Opdrachtgever heeft het recht na overleg met Opdrachtnemer gedurende de looptijd van de Overeenkomst een andere factuurfrequentie af te spreken*

Hoofdstuk 4. Eisen m.b.t. juridische kaders

Alle algemene (levering-)voorwaarden van Opdrachtnemers en derden dan wel branchevoorwaarden zijn niet van toepassing.

16.	*Op deze aanbesteding is uitsluitend de ARBIT 2022 van toepassing zijn.*

Deze aanbestedingsprocedure, de overeenkomsten en alle overige aspecten worden beheerst door het Nederlands recht.

De in Bijlage 5 concept Overeenkomst en Bijlage 7 concept Verwerkersovereenkomst CIAM van het Beschrijvend document opgenomen concept overeenkomsten kunnen – alvorens deze door Opdrachtnemer(s) worden ondertekend, door Opdrachtgever worden gewijzigd en nader uitgewerkt, mede naar aanleiding van de door de Opdrachtnemer(s) gedane opmerkingen en tekstsuggesties als bedoeld in paragraaf 3.6 van het Beschrijvend document (Nota van Inlichtingen). De wijzigingen en/of de aangepaste overeenkomsten zullen/zal de Opdrachtnemers per Nota van Inlichtingen kenbaar worden gemaakt.

17.	*Opdrachtnemer gaat akkoord met de concept overeenkomsten (bijlage 5) en concept verwerkersovereenkomst (bijlage 7) met inbegrip van de eventuele per Nota van Inlichtingen kenbaar gemaakte wijzigingen zoals genoemd in deze paragraaf.*

Hoofdstuk 5. Functionele eisen en wensen

5.1. Context CIAM

De bestaande inrichting van ‘CIAM’ binnen Kadaster vindt zijn oorsprong in 2006 en kent een aanzienlijk maatwerk deel (‘MYK’). MYK is een afkorting van ‘Mijn Kadaster’ en biedt een centrale landingsplek (portaal) voor gebruikers van geregistreerde en gecontracteerde rechtspersonen. Betreffende gebruikers kunnen op rekening van de rechtspersoon waarbij ze horen, bestellen. Gelieerde rechten worden eenmalig verstrekt aan de gedelegeerd beheerder, ook wel Beheerder Mijn Kadaster (BMK) genoemd, een gebruiker van een klant die een beheerrol vervult binnen de rechtspersoon: de BMK kan andere gebruikers, werkzaam voor betreffende organisatie, beheren (aanmaken, machtigen, aanpassen en verwijderen). De BMK kan ook andere beheerders binnen de betreffende organisatie benoemen.

Mijn Kadaster biedt meerdere functionaliteiten, waaronder:
- ID self service; gebruikers- en accountbeheer door de klant zelf
- Authenticatie; MYK biedt een ID-Provider (ID-P)functie om gebruikers te authentiseren op basis van gebruikersnaam + wachtwoord.

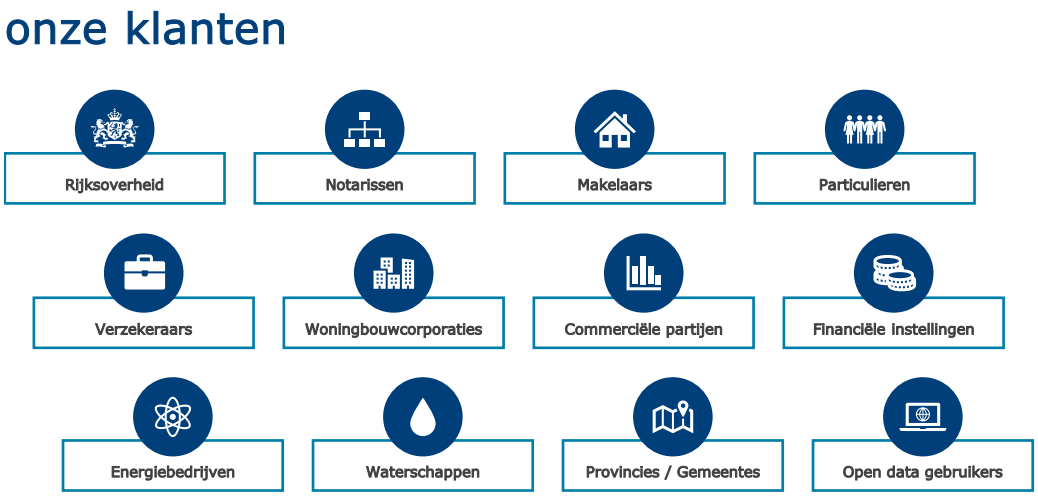
De huidige CIAM maakt gebruikt van de ‘Toegangsdienst’ (ook wel Generieke Authenticatie en Autorisatie dienst, GAA genoemd). De ‘Toegangsdienst’ biedt een primaire functie om de toegangscontrole tot beschermde bronnen van Kadaster af te dwingen (Access Management), maar biedt in de huidige vorm daarvoor ook ondersteuning voor OAuth 2 en een authenticatievorm op basis van certificaten. In dit document wordt nog verder ingegaan op de rol van de toegangsdienst.

Herzien bestaande inrichting

Kadaster wil de bestaande CIAM inrichting herzien op basis van de volgende hoofdargumenten:
- Vervangen maatwerk door moderne SAAS oplossing; functioneel doorgroeien en voldoen aan veiligheid/compliancy
- Meer grip en flexibiliteit op on- en offboarding flows (provisioning en deprovisioning)
- Beter (expliciet) beheer (governance) op de inrichting
- Betere ondersteuning voor API management; policy enforcement waaronder fijnmazige autorisatie
- Generieke ondersteuning gedelegeerd werk
- Vereenvoudigen van de klant- en debiteuradministratie i.c.m. gebruik van eFacturatie

5.2. Klanten, gebruikers en accounts

Kadaster is verantwoordelijk voor het registreren van rechten in openbare registers, maar ook het beheren van landelijke voorzieningen. Hiermee is de klantenkring zeer divers van particulier tot infrastructuur netbeheerder.



Figuur 1: Kadaster globaal beeld klanten

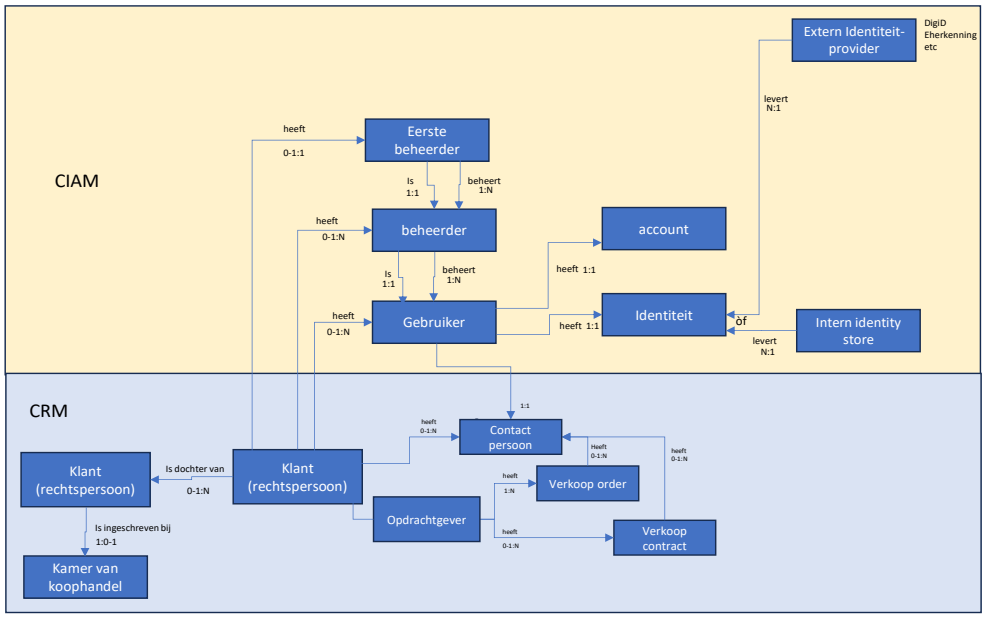
Als Kadaster staan we in dienst van de samenleving. De maatschappij verandert, nieuwe technologieën worden ontwikkeld en gebruikswensen en verwachtingen van zowel burger als professional veranderen mee. Nu de veranderingen in snel tempo doorzetten, voelen we de druk om met onze diensten, producten en klantinteractie mee te bewegen met de ontwikkelingen. Alleen dan kunnen we onze positie als betrouwbare, relevante en gedreven partner blijven vervullen. Dit vraagt dan ook dringend aandacht om iedereen te kunnen laten vertrouwen op onze informatie, kanalen en processen. Het Kadaster hanteert 3 klantwaarden die leidend zijn bij de uitvoering van onze dienstverlening: **soepel, van waarde en vertrouwen**. Het Kadaster zet nadrukkelijk voor haar hele dienstverlening in op het bieden van producten en diensten met een betrouwbare kwaliteit tegen aanvaardbare kosten voor de klant.



Het belangrijkste is dat de klant een logische, eenvoudige en veilige toegang ervaart. Een beter access management geeft veel meer mogelijkheden tot personalisatie (van content, data, selfservicing, etc.).

De groep zakelijke klanten (debiteur-relatie) is de grootste groep klanten die Kadaster nu actief registreert. Kadaster hanteert branches en sluit contracten met klanten waarin opgenomen is welke dienst een klant gebruikt. Deze combinatie van branche, contract en dienst (in de vorm van een artikelcode) is een belangrijk gegeven om gebruikers van klanten van rechten te voorzien.
De branches worden gebruikt voor marketingdoeleinden, maar zijn daarnaast mede bepalend voor de rol en rechten die gebruikers toebedeeld krijgen. Van elke klant worden gegevens geverifieerd. Dit is nu een vooral

handmatig proces waarbij gegevens bij externe bronnen worden gecontroleerd, zoals bij de KvK, Koninklijke Notariële Beroepsorganisatie in het geval van notarissen, De Nederlandsche Bank en Autoriteit Financiële Markt voor financiële instellingen, NPO en andere media organisaties voor journalisten, de NVM en andere brancheverenigingen voor makelaars, etc.



Figuur 2: Relaties tussen klanten, gebruikers en accounts

Figuur 2 toont de verschillende relaties van begrippen zoals klant en gebruiker tussen CIAM en CRM. Korte toelichting:
Bij grote organisaties is er sprake van moeder en dochter klanten. De moeder klant is de rechtspersoon waarmee zaken wordt gedaan. Een dochter klant is een suborganisatie van de desbetreffende klant. Bijvoorbeeld een Gemeente X is opgevoerd als moeder, de afdelingen van de gemeente zijn opgevoerd als dochter. Zowel moeder als dochters zijn opgeslagen als klant binnen CRM. Indien sprake is van moeder en dochters bij een klant, kan alleen de moeder organisatie ingeschreven zijn bij de kamer van koophandel In dit geval worden zowel moeder als dochter klant met hetzelfde KVK nummer geregistreerd in CRM, waardoor het KVK nummer niet uniek is.
Een klant heeft altijd maximaal één eerste beheerder (BMK), die is opgenomen in CRM. Een eerste beheerder kan andere beheerders opvoeren. Qua rechten/rollen beheer is er geen verschil tussen een eerste beheerder en een beheerder. Alle beheerders kunnen gebruikers opvoeren. Het is de bedoeling dat alle gebruikers zijn opgenomen als contactpersoon bij de klant in CRM: in de IST situatie zijn alleen eerste beheerders opgenomen in CRM.

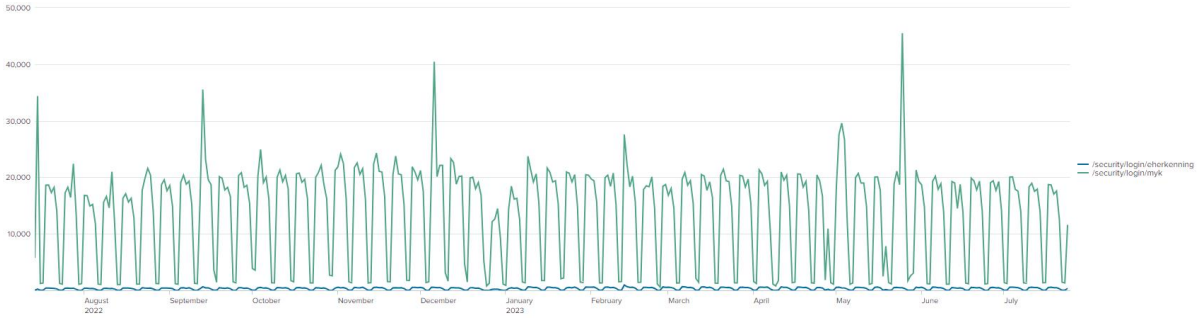
Binnen de huidige CIAM inrichting zijn klanten vooral zakelijk met veelal een inschrijving in het Handelsregister (KvK). Qua aantallen kenmerkt zich dit in productie als volgt:

1 Aantal zakelijke klanten (rechtspersonen) : 110.000

2	Accounts van gebruikers	:	160.000
3	Gemiddeld aantal logins / dag (excl M2M koppelingen)	:	14.000
4	Aantal producten/diensten	:	80
5	Aantal mutaties in klantgegevens in CRM op dag basis	:	60
6	Gemiddeld aantal voorziene beheerders/super users per klant	:	100

Een klein groeiend deel van de gebruikers (momenteel ca. 8 %) maakt nu al gebruik van eHerkenning. Voor de WDO-plichtige diensten geldt v.a. 01-07-2024 een verplichting van het gebruik van de authenticatiemiddelen van het stelsel van elektronische toegangsdiensten.

Figuur 3 geeft het aantal succesvolle logins weer over de tijd.



Figuur 3: Aantal web logins 2022

Bovengenoemde getallen gaan over gebruikers die inloggen via de web-interface en niet over M2M koppelingen. De verwachting is dat het aantal klanten, gebruikers en logins voor de zakelijke markt vergelijkbaar zullen zijn voor de komende jaren.

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 in combinatie met contract waarin toegang tot producten/diensten van toepassing zijn geregeld, de toegangsrechten. Het toekennen en (periodiek) controleren van dit recht moet beter worden ingericht en volgt daarbij het liefst het least privilege principe.

5.2.1. Nieuwe doelgroepen

De verwachting is dat in de toekomst andere doelgroepen zullen worden toegevoegd als klant. Denk daarbij aan particulieren (burgers) en ontwikkelaars die gebruik willen maken van de API's van Kadaster. Particuliere klanten worden in de huidige situatie niet geregistreerd. Particuliere klanten bestellen in de webwinkel, worden gekoppeld aan de transactie en rekenen direct af met iDeal. Bestelde producten worden veelal via email geleverd. Met nieuwe wetgeving (Wet Modernisering Elektronisch Bestuurlijk Verkeer) gaat dat mogelijk veranderen en zullen ook particuliere klanten de mogelijkheid moeten hebben om zich te registeren als klant. Het is een mogelijk scenario om een Mijn-Omgeving voor particulieren te maken zodat alle rechthebbenden

(iemand die betrokken is bij de rechtssituatie van een perceel) een account bij het Kadaster kan krijgen. Verwacht aantal rechthebbenden die toegang krijgt tot zo'n Mijn-Omgeving zit in de range van 5.000.000 - 10.000.000. Voor rechthebbenden is het verwachte gebruik 'incidenteel' en kent een piekgedrag, terwijl voor zakelijke klanten deze frequentie veel hoger ligt. Het voorbeeld is: tbv de WOZ bepaling wordt er een voorziening voor huizenbezitters aangeboden, waarmee huizenbezitters beter kunnen schatten wat hun WOZ waarde is in de periode maart/april als belastingzaken spelen. Stel dat in 50% van de huizenbezitters hier jaarlijks 1x gebruik van maakt, dan praten ongeveer over 4.000.000 keer

18.	*Eis: CIAM dient schaalbaar te zijn en mee te bewegen met de actuele behoefte van het Kadaster*

5.2.2. Vrijwillige registratie

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 registeren voor diensten die een authenticatievorm vereisen.

5.2.3. Wet Digitale Overheid | WDO

De WDO is aangenomen en 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). De WDO treedt gefaseerd in werking en het is de bedoeling dat alle overheidsorganisaties in de tweede helft van 2026 op het nieuwe stelsel over zijn. Kadaster is reeds begonnen met het implementeren van eHerkenning naast het eigen authenticatiemiddel (MYK). Klanten kunnen nu nog kiezen welk middel ze willen gebruiken.

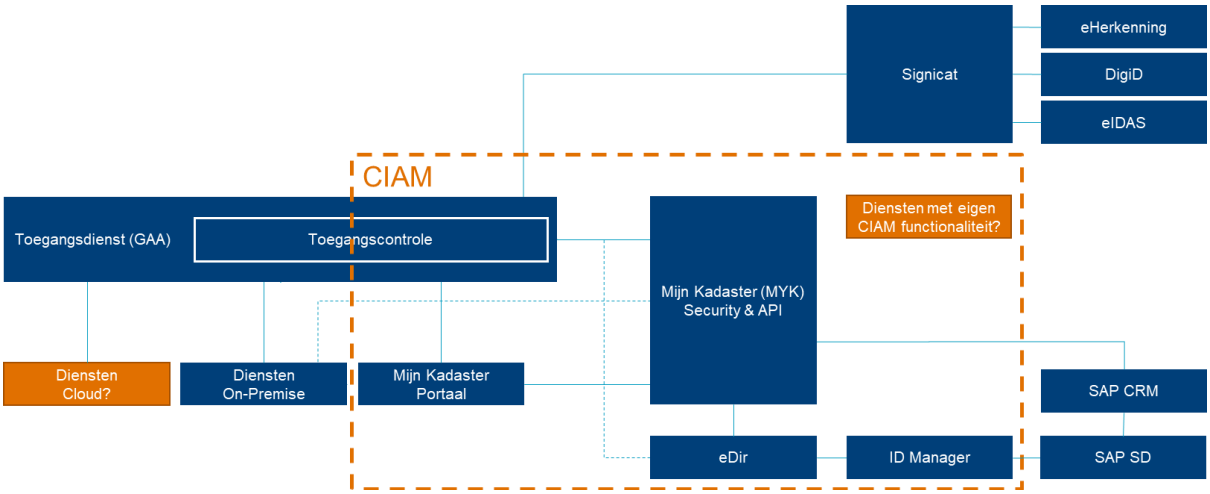
Ondersteuning stelsels zoals eIDAS

De doorlopende ontwikkeling van stelsels zoals eIDAS, biedt ook Kadaster de mogelijkheid om de CIAM inrichting te normaliseren en vereenvoudigen. European Digital Identity (EUDI) Wallet biedt nieuwe pan-Europese federatiemogelijkheden waardoor dienstverleners veel meer met vertrouwensrelaties kunnen werken op basis van authentieke bronnen zónder deze gegevens te kopiëren en synchroniseren. Kadaster wil met de herinrichting van CIAM een oplossing die compliant is met gevestigde (formele) stelsels zoals de eIDAS verordening en toekomstige opvolgers binnen het werkveld van het Kadaster.

19.	*Eis: CIAM dient federatie met aanbieders van WDO middelen te ondersteunen, al dan niet via een broker.*

5.3. Bestaande CIAM inrichting

Grof geschetst ziet de bestaande CIAM oplossing er als volgt uit:



Figuur 4: Globaal componenten model bestaande CIAM inrichting

De huidige CIAM oplossing is een combinatie van de verschillende componenten:

- **MYK Security**: Maatwerk oplossing waar gebruiker geauthentiseerd wordt, autorisaties worden toegekend en waar de gebruiker een wachtwoord-reset kan doen.
- **Mijn Kadaster Portaal**: Een portaal waarin de gebruiker self-service functionaliteit wordt geboden. Het portaal wordt gehost op Liferay DXP. Voor een door MYK geauthentiseerde en geautoriseerde gebruiker wordt in Liferay een gebruiker aangemaakt met de juiste rechten. Op basis van deze rechten mag de gebruiker bepaalde pagina's zien met daarop client-side applicaties. Deze client-side applicaties kunnen bedoeld zijn voor self-service functionaliteit met betrekking tot CIAM maar kunnen ook de presentatieschil bevatten voor Kadaster diensten (zoals KLIC).
- **MYK API**: Maatwerk oplossing die als backend dient voor de self-service (client-side) applicaties in het Mijn Kadaster Portaal.
- **Micro focus | OpenText NetIQ eDIR**: Identity store, bevat de MYK accounts
- **Micro focus | OpenText NetIQ ID Manager**: Wordt gebruikt om eDIR te provisionen op basis van mutaties in SAP CRM (klantgegevens) en SAP SD (contracten met artikelcodes) (ERP).
- **Toegangsdienst | Broadcom Layer7 API Gateway** (GAA, Generieke Authenticatie en Autorisatie dienst): Wordt gebruikt voor toegangscontrole tot webapplicaties en webservices.

Entitlements / Autorisaties

Een entitlement voor een dienst wordt door MYK Security toegekend afhankelijk van bepaalde waardes in de Identity Store die zijn opgeslagen op organisatie en/of gebruiker niveau:

- Een gebruikersentitlement wordt toegekend als voor de klant een dienst is opgenomen in het contract, de dienst is 'ingeschakeld' op klant niveau en toegang tot de dienst is toegezegd op gebruikersniveau. Wordt aan één van deze criteria niet voldaan, dan krijgt de gebruiker geen entitlement.

- Voor machine-to-machine toegang moet het recht zijn toegekend op contract en organisatie-niveau.

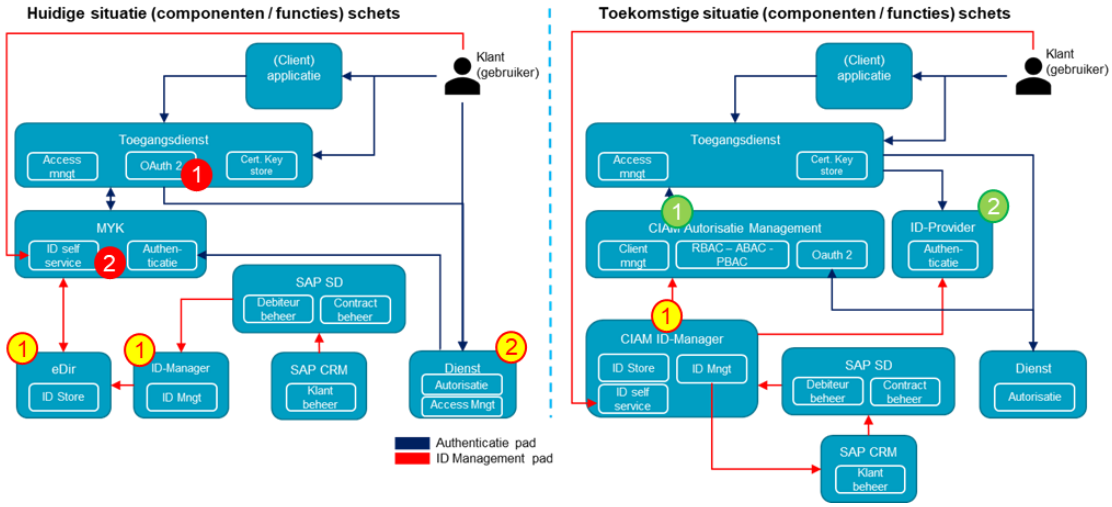
De huidige aanpak komt voort uit een aantal requirements:

- Er moet een mogelijkheid zijn om (tijdelijk) de dienstverlening voor een organisatie op te schorten, al dan niet voor een deel van de diensten. Bijvoorbeeld als een organisatie een betalingsachterstand heeft of niet langer kredietwaardig is.
- Wanneer een klant tijdelijk een dienst niet wenst af te nemen, bijvoorbeeld vanuit kostenoverwegingen, moet de klant deze voor alle gebruikers in één keer uit kunnen zetten.
- Wanneer een klant voor alle gebruikers een dienst heeft uitgezet en deze weer aanzet, moeten alle gebruikers die voor het uitzetten toegang hadden opnieuw toegang krijgen. Dit voorkomt dat (handmatig) de gebruikers weer opnieuw toegang tot de dienst moet worden toegezegd.

Voor deze aanbesteding geldt dat MYK Security, MYK API, eDIR en ID Manager worden vervangen. De rol van de toegangsdienst willen we op termijn terugbrengen naar access management. De self-service applicaties in Mijn Kadaster Portaal dienen te worden aangepast conform de CIAM herinrichtingseisen en de daaruit te selecteren cloud dienst (SAAS). De aan te besteden CIAM oplossing moet hoofdzakelijk configurabel zijn en in exceptionele gevallen een mogelijkheid bieden om Kadaster specifieke logica op te nemen op een gecontroleerde- en door de leverancier ondersteunde manier.

In paragraaf 5.4 wordt de bestaande situatie en de voorziene transitie nog verder beschreven.

5.4. Scope en (globale) transitie



Figuur 5: CIAM transitie

Figuur 5 toont een globaal overzicht van de voorziene CIAM inrichting transitie. De blauwe blokken zijn logische *componenten* en de wit omlijnde blokken vormen globale *logische functies*:

NIEUW (groene nummering)

1. Centraal autorisatie management obv standaarden (zoals OAuth 2)
2. Kadaster ID-entity Provider (ID-P) met 2 factor authenticatie

- **Centraal autorisatiemanagement**

Er is nu geen centrale autoriteit voor autorisaties. In de bestaande situatie vormt Mijn Kadaster (MYK) 'Security' de centrale component voor authenticatie (enkel-factor) én uitgeven van een zgn 'verificatie document' waarin de entitlements van een digitale identiteit zijn opgenomen (met name product-artikelnummers en eventueel aanvullende applicatierollen). Op basis van het verificatiedocument bepaalt de gateway of toegang mag worden verleend tot een dienst en wordt door de gateway een JWT gecreëert een meegegeven aan de achterliggende dienst.
Daarnaast kent Kadaster nu een zeer basale implementatie van de Autorisatieserver op basis van de Layer7 OTK (OAuth Tool Kit) welke sterk is gerelateerd aan de andere Broadcom Layer7 componenten; de Gateway en API-Portal. Al deze componenten vallen onder de centrale 'Toegangsdienst', ook wel Generieke Authenticatie en Autorisatie (GAA) genoemd. GAA houdt zich met name bezig met uniforme toegangsautorisatie voor extern binnenkomend verkeer. Hiermee vormt de gateway van de toegangsdienst een centraal punt waarin toegang tot de 'Diensten' (protected resources) wordt gereguleerd. De OTK wordt met name gebruikt voor toegang tot API's (registreren clients en gebruik als autorisatieserver, OIDC en token introspection). Kadaster zou graag met een Authorisation Server de ingetekende functies centraliseren en hiermee MYK security vervangen en de gateway terugbrengen naar de basisfunctie van Policy Enforcement.

- **Kadaster ID-Provider (ID-P)**

De bestaande authenticatiefunctie is opgenomen in MYK als maatwerk. Voor de bestaande (klant) rechtspersonen wordt voor web authenticatie naar MYK gerouteerd waarna MYK een inlog- en keuzescherm presenteert om te kiezen voor de gewenste authenticatiemethode (nu eigen inlogmiddel en eHerkenning).
De nieuwe ID-P moet multi-factor aankunnen en indien meerdere ID-P's mogelijk zijn, moet de gebruiker kunnen kiezen welke ID-P hij/zij wil gebruiken.

VERVANGEN / WIJZIGEN (geel/rode nummering)

1. Identity management en store
2. Aansluiting diensten

1. Identity management / store

Bestaande identity (ID) manager en store worden vervangen; bestaande functionaliteit zal overgenomen moeten worden door standaard functies binnen de nieuwe CIAM inrichting.
De huidige CIAM is alleen ingericht voor zakelijke klanten (rechtspersonen) en onboarding van die klanten vindt plaats op basis van een webformulier. Een ingevuld formulier leidt tot een opdracht voor de Klant Contact Administratie (KCA) om een klant verder te registeren met de onboarding. KCA voert de volgende acties uit:

- Validatie van ingevoerde gegevens
- Opvoeren van een klant in CRM
- Aanmaken "1e beheerder" (Beheerder Mijn Kadaster, BMK) als contactpersoon in CRM
- Koppelen contract tbv gewenste diensten in ERP (SAP SD)

Na het aanmaken van de klant en eerste beheerder, wordt via de Identity manager een nieuw organisatie (Organizational Unit; OU) in eDir opgenomen met een eerste Beheerder die alle rechten heeft van de organisatie. De beheerder krijgt zijn credentials in verschillende berichten. De huidige manier is foutgevoelig en relatief arbeidsintensief.
Voor de nieuwe inrichting geldt een Straight Through Processing (STP) manier als basis wat alleen bij uitval of time-outs een interventie van Kadaster beheerorganisatie (Klant Contact Administratie; KCA) vraagt.
De eerste beheerder kan vervolgens met selfservice voor zijn organisatie nieuwe gebruikers aanmaken/uitnodigen en rechten toekennen alsook verwijderen en intrekken. Dit geldt ook voor het beheer recht.

2. Aansluiten diensten

Diensten worden aangesloten op de centrale CIAM inrichting op basis van OAuth 2.
In de huidige situatie wordt voor toegang door de gateway, door de reverse-proxy functie, de authenticatie afgedwongen. Na authenticatie door de gebruiker kan de gateway op basis van een ‘ticket-ID’ het ‘verificatiedocument’, via een API van MYK, opvragen van de geauthenticeerde identiteit. Vervolgens vertaalt de GAA Gateway het verificatie-document naar een GAA-token (JWT) wat vervolgens wordt ‘gepropageerd’ naar de dienst samen met het originele request van de klant. De dienst haalt uit het token wat het nodig heeft om de gebruiker te authenticeren (in de basis zijn dit product-artikel codes en applicatierollen).
Met OAuth 2 wil Kadaster identity propagation vervangen door gebruik van OAuth 2 met een least privilege principe op basis van claims waardoor diensten alleen identiteitsgegevens kunnen opvragen die het strikt nodig heeft voor verdere autorisatie van de gebruiker.

20.	*Eis: Met OAuth 2 wil Kadaster het huidig gebruik van identity propagation vervangen door gebruik van OAuth 2 met een least privilege principe op basis van scopes en claims waardoor diensten alleen identiteitsgegevens kunnen opvragen die het strikt nodig heeft voor verdere autorisatie van de gebruiker.*

BEËINDIGEN (rode nummering)

1. OAuth 2 support toegangsdienst (OTK)
2. MYK Security

1. OTK

OAuth 2.0 support van OTK zal afgebouwd worden; de authorization server zal vervangen worden door de nieuwe CIAM oplossing, hoewel de gateway en de OTK gerelateerd zijn. De OTK wordt met een eigen webapplicatie ontsloten voor beheer (OAuth manager) en biedt bestaand functioneel beheer (Operationeel Informatie Manager; OIM) de mogelijkheid om -voor klanten- API Clients te registeren voor zowel de Authorization Code Grant (PKCE) flow en de Client Credentials flow .

2. MYK Security

Bestaand maatwerk opgebouwd vanaf 2006 en is voorzien te worden vervangen door de nieuwe CIAM inrichting. De selfservice GUI zal wel weer aangesloten moeten worden op de nieuwe CIAM inrichting waarbij idealiter de functionele verandering voor de klant beperkt gehouden wordt.

Overig

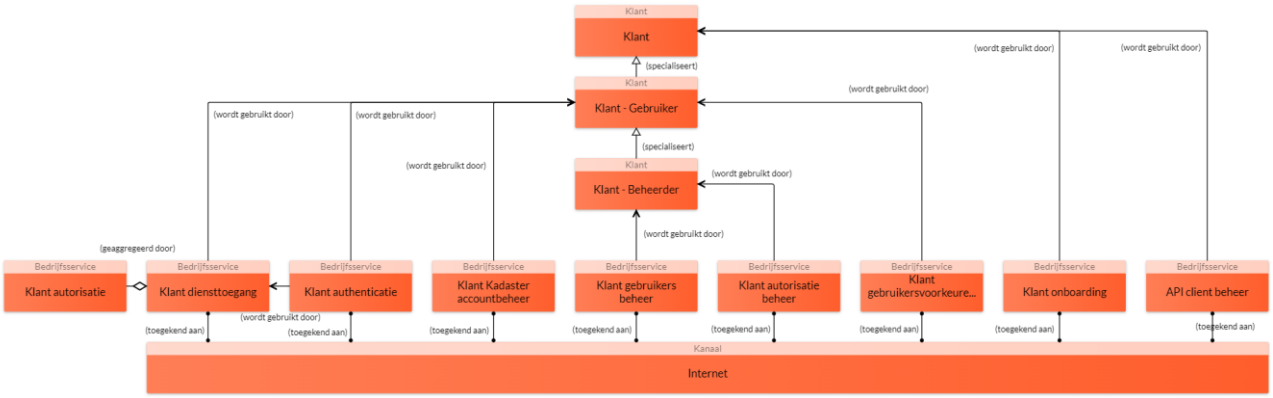
Figuur 5 is omwille van het overzicht eenvoudig gehouden. Kadaster zet voor de doel-inrichting in een ‘API-first’ beleid waarmee gelaagdheid en flexibiliteit wordt beoogd. Kadaster kent een grote diversiteit aan diensten die van oudsher product-georiënteerd zijn ontwikkeld. De nieuwe strategie gaat echter uit van ketenintegratie (‘kennis delen is kracht’) en een klant-centrale aanpak van de ontwikkeling van de propositie.
Met paragraaf 5.4 is globaal de voorgenomen herinrichtingvan CIAM beschreven met als doel een globaal beeld te geven. In de rest van dit hoofdstuk wordt verder doorgekeken naar de doelarchitectuur en de specifieke eisen en wensen hiervoor.

5.5. Gewenste situatie (‘SOLL’)

5.5.1. Bedrijfsservices

5.5.1.1. Extern (klant)

Kadaster probeert haar dienstverlening zoveel mogelijk met services te definieren. Deze zijn doorgaans bestendig in de tijd en kunnen op lifecycle/implementatie en operatie bestuurd worden.
Onderstaand model toont de geidentificeerde services waarin CIAM een belangrijke bijdrage levert en is bepalend voor dit deel van de uitvraag.



Figuur 6: externe (bedrijfs)services CIAM

Klant

De klant neemt Kadaster producten/diensten af, zie paragraaf 5.2. Naast genoemde uitbreidingen voorziet Kadaster ook toename in het gebruik van API’s door klanten. Hiervoor zijn ook selfservice oplossingen gedefinieerd waaronder die voor software developers (oa API Client beheer). Ook die doelgroep is voorzien om bediend te worden met de nieuwe CIAM inrichting.

Zakelijke klanten zijn organisaties, die één of meerdere accounts hebben. Er zijn twee soorten accounts:

- Gebruiker. Dit is een account die gebruik wil maken van de producten en diensten van het Kadaster.
- Beheerder. Dit is een account die extra rechten heeft om alle accounts van één klant te beheren. Nieuwe accounts opvoeren, stopzetten en/of muteren indien gewenst.

Klant onboarding
De bestaande ‘klant worden’-processen bij Kadaster maken gebruik van webformulieren met beperkte validaties en -daardoor ook- veel handmatige interventie van de Kadaster Klant Administratie (KCA). Hier moet veel betere Straight Through Processing (STP) voor komen door oa gebruik te maken van vertrouwde autoriteiten/bronnen. In het onboardingsproces, welke invulling geeft aan de service, moet er omgegaan kunnen worden met verschillende klantgroepen, het conditioneel toewijzen van entitlements en controles (automatisch en via medewerker). Dit wordt verder beschreven in sectie 5.6.1.

Klant gebruikersbeheer
Voor rechtspersonen, biedt Kadaster met deze service het gebruikers accountbeheer voor de gedelegeerd beheerder op basis van selfservice. De (eerste) beheerder (rol) wordt door Kadaster aan een natuurlijk persoon toegekend en kan vervolgens nieuwe gebruikers opvoeren, wijzigen en verwijderen.

Klant autorisatiebeheer
In de bestaande situatie biedt Klant autorisatiebeheer selfservice voor rechtspersonen waarbij Kadaster tijdens onboarding een eerste beheerdersidentiteit heeft aangemaakt en op basis van het contract de juiste entitlements heeft toegekend. Binnen de klant kan de beheerder (rol) rechten aan gebruikers toekennen cq intrekken zoals deze zijn afgeleid van de overeenkomst tussen Kadaster en de rechtspersoon (contract).

Klant diensttoegang
Service om veilig en met passende betrouwbaarheid toegang te krijgen tot Kadaster producten/diensten. Deze service maakt gebruik van de *Klant authenticatie* service. De bestaande oplossing van deze service werkt grotendeels op ‘artikelnummers’ die binnen het ERP worden uitgegeven en één op één worden gebruikt voor autorisatie.

Klant authenticatie
Service om, conform noodzakelijke betrouwbaarheid, de klant, danwel de gebruiker van de klant, te identificeren. Binnen deze service valt de twee-factor authenticatie (2FA) welke als belangrijke eis geldt voor de herinrichting van CIAM. Klant authenticatie kent meerdere authenticatievormen en providers (ID-Ps).

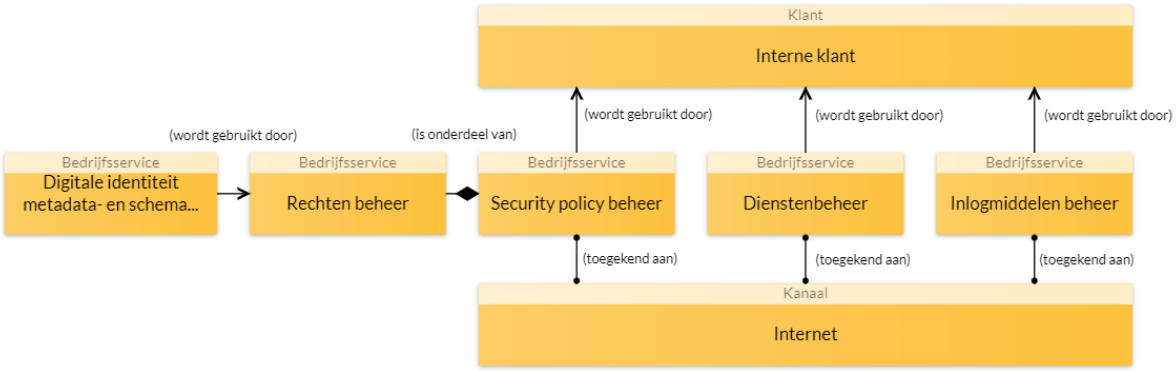
Klant gebruikersvoorkeuren beheer
Met deze service kan een gebruiker van een klant voorkeuren binnen de dienstverlening van Kadaster beheren. Denk daarbij aan het wel/niet willen ontvangen van bepaalde e-mails. Tijdens de marktconsultatie is wel naar voren gekomen dat consent-management niet alleen binnen het CIAM domein valt, maar juist ook- en in samenhang met CRM.

API Client beheer
Het kunnen registreren van een API-Client voor een API die een product/dienst ontsluit waarvoor de klant (OU) gerechtigd is om die te gebruiken. Zo kan een API Client registratie ID’s en secrets opleveren waarmee de bijbehorende authenticatiemethode gebruikt kan worden. Uiteraard biedt de service ook mogelijkheden clients te muteren of te verwijderen.

Het primaire kanaal waarmee de beschreven services worden ontsloten is internet (al dan niet via -mutual- TLS, of specifieker, web-GUI of API's. Web GUI's volgen centraal beleid (oa opmaak, compliancy) en worden door specifieke teams ontwikkeld en/of geconfigureerd.

5.5.1.2. Intern (beheer)

De bestaande CIAM inrichting is gericht op rechtspersonen met een grote diversiteit aan markten/branches. Autorisatie is vooral gebaseerd op product-dienst kenmerken. Met de nieuwe CIAM inrichting verwacht Kadaster meer soorten van 'access control' te kunnen inrichten waarbij gegevens minimaal worden gerepliceerd (data bij de bron) en er meer grip is op de totale set aan entitlements. Dat vraagt ook expliciete beheerservices binnen de organisatie die op hun beurt ook selfservice aanbieden waar mogelijk zodat bijvoorbeeld een product-dienst manager niet hoeft te wachten op een collega om bepaald configuratiewerk te verrichten.



Figuur 3: CIAM Interne bedrijfsservices

Figuur 3 toont een 'interne klant' voor de services, maar dit moet in de praktijk opgesplitst worden in verschillende beheerrollen.

Security policy beheer
Diensten bepalen zelf voor welke doelgroepen de dienstverlening bedoeld is en hoe ze daarbinnen de gebruikers kunnen autoriseren. Het autorisatiemodel van de dienst moet wel gemapped kunnen worden op de entitlements die zijn toegekend aan de digitale identiteit van een gebruiker. Welke policies voor toegang en autorisatie van toepassing moeten zijn, wordt via deze service geregeld.

Rechtenbeheer
Welke 'entitlements' (rechtgevende informatie) voor welke dienst –en in samenhang- van toepassing kunnen zijn, vraagt om een centraal beheer van de betreffende rollen, attributen, etc waarin naamgeving en normalisatie belangrijk is. Hiervoor wordt gebruik gemaakt van de service "Digitale identiteit metadata beheer". In de bestaande situatie worden rechten direct ontleend aan 'artikelen' geadministreerd in ERP. Dit is niet langer gewenst. Er is geen verdere vertaling/normalisatie/metadatering wat leidt tot enorme hoeveelheden artikelen en

het ontbreken van het totale overzicht van rechten van een digitale identiteit of de groep waar deze toe behoord. Fijnmazige autorisaties voor bijvoorbeeld APIs kunnen hierdoor niet verantwoord worden ingericht.

Digitale identiteit metadata- en schema beheer
Beheren/bewaken van het genormaliseerde schema en eenduidige definitie van entiteiten voor de digitale identiteit van een klant (organisatie en gebruiker). In de basis bevat het schema alleen elementen voor identificerende gegevens en entitlements binnen een groepen structuur. In de bestaande situatie bevat de identity store ook CRM gegevens.

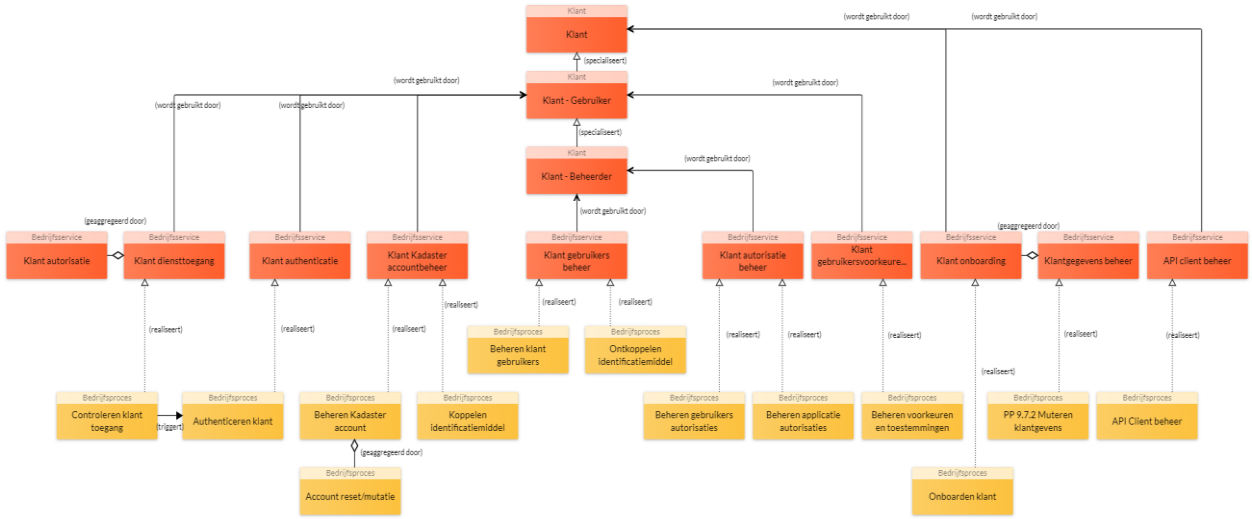
Dienstenbeheer
Bij veranderingen in het dienstenaanbod van Kadaster, kan dit effect hebben op de aansluiting op de CIAM functies en is hiervoor centraal beheer nodig. Ook wordt hier bepaald welke authenticatiemiddelen zijn toegestaan voor welke dienst.

Inlogmiddelen beheer
Kadaster maakt gebruik van verschillende Identity Providers zoals eHerkenning, DigID, maar ook het eigen – aan te besteden- middel. In de toekomst worden ook andere authenticatievormen verwacht (password-less, wallets, ..). Het beheer (aansluiting) van de mogelijke middelen wordt binnen deze service geregeld.

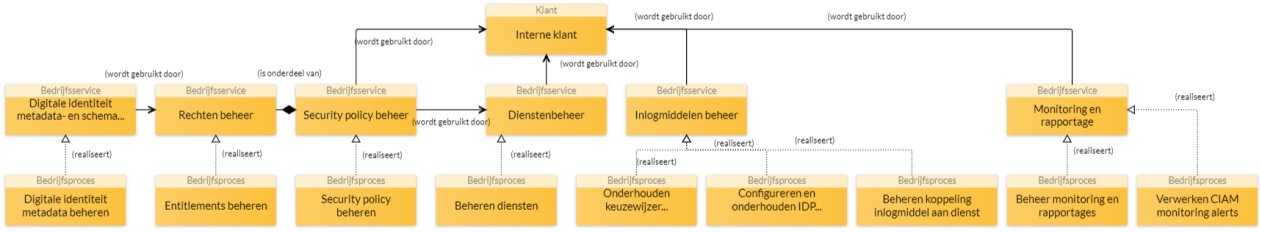
21.	*Wens: Het Kadaster zal moeten blijven voldoen aan de afspraken op Europees en/of Nederlands niveau. Leg uit hoe U het Kadaster met uw oplossing hierbij ondersteunt.*

5.6. Processen en CIAM functionaliteiten

Figuur 4 toont een overzicht van alle processen (geel) die invulling geven aan de klant services (oranje). Figuur 5 beoogt hetzelfde, maar dan voor de interne services (tbv Kadaster medewerkers) voor met name beheer en support.



Figuur 4: Processen voor externe dienstverlening

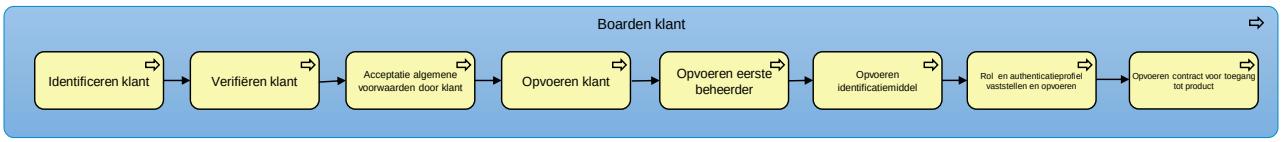


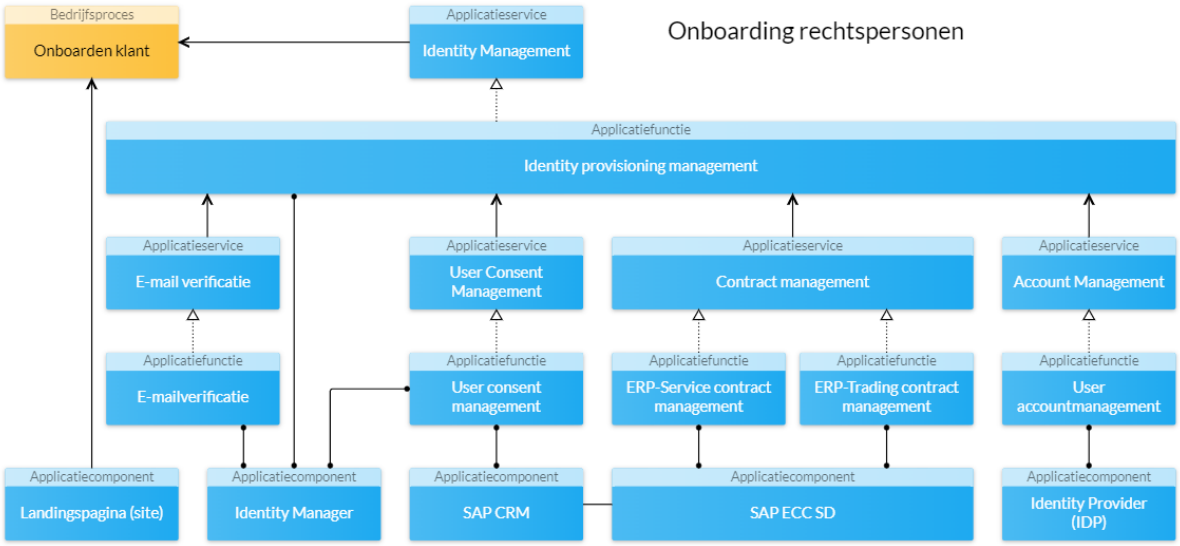
Figuur 5: Processen voor interne dienstverlening

In de volgende paragrafen worden de belangrijkste processen verder beschreven en de specifieke eisen die Kadaster stelt aan de CIAM inrichting. Specifieke koppelingen die Kadaster voorziet worden in paragraaf 5.14 samengevat (doel, type en data).

5.6.1. Klant on- en offboarding

Op jaarbasis worden nieuwe zakelijke klanten opgevoerd en klanten afgevoerd. Het netto klantenbestand is echter stabiel in omvang. Het proces voor onboarding volgt grofweg de volgende stappen:





Figuur 6: Globaal proces onboarding; applicatieservices en processen

Onboarden van Kadaster Klantgroepen gaat zo veel mogelijk volgens Straight Through Processing (STP) op basis van betrouwbare (referentiele) bronnen. Kadaster wil de onboardings procesflow kunnen modeleren en operationaliseren / monitoren zodat eventuele incidenten/vragen door het Klant Contact Center kunnen worden opgelost. In een ander uiterst geval kan Kadaster zelf de proceslogica bouwen tegen een API van de Identity Manager.

22.	*Eis: Kadaster kan binnen de CIAM oplossing het onboardingsproces zelf vormgeven (flow, condities, data- en datavalidatie) en operationaliseren.*
23.	*Eis: Onboardingsfuncties worden ook via een API aangeboden.*
24.	*Eis: Onboardings (proces) logica kan koppelen met externe bronnen (file/API).*
25.	*Eis: Als het Onboardingsproces een externe bron gebruikt en deze externe bron reageert niet, dan kan de oplossing hierin middels een exceptie voorzien zodat het proces hierop kan acteren met een foutmelding (exception handling) ipv blokkering.*
26.	*Eis: API's zijn gedocumenteerd.*

De potentiele klant zal zich in eerste instantie moeten identificeren om te bepalen om wie het gaat. De CIAM oplossing moet hiervoor met verschillende bronnen kunnen omgaan waaronder verschillende ID-Providers (federatie). Voor rechtspersonen moet de aanvrager bijvoorbeeld geidentificeerd worden met eHerkenning waarna de identificerende kenmerken (KvK, Handelsnaam, …) kunnen worden gebruikt voor 'prefilling' en verdere verificatie van gegevens.
Daartoe zullen interne en externe bronnen worden gebruikt om de identiteit vast te stellen.
Voorbeelden van externe bronnen zijn: KvK, Koninklijke Notariële Beroepsorganisatie in het geval van notarissen, De Nederlandsche Bank en Autoriteit Financiële Markt voor financiële instellingen, NPO en andere media organisaties voor journalisten, de NVM en andere branchevereningen voor makelaars etc.

27.	*Eis: CIAM ondersteunt het kunnen raadplegen van externe resources (bronnen) ten behoeve van identiteit verificatie.*
28.	*Eis: Verificatie van klantgegevens, zoals e-mail en telefoonnummer moet mogelijk zijn tegen door Kadaster configureerbare condities (beheer/configuratie functie)*
29.	*Wens: het is mogelijk om identiteit op basis van paspoort, rijbewijs en/of identiteitskaart vast te stellen*
30.	*Wens: het is mogelijk om het onboardingsproces te starten met een 'challenge' (bijvoorbeeld QR-code) op basis van bestaande (bijv. CRM) data. Zo ja, geef aan hoe de aangeboden oplossing hierin voorziet*

Landingspagina / toeleiding en GUI

Kadaster moet onder eigen beheer verschillende landingspagina's voor verschillende Kadaster doelgroepen kunnen ontwikkelen waarmee toeleiding voor onboarding geregeld kan worden.
Het online- en UX team binnen Kadaster zorgen voor eenduidige oplossingen waarbij ook WCAG compliancy wordt geborgd. Kadaster moet tenminste de web-GUI voor de eindgebruiker zelf kunnen opmaken. Daarnaast is er de eis dat Kadaster de Web-GUI zelf kan bouwen met client- en serverside logica (momenteel Bootstrap, Angular en Liferay W-CMS, ..), zie eis 23.

31.	*Eis: Onboardingsproces kan context sensitief zijn (per Kadaster label, doelgroep, product-dienst bijvoorbeeld)*

Klant contract management

Afhankelijk van de (klant)doelgroep zal er sprake kunnen zijn van een overeenkomst voor het gebruik van de beoogde diensten. Het contract bevat de producten/diensten en condities voor het gebruik (SLA, financiele voorwaarden, opzeggingstermijn, …). Contracten worden beheerd in het bestaande CRM en ERP (SAP) en zijn gekoppeld aan een klant/debiteur. Kadaster voorziet via de STP onboarding met name de standaard contracten die getoond en getekend (akkoord bevonden) kunnen worden. Speciale product/dienst wensen/eisen lopen via KCA en Kadaster Accountmanagement. Contractcondities vinden hun oorsprong en beheer bij product (/ dienst) management. Indien een klant een contract akkoordeert, moeten de condities leiden tot entitlements. Kadaster zou graag zien dat de aanbieder een visie heeft op integraal beheer van producten, voorwaarden en entitlements zodat het totaal aan gegevens sluitend beheerd kan worden waarbij de aangeboden CIAM technologie ook ondersteunend is.

32.	*Wens: de oplossing ondersteunt integraal beheer van product-, product(gebruiks)voorwaarden- en rechtgevende (entitlements) data. Zo ja hoe ziet die ondersteuning er uit en op basis van welke visie?*

Kadaster is overigens nog niet zo ver dat condities ook direct vertaald kunnen worden naar policies voor API Management (bijvoorbeeld een rate limit), maar voorziet dit wel in de toekomst. De gateway kan hier ook als Policy Enforcement Point functioneren.
Standaard contracten moeten digitaal kunnen worden gepresenteerd en goedgekeurd als onderdeel van de onboarding.

33.	*Wens: CIAM ondersteunt het contract management proces; aanbieden/tonen en expliciet goedkeuren.*

Email verificatie

Email is een belangrijk gegeven voor contact, maar mogelijk ook als inlognaam en/of herstel van account. Email verificatie is een standaard functie van de nieuwe CIAM inrichting en kan onderdeel worden van de onboarding flow. Kadaster wil de dienstverlening zo veel mogelijk personaliseren waarbij het emailadres een belangrijk gegeven is voor de communicatie. Eventueel kan een klant(gebruiker) meerdere emailadressen opgeven voor meerdere doeleinden en kunnen deze met de standaard emailverificatie gecontroleerd worden op bestaan en toegang door de gebruiker. Email-verificatie moet als conditie voor onboarding kunnen worden afgedwongen.

34.	Eis: *Tijdens* de onboarding van een nieuwe gebruiker is het mogelijk om het emailadres (conditioneel) te laten bevestigen door de gebruiker
35.	Eis: Het moet mogelijk zijn om een emailadres te verifiëren zodra deze gewijzigd wordt
36.	*Eis: Het moet mogelijk zijn om de verificatie-email aan te passen qua inhoud en styling*
37.	*Wens: CIAM ondersteunt het opslaan van meerdere emailadressen bij één identiteit.*

Onboarding

Het onboarding proces wordt in de basis geautomatiseerd aangeboden met minimale ondersteuning van het KCC. In de basis is het idempotent en biedt het Kadaster inzage tbv optimalisatie.

38.	*Eis: Onboardingsproces is "idempotent" zodat de afhandeling eenduidig is en herhaling (door bijvoorbeeld dezelfde persoon met dezelfde gegevens) niet leidt tot dubbelingen of data integriteitsissues.*
39.	*Wens: CIAM onboardingprocessen status kunnen worden ingezien door Kadaster service medewerkers.*

Offboarding

Klanten moeten onder selfservice afscheid kunnen nemen van Kadaster, maar ook via het KCC moet een verzoek tot beeidiging van overeenkomst en registratie kunnen worden uitgevoerd. Een individu heeft het recht om vergeten te worden.

40.	*Eis: aangeboden CIAM oplossing ondersteunt het offboardingsproces van klanten.*
41.	*Eis: aangeboden CIAM oplossing ondersteunt het recht om vergeten te worden (AVG)*

Service: User Consent Management

Het is een wens van het Kadaster dat de CIAM-oplossing consent management ondersteunt. Figuur 6 laat zien dat Kadaster die functie door een combinatie van CIAM (Identity manager) en CRM voorziet. Graag hoort Kadaster op welke manier de Inschrijver user consent management ziet en welke bijdrage geleverd kan worden.

42.	*Wens: CIAM ondersteunt consent management, al dan niet in samenwerking met CRM; geef aan op welke wijze uw oplossing consent management ondersteunt*

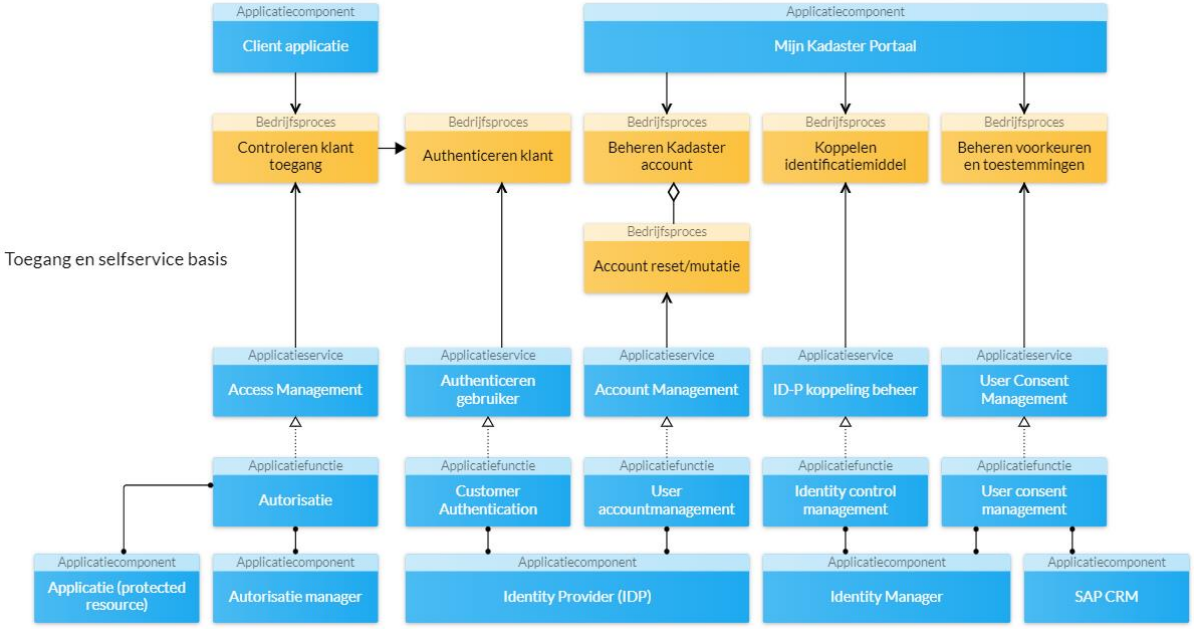
Service: Accountmanagement
Aanmaken en uitgeven van een Kadaster (klant) gebruikersaccount tegen de geldende policies waardoor het juiste authenticatieniveau mogelijk wordt voor de gewenste dienst(en).

- Mogelijkheid om wachtwoord policies te definieren en af te dwingen
- 2FA op basis van TOTP, SMS en Email
- Password-less

43.	*Eis: CIAM biedt een MFA ID-P met TOTP/SMS en Email als factoren*
44.	*Eis: CIAM ondersteunt wachtwoord policies (lengte, karakters, verversfrequentie)*
45.	*Wens: CIAM ondersteunt passwordless authenticatie; welke methoden worden ondersteund door de oplossing en welke roadmap is er voor passwordless authenticatie?*

Bij het onboarden van een zakelijke klant (rechtspersoon) is het nu zo dat de eerste gebruiker (‘1e beheerder’) alle rechten krijgt namens de klant (organisatie). Met de rechten kunnen nieuwe gebruikers worden aangemaakt/beheerd en kunnen rechten die aan de beheerder zijn toegekend, worden doorgezet/gedelegeerd aan andere gebruikers. Voor andere klantgroepen is dit niet voorzien en zal onboarding met name registratie van klantgegevens zijn en/of het uitgeven van een Kadaster account.

5.6.2. Toegang en selfservice basis



Figuur 7: Toegang en selfservice; applicatieservices en processen (globaal)

Figuur 7 toont een abstracte weergave van de voorziene processen en applicatieve ondersteuning voor toegang en selfservice voor basis gebruik. Voor aanvullend beheer namens een organisatie is een -eerder beschreven- beheerder rol voorzien (paragraaf 5.6.1).

Toegang

Voor alle niet-open diensten is identificatie van de gebruiker vereist. Het authenticatieproces wordt opgestart als de gebruiker geen geldig accesstoken mee kan geven in het aanspreken van de gewenste dienst. Kadaster voorziet hiervoor de bestaande GAA gateway als policy enforcement point (PEP) die op basis van het wel/niet beschikbaar zijn van een geldig accesstoken, de gebruiker voor de betreffende dienst naar de centrale authenticatiedienst stuurt waarna de inlog-opties voor de betreffende dienst worden getoond. Dit kunnen er één of meerdere zijn. Diensten als Keten Integratie Kadaster (KIK) zijn WDO plichtig en vereisen authenticatie met eHerkenning of een certificaat (machine-to-machine API toegang). Digikoppeling is een bestaande standaard waarmee klanten (doorgaans gemeenten) een mutual TLS verbinding kunnen opbouwen en de gateway TLS offloading verzorgt waarbij authenticiteit van het certificaat wordt gecontroleerd én op basis van het certificaatnummer de klant wordt geïdentificeerd. Hiervoor gebruikt de gateway nu een MYK API waarbij het certificaatnummer (Subject.organizationIdentifier) input is en als output het 'verificatiedocument' wordt geleverd wat vervolgens door de gateway wordt getoetst op de juiste entitlements en -indien akkoord- wordt vertaald naar een ('GAA') token (JWT) en tot slot wordt gepropageerd naar het door de gebruiker beoogde endpoint. Het certificaat nummer (OIN / Sub-OIN) moet dan echter wel zijn geregistreerd bij Kadaster.

46.	*Eis: CIAM ondersteunt meerdere ID-P's (inlogmiddelen) op basis van federatie volgens standaarden (zoals bijvoorbeeld SAML-2 en/of OIDC).*
47.	*Eis: CIAM ondersteunt het aanpassen van de OAuth 2 / OIDC implementatie zodat bijvoorbeeld de NL GOV standaard van het forum standaardisatie geïmplementeerd kan wordenC*
48.	*Wens: Het gebruik van meerdere ID-P's tegen condities kan geconfigureerd worden; beschrijf hoe dit werkt*
49.	*Eis: indien een dienst meerdere authenticatiemiddelen accepteert (bijvoorbeeld eHerkenning en eigen ID-P), faciliteert CIAM de mogelijkheid voor de gebruiker om te kiezen*
50.	*Eis: CIAM ondersteunt step-up authenticatie (eIDAS Level of Assurance; LoA) op basis van Kadaster instelbare condities*
51.	*Eis: CIAM ondersteunt het proces waarbij de gateway authenticatie op basis van een certificaat uitvoert (noodzakelijk voor onder andere DigiKoppeling). Voorzien is dat de gateway de authenticatie uitvoert, maar CIAM de mogelijkheid biedt om de entitlements van de identiteit te bepalen en deze aan de gateway te voorzien.*

De bestaande authenticatievormen zijn statisch; dwz per dienst wordt gekeken naar het noodzakelijke authenticatiemiddel/niveau. Indien een gebruiker is ingelogd en het authenticatieniveau niet voldoende is voor een (subsequente) dienst, zal om een step-up worden gevraagd en dat betekent nu inloggen met een WDO compliant middel (dus nadat eerst is ingelogd met het Kadaster middel). In de toekomst wil Kadaster ook op basis van aanvullende condities of patronen/gedrag het authenticatieniveau kunnen verhogen of de gebruiker opnieuw kunnen vragen zich te identificeren.

52.	*Eis: CIAM biedt Risk-Based Authentication (RBA) voor tenminste beperken aantal inlogpogingen en detecteren mogelijk misbruik van een dienst waardoor de afnemer opnieuw moet authenticeren*

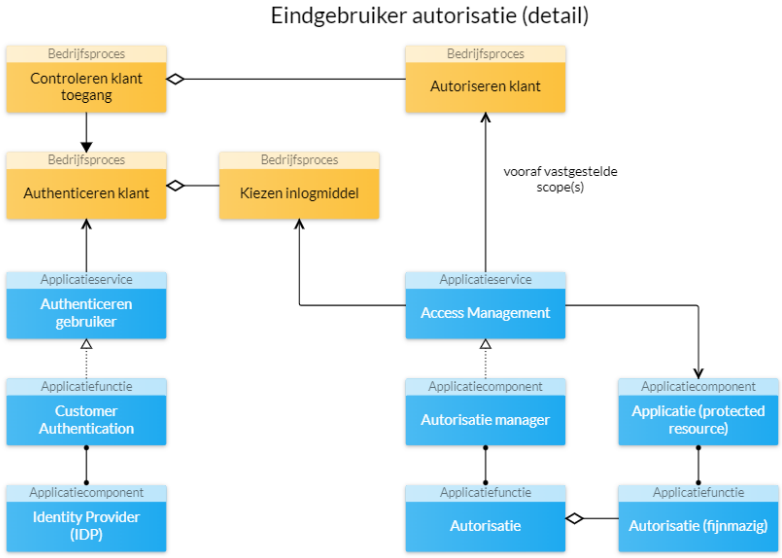
In de bestaande situatie verzorgt Signicat (ID-P Broker) een dienst waarmee Kadaster met 1 SAML koppelvlak, meerdere ID-P's kan gebruiken voor authenticatie en Signicat vervolgens de koppeling met de ID-P's onderhoudt. Vanuit beheer en ontwikkeling biedt dit gemak, maar met de voorziene toename van het aantal login sessies wil Kadaster de rol van de broker icm de aangeboden CIAM oplossing herijken.

53.	*Eis: bestaande Signicat Broker dienst kan hergebruikt worden (SAML2/OIDC)*
54.	*Wens: aangeboden oplossing biedt een alternatief voor de ID-P broker functie van Signicat. Kadaster stelt zich voor dat de aangeboden oplossing dan standaard federatie met eIDAS, DigID en eHerkenning biedt.*

Autorisatie

Het autoriseren is in de bestaande situatie in veel gevallen gesplitst in:

- Toegangsautorisatie
- Applicatieautorisatie



Figuur 8: Toegangs- en applicatie autorisatie; processen en applicatieve services

In de nieuwe situatie voorziet Kadaster dat de gateway zich gedraagt als resource server proxy en client van de 'Autorisatie server' (centrale autorisatie autoriteit) en claimt alleen die entitlements die het nodig heeft om toegangscontrole te verzorgen op basis van het accesstoken uitgegeven door het authenticatieproces. Op basis van hetzelfde accesstoken kan vervolgens de doelapplicatie ook de entitements van de digitale identiteit opvragen die het nodig heeft om de (fijnmazige) autorisatie binnen de applicatie te verzorgen op basis van attributen, groepen, rollen, relaties, etc.

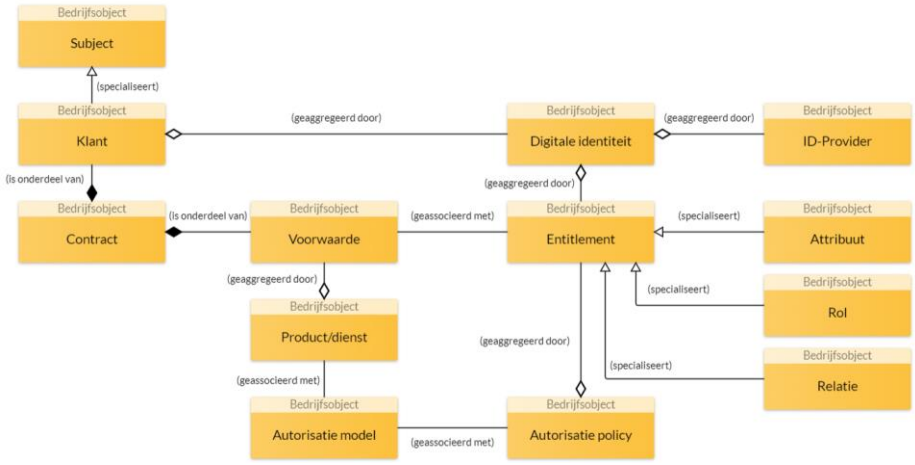
Kadaster wil gelaagdheid in de autorisatie aanhouden.

55.	*Eis: autorisatie kan gelaagd worden opgebouwd waarbij het bestaande 2-laags model (toegang tot dienst en toegang binnen dienst) wordt ondersteunt.*
56.	*Wens: de aangeboden oplossing faciliteert de protected resources / service providers met OAuth 2 ondersteuning. Zo ja, past dit in de voorgestelde oplossing, zo nee, welk alternatief wordt er dan geboden?*

In de bestaande situatie kent Kadaster ERP artikelnummers waarvan de gateway en de diensten de aanwezigheid in een digitale identiteit controleren om functie, data en toegang te autoriseren. Aanvullend kunnen per applicatie ook applicatierollen worden gedefinieerd binnen de Portaalbeheer functie van MYK en deze kunnen met selfservice per applicatie aan gebruikers worden toegekend.
Het bestaande schema van een digitale identiteit is bij Kadaster opgebouwd uit een Organizational Unit (OU), artikelnummers, branchecodes en applicatierollen. Dit moet verder worden genormaliseerd en gemoderniseerd zodat meerdere vormen van Access Control mogelijk worden (ABAC, RBAC, PBAC, ..) en fijnmazige autorisatie afgedwongen kan worden met een zero trust uitgangspunt.

57.	*Eis: De oplossing biedt functionaliteit om het schema (metamodel) van de digitale identiteit te kunnen aanpassen. Hiermee wordt o.a. bedoeld dat attributen aan de digitale identiteit kunnen worden toegevoegd. .*
58.	*Eis: voor het autorisatieproces kunnen andere bronnen worden geraadpleegd (bijvoorbeeld Policy Information Points; PIP)*

Figuur 9 toont een samenvattende context van primaire gegevens rond het autorisatiemodel voor een klant. Producten-diensten kennen voorwaarden voor het gebruik die bij de juiste onboarding leiden tot entitlements binnen de digitale identiteit van een gebruiker óf verwijzingen naar externe -vertrouwde- bronnen hebben. Het repliceren van gegevens van authentitieke- vertrouwde bronnen wordt idealiter voorkomen.



Figuur 9: Digitale identiteit en autorisatie; bedrijfsobjecten model (globaal)

Wij willen voor de diensten toegang verlenen op basis van een aantal attributen zoals artikelcodes, branches en contracten. Deze attributen bepalen de wijze van toegang.

59.	Eis: CIAM ondersteunt autorisatie op basis van attributen (ABAC) en rollen (RBAC)
60.	Wens: Kadaster wil op termijn policy based werken (PBAC). De aangeboden oplossing faciliteert hierin.

CIAM Selfservice basis

De basis selfservice functionaliteit is voorzien in grofweg drie delen:

1. Selfservice/beheren voor Kadaster account
2. Selfservice voor federatie; koppelen identificatiemiddel(en)
3. Beheren van voorkeuren en toestemming (consent)

Aanvullende selfservice functies kunnen door andere applicaties worden gefaciliteerd zoals beheren van klant- , persoons-, en contractgegevens door CRM/ERP.

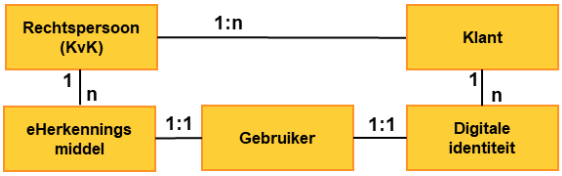
Voor selfservice biedt Mijn Kadaster nu specifieke functionaliteit en een eigen web front-end. Zoals eerder is beschreven geldt voor alle web-GUI's (ook voor beheer) specifieke, uniforme opmaak en WCAG compliancy.

61.	Wens: CIAM biedt een configureerbaar standaard web-GUI voor gedelegeerd beheer aan onze eindklanten. De opmaak van de web-GUI kan aangepast worden . conform Kadaster-huisstijl.
62.	Eis: CIAM biedt Identity management selfservice functionaliteit op basis van API(s)
63.	Wens: CIAM biedt Identity management selfservice functionaliteit op basis van SCIM

Op basis van API's kan Kadaster zelf de web-GUI (front-end) voor de selfservice basis functionaliteit bouwen. Voor alle API's geldt dat deze veilig ontsloten worden op basis van OIDC.

64.	Eis: CIAM klant/selfservice API's volgen OAuth 2 (/OIDC)

Het Kadaster account biedt de basis voor authenticatie van gebruikers, maar voor bijvoorbeeld WDO compliancy moeten WDO kerkende authenticatiemiddelen gekoppeld kunnen worden zoals eHerkenning voor organisaties. Het huidige proces biedt de mogelijkheid om een eHerkenningsmiddel te koppelen aan een gebruikersidentiteit. Op basis van een aantal identificerende kenmerken, waaronder het KvK nummer, kan gekoppeld worden door in te loggen met eHerkenning waarbij de volgende verhoudingen van entiteiten gelden:



Figuur 10: gegevensobjecten koppelen eHerkenning

Aangezien Kadaster meerdere klanten heeft geregistreerd voor 1 KvK nummer, kan een gebruiker binnen een organisatie (KvK) meerdere accounts bij Kadaster hebben voor meerdere Kadaster klanten. De gebruiker heeft echter maar 1 eHerkenningsmiddel en moet die dus kunnen koppelen aan meerdere digitale identiteiten. Als dit het geval is, moet na authenticatie met eHerkenning gekozen kunnen worden met welk account (cq voor welke klant) de gebruiker wil gaan werken.

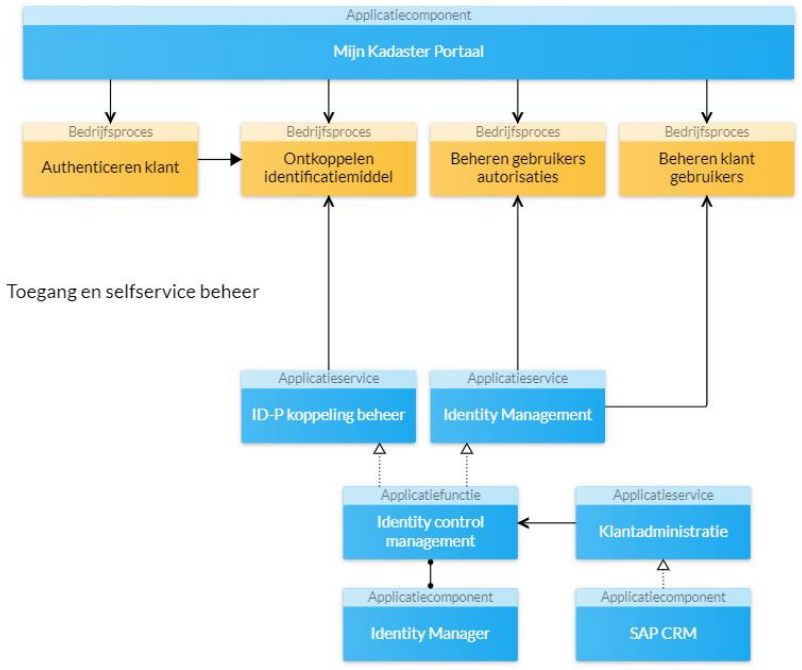
65.	*Wens: De aangeboden oplossing moet voorzien in de functionele behoefte dat gebruikers voor meerdere klanten kunnen werken op basis van 1 identiteit (ID-P account; bijvoorbeeld eHerkenning).*

Figuur 10 laat de bestaande werking zien; een gebruiker kan zijn/haar eHerkenningsmiddel koppelen aan meerdere Kadaster gebruikers identiteiten. In de nieuwe situatie kan dit mogelijkerwijs anders opgelost worden in plaats van werken met meerdere identiteiten.

Beheren voorkeuren en toestemming; kanaal-overstijgende voorkeuren zullen met name in CRM worden opgeslagen. In de bestaande situatie heeft Kadaster CRM nog niet ingeregeld op het niveau van de (eind)gebruiker. Dat is wel de wens om de dienstverlening en ondersteuning persoonlijker te maken.

66.	*Wens: Indien CIAM consent-management ondersteunt voor het gebruik van (identificerende) gegevens, beschrijf hoe de ondersteuning in de aangeboden oplossing is opgenomen en met welke visie in relatie tot CRM*

5.6.3. Toegang en selfservice beheer



Figuur 11: Toegang en selfservice tbv beheer; applicatieservices en processen (globaal)

Figuur 11 toont een abstracte weergave van de voorziene processen en applicatieve ondersteuning voor toegang en selfservice voor gebruik door de beheerder van de klant (organisatie).
Aanvullend op de basis selfservice functies en bijbehorende uitgangspunten (oa API support), kan de 'beheerder' rol aanvullende functies gebruiken voor gedelegeerd beheer. Om gebruikers te kunnen beheren zijn functies voor vinden, selecteren en inzien noodzakelijk.

67.	*Eis: Voor het beheren van gebruikers binnen selfservice biedt CIAM zoek, selecteer, inzien, aanmaken en wijzigen functionaliteit (CRUD) middels API(s) en -optioneel- web-GUI*

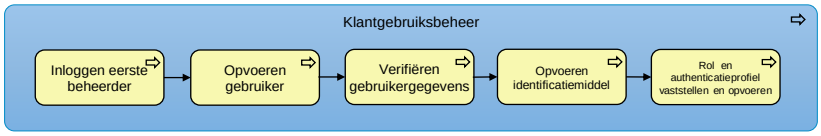
Ontkoppelen identificatiemiddel
De huidige CIAM inrichting biedt de gedelegeerd beheerder de functie om gebruikers voor zijn/haar organisatie te ontkoppelen van eHerkenning. Dus wanneer een gebruiker is gekoppeld aan een externe ID-P (eHerkenning in dit geval), kan de beheerder dit ongedaan maken wanneer er bijvoorbeeld een fout is gemaakt bij het koppelen.

68.	*Eis: CIAM biedt de mogelijkheid om verschillende beheerrollen te onderscheiden met verschillende autorisaties*
69.	*Eis: CIAM ondersteunt met federatie ook het ontkoppelen van externe ID-P's op (gebruikers)identiteitsniveau*

Beheren gebruikers autorisaties
CIAM identity management biedt voor de (gedelegeerd klant-) beheerder functionaliteit om van een gebruiker te zien welke entitlements (rollen, attributen, groepen, etc) zijn toegekend en welke er nog toegekend zouden kunnen worden. Vervolgens kunnen entitlements worden toegekend en onttrokken.

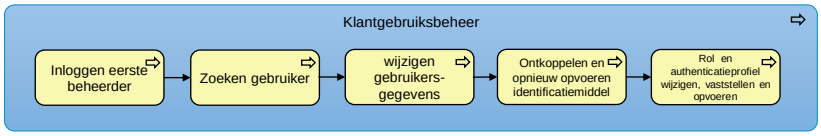
70.	*Eis: de beheerder kan eigen (beschikbare) rechten aan gebruikers toekennen en weer intrekken*

Beheren klant gebruikers



De bestaande oplossing voorziet in selfservice voor het aanmaken van nieuwe gebruikers. De CIAM functionaliteit moet hierin kunnen voorzien waarbij een gebruiker wordt uitgenodigd om te onboarden. Als alternatief voorziet Kadaster voor vertrouwde ID-P's zoals eHerkenning de mogelijkheid dat een nieuwe gebruiker kan inloggen met het bestaande middel waarna er een premature digitale identiteit wordt aangemaakt en de beheerder deze kan afkeuren of goedkeuren en van rechten kan voorzien. Het aanvraagproces kent een geldigheidsduur en aanvragen verlopen indien niet tijdig behandeld door een eerste beheerder.

Naast het aanmaken/onboarden van nieuwe gebruikers kan de beheerder ook gebruikers blokkeren en deactiveren/archiveren/verwijderen.



71.	*Eis: de gedelegeerd beheerder kan gebruikers aanmaken en uitnodigen voor onboarding*
72.	*Wens: de gedelegeerd beheerder kan gebruikers voor onboarding uitnodigen op basis van externe bronnen, bijvoorbeeld een lijst met gebruikersgegevens ('batch')*
73.	*Eis: de gedelegeerd beheerder kan gebruikers blokkeren, deactiveren/archiveren, verwijderen*
74.	*Eis: de gedelegeerd beheerder kan onboarding aanvragen inzien, verwijderen, afwijzen of goedkeuren*
75.	*Eis: de gedelegeerd beheerder kan voor een gebruiker een ID-P account 'resetten', bijvoorbeeld wanneer de tweede factor niet meer bruikbaar is (geen toegang meer tot mobiel nummer of toestel verloren, ..)*

Bij het onboarden van nieuwe gebruikers moet het ook mogelijk zijn om bijvoorbeeld persoonsgegevens aan CRM door te geven wanneer CIAM leidend is voor het onboardingproces. Ook hier geldt dat selfservice functionaliteit zo veel mogelijk met ondersteuning van een API (bijvoorbeeld SCIM) door Kadaster gebouwd kan worden, maar Kadaster staat ook open voor standaard processen die de CIAM oplossing voorziet en door Kadaster geconfigureerd kunnen worden.

76.	*Eis: beheer- selfservice functies kunnen via API worden ontsloten*

Het moet mogelijk zijn om extra gegevens van een gebruiker op te halen, danwel de gebruiker te autoriseren indien blijkt dat dit nodig om toegang te krijgen tot specifieke gegevens waar een hogere autorisatie voor nodig is. Denk aan zaken zoals:

- Just-in-time provisioning het vragen om extra gegevens indien dit een voorwaarde is voor het uitvoeren van een gebruikersactie.
- "Progressive profiling" (bijv. na ontvangen informatie van DigiD / eHerkenning extra informatie ophalen uit andere bronnen of door de gebruiker te vragen om aanvullende informatie. Deze gegevens kunnen opgeslagen worden, maar dat hoeft niet als dat bijvoorbeeld wettelijk gezien niet mag)

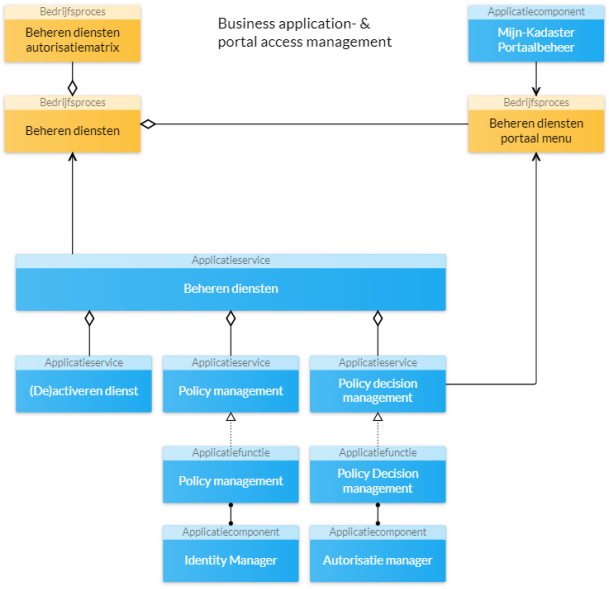
77.	*Eis: CIAM ondersteunt progressive profiling*
78.	*Eis: CIAM ondersteunt just-in-time provisioning door het raadplegen van externe bronnen tbv het aanvullen/verbeteren van identiteitsgegevens*

5.6.4. API Client registratie

API Client registratie biedt een klant van Kadaster de mogelijkheid clients te registreren tbv OAuth 2/OIDC. In de huidige situatie gebeurt dat nog door interventie van Operationeel Informatie Managers. Er is nu geen selfservice. In paragraaf 5.9. wordt de bestaande situatie en de gewenste ondersteuning van CIAM verder beschreven.

5.7. Functioneel- en operationeel beheer CIAM services (voor Kadaster medewerkers)

5.7.1. Toegang- en portaal beheer



Figuur 12: Toegang- en portaal beheer; applicatieservices en processen (globaal)

Binnen Kadaster vallen diensten onder verantwoordelijkheid van Product Management om te komen tot de juiste (door)ontwikkeling van de diensten. In de basis geldt een klant georiënteerde propositie, maar in de praktijk is dit nog steeds sterk product georiënteerd. Met de nieuwe CIAM moet aan beide proposities invulling gegeven worden zodat de overgang ook gefaciliteerd wordt. Met ABAC, RBAC en -verdere toekomst- PBAC moet integraal grip gehouden worden condities en conventies.

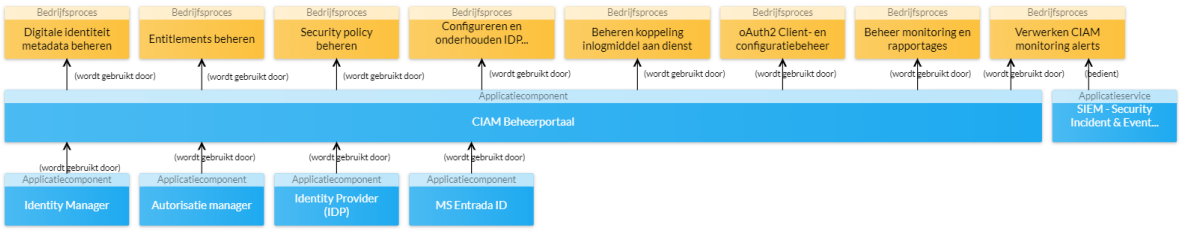
79.	*Eis: CIAM biedt Kadaster functioneel beheerders autorisatiebeheer functionaliteit op mogelijke entitlements zoals een rol en een attribuut*

Figuur 12 laat zien dat voor de bestaande zakelijke klanten een nieuwe dienst (minimaal) betekent:

- Dienst definiëren en endpoint(s) registreren
- Applicatie autorisatie policy management bepalen
- Toegangsautorisatie inregelen: toegangscondities waartegen de gateway toegang verleent

- Applicatie autorisatie inregelen: registreren OAuth 2 scopes voor endpoint (target applicatie)
- Mijn Kadaster portaalbeheer; nieuwe applicatie (menu-item/'tegel')

5.7.2. Overig functioneel- en operationeel beheer



Figuur 13: functioneel- en operationeel beheer; applicatieservices en processen (globaal)

Figuur 13 toont de beheerprocessen die voorzien zijn invulling te geven aan de eerder (globaal) beschreven services voor functioneel- en operationeel beheer, paragraaf 5.5.1.2.

Digitale identiteit metadata beheren
Integraal beheer van de structuur en entitlements van een digitale identiteit van en klant (organisatie en/of eindgebruiker). Van zowel eindgebruiker als organisatie onderhoudt Kadaster nu een 'digitale identiteit'; een gegevensstructuur met identificerende gegevens en entitlements (rechtgevende elementen zoals bijvoorbeeld een artikel of een rol). Entitlements worden oa gebruikt door service providers / protected resources.

80.	*Wens: Kadaster heeft de behoefte aan gegevensbeheer. Leg uit hoe gegevensbeheer binnen CIAM is ingeregeld? Denk aan metadata, data lineage, referentiële integriteit (waar worden gegevens gebruikt), versionering*

Security policy beheren
Integraal beheer van policies voor toegang en autorisatie en onderliggend gebruik van entitlements zoals:
- Subject attributen, bijvoorbeeld afdeling of job title
- Object attributen: beschrijving van de brongegevens
- Action attributen: wat probeert de gebruiker te doen
- Contextuele of environment attributen, zoals tijdstip, locatie etc

81.	*Eis: CIAM biedt beheer van policies.*

Dienstenbeheer
Bij veranderingen in het dienstenaanbod van Kadaster, kan dit effect hebben op de aansluiting op de CIAM functies en is hiervoor centraal beheer nodig. Ook wordt hier ingesteld welke authenticatiemiddelen zijn toegestaan voor welke dienst. Indien een dienst meerdere authenticatiemiddelen toestaat (bijvoorbeeld het eigen middel en eHerkenning), moet de gebruiker voor inloggen kunnen kiezen voor het gewenste middel.

82.	*Eis: CIAM kan per dienst (protected resource / service provider) configureren welke authenticatiemiddelen zijn toegestaan*

Configureren en onderhouden ID-P aansluiting (federaties)
Kadaster maakt gebruik van verschillende Identity Providers zoals eHerkenning, DigID, maar ook het eigen – aan te besteden- middel. In de toekomst worden ook andere authenticatievormen verwacht (password-less, wallets, ..). Het beheer (aansluiting) van de mogelijke middelen wordt binnen deze service geregeld zodat de middelen gekozen kunnen worden door de eindgebruiker en de juiste federatie wordt opgestart.

83.	*Eis: CIAM biedt de mogelijkheid om te federeren met meerdere ID-Ps en dit centraal te configureren*

5.8. “Interne” klanten

Diensten die Kadaster primair voor klanten heeft ontwikkelt, worden nu ook gebruikt door andere Kadaster diensten. Om het subject ‘klant’ aan te kunnen houden zijn hiervoor interne klanten vastgelegd en hebben die ook eigen gebruikers. Zowel voor API’s als (web)GUI’s ontstaat er nu een uitdaging bij de WDO plichtige diensten. Zonder aanpassingen moeten interne klanten zich als externe klanten identificeren en dat betekent eHerkenning of gebruik PKI-O certificaten (met sub-OINs). Beiden is niet wenselijk. Indien toch 1 endpoint voor de dienst wordt aangehouden, moet deze om kunnen gaan met beide doelgroepen (klanten, klantgebruikers en -API-clients van klanten). Verschillende authenticatievormen worden dan van belang voor hetzelfde endpoint.

84.	*Wens: CIAM biedt een ondersteuning waarmee medewerkers van Kadaster klantoplossingen ook zelf kunnen gebruiken. Idealiter rol-gebaseerd op basis van 1 digitale identiteit.*

5.9. API Management

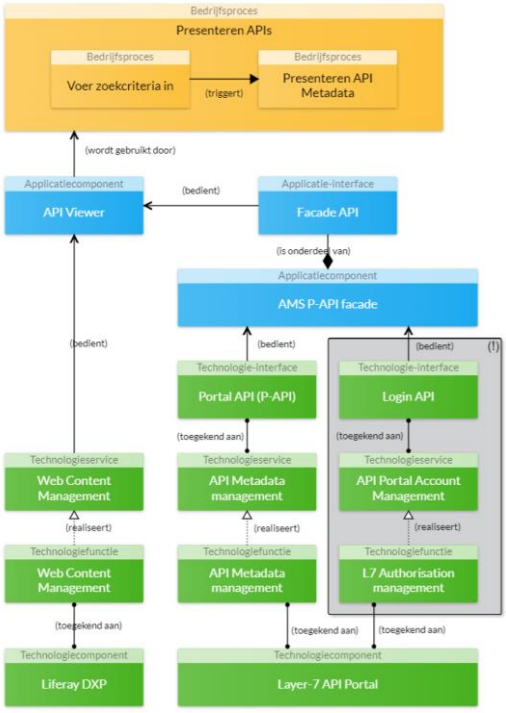
Bij Kadaster geldt een “API-First” beleid wat betekent dat producten/diensten bij voorkeur minimaal worden ontsloten met een API. Per API gelden toegangspolicies afhankelijk van doelgroep en gebruik. API Clients worden nu expliciet geregistreerd met de OAuth Manager van de Layer-7 OTK of Layer-7 API Portal. In beide gevallen worden er policies (XACML format) gegenereerd om de gateway als PEP te instrueren:

- Authenticatie route bij ongeldig accesstoken (OAuth 2 Authorization code grant flow)
- Trust / controle authenticiteit access token
- Resolven van een access token om toegang wel/niet te mogen verlenen
- Optioneel resolven API-Key om juiste SLA policies af te roepen (PDP)

Aanvullend moeten voor de client scopes kunnen worden vastgelegd waarmee een PEP (gateway of resource server) autorisatie kunnen controleren. Kadaster is benieuwd hoe dit beheer integraal het beste geregeld kan worden (gateway, autorisatie server, resource server). Het huidige Layer-7 API Portal kent een eigen gebruikersadminisratie en autorisatiematrix (/ACL).

Self service

Het moet mogelijk worden dat klanten hun eigen API Client applicaties kunnen registreren. Het bestaande API Portal bevat nu de API Catalogus waarvan een subset aan informatie voor externe klanten beschikbaar gemaakt kan worden tbv ontwikkeling/configuratie van de API Client. Momenteel kent API Portal geen relatie met de bestaande CIAM inrichting waardoor het gebruik beperkt is tot open data (API catalogus) en medewerkers de API Clients kunnen registreren/beheren voor klanten. In de toekomst voorziet Kadaster een breder gebruik van API Portal waardoor klanten, binnen de bestaande product/dienst autorisatie van de klant, API clients kunnen registeren.



Figuur 14: ontsluiten van de Kadaster API 'catalogus'

Figuur 14 laat zien waar Kadaster nu staat bij het ontsluiten van de catalogus en de rol van Layer-7 API Portal. API Portal kent een eigen ID-P met eigen account beheer en zal tzt moeten federeren met de nieuwe CIAM inrichting.

85. *Wens: CIAM ondersteunt centraal API Management, zoals self service client registratie.*

5.10. Klant ondersteuning

Het Klant Contact Center (KCC) wil toegang tot identiteitsgegevens en welke rollen/rechten/entitlements zijn toegekend. Welke mogelijkheden heeft CIAM om hier ondersteuning voor te bieden?

Achtergrond informatie: Binnen Mijn Kadaster (MYK) heeft een KCC medewerker nu de mogelijkheid om met klanten 'mee te kijken' (op basis van impersonatie). Een KCC medewerker heeft hiervoor een MYK ('interne klant') account en het specifieke recht om betreffende functie te activeren en vervolgens de betreffende klant op

te zoeken op klantnummer of gebruikersnaam (gebruikersnaam is een uniek identificerend gegeven binnen het bestaande MYK).

86.	*Wens: De Oplossing biedt ondersteuning voor een KCC medewerker. Zo ja, beschrijf hoe de ondersteuning er uit ziet.*

5.11. Machtigingen (mandateren)

Kadaster levert momenteel diverse oplossingen waarin klanten (met name ketenpartners) elkaar kunnen machtigen. Zo kan bijvoorbeeld een gemeente A -als bronhouder- een gemeente B machtigen om namens A als bronhouder op te treden. Het gaat dan om partijen die beiden bij Kadaster bekend zijn en waarvan een specifiek deel van de rechten tijdelijk kan worden overgedragen. Dat betekent dat de machtiging ook kan worden beheerd (rechten uitbreiden/intrekken).

87.	*Wens: de oplossing ondersteunt de gewenste machtigingen functie waardoor 'lokale' (per dienst) oplossingen kunnen worden vervangen door een centrale oplossing. Zo ja, geef aan hoe het mandateren en beheren dan werkt.*

5.12. Fraude detectie en preventie

5.12.1. Logging en auditing

88.	*Eis: De Oplossing biedt de mogelijkheid om auditlogs bij te houden zodat alle mutaties die plaatsvinden op data (configuratie-, operationeel-, transactioneel) te herleiden zijn. Dit omvat mutaties die door Kadaster beheerders gedaan zijn, maar ook mutaties op klant- en gebruikersobjecten.*

5.12.2. Alerts (security events)

89.	*Eis: De Oplossing biedt de mogelijkheid om tegen instelbare condities security events te genereren ten behoeve van een SIEM (Security Incident Event Management).*
90.	*Eis: De data in security events bevatten identificerende gegevens zodat deze gecorreleerd kunnen worden en volgordelijkheid kan worden vastgesteld bij het onderzoeken van events*

5.13. Service Operation Center (SOC)

Kadaster richt zich voor operationeel beheer op het gebruik van een centrale Service Operation Center (SOC) oplossing om operationele issues vanuit de volledige informatievoorziening te kunnen monitoren en aanvullend hierop te kunnen handelen om deze op te lossen of te voorkomen.

91.	*Eis: De Oplossing biedt een centrale logfaciliteit voor operationele logmeldingen waarbij het log-niveau instelbaar is (bijvoorbeeld WARNING, ERROR, FATAL) en de meldingen herleidbaar zijn (datum-tijd, bron, foutcode, foutmelding)*
92.	*Eis: De operationele logberichten van de dienst kunnen actief worden doorgezet naar het SOC van Kadaster op basis van een API **of** Kadaster kan de logging scannen met een SOC Agent. Essentie is dat*

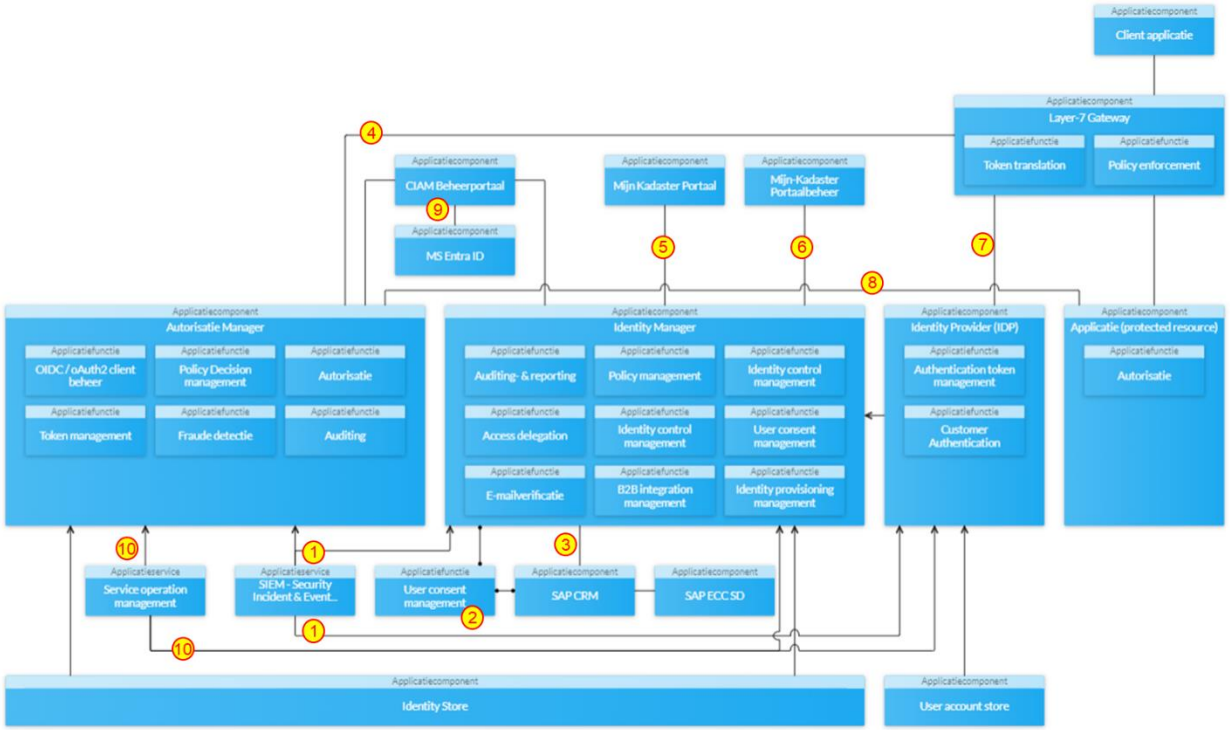
	de aangeboden oplossing geïntegreerd kan worden met een centraal SOC zodat operationeel beheer met het SOC kan werken.
93.	*Wens: De operationele logs kunnen door Kadaster direct benaderd worden binnen de aangeboden beheerfunctionaliteit. Beheerfunctie biedt Kadaster de mogelijkheid te zoeken in de logs met standaard filters (bijvoorbeeld datum-tijd, foutcode, sleutelwoorden, log-level).*

5.14. Integratie

CIAM vormt een Kadaster-brede centrale faciliteit voor het dialoog met de klant.
De oplossing dient te kunnen koppelen met bestaande applicaties en infrastructuur, maar moet ook bestendig zijn voor nieuwe/aanvullende integraties.

De reeds geïdentificeerde koppelingen zijn in voorgaande paragrafen al meer in context beschreven.
Figuur 15 toont het globale doel (SOLL) applicatie functie- en componentenmodel zoals Kadaster zich dat nu kan voorstellen Kadaster staat open voor alternatieve zienswijzen.

Hierbij expliciet een aantal verbindingen/integraties met de gevraagde CIAM services genummerd:



Figuur 15: Applicatie functie- en componentenmodel (SOLL)

#	Van	Naar	Type | Payload	Beschrijving / details
1	CIAM	SIEM	API, events	Security (alert) events met vaste- en configureerbare condities waarmee mogelijke cyberaanvallen danwel fraudepogingen kunnen worden geregistreerd voor operationele- en analytische doeleinden
2	ID-M (ID-Manager)	CRM (via PO)	API, user consent data	In geval de ID-Manager consent uitvraagd wat binnen het CRM gegevensdomein valt, zal de ID-Manager een API van SAP moeten kunnen aanroepen. Integratie met SAP loopt altijd via SAP middleware, Process Orchestrator (PO).
3	ID-M	CRM (via PO)	API, klant/user persoonsgegevens	Vanuit het onboardingsproces geleid door CIAM moeten persoonsgegevens aan CRM kunnen worden doorgegeven.
4	Gateway	Autorisatie Manager	API, introspection/PIP	1. De gateway moet een ID-P (access)token kunnen ‘resolven’ om als PEP de toegang te kunnen autoriseren. 2. De gateway doet de certificaat gebaseerde authenticatie, en moet een subjectgegeven als attribuut kunnen resolven naar een digitale (klant)identiteit zodat deze gepropageerd kan worden naar de serviceprovider/protected resource (IST) óf omgewisseld voor een accesstoken (SOLL)
5	MYK Portaal	ID-M	API (bijvoorbeeld SCIM), identity selfservice	Bestaand MYK selfservice front-end aansluiten op de CIAM ID-M waarbij ook rekening gehouden wordt met de rechten van de gebruiker (oa rol beheerder)
6	MYK Portaal beheer	ID-M	API (zoeken/lezen)	Ten behoeve van MYK portaal configuratie Is het de wens dat MYK Portaal gebruik functies (bijv. Menu-items) kan mappen tegen entitlements beheerd in de ID-Manager.
7	Gateway / client	ID-P	Authenticatie, OIDC, SAML	OIDC of SAML tbv authenticatie van de gebruiker/client.
8	Service provider	Autorisatie manager /server	API, introspection (userinfo / token)	Userinfo / identity introspection op basis van een accesstoken. PBAC als leidend principe mogelijk icm OPA.
9	CIAM Beheer	Entrada ID | AAD	SAML – OIDC – OAuth 2	SSO en autorisatie Kadaster medewerker voor CIAM beheer. Mogelijk aanvullend gekoppeld met (IAM) Identity Governance Administration (IGA) voor provisioning/deprovisioning processen bij medewerker in-, door- en uitstroming.

10	CIAM	SOC	Operationele logs	Subset (instelbaar) van CIAM operationele logs.

94.	*Wens: De oplossing past standaard op de beschreven (Figuur 15) koppelvlakken of biedt hiervoor een alternatief. Indien er sprake is van het alternatief, dan deze graag beschrijven voor de betreffende koppelvlakken. Beschrijf de functionele dekking en mogelijke alternatieven.*
95.	*Eis: De Inschrijver heeft aantoonbare ervaring met integraties met CRM en ERP*
96.	*Eis: Alle toegang tot Kadaster CIAM data en beheerfunctionaliteit moet ofwel verlopen via Azure AD / Entra-ID security groepen middels OIDC/Oauth 2 koppeling tussen CIAM en Azure-AD / Entra-ID, dan wel verlopen via een API (bijvoorbeeld SCIM) tussen CIAM en de Kadaster IAM/IGA voorziening*
97.	*Eis:* Voor een beperkt aantal geprivilegieerde beheerhandelingen wil Kadaster gebruik kunnen maken van Privileged Access Management (PAM). Dit vereist dat CIAM een API beschikbaar heeft voor het geautomatiseerd uitvoeren van password resets van beheer accounts die niet persoonsgebonden zijn en via PAM voor een specifieke beheerhandeling gebruikt kunnen worden.
98.	Eis: voor alle koppelvlakken van de aangeboden oplossing geldt dat bij het vernieuwen of beëindigen van een koppelvlak, Kadaster na de aankondiging door de leverancier een overgangstijd heeft van minimaal 1 jaar.
99.	Eis: CIAM moet open en hedendaagse communicatie standaarden ondersteunen (bijv. JSON over HTTP)

5.15. Rapportages

In de bestaande situatie worden diverse rapportages gegenereerd voor met name intern gebruik. Voorbeelden:

1. Totaal aantal digitale klant identiteiten
2. Totaal aantal digitale klant-gebruikers identiteiten
3. Aantal digitale klant-gebruikers identiteiten per klant
4. Totaal aantal Mijn Kadaster accounts
5. Totaal aantal ‘actieve’ Mijn Kadaster accounts (gebruikt binnen bepaalde tijdsperiode)
6. Aantal klant-gebruikers en gekoppelde ID-P’s (eHerkenning)
7. . . .

Veel van deze rapportages worden gebruikt voor Kadaster eigen inzichten en -indirect- voor afstemming met klanten. Voor de nieuwe CIAM inrichting moeten deze inzichten ook verkregen kunnen worden en direct ook beschikbaar gesteld kunnen worden aan eindklanten (beheerders). Ook dient data ontsloten te kunnen worden voor analytische doeleinden (BI). In alle gevallen geldt voor de eisen bijpassende authenticatie en autorisatie.

100.	*Wens: Kadaster wil graag ook voor de herinrichting van haar CIAM een oplossing hebben voor genoemde soort operationele rapportages; beschrijf welke oplossing de aangeboden oplossing biedt m.b.t. operationele rapportages?*
101.	*Wens: Rapportages kunnen via een web-GUI worden geraadpleegd en geëxporteerd in opgemaakte (afbeelding/PDF) vorm of ruwe (CSV/XML) vorm.*
102.	*Wens: Data ten behoeve van BI toepassingen kan via een API onttrokken worden.*

103.	*Wens: Data ten behoeve van BI toepassingen kan selectief en gepland periodiek geëxporteerd worden naar een bestand.*

Hoofdstuk 6. Migratie en implementatie

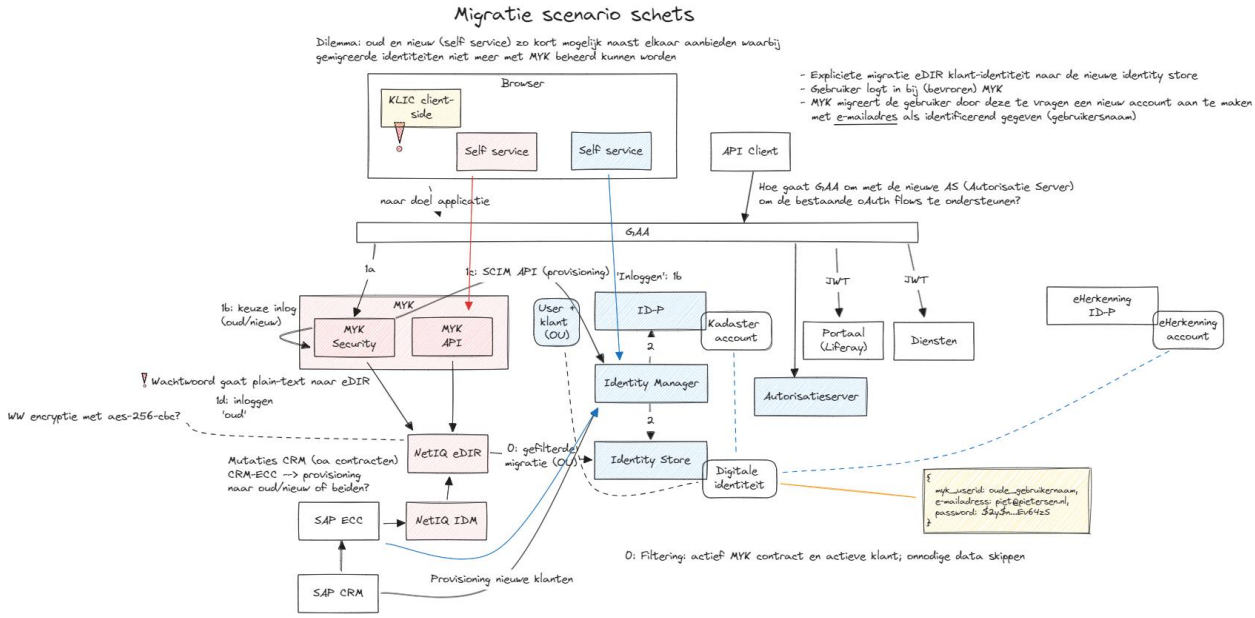
6.1. Inleiding / context

Voor de overgang van de bestaande/huidige CIAM situatie naar de uiteindelijke doel situatie, heeft Kadaster grofweg twee stappen voorzien:

1. Introductie van een eigen ID-P met 2FA
2. Vervangen bestaande identity store (NetIQ eDir) én Identity Manager (NetIQ IDM)

Kadaster heeft nagedacht over stappen die uitgevoerd moeten worden t.b.v. de migratie van gebruikers. Eén van de uitgangspunten is dat wachtwoorden geëncrypt zijn opgeslagen in eDIR (identity store) en niet gemigreerd kunnen worden naar de nieuwe identity store. Om deze reden heeft Kadaster een belangrijke rol voor MYK voorzien in de migratie van gebruikers.

NB: Vanzelfsprekend staat het Kadaster open voor alternatieve/betere migratiescenario's. Het Kadaster laat zich graag adviseren. De volgende tekst is dus slechts ter illustratie.
In dit hoofdstuk worden hiervoor genoemde stappen verder geschetst met bijbehorende argumenten/overwegingen. Dit geeft de Inschrijver een beeld van de gedachten binnen Kadaster en de mogelijkheid hier op te reageren in een plan van aanpak (SGC 2.1).

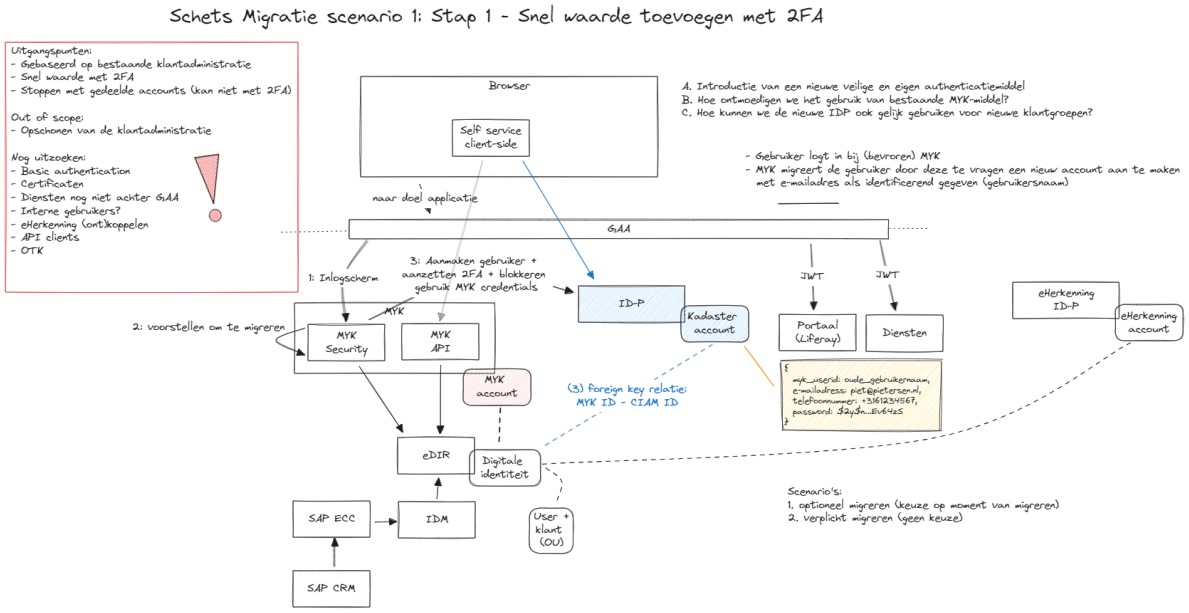


Figuur 16: Migratieschets CIAM

Figuur 16 toont een schets van een mogelijke migratie waarbij de rood gearceerde delen worden uitgefaseerd en de blauw gearceerde delen worden geïntroduceerd. De transparantie/witte delen zullen nodig blijven, maar waarschijnlijk worden aangepast.

6.2. Stap 1: introductie ID-P met 2FA

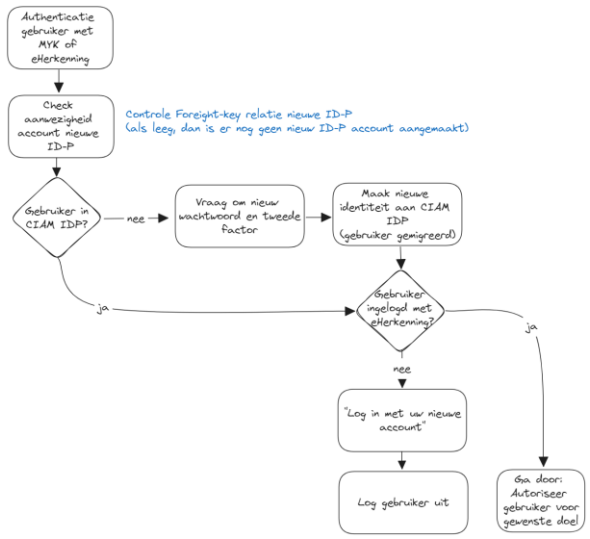
Met de eerste stap wil Kadaster de acute kwetsbaarheid van een enkel-factor authenticatiemiddel zo snel mogelijk oplossen door gebruikers in een overgangsperiode ‘over te zetten’ naar de nieuwe ID-P waar vervolgens ook een tweede factor zal worden uitgevraagd en gebruikt voor het authenticatieproces. Het snel introduceren van 2FA heeft hoge prioriteit vanuit het perspectief van security en dit kan betekenen dat er tijdelijk een andere inrichting wordt geaccepteerd dan voorzien voor de hele oplossing.



Figuur 17: Migratie/transitie stap 1: snel waarde met 2FA

Het introduceren van 2FA zal niet ongemerkt kunnen voor gebruikers. Figuur 17 toont de schets van de eerste stap van de transitie waarin (blauw) de nieuwe ID-P wordt geïntroduceerd en het MYK account wordt ‘vervangen’ door het nieuwe ID-P account. Om hier te komen moeten zowel het authenticatieproces als het beheerproces worden aangepast.

Impact authenticatieproces

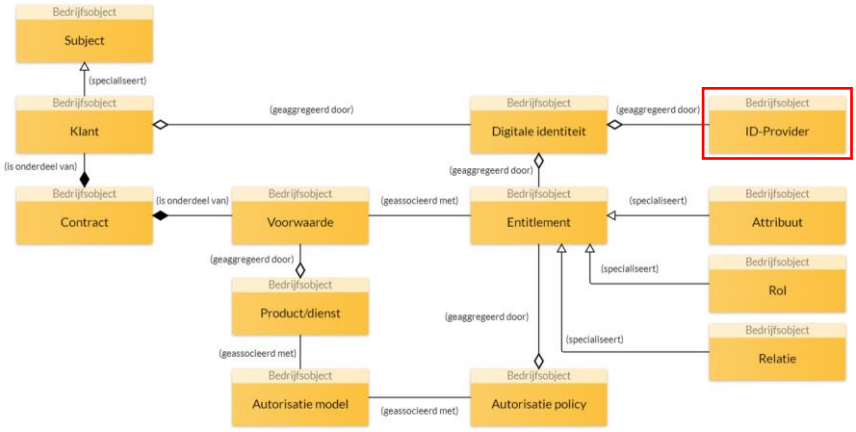


Figuur 18: account 'migratie' proces flow

Figuur 18 laat de vereenvoudigde flow zien waar Kadaster aan denkt voor de eerste stap van het transitietraject. Met het bestaande MYK, krijgt de gebruiker de mogelijkheid om in te loggen met MYK (oud), eHerkenning of het nieuwe 2FA MYK account (nieuwe ID-P). Als de gebruiker kiest voor MYK oud of eHerkenning, wordt die authenticatie uitgevoerd en de digitale identiteit in de bestaande eDir vault (store) vastgesteld op de bestaande manier. Vervolgens wordt gekeken of de gebruiker al een nieuw 2FA account heeft doordat de bestaande vault een ingevulde sleutel (foreign key) heeft met een account in de nieuwe ID-P. In dat geval kan de gebruiker niet meer met het oude MYK account inloggen en zal de gebruiker een melding krijgen dat het nieuwe account met de tweede factor gebruikt dient te worden en wordt de gebruiker vervolgens uitgelogd.
Indien de gebruiker nog geen nieuw account heeft, wordt deze gevraagd een nieuw account aan te maken tegen de nieuwe policies inclusief keuze/activering tweede factor. Verwacht wordt dat MYK Security via een API (bijvoorbeeld SCIM) een prematuur account kan aanmaken en de gebruiker vervolgens verder wordt begeleid met het aanmaak proces inclusief verificatie van emailadres en de tweede factor.

De digitale identiteiten die Kadaster nu onderhoudt zijn wel af te beelden op het doelmodel wat Kadaster voor ogen heeft met Figuur 9. De digitale identiteit wordt opgeslagen in een identity store en bewerkt door de Identity Manager en door de -maatwerk- selfservice GUI. De relatie met de ID-P wordt hier ook onderhouden. Voor eHerkenning zijn dat de identificerende kenmerken KvK-nummer en Pseudo (zie attributencatalogus stelsel elektronische toegangsdiensten). De federatie met eHerkenning is praktisch verdeeld in het authenticatieproces en het beheerproces. Het authenticatieproces betekent het kunnen kiezen van eHerkenning als inlogmiddel en de federatie flow (SAML).

Met het introduceren van een nieuwe ID-P naast de bestaande (MijnKadaster) ID-P, zal ook hiervoor een relatie moeten worden gelegd (rood kader):


Bedrijfsobject
Subject
(specialiseert)
Bedrijfsobject
Klant
(geaggregeerd door)
Bedrijfsobject
Digitale identiteit
(geaggregeerd door)
Bedrijfsobject
ID-Provider
(is onderdeel van)
(geaggregeerd door)
Bedrijfsobject
Contract
(is onderdeel van)
Bedrijfsobject
Voorwaarde
(geassocieerd met)
Bedrijfsobject
Entitlement
(specialiseert)
Bedrijfsobject
Attribuut
(geaggregeerd door)
(specialiseert)
Bedrijfsobject
Rol
Bedrijfsobject
Product/dienst
(geaggregeerd door)
(specialiseert)
Bedrijfsobject
Relatie
(geassocieerd met)
Bedrijfsobject
Autorisatie model
(geassocieerd met)
Bedrijfsobject
Autorisatie policy

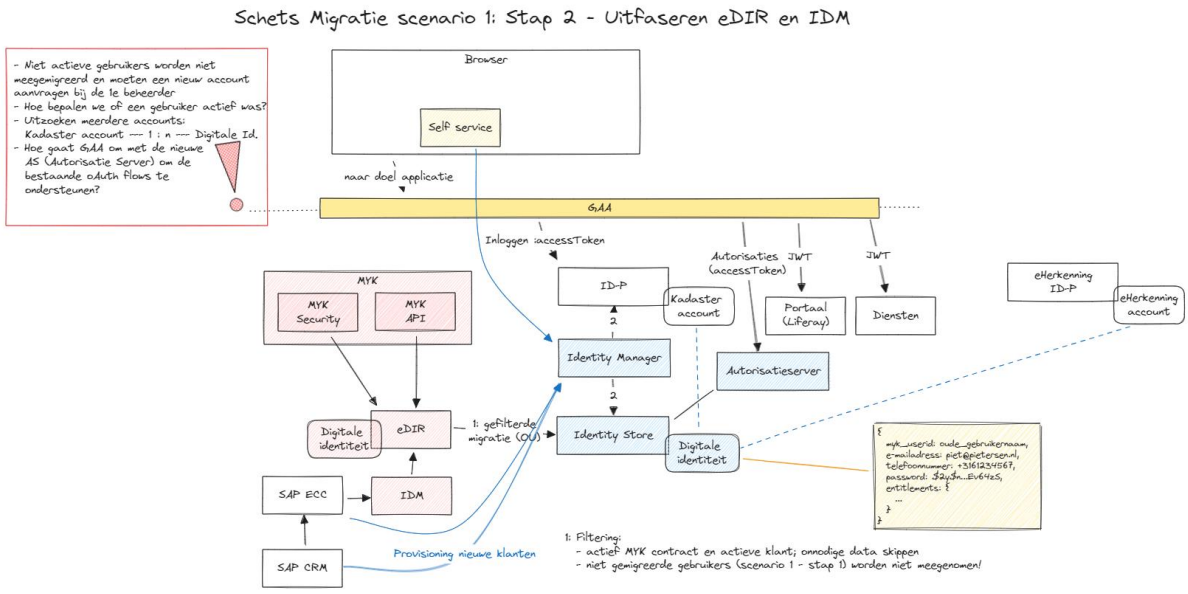
Impact beheerproces

Gebruikersbeheer
Nieuwe gebruikers krijgen geen oud MYK middel meer, maar worden binnen de bestaande beheerapplicatie binnen Mijn Kadaster (beheerder selfservice) uitgenodigd om een account aan te maken in de nieuwe ID-P. Vanuit functioneel beheer moet het dan mogelijk zijn om nieuwe accounts aan te maken, status te bekijken en accounts te verwijderen. Het account emailadres wordt een uniek gegeven. Dat betekent ook dat gebruikers van klanten geen accounts meer kunnen delen.

Account selfservice
Gebruikers die een account hebben op de nieuwe ID-P, moeten deze vanaf dat moment gebruiken en ook kunnen onderhouden
1: Aanpassen loginnaam en/of emailadres
2: Aanpassen tweede factor (TOTP, mobiel nummer, emailadres)
3: Reset wachtwoord

6.3. Stap 2: uitfaseren bestaande CIAM componenten

Met stap 2 stelt Kadaster voor om NetIQ eDir, NetID ID-M (ID Manager) en MYK Security maatwerk uit te faseren en te vervangen door de gewenste CIAM cloud oplossing. Dit is een hele forse stap, maar het naast elkaar draaien van overlappende functies in de oude en nieuwe inrichting, is al snel erg complex en raakt ook de klantprocessen wat kan leiden tot veel verwarring.



Figuur 19: Migratie/transitie stap 2; vervangen bestaande CIAM componenten

Rood gearceerde delen worden uit-gefaseerd, transparante (witte) delen aangepast of ongewijzigd en de blauwe delen zijn nieuw.

Impact beheerproces

Nieuwe ID-Store en identity schema
Gebruikers (van klanten) die nog geen account in de nieuwe ID-P hebben, worden niet gemigreerd naar de nieuwe ID-Store. Mogelijk moeten die door de beheerder opnieuw worden uitgenodigd of de klant (OU) moet volledig opnieuw onboarden. Kadaster zal vanzelfsprekend voor passende communicatie naar de klanten moeten zorgen.

Klant- en contractmanagement
Bestaande provisioning en deprovisioning flow vanuit SAP (CRM-ERP) moet worden aangepast. In de basis geldt een STP flow zoals beschreven in het doel onboardingsproces (paragraaf 5.6.1), maar bij het beëindigen en aanpassen van contracten, zal de impact op entitlements via deze route moeten lopen (dus aanpassing CRM/contract leidt tot aanpassen digitale identiteit/entitements klant). Overigens is wel de intentie om klanten aanpassingen van de overeenkomst digitaal aan te laten vragen met passende autorisatie van de aanvrager (bijvoorbeeld de beheerder van een organisatie). Op die manier kan een geautoriseerd verzoek worden behandeld door bevoegde Kadaster medewerkers en, na goedkeuring/vastlegging, leiden tot aanpassen van rechten.

Klant selfservice
MYK security wordt vervangen door selfservice functies op de nieuwe Identity Manager (ID-M) waarbij het web front-end idealiter niet wordt gewijzigd om de functionele impact voor de klant beperkt te houden. In de praktijk zal echter zo veel mogelijk gewerkt moeten worden met de standaard functies van de ID-M om maatwerk te voorkomen. Met PBAC als uitgangspunt zal gekeken moeten worden naar een hybride oplossing van het identity schema waarin afscheid wordt genomen van niet-identificerende kenmerken (zoals bijvoorbeeld adresgegevens die nu ook in de ID-Store staan) en oude entilements op basis van artikelnummers, branches en applicaterollen een substituut krijgen zodat de achterliggende nog agnostisch kunnen zijn voor de veranderingen op dit niveau zónder dat gewenste structuur van de digitale identiteit voor de toekomst teveel wordt gebaseerd op de bestaande situatie. Voorzien is dat de GAA Gateway (geel gearceerd) een belangrijke vertaalrol kan spelen in de transitie.

Impact authenticatie- en autorisatieproces
MYK-Security wordt vervangen en vormt niet meer het startpunt voor de authenticatie waardoor de keuze voor de login methode elders gefaciliteerd moet worden door de CIAM cloud services. Na keuze kan de gateway het federatieve authenticatiepad weer faciliteren.
De diensten zijn in deze fase nog niet aangesloten op de nieuwe Autorisatieserver en krijgen nog op de oude manier een een ‘GAA’ JWT gepropageerd. Dat betekent dat de gateway een transformatie rol krijgt náást de toegangsautorisatie rol.

OAuth 2 support en certificaat gebaseerde authenticatie
De Layer-7 OTK wordt zo veel mogelijk vervangen; bestaande clients die daar nu geregistreerd zijn, moeten worden geregistreerd in de nieuwe CIAM inrichting met de volgende authenticatie- en autorisatie flows:

1. Certificaat gebaseerd; mutual TLS (Digikoppeling)
2. OAuth 2 Client Credentials flow met signed JWT
3. OAuth 2 authorization code grant flow met PKCE

Zoals eerder beschreven heeft de mTLS optie niet de voorkeur van Kadaster, maar deze methode moet wel ondersteund worden zolang er voor de Digikoppeling standaard geen alternatief is. Binnen optie 2 wordt het JWT gesigned met een PKI-O certificaat waarbij het geregistreerde Client-ID en het certificaat leiden tot de uiteindelijke autenticatie waarna autorisatie kan volgen. Voor zowel optie 1 als 2 moet de aangeboden CIAM oplossing ondersteuning bieden en kunnen werken met certificaten.

6.4. Stap 3: aansluiten diensten op nieuwe access control methoden

Deze stap valt buiten de scope van het eerste deel van de herinrichting van CIAM.(implementatie plan SGC 2.1) Nadat de implementatie heeft plaatsgevonden zal er op een nader te bepalen moment in het contractperiode per dienst worden aangesloten op het nieuwe beleid en bijbehorende centrale CIAM functionaliteit met PBAC/RBAC als uitgangspunt.
De verwachting van het Kadaster is dat een overgang als hierboven aangegeven projectmatig over de diensten wordt uitgerold met een geschatte doorlooptijd van 2-4 jaren. Het projectteam wordt mogelijk versterkt met 2 specialisten van de opdrachtnemer.

6.5. Implementatie

Volgend op de migratie/transitie context (6.1 t/ 6.4) beschrijven we in deze en volgende paragrafen de implementatie en de verwachtingen en eisen die we hieraan stellen.

6.5.1. Algemeen

De implementatie zal starten na de ondertekening van de overeenkomst en bevat de volgende hoofd componenten:

- inrichten solution
- pilot nieuwe dienstverlening
- uitrol kadaster + voorbereiding verdere functionaliteiten

Zie overzicht van werkzaamheden in Figuur 20 op bladzijde 54.

6.6. Inrichting solution

6.6.1. Design en inrichten solution

Na het tekenen van de overeenkomst wordt het implementatieplan uitgewerkt op basis van het plan van de opdrachtnemer. (Zie BD SGC 2.1) In parallel wordt er gewerkt aan de solution architectuur, het concrete solution design en onderliggende werkzaamheden die input vormen voor de definitieve planningen, de teams en de deliverables.
Aansluitend zullen de componenten voor de inrichting worden opgeleverd door de verschillende teams.

6.6.2. Design en inrichten beheerorganisatie[1] (MVP)

Na het tekenen van de overeenkomst zal de beheerorganisatie en alle andere afspraken op het gebied van financiën en logistiek worden uitgewerkt in een organisatie ontwerp en worden vast gelegd in de SLA. Belangrijk is dat de taken en verantwoordelijkheden van opdrachtgever en opdrachtnemer zijn uitgewerkt. Onderdeel van deze fase is ook het trainen van de medewerkers binnen het kadaster.

6.7. Pilot nieuwe dienstverlening

Hier worden zowel de solution voor de basis inrichting als de beheerorganisatie en de support processen getest.

6.7.1. CIAM operationeel (6.1 t/m 6.3) (As-is overgezet) (MVP) (maart 2025)

Hierbij ligt de focus op het overzetten van componenten naar de SAAS solution van opdrachtnemer en het inregelen van componenten van on-boarding.

[1] De Beheerorganisatie wordt nader toegelicht in Hoofstuk 9.2 en 9.3

6.8. Operationaliseren 2FA (MVP) (bij voorkeur nov 2024)

2FA is als eerder aangegeven een belangrijke voorziening voor het Kadaster die als eerste in de nieuwe CIAM omgeving noodzakelijk is om aan de gebruikers aan te bieden. Dit mag met een tijdelijk afwijkende inrichting zijn.

6.9. CIAM volledig ingericht (MVP) voorbereid voor migratie (juni 2024)

Essentie is dat de hele solution zoals beschreven en geëist in dit PvE werkend wordt opgeleverd. Dit betreft ook de benoemde componenten tbv zero trust, consent management en verbeterde autorisatie voor het Kadaster op basis van RBAC/PBAC.(laatste 2 methoden uiteraard afhankelijk van geboden solution en het Design.) De uitrol naar de organisatie is voor de implementatie out of scope. De kosten van support voor een uitrol door de opdrachtnemer worden projectmatig uitgevraagd.

6.10. Bredere Kadaster context

Het Kadaster bevindt zich momenteel in een overgangsfase van on-premise naar cloud-gebaseerd werken. (zie ook BD 1.1.2 en 1.1.3). Deze overgang vereist aanzienlijke flexibiliteit van de organisatie, aangezien er druk staat op de trajecten die gerelateerd zijn aan zowel de overgang naar de cloud als de verbetering van toegang en beveiliging op basis van wetgeving. De opdrachtgever kan niet garanderen dat de werkzaamheden ononderbroken en volgens het voorgestelde schema verlopen, en vraagt daarom ook flexibiliteit van de opdrachtnemer. Niettemin zullen de planningen en leveringen zoals vastgelegd in het definitieve implementatieplan worden nageleefd. Het is belangrijk op te merken dat de implementatie niet aaneengesloten kan verlopen en dat de veranderingen ook afhankelijk zijn van zowel andere ontwikkelingen binnen het Kadaster als de beschikbare resources.

104.	*Wens: Inschrijver kan flexibel omgaan met een vooraf gezamenlijk vastgestelde planning. Deze kan onderbroken worden door een periode zonder activiteiten.*

In het kader van de overgang naar een cloud-gebaseerde omgeving zal het Kadaster ook gebruik gaan maken van een ander IT-leverancierslandschap. Het IT-leverancierslandschap van het Kadaster zal evolueren naar een multi-sourcing ecosysteem, waarin zowel interne als externe leveranciers gezamenlijk IT-diensten aan Kadaster-gebruikers leveren. De Kadaster Regie, die kaderstellend is en toeziet op het functioneren van het ecosysteem, maakt zelf ook integraal deel uit van dit ecosysteem. Om een optimale dienstverlening en samenwerking tussen de verschillende partijen in het zogenaamde ecosysteem te waarborgen, zullen de afspraken in de toekomst worden vastgelegd in de vorm van een samenwerkingsovereenkomst inclusief samenwerkingsdocument. Elke partij die door het Kadaster gecontracteerd wordt, wordt geacht deze samenwerkingsovereenkomst te ondertekenen en zich contractueel te committeren aan de uitgangspunten en werkwijze zoals die zijn beschreven in de samenwerkingsovereenkomst respectievelijk -document. De bestaande leveranciers, zoals opdrachtnemer op dat moment, zullen een on-boardingproces doorlopen om hun processen en werkwijzen in te passen. De afspraken die zijn vastgelegd in deze CIAM-implementatie kunnen op termijn deels worden aangepast aan de dan geldende organisatiestructuur en doelstellingen. Van de opdrachtnemer wordt verwacht dat deze zich conformeert aan deze veranderingen, waarbij eventuele extra inspanningen als betaalde changes worden behandeld.

6.11. Voorbereiding (eisen)

Opdrachtnemer is verantwoordelijk voor de Implementatie van de solution en dient dan ook de leiding te nemen bij de Implementatie van de totale Oplossing. Om inzicht te krijgen op welke wijze de Opdrachtnemer de Implementatie voorziet uit te gaan voeren, dient de Opdrachtnemer een Implementatieplan van de Oplossing te leveren, zoals beschreven in het Beschrijvend Document SGC 2.1. In het Implementatieplan dient rekening gehouden te worden met de gebruiksklare oplevering van de volledige Oplossing uiterlijk per 30-06-2024. De projectmanager van Opdrachtnemer voert de Implementatie uit in samenwerking met de projectmanager van Opdrachtgever conform het gezamenlijk akkoord gegeven Implementatieplan. De projectmanager Opdrachtgever is uiteraard verantwoordelijk voor de Kadaster inzet en opleveringen. Het gecombineerde projectmanagement rapporteert aan een Stuurgroep.
De tussentijdse oplevering van de nieuwe prioriteitsdienstverlening 2FA uiterlijk 30-11-2024 is hierin opgenomen[2].

105.	*Eis: Na akkoord tussen Partijen over het Implementatieplan wordt gestart met de uitvoering van de Implementatie.*

6.11.1. Implementatie (eisen)

De in dit PVE opgenomen eisen en wensen vormen de basis voor de op te leveren dienstverlening, maar uiteraard zal het solutiondesign meer details geven en op basis daarvan zal ook bepaald worden wanneer de implementatie op het te accepteren niveau is.
De onderstaande eisen geven richting aan de planning maar zowel opdrachtgever als nemer zijn verantwoordelijk voor het beschikbaar stellen van de juiste resources.
Voor componenten van de oplossing zal er zeker gedurende de contractperiode, of een vast te stellen periode ervan, gebruik gemaakt worden van andere partijen, dan opdrachtgever en opdrachtnemer, die solution componenten beheren. Het is duidelijk dat deze partijen participeren in implementatie van CIAM en samenwerking met opdrachtnemer noodzakelijk is.[3]

106.	*Wens: Het solution design dient uiterlijk op 01 november 2024 gereed te zijn.*
107.	*Eis: Opdrachtnemer is bereid tot overleg en samenwerking met andere partijen en hun systemen binnen de CIAM of aanpalend aan de CIAM oplossing. (ID-P broker, Identity vault, gateway etc).*

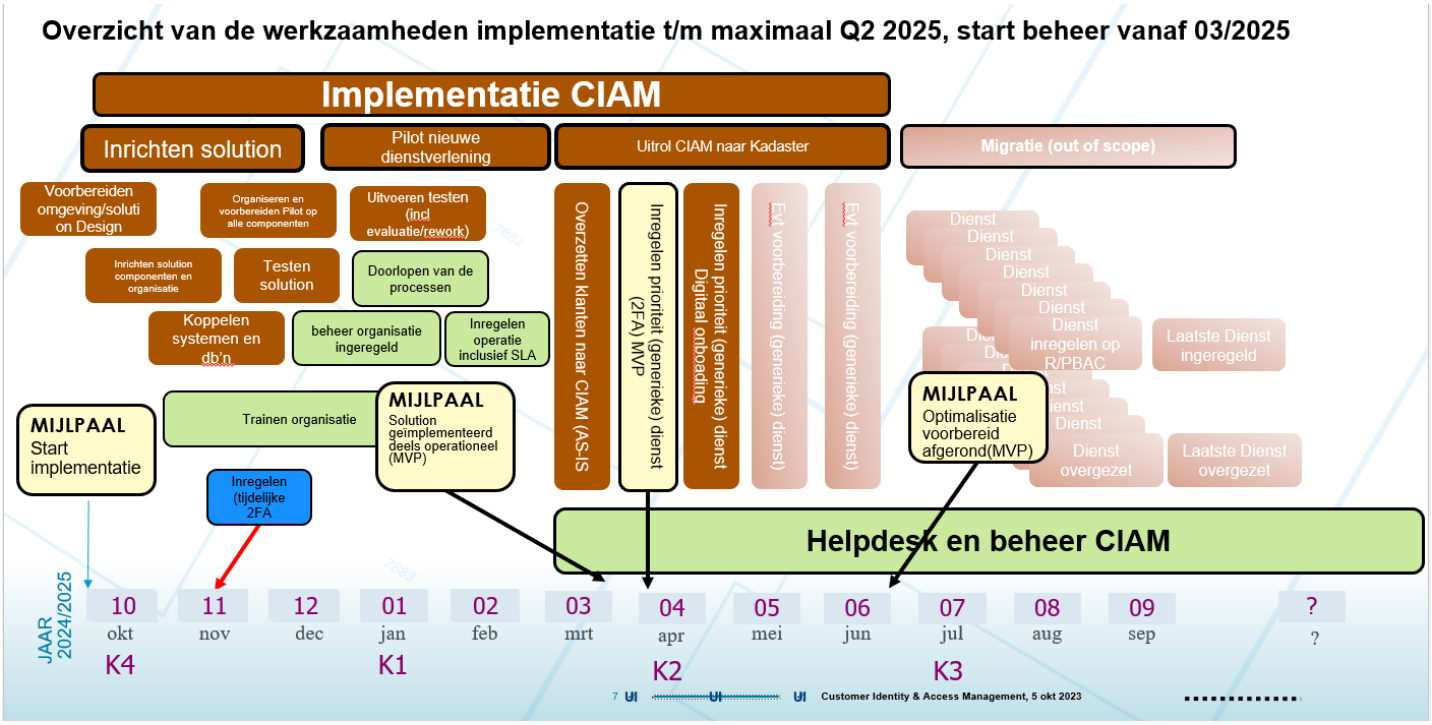
6.11.2. Acceptatie

Tijdens het opstellen van het implementatieplan wordt de acceptatie(test) vastgelegd in een acceptatie document op basis waarvan de dienstverlening wordt geaccepteerd. De test is onderdeel van het implementatieplan en zowel opdrachtgever als -nemer zijn hier akkoord mee.

108.	*Eis: Opdrachtgever voert een Acceptatietest uit inzake de dienstverlening. Voor deze test gelden de onderstaande uitgangspunten:*

[2] Uitgaande van een aaneengesloten implementatie!.
[3] Voor nadere duiding zie oa hfdst 5 van dit PvE

- *In het acceptatiedocument is specifiek aandacht voor het testen van alle geboden functionaliteiten. (ook die ter voorbereiding op latere uitrol binnen de organisatie)*
- *De Acceptatietest vindt plaats op de locatie van opdrachtgever en wordt uitgevoerd binnen de reguliere CIAM omgeving.*
- *Componenten die niet voldoen aan de acceptatie criteria worden in overleg hersteld.*
- *In overleg kunnen componenten ook later hersteld worden en wordt dit gemeld op het implementatie decharge formulier.*
- *Indien de dienstverlening in haar geheel of voor een groot deel niet functioneert kan er geen sprake van decharge op de implementatie zijn.*



Figuur 20 Implementatieverloop

Hoofdstuk 7. Non-functionals

7.1. Beschikbaarheid

De CIAM dienstverlening is cruciaal voor de opdrachtgever, dus de beschikbaarheid moet maximaal zijn.

109.	*Eis: De Beschikbaarheid van de oplossing is voor CIAM minimaal 99,90%. .*

7.2. Performance

Voor de eind-gebruiker is performance van grote invloed op de gebruikerstevredenheid.

110.	*Eis: De Inschrijver bewaakt de performance van de geleverde CIAM dienstverlening en handelt pro-actief als er sprake is van performance degradatie.*
111.	*Eis: De Inschrijver levert op verzoek performance overzichten per geleverde functionaliteit.*

7.3. Continuiteit

Continuïteit kan worden beschouwd als een aspect van Beschikbaarheid en is relevant bij een Calamiteit. De parameters welke relevant zijn voor Continuïteit zijn RPO (Recovery point Objective) en RTO (Recovery Time Objective).

112.	*Eis: Continuïteit ligt opgesloten binnen het ontwerp van de CIAM oplossing*
113.	*Eis: De RPO (Recovery Point Objective cq dataverlies) is maximaal 2 uur.*
114.	*Eis: De RTO (Recovery Time Objective cq uitvalsduur) (ook wel Hersteltijd) genoemd is maximaal 24 uur. Deze eis heeft geen betrekking op de SAAS oplossing, uitsluitend op aanvullende diensten en Kadaster specifieke solutioncomponenten.*

7.4. Bewaken van de Oplossing

115.	*Eis: De Oplossing wordt door Opdrachtnemer continue gemonitord op Beveiligingsaspecten, Capaciteit, Performance en Beschikbaarheid. In geval van afwijkingen wordt pro actief actie genomen en opdrachtgever geïnformeerd. Alle afwijkingen worden gerapporteerd in de Service Level Rapportage aan de Contractmanager van Opdrachtgever.*

7.5. Privacy en security

Opdrachtgever hanteert een strikt security- en privacybeleid en eist van partners en leveranciers zich te conformeren aan de vigerende kaders. Opdrachtgever verwerkt gegevens van particulieren en ondernemingen. Opdrachtgever is daarmee zelf ook gebonden aan wet- en regelgeving, zoals het blijven voldoen aan het gestelde in de actuele Baseline Informatiebeveiliging Overheid ('BIO/BIO2.0', de interpretatie van de ISO27001 en ISO27002 kaders) en aan de Algemene Verordening Gegevensbescherming (de 'AVG', zijnde de Nederlandse uitwerking van de Europese GDPR richtlijn). Daarnaast zal opdrachtgever moeten voldoen aan de eisen vanuit de Europese eIDAS2.0 richtlijn en de NIS2-regulering. Al deze richtlijnen zullen geldig zijn gedurende de contracttermijn van het CIAM-contract.
Het inzetten van een CIAM-component in de vorm van een SAAS-contract impliceert dat er verschillende partijen betrokken zijn, waarbij opdrachtnemer verantwoordelijk is voor conformiteit van de betrokken partijen aan deze geldende wetten en regels.

116.	*Eis: Opdrachtnemer garandeert dat de afgenomen dienst wordt geleverd conform de gestelde privacywetten en -regels, in het bijzonder dat op grond van de AVG de verwerking en opslag van gegevens plaatsvindt binnen de EU of EER.* *Ten aanzien van het conformeren aan de AVG worden in ieder geval ook bedoeld zaken rondom bewaartermijnen, de gevolgen van het intrekken van consent en de directe verwerking daarin en maatregelen voor het opleveren van AVG informatie- & verwijderverzoeken.*
117.	*Eis: Opdrachtnemer voldoet blijvend materieel aan het gestelde in de BIO, blijkend uit een overlegde actuele ISO27001 certificering of gelijkwaardig met verklaring van toepasbaarheid, met als scope de dienstverlening bestaande uit consultancy, implementatie, supportservices en beheer van CIAM-oplossingen. Deze eis geldt voor het gestelde in BIO en opvolgende versies van de BIO (lees: BIO2.0).*
118.	*Eis: Opdrachtnemer garandeert dat betrokken onderaannemers (zoals software vendors en cloud service providers) voldoen aan het gestelde in de actuele BIO, aangetoond door een actueel ISO27001 certificering of een soortgelijk bewijs van conformiteit zoals een SOC2 of daaraan gelijkgesteld certificaat.*
119.	*Eis: Opdrachtnemer toont jaarlijks aan dat de geleverde dienst wordt onderworpen aan security en vulnerability tests, blijkend uit overlegging van third party memorandums of samenvattende pentestverslagen.*
120.	*Eis: Bij beëindiging van het contract draagt opdrachtnemer zorg voor overdracht van de gegevens aan de door opdrachtgever gecontracteerde partij in een format waarmee deze partij deze gegevens ook daadwerkelijk kan gebruiken en vervolgens, mits het door de opdrachtgever bevestigende antwoord dat de gegevens vanuit de CIAM-omgeving goed en volledig zijn ontvangen, voor vernietiging van de gegevens van opdrachtgever. De vernietiging wordt aangetoond door een bewijs van vernietiging, dat door een onafhankelijke derde is getoetst en bevestigd.*
121.	*Eis: er moet door de Opdrachtnemer worden meegewerkt aan Privacy Impact Assessments (PIA's) door Opdrachtgever, en eventueel te nemen maatregelen die daaruit voortvloeien..*
122.	*Eis: er moet een samenhangende risicoanalyse voor de aangeboden CIAM-oplossing worden uitgevoerd en de resultaten daarvan dienen te worden opgevolgd. De uitkomsten worden vastgelegd en (auditeerbaar) gecommuniceerd. Evt. restrisicio's dienen door de opdrachtgever vooraf te worden/zijn geaccepteerd.*

7.6. Artificial Intelligence (AI)

Voor zover er in de aangeboden (software)oplossing c.q. inschrijving van Inschrijver onderdelen zitten met een algoritmische toepassing c.q. met AI-elementen, dan geldt het volgende:

123.	*Eis: De als gevolg van uitvoering van de opdracht user generated content mag niet gebruikt worden voor productverbetering;*
124.	*Eis: Eventueel toegepaste AI is standaard en uniform voor alle klanten en bovendien instelbaar en herleidbaar;*
125.	*Eis: binnen de op te leveren roadmaps wordt het Kadaster tijdig op de hoogte gebracht van eventuele nieuwe AI-toepassingen.*

7.7. Voorzieningen en Licenties

De leverancier is verantwoordelijk voor de dienstverlening en eventueel noodzakelijke voorzieningen hiervoor.

126.	*Eis: De werking van CIAM mag nooit belemmerd worden door beschikbaarheid voorzieningen en licentiebeperkingen. Uitgangspunt is dat de dienstverlening voor opdrachtgever beschikbaar blijft.*

7.8. Testen van de Oplossing

127.	*Eis: Wijzigingen in de Oplossing, zoals aanpassing van de configuratie door medewerkers van Opdrachtnemer of Opdrachtgever, dienen onafhankelijk van de productieomgeving door Opdrachtgever getest en geaccordeerd te kunnen worden. De Oplossing voorziet hiervoor in de juiste faciliteiten, zoals bijvoorbeeld een Testomgeving.*

7.9. Migratie kaders (re)transitie en exit

De doelstellingen voor de overgang van het einde van deze nieuwe Overeenkomst naar een volgende overeenkomst is:

128.	*Eis: Opdrachtnemer verleent algehele medewerking aan de uitvoering van noodzakelijke en door Opdrachtgever gewenste werkzaamheden en maatregelen. Dit betekent, dat leverancier indien gewenst direct zal overleggen met de toekomstige leverancier .*
129.	*Eis: Opdrachtnemer werkt mee aan het opstellen en uitvoeren van een exit/retransitieplan. In dit plan zijn de uit te voeren activiteiten, risico's, planning en de daarbij behorende kosten opgenomen.*
130.	*Eis: Gedurende de exit/retransitie periode verplicht de Inschrijver zich om de Continuïteit van de dienstverlening te borgen.*
131.	*Eis: Exit/retransitie zal jaarlijks worden besproken met het Kadaster. Opdrachtnemer levert hiervoor een geactualiseerd retransitie/exit plan op, dat inzicht geeft in de activiteiten, de planning, risico's en kosten. Tevens zal Opdrachtnemer het Kadaster waarschuwen / adviseren met betrekking tot nieuw uit te voeren werkzaamheden en/of maatregelen.*
132.	*Eis: Voorafgaande aan de daadwerkelijke exit/retransitie wordt het exitplan door beide partijen vastgesteld en vervolgens uitgevoerd in lijn met het prijzenblad.*

7.10. Toegankelijkheid

Kadaster wordt vanuit de overheid verplicht om aan de WCAG 2.1 AA richtlijn te voldoen. Dit betekent dat als de CIAM oplossing schermfunctionaliteit biedt, dat deze daar ook aan moet voldoen.

133.	*Wens: Alle GUI schermen van de CIAM oplossing dienen te voldoen aan de webrichtlijnen standaard (WCAG 2.1 AA of hoger) en in de toekomst ook aan eventuele nieuwe eisen vanuit de rijksoverheid. Heeft u een recent rapport waarin u kunt laten zien dat de schermen WCAG 2.1 AA compliant zijn?*

Hoofdstuk 8. Support

8.1. Support gerelateerd

134.	*Eis: De uiteindelijke dienstverlening m.b.t. service & support van Inschrijver voor Opdrachtgever wordt vastgelegd in een SLA tussen Inschrijver en Opdrachtgever. Deze SLA wordt opgeleverd door de Inschrijver en zal vervolgens in overleg tussen Partijen definitief worden vastgesteld. Dienstverlening zoals vastgelegd in SLA zal gebaseerd zijn op de in dit PVEW gestelde eisen aan dienstverlening en service levels.* ***Extra instructie****: Voeg een concept SLA toe aan de inschrijving aan de hand van Bijlage H.*
135.	*Eis: Support Window: De periode waarbinnen een systeem of dienst volledig wordt ondersteund door Inschrijver. Voor CIAM is dat van 9:00 tot 17:00 op Werkdagen.*
136.	*Eis: Service Window: De periode waarbinnen een systeem of dienst geleverd en gebruikt kan worden. Voor CIAM is dat 7*24. (SAAS dienst)*
137.	*Eis: CIAM ondersteunt Nondisruptive upgrade. NDU is een software-upgrade, hardware-uitbreiding en/of vervanging die geen invloed heeft op de Beschikbaarheid of Prestaties van de service. In een ideaal scenario betekent dat geen downtime, geen datamigraties en geen prestatievermindering.*

8.2. Helpdesk (CIAM)

Opdrachtgever wil gebruik kunnen maken van de helpdesk van Inschrijver.

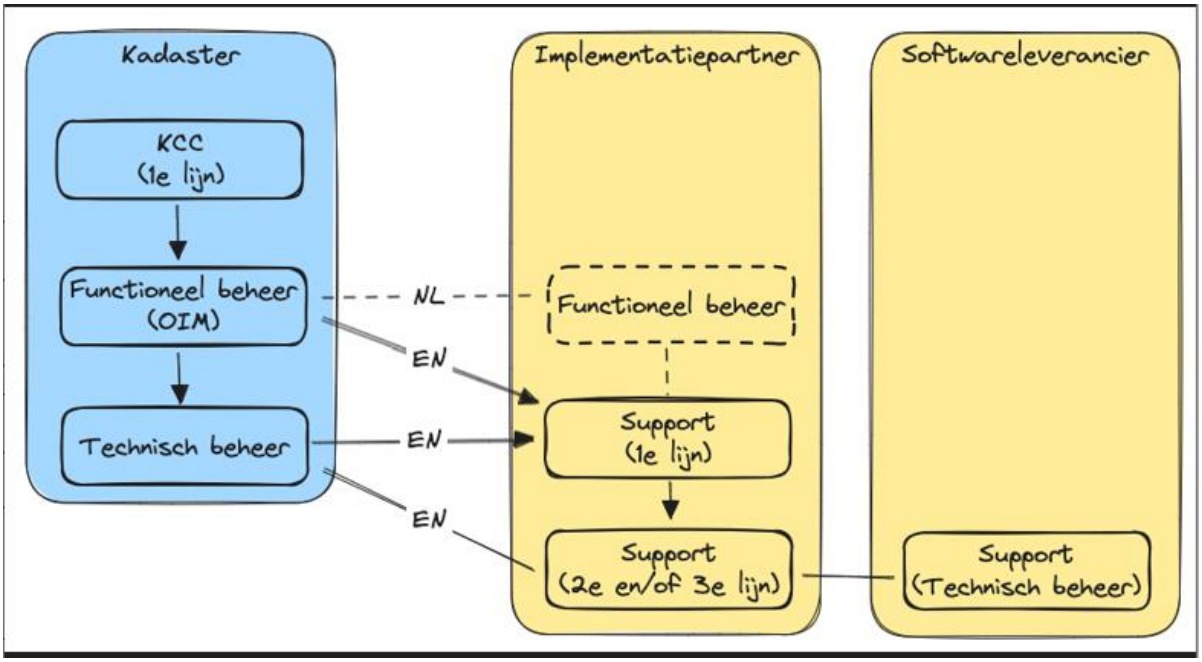
138.	*Eis: De helpdesk is minimaal zowel per e-mail als telefonisch bereikbaar*
139.	*Eis: De medewerkers van de helpdesk beheersen de Engelse taal in woord en geschrift.*
140.	*Wens: De medewerkers van de helpdesk beheersen de Nederlandse taal in woord en geschrift.*
141.	*Eis: Inschrijver levert maandelijks rapportages aan, die inzicht geven in de gerealiseerde service levels, het gebruik en de kosten.*
142.	*Eis: Maximale reactietijden :* *Prioriteit — Reactietijd* *Onmiddellijk (P1) — 30 min* *Urgent (P2) — 1 uur* *Normaal (P3) — 1 uur* *Laag (P4) — 1 uur*
143.	*Eis: De helpdesk van Inschrijver is beschikbaar voor technische en functionele CIAM vragen vanuit Opdrachtgever zonder dat daarvoor aanvullende kosten in rekening worden gebracht.*
144.	*Eis: De helpdesk van Inschrijver beantwoordt vragen binnen de Reactietijd benoemd in de SLA.*
145.	*Eis: Inschrijver verhelpt benoemde storingen binnen de Oplostijden in de SLA. Afwijkingen van deze termijnen vinden plaats in overleg en voorzien van een motivatie. De locatie van de helpdesk van de dienst is in Europa.*
146.	*Eis: Inschrijver dient over een portal te beschikken voor het melden van storingen. De status van de melding dient zichtbaar te zijn in deze portal.*
147.	*Eis: Inschrijver is in staat aan te sluiten op het ticket systeem van opdrachtgever. Kosten van koppeling via changeproces.*

8.3. 2de , 3de en 4de lijns support van opdrachtnemer

Voor deze CIAM dienstverlening is het incidentmanagement, problemmanagement, changemanagement, belegd bij de opdrachtnemer. Wel zal er in het geval van koppelingen en Kadasterinfrastructuur nauw samengewerkt moeten worden. Dit wetende zal tijdens het design van de operationele organisatie nauw samengewerkt worden. In deze context is 2de lijns support gezien vanuit de opdrachtnemer (dus na de CIAM Helpdesk van de opdrachtnemer).

In figuur 21 wordt indicatief geschetst hoe het Kadaster de support relaties ziet. Het design van de support/beheer organisatie is onderdeel van de implementatie, maar het Kadaster kent een eerste lijn die bestaat uit een helpdesk en supportspecialisten. (OIM'ers) De laatsten zullen ook deels het functioneel beheer doen. Voor de eerste lijn van het kadaster is de Nederlandse taal vereist van de medewerkers al is de verwachting niet dat er vanuit hen veel call zullen worden gedaan naar opdrachtnemer. Tijdens de implementatie is er een breder team aanwezig derhalve kan de eerste lijn van de implementatiepartner Engelstalig zijn. Hoe de verhoudingen bij de opdrachtnemer precies liggen is voor het Kadaster minder relevant. Het technisch beheer van het Kadaster zal na de implementatie uitsluitend voor ingrijpende wijzigingen in beeld komen. Engelse taal is dan standaard.

In het geval van een grote verstoring zal opdrachtgever ook een incident manager benoemen zodat samenwerking tussen partijen gegarandeerd is, mocht dat essentieel zijn.



Figuur 21 Organisatie schets

148.	*Eis: Het 2de, 3de en 4de lijns support na de helpdesk/functioneel beheer van opdrachtgever, is de verantwoording van de opdrachtnemer.*
149.	*Eis: Opdrachtnemer voorziet de Kadaster Service desk (1ste lijn) en functioneel beheer van toegang tot de CIAM Applicatie om basis werkzaamheden uit te voeren. (meekijken met de klant, volgen van incidenten/calls, eenvoudige reset handelingen)*
150.	*Eis: Opdrachtnemer voorziet de Kadaster Service desk van actuele FAQ's.*
151.	*Wens: opdrachtnemer faciliteert de opstart van het CIAM beheer door het Kadaster, waarbij functioneel beheer en service calls worden ingeregeld. Beschrijf hoe opdrachtnemer dit uitvoert.*
152.	*Wens: Service desk Kadaster kan middels een rapportage tool overzichten maken van gebruikersgroepen etc.*

8.4. Upgrades en changes

Indien er wijzigingen zijn die de dienstverleningsportfolio veranderen verwacht opdrachtgever hierover geinformeerd te worden.

153.	*Eis: Inschrijver voorziet Opdrachtgever van informatie over gewijzigde of nieuwe functionaliteiten.*
154.	*Wens: Experts van de opdrachtnemer benodigd om de gewijzigde functionaliteiten in te richten zijn op eerste verzoek maar iig binnen redelijke termijn beschikbaar.*

Hoofdstuk 9. Contractmanagement en rapportage

9.1. Contractmanagement:

Opdrachtgever is voornemens om contractmanagement binnen de kaders van de overeenkomst in te richten. Contractmanagement betreft het op tactisch en operationeel niveau managen van alle contractueel vastgelegde verantwoordelijkheden, verplichtingen, procedures, afspraken, voorwaarden en tarieven rond een bepaalde overeenkomst plus het managen van alle onduidelijkheden.

Opdrachtgever heeft haar ambitie op het gebied van contractmanagement vertaald in de navolgende activiteiten:

1. het proactief managen van alle afspraken, verplichtingen, voorwaarden, aannames, verwachtingen en doelstellingen met betrekking tot het contractueel bepaalde tussen Opdrachtgever en Opdrachtnemer;
2. het elimineren van gebreken, hiaten, onduidelijkheden en verschil van interpretatie in de onder 1 genoemde aspecten;
3. het volgens afspraak of op verzoek tijdig (laten) verschaffen van zo correct mogelijke informatie met betrekking tot status, voortgang, financiën, risico's, besluiten, acties en openstaande issues tussen Opdrachtnemer aan Opdrachtgever.
4. het organiseren, voeren en administreren van het noodzakelijke overleg tussen Opdrachtgever en Opdrachtnemer;
5. het managen van niet contractueel vastgelegde, maar voor partijen wel belangrijke aspecten of nevendoelstellingen.
6. Van inschrijver wordt verwacht als expert om minimaal 2 keer per jaar opdrachtgever te informeren over de meest recente ontwikkelingen en te bespreken wat hiervan voor het Kadaster nuttig is.

Contractmanagement kan pas tot goede resultaten leiden als betrokken partijen op een proactieve en transparante wijze invulling geven, respectievelijk bijdragen, aan deze activiteiten.

Om bovengenoemde ambitie te realiseren zal maandelijks een "contractmangementoverleg (cmo)' worden gehouden. In overleg kunnen partijen besluiten de frequentie van het overleg aan te passen. Deelnemers aan dit overleg zijn de contractmanagers van beide partijen en business vertegenwoordigers. Doel van het overleg is om contractuele afspraken te bewaken en te anticiperen op komende ontwikkelingen. Tevens worden licentie – en Service level rapportage hier besproken en vastgesteld.

155.	*Eis: Opdrachtnemer onderschrijft bovengenoemde contractmanagementactiviteiten en zal zich gedurende de contractperiode verbinden aan de samen vastgestelde uitkomsten van bovengenoemde activiteiten. Hij stelt zich daarbij meedenkend op.*

9.2. Service Level Rapportage

156.	*Opdrachtnemer levert maandelijks een service level rapportage op*
157.	*Wens: opdrachtnemer levert op verzoek een rapportage over gebruik op.*

De servicelevel rapportage bevat minimaal de volgende onderdelen dan wel informatie over:

- Management samenvatting en trendanalyse;
- Kwaliteit van de geleverde services
- Trendweergave over minimaal de afgelopen 12 rapportagecycli;
- Beschikbaarheid over de afgelopen 12 rapportagecycli;
- Aantal Incidenten, Problemen, Bevindingen van de afgelopen maand, inclusief prioriteit en Norm;
- Aantal openstaande en gesloten Incidenten, Problemen, Bevindingen van de afgelopen maand;
- Gerealiseerde Beschikbaarheid afgelopen maand;
- Aantal Incidenten die niet tijdig zijn opgelost van de laatste 12 maanden;
- Aantal Incidenten die tijdig zijn opgelost van de laatste 12 maanden;
- Overzicht van de beschikbare en/of in gebruik genomen Licenties/abonnementen;
  Maandelijkse rapportages, die inzicht geven in het gebruik van de CIAM dienstverlening
- Financiële rapportage inclusief eventuele overschrijdingen van de fair use policy;

Tevens worden volgende onderdelen verwacht indien deze van toepassing zijn:

• Status (Additionele) dienstverlening (opdrachten en/of strippenkaart). Hierbij wordt minimaal aangegeven: datum opdrachtverstrekking, startdatum, (verwachte) opleverdatum, (verwachte) acceptatiedatum, uitnutting budget;

• Gebruikersinfo (aantal Gebruikers incl. autorisatieprofielen en Deelnemers);

• Licentie gebruik (t.o.v. aantal gekochte licenties).

Hoofdstuk 10. Toegevoegde Diensten Inschrijver

In de vorige hoofdstukken zijn inhoudelijke aspecten benoemd, waarbij Opdrachtgever in dit hoofdstuk expliciet de Toegevoegde Diensten van de Inschrijver rondom CIAM wil uitvragen. Het gaat hier om diensten m.b.t. ondersteuning in inrichting, begeleiding in uitvoering, Migratie en ook Training en opleiding. We vragen hierbij werkzaamheden uit, en verantwoordelijken van de Inschrijver om dit te realiseren.

10.1. CIAM specialisten

Nadat Inschrijver de volledige technische en functionele inrichting heeft voltooid, biedt Inschrijver ondersteuning aan de Functioneel beheerders van Opdrachtgever ter overdracht van de Implementatie en verdere aanvullende functionele inrichting.
Inschrijver zorgt voor (on-site) begeleiding op de locatie van Opdrachtgever gedurende de momenten van operationalisering in de verschillende fasen.
Voor Implementatie zie hoofdstuk 6 PVEW en BD paragraaf 7.4.1.

158.	*Eis: CIAM-Specialisten van de Inschrijver configureren de CIAM-onderdelen en richten de dienstverlening in voor Opdrachtgever en zorgt voor begeleiding en uitvoering van Implementatie en Nazorg*

Mocht blijken dat een CIAM-Specialist de opgedragen werkzaamheden naar inzicht van Opdrachtgever niet naar tevredenheid uitvoert, kan Opdrachtgever deze CIAM-Specialist per direct de werkzaamheden laten beëindigen en laten uitvoeren door een andere CIAM-Specialist. Inschrijver zal dan binnen één week een anderer CIAM-specialist aanleveren.
Indien deze eveneens niet voldoet dan is Opdrachtgever gerechtigd de CIAM-specialist rechtstreeks bij de fabrikant of elders uit te vragen op kosten van Inschrijver.

159.	*Eis: CIAM-Specialist is aantoonbaar opgeleid door de fabrikant, door een verklaring van de fabrikant of certificering.*
160.	*Eis: CIAM-Specialist spreekt Nederlands of Engels op een voor goed functioneren noodzakelijk niveau.*
161.	*Eis: CIAM-Specialist heeft aantoonbare ervaring met Implementatie van CIAM in een vergelijkbare omgeving en omvang. (Aantoonbaar=de afgelopen twee jaar te hebben gewerkt met Implementatie van de aangeboden CIAM).*
162.	*Eis: De CIAM-Specialist is gedurende de hele Projectfase beschikbaar aangaande de werkzaamheden die bij zijn/haar rol horen.*
163.	*Eis: De Inschrijver draagt zorg voor de integratievraagstukken.*
164.	*Eis: De Inschrijver heeft aantoonbare ervaring met integratievraagstukken vergelijkbaar qua inrichting en omvang (aantoonbaar = de afgelopen twee jaar te hebben gewerkt met dit soort vraagstukken).*
165.	*Eis: De CIAM-Specialist wordt middels een Strippenkaart (in staffels) uitgevraagd.*
166.	*Eis: De CIAM-Specialist en/of Professional services zijn op wens van Opdrachtgever op locatie van het Kadaster beschikbaar.*

10.2. Kennispartner

Kadaster wil, voor de looptijd van het contract, ondersteund worden met kennis en kunde op het gebied van CIAM en ontwikkelingen in de markt waarbij CIAM ondersteuning kan bieden. Hiervoor zoekt het Kadaster een Kennispartner. Zie ook paragraaf 7.3 BD SGC 2.4.

10.3. Training niveau en voor wie

De Opdrachtgever wil borgen dat tijdens de Implementatie en productie-werkzaamheden ook de diverse gebruikers een passende Training ontvangen. In deze paragraaf worden algemene eisen en wensen gesteld die van toepassing zijn voor het hele CIAM inclusief de Opties tot Opdracht.

167.	*Eis: Alle gebruikers-opleidingen, Trainingen en Documentatie worden bij voorkeur in de Nederlandse taal verzorgd. Indien Nederlandse documentatie niet voorhanden is mag dit ook Engelstalig zijn.*
168.	*Eis: Inschrijver heeft voor alle onderdelen van CIAM Trainingen beschikbaar voor de verschillende rollen die nodig zijn voor CIAM (specialist, beheerder etc).*
169.	*Eis: Bij alle Trainingen dient het betreffende opleidingsmateriaal voor cursisten beschikbaar te zijn in de vorm van fysieke of digitale hand-outs/ cursusboeken of audiovisuele trainingsmiddelen welke door Opdrachtgever ingezet kunnen worden voor naslag en zelfstudie.*
170.	*Eis: Inschrijver verzorgt een Training op locatie in geval Opdrachtgever dit wenst.*

10.4. Documentatie

171.	*Eis: Inschrijver levert alle benodigde up-to-date digitale gebruikershandleidingen en soortgelijke informatie op in de Nederlandse taal. Indien specifiek technische informatie niet beschikbaar is in het Nederlands dan dient de Documentatie in het Engels gesteld te zijn. Andere talen zijn niet toegestaan.*
172.	*Eis: Inschrijver levert na Oplevering van alle door Inschrijver gerealiseerde CIAM een functionele en technische beschrijving op (koppelingen tussen de door Inschrijver geleverde systemen en de systemen en/of infrastructuur van Opdrachtgever of van derden).*

10.5. Lifecyclemanagement

Identiteits- en accountgegevens kennen een life cycle. Het is zaak dat Opdrachtnemer maatregelen neemt om ervoor te zorgen dat zorgvuldig met deze gegevens gedurende de life cycle wordt omgegaan, vooral bij het onstaan en het verwijderen/beëindigen van deze gegevens. Identiteits- en accountgegevens vallen ook onder de AVG richtlijnen. Er bestaat een nauwe relatie met klantgegevens in CRM. Wijzigingen in de CIAM gegevens moeten zoveel als mogelijk synchroon lopen met wijzigingen in CRM. Dit betekent dat als klantgegevens in CRM worden opgenomen, gemuteerd danwel verwijderd deze ook in CIAM moeten worden verwerkt indien deze wijzigingen ook de identiteitsgegevens omvat. Op dit moment gebruiken we SAP-CRM. Dit CRM systeem is end of life en zal via een aanbestedingsprocedure worden vervangen door een nieuw nog te selecteren CRM. De implementatie van dit nieuwe CRM zal plaatsvinden na gunning en implementatie van CIAM.

173.	*Wens: De CIAM ondersteunt klant data life cycle management.*

174.	*Wens: De oplossing voorziet in de synchronisatie met CRM; klantdata en identiteitsdata zijn dan complementair*

Bewaartermijnen

Voor bepaalde wettelijke doeleinden is het noodzakelijk om via logging of een vergelijkbaar mechanisme te achterhalen wat in het verleden is gebeurd. Bijvoorbeeld kan een klant vragen die inzage/toegang heeft gehad tot zijn of haar gegevens. De bewaartermijnen voor deze gegevens kunnen een aantal jaar bedragen, afhankelijk van de desbetreffende wetgeving.

175.	*Wens: CIAM ondersteunt audit trailing*

Actualiteit

Het is de bedoeling dat account gegevens van klanten op regelmatige basis worden geactualiseerd. De eerste taak ligt hiervoor bij de (eerste) beheerder van de klant. Dit moet worden ondersteund door accounts die een bepaalde termijn inactief zijn op te sporen en de gebruiker te vragen of zijn account nog nodig is, danwel de (eerste) beheerder hiervoor te benaderen. Verder is het zaak om de klant op gezette tijden te vragen om zijn gegevens te verifiëren.

176.	*Wens: CIAM ondersteunt het actueel houden van identiteitsgegevens. Kunt U toelichten op welke wijze dit gebeurt?*

Vernietiging

Bij het definitief verwijderen van identiteitsgegevens moet dit zo gebeuren dat het niet meer mogelijk is de identiteitsgegevens te raadplegen of anderszins te gebruiken.

177.	*Eis: Identiteitsgegevens dienen bij definitieve verwijdering zodanig te worden vernietigd dat het onmogelijk wordt om deze gegevens nog te raadplegen of op enige andere wijze te gebruiken.*

Hoofdstuk 11. Opdracht

11.1. Marktconformiteit

Het is voor Opdrachtgever van belang dat de inkoopprijs van Opdrachtnemer ten minste marktconform is. Onder marktconforme prijs wordt verstaan wat op een bepaald moment in de tijd voor de invulling van een specifieke behoefte de gangbare prijs is onder gelijke omstandigheden die in de markt wordt aangeboden. Marktconformiteit kan worden bepaald aan de hand van benchmarking, bijvoorbeeld het vergelijken van prijslijsten, of het opvragen van offertes.

Opdrachtgever kan een check op Marktconformiteit van de Offerte doen. Voor het vaststellen van de Marktconformiteit van de aanbieding kan Opdrachtgever een (externe) partij aanwijzen.

178.	*Eis: Opdrachtnemer onderschrijft dat de aan Opdrachtgever te leveren diensten tegen tarieven plaats vinden die ten minste marktconform of lager zijn.*
179.	*Eis: Opdrachtnemer gaat akkoord met het op Marktconformiteit laten toetsen van offertes door een derde, door Opdrachtgever aan te wijzen, partij.*

11.2. Opdrachtverstrekking n.a.v. offertetraject

Opdrachtnemer zal naar aanleiding van een Offerte-aanvraag een Marktconforme (zie voorgaande paragraaf) offerte indienen conform het door Opdrachtnemer ingevulde prijsmodel toegevoegd als Bijlage F.
Na een positieve beoordeling van de ontvangen offerte en vindt opdrachtverstrekking plaats.

Bij opdrachtverstrekking wordt een Nadere Overeenkomst gesloten met Opdrachtnemer. Onderdeel van de Nadere Overeenkomst zijn de offerteaanvraag en de Offerte van Opdrachtnemer.

Opdrachtgever stelt de Nadere Overeenkomst op conform de afspraken in de offerte-aanvraag en de Offerte.

11.3. Acceptatietest

De Opdrachtgever is bevoegd, maar niet verplicht om eisen van een opdracht te testen in een Acceptatietest, zoals ook beschreven in 6.11.2 voor de implementatie.
Verder wordt er een meer gedetailleerd acceptatieproces gevolgd voor separate opdrachten als dat door partijen is vastgelegd in de SLA.