Bijlage B1 Programma van Eisen, Wensen en Functionele vragen

Hieronder treft u de eisen en wensen aan die Opdrachtgever stelt aan Inschrijver inzake CIAM-systeem KB. Het Programma van Eisen, Wensen en Functionele vragen vormt een bijlage bij het Beschrijvend document voor de Europese Aanbesteding CIAM-systeem van de KB, hierna te noemen Opdrachtgever.

In dit Programma van Eisen, Wensen en Functionele vragen staan alle eisen, wensen en een aantal functionele vragen ten aan zien van het CIAM-systeem en de bijbehorende dienstverlening tezamen beschreven en zijn deze voorzien van inleidende of begeleidende context.

Beantwoordingsinstructie

De **eisen** zijn verplicht, dat wil zeggen, als u niet aan een eis kunt voldoen dan is uw inschrijving ongeldig. Alle eisen zijn opgesomd in een pdf-document: **Bijlage B2** Programma van eisen. Om aan te geven dat u aan alle eisen kan voldoen, dient u het Uniform Aanbestedingsdocument (UEA), opgenomen als **Bijlage L**, te ondertekenen.

De **wensen** bestaan uit gewenste functionaliteit of dienstverlening, waarop u met ‘Ja’ of ‘Nee’ kan aangeven of u deze gewenste functionaliteit of dienstverlening kan bieden. Daarnaast geeft u een korte toelichting ter onderbouwing van het Ja/Nee-antwoord. De beantwoording van de wensen kunt u doen in het Excel bestand, opgenomen als **Bijlage J**. Antwoord u met ‘Ja’, dan maakt de gewenste functionaliteit of dienstverlening van de betreffende wens daarmee onderdeel uit van de door u aangeboden oplossing of scope van dienstverlening. **Houd hier ook rekening mee in de kosten die u invult in het Prijzenblad (Bijlage I).**

Voor de beantwoording van de **functionele vragen** (deze staan ook vermeld in het Beschrijvend Document) kunt u maximaal 5 pagina’s A-4 aan tekst aanleveren in uw eigen bestand.

Beoordeling

Uw beantwoording van de **wensen** wordt als volgt beoordeeld: bij een ‘Ja’ wordt het maximaal aantal punten toegekend, mits de toelichting voldoende onderbouwt dat in de wens voorzien wordt. Bij een onvoldoende onderbouwing of een ‘Nee’ worden geen punten aan de wens toegekend. Er zijn wensen van 3 en van 6 punten. Op dit onderdeel kunnen maximaal 120 punten worden behaald.

Uw beantwoording van de **functionele vragen** wordt beoordeeld aan de hand van de beoordelingstabel uit paragraaf 5.4 van het Beschrijvend Document. Voor de antwoorden op de open vragen kunnen maximaal 80 punten worden behaald.

KB nationale bibliotheek

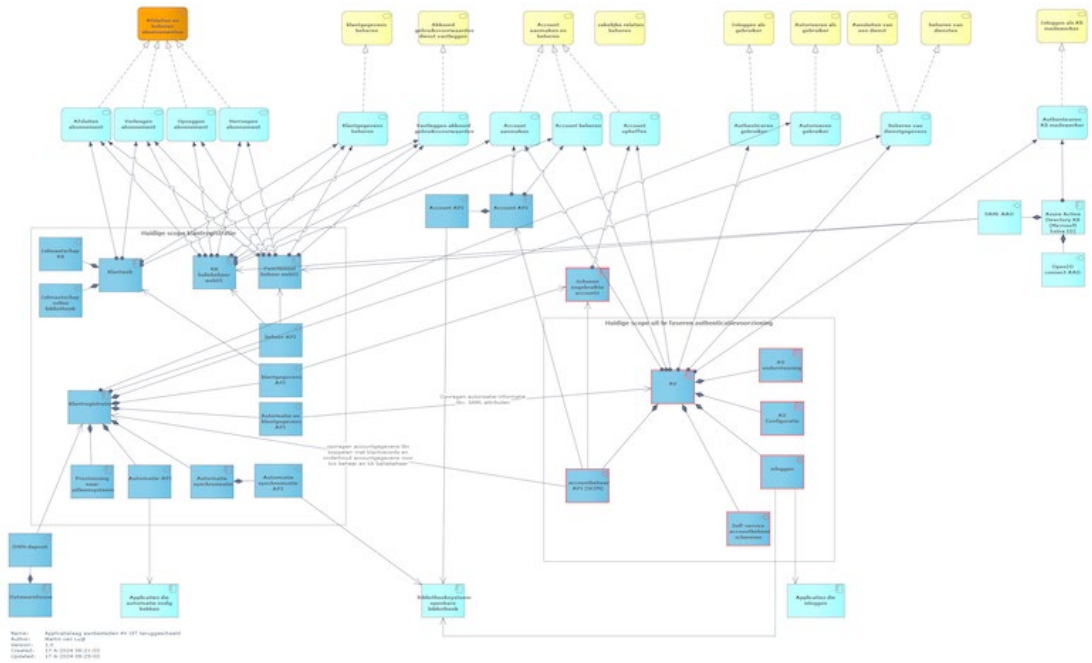
Inhoudsopgave

Inleiding 3
1. Klantgegevens & accountgegevens 5
2. Registratie (account aanmaken via selfservice) 7
3. Authenticatie 8
3.A Inloggen 8
3.B Pseudoniemen 9
4. Autorisatie 9
5. Selfservice accountcreatie en -beheer 10
6. Beheer door KB-medewerkers 12
6.A Accountbeheer 12
6.B. Monitoring op basis van logging 13
6.C. Onboarding van aan te sluiten applicaties of diensten 13
7 Dataschoning en datauitvoer 14
8. Provisioning 14
9 API's en protocollen 15
10. Implementatie & uitfasering 16
10.A. Implementatie en migratie 16
10.B. Uitfasering (exitplan) 17
11. Training, e-learning, handleidingen en overige documentatie 18
12. Performance en schaalbaarheid 18
13. Servicemanagement 20
13.A. SLA 20
13.B. Servicelevel Rapportages 21
14. Gebruiksvriendelijkheid en Toegankelijkheid 22
15. Privacy, techniek en veiligheid 23
15.A. Privacy 23
15.B. Techniek en veiligheid 24
15.C. Risicomanagement, logging, backup&restore 25
16. Juridische en overige (rand)voorwaarden 26

Inleiding

De KB wil zo laagdrempelig mogelijk toegang bieden tot haar online diensten. Daarom dient het inloggen zo eenvoudig mogelijk te zijn maar is het ook belangrijk dat zo min mogelijk gegevens benodigd zijn van de gebruiker.

Voor deze toegang gebruikt de KB momenteel twee applicaties: een Klant Registratiesysteem (KRS) en een Authenticatie Voorziening (AV). De AV is een ingekochte SaaS-dienst en verzorgt accountbeheer (via API's) en authenticatie. KRS is een zelfontwikkelde backend applicatie voor het beheren van klantgegevens, abonnementen, akkoord op gebruiksvoorwaarden en rechten op diensten. KRS verzorgt ook de dienst-autorisatie voor diensten die door de KB geleverd worden (dienstautorisatie = beslissen of een gebruiker toegang krijgt tot een dienst). Daarnaast zijn eigen userinterfaces/beheertools ontwikkeld voor selfservice en voor functioneel beheer- en klantenservicemedewerkers.

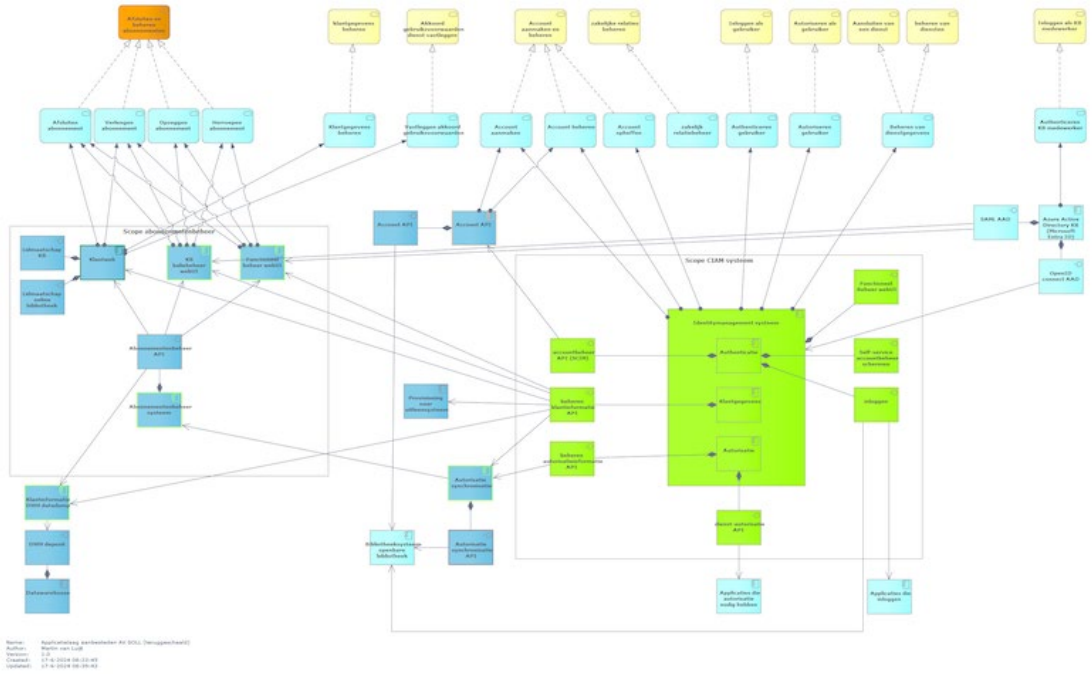


Afbeelding1: illustratie van applicatielaag in de IST-situatie, detailtekening (bijlage K) wordt toegestuurd.

De authenticatievoorziening (AV) wordt door een grote groep Nederlanders gebruikt: de KB heeft als nationale bibliotheek een regierol in het netwerk van de 140 openbare bibliotheken in Nederland en draagt zorg voor de Landelijke digitale infrastructuur, waar bijvoorbeeld de online bibliotheek onderdeel van uitmaakt.
Sinds juli 2024 is er een grote groep gebruikers van de AV bijgekomen: alle leden van de openbare bibliotheken loggen nu ook in via de authenticatievoorziening van de KB. De KB is daarmee ‘identity provider’ geworden voor al deze leden. Bibliotheekleden gebruiken deze ‘single identity’ bijvoorbeeld om in te loggen op de selfservicefuncties van hun lokale bibliotheek (zoals het online verlengen van geleende fysieke boeken). Het lokale bibliotheeksysteem

verzorgt dan de autorisatie. Maar ze kunnen ook inloggen op diensten die de KB aanbiedt. In dat geval verzorgt de KB de autorisatie van deze leden en daartoe ontvangt de KB lidmaatschapsgegevens uit alle lokale bibliotheeksystemen.

Omdat er een flinke toename is in gebruik van de authenticatievoorziening en de KB minder afhankelijk wil zijn van de beschikbaarheid van interne IT-medewerkers wil de KB meer gebruikmaken van externe applicaties en minder van eigen maatwerk. Op basis van inzichten uit de marktconsultatie in 2023, wil de KB daarom zoveel mogelijk gebruik gaan maken van een SaaS Customer Identity & Access Management (CIAM) voorziening. Deze voorziening dient dan naast de authenticatie ook de autorisatie uit te gaan voeren op basis van klantrechten/klantgegevens. Daarmee blijft alleen het Abonnementenbeheer bij de KB zelf belegd, samen met diverse (externe) koppelvlakken en enkele provisioningstromen.



Afbeelding2: illustratie van applicatielaag in de SOLL-situatie, detailtekening (bijlage K) wordt toegestuurd.

Leeswijzer

In de volgende hoofdstukken zal de gewenste functionaliteit en ondersteuning worden toegelicht met aan het eind van elke paragraaf of hoofdstuk de bijbehorende Eisen (E), Wensen (W) en Functionele vragen (F).

1. Klantgegevens & accountgegevens

Zoals eerder vermeld streeft de KB naar een zo laagdrempelige authenticatiefunctie voor haar eindgebruikers én naar dataminimalisatie. Daarom moet het inlogaccount alleen die gebruikersgegevens bevatten die nodig zijn voor het uitvoeren van de authenticatiedienst (momenteel zijn dat gebruikersnaam, wachtwoord en een contact-emailadres t.b.v. accountverificatie en -recovery). Bij elk inlogaccount moet ook een uniek ID gegenereerd worden, het 'KB-id'.

De KB zoekt een CIAM-systeem waarin naast inlogaccountgegevens ook klantgegevens bewaard en beheerd kunnen worden die nodig zijn voor autorisatie. Onder klantgegevens vallen NAW- en contactgegevens die door verschillende KB-diensten gebruikt worden, gegevens die nodig zijn voor wettelijke rapportages of om klantondersteuning te kunnen leveren (bijvoorbeeld een extern aangeleverd lidmaatschapsnummer van openbarebibliotheekleden). Het unieke KB-id is de sleutel voor de koppeling tussen de inlogaccountgegevens en de klantgegevens.

1	Type	Punten	Omschrijving
E1.1	Eis		In het CIAM-systeem moeten klantgegevens zoals (maar niet beperkt tot) NAW-gegevens en contactgegevens beheerd kunnen worden.
E1.2	Eis		De KB moet zelf kunnen definiëren welke set aan klantgegevens in het CIAM-systeem beheerd wordt.
E1.3	Eis		Deze klantgegevens zijn via een API te benaderen (CRUD- en zoek/selecteer operaties).

Optionele relatie tussen account en klantgegevens
De KB is sinds juli, naast voor haar eigen gebruikers, ook de identityprovider geworden voor alle openbarebibliotheekleden, Deze OB-leden zijn lang niet allemaal ook lid of gebruiker van diensten van de KB. Zo'n OB-lid heeft dan in het CIAM-systeem alleen een inlogaccount. Pas als dit OB-lid ook gebruik gaat maken van een KB-dienst (zoals bijvoorbeeld de online bibliotheek) worden er ook klantgegevens vastgelegd van deze gebruiker.

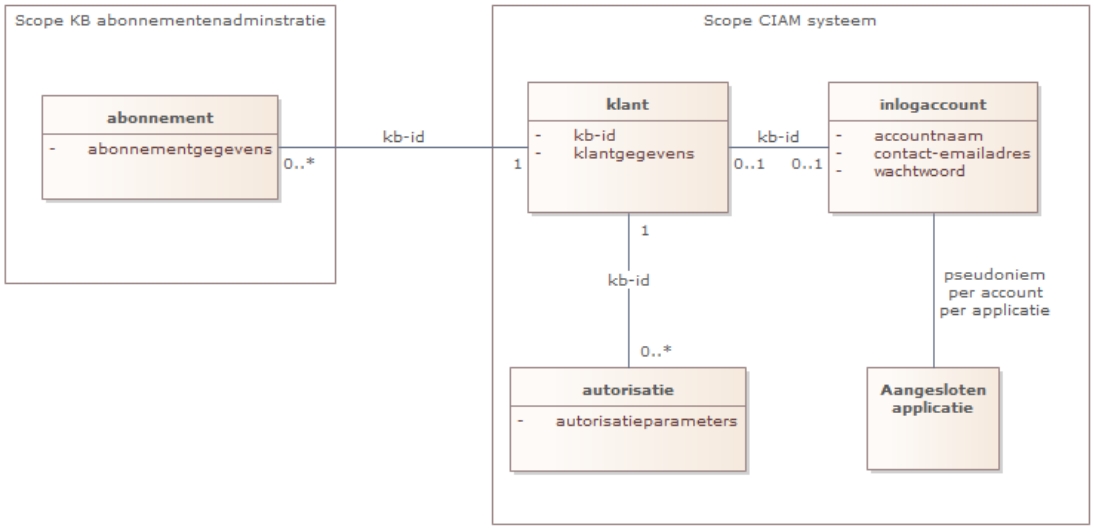
Een ander scenario is dat een gebruiker het account opheft, dan dient het mogelijk te zijn de klantgegevens te behouden. Klantgegevens verdwijnen pas als ook de klantrelatie wordt opgeheven (bijvoorbeeld door het opzeggen van het abonnement).

Daarom is een optionele relatie nodig tussen inlogaccounts en klantgegevens: bij een account **kan** een set klantgegevens horen en bij een set klantgegevens **kan** een account horen.

1	Type	Punten	Omschrijving
E1.4	Eis		In het CIAM-systeem kan een inlogaccount gekoppeld worden met de klantgegevens van een specifieke klant.
E1.5	Eis		De koppeling tussen de klantgegevens en een account kan opgeheven worden door een beheerder of als de eindgebruiker via self-service het account verwijdert. De klantgegevens blijven bestaan als het account wordt opgeheven en vice versa.

E1.6	Eis		Een account kan als zelfstandige entiteit bestaan in het CIAM-systeem. Het kan aangemaakt worden door een eindgebruiker via self-service schermen. Een eindgebruiker kan ermee inloggen op applicaties die het CIAM-systeem als authenticatiedienst gebruiken.
W1.1	Wens	6	Een account kan in ieder geval de volgende statussen te hebben: niet-gevalideerd/inactief, actief, grace (soft-deleted), geblokkeerd.

Deze constructie wordt geïllustreerd in onderstaand datamodel in de SOLL-situatie:



Name: Conceptueel datamodel CIAM tbv aanbesteding SOLL
Author: Martin van Luijt
Version: 1.0
Created: 12-3-2024 14:32:50
Updated: 12-3-2024 15:30:38

2. Registratie (account aanmaken via selfservice)

De KB zoekt een CIAM-systeem, waarbij eindgebruikers via selfservice een nieuw account kunnen aanmaken. Het is voor de KB belangrijk dat er geen verplichting is dat de gebruikersnaam een emailadres moet zijn. De reden hiervoor is dat ook jeugdleden (zonder emailadres) gebruik moeten kunnen maken van deze inlogfunctionaliteit. Naast het opgeven van een gebruikersnaam en wachtwoord wordt wel om een emailadres gevraagd als contactgegeven. Dat e-mailadres hoeft niet uniek te zijn om het mogelijk te maken dat ouders de accounts van hun kinderen kunnen beheren met een en hetzelfde e-mailadres. Het e-mailadres moet bevestigd worden als voorwaarde voor het activeren van het account.

2	Type	Punten	Omschrijving
E2.1	Eis		De eindgebruiker kan een zelfgekozen gebruikersnaam invoeren (binnen bepaalde grenzen zoals minimale en maximale lengte, karakterset).
F2.1	Funct. vraag	15	Het CIAM-systeem doet suggesties voor een gebruikersnaam indien de ingevoerde gebruikersnaam al bestaat. Dit geldt ook bij het wijzigen van de gebruikersnaam.
E2.2	Eis		De eindgebruiker kan een zelfgekozen wachtwoord invoeren dat voldoet aan het ingestelde wachtwoordbeleid van de KB (zoals minimale en maximale lengte, karakterset). Dit geldt ook bij een wachtwoordherstel of wachtwoordwijziging.
W2.2	Wens	3	Bij het invoeren van het wachtwoord wordt de eindgebruiker geholpen met het kiezen van een sterk wachtwoord (bijvoorbeeld dmv een sterktemeter).
E2.3	Eis		De eindgebruiker moet een e-mailadres invoeren, met validatie van de syntax, dat niet uniek hoeft te zijn binnen het CIAM-systeem.
E2.4	Eis		Het CIAM-systeem valideert het opgegeven e-mailadres (bijvoorbeeld middels een door het systeem verzonden e-mail met een activatielink).
W2.3	Wens	6	Het registratieproces voorziet in de mogelijkheid dat het blijft wachten tot de eindgebruiker de activatie (mogelijkerwijs op een ander device of via andere browser) heeft uitgevoerd.
E2.5	Eis		De activatielink vervalt na een ingestelde periode (bijvoorbeeld 24 uur), waarna het inactieve account door het CIAM-systeem wordt opgeruimd. Op deze wijze komt de opgegeven gebruikersnaam weer beschikbaar.
E2.6	Eis		De vervaltijd van het activatiemechanisme is configureerbaar per omgeving (TAP = TEST, ACCEPTATIE, PRODUCTIE).
E2.7	Eis		Gedurende de periode dat het e-mailadres niet is gevalideerd, kan de eindgebruiker niet inloggen.
E2.8	Eis		Het CIAM-systeem moet de return-URL van de aanroepende dienst/applicatie kunnen onthouden, om de eindgebruiker na accountregistratie terug te kunnen sturen naar de aanroepende applicatie.
W2.4	Wens	6	Als de eindgebruiker na afronding van de registratie (inclusief validatie van het emailadres) wordt teruggestuurd naar de aanroepende applicatie, dan is deze automatisch ingelogd (actieve SSO-sessie).

F2.5	Funct. vraag	15	Ingevoerde wachtwoorden (ook bij wachtwoord vergeten of wachtwoord wijzigen) worden gecontroleerd tegen een online dienst met zwakke en gelekte wachtwoorden, bijvoorbeeld haveibeenpowned.com.

3. Authenticatie

3.A Inloggen

De KB zoekt een CIAM-systeem waarbij eindgebruikers kunnen inloggen met de gebruikersnaam en het wachtwoord die ze zelf bij registratie hebben opgegeven, of met de inloggegevens die gesynchroniseerd zijn vanuit de lokale bibliotheeksystemen. Op termijn moet ook multi-factor authenticatie met standaard authenticator ondersteund worden, net als wachtwoordloos inloggen (bijvoorbeeld via een QR-code).

3A	Type	Punten	Omschrijving
E3A.1	Eis		Een eindgebruiker kan inloggen met gebruikersnaam en wachtwoord.
E3A.2	Eis		Bij onjuiste combinatie van gebruikersnaam en wachtwoord wordt een melding gegeven dat de combinatie onjuist is zonder te vermelden welke van de twee niet klopt.
E3A.3	Eis		Op het loginscherm kunnen hyperlinks naar achterliggende functies of informatie worden geplaatst en kan gewisseld worden tussen Nederlands en Engels.
E3A.4	Eis		Na succesvolle authenticatie wordt de eindgebruiker teruggestuurd naar de applicatie, waarbij voor OAuth/OIDC de redirect_uri's zijn opgenomen in een lijst met toegestane url's per aanroepende applicatie. Er zijn meerdere redirect_uri's mogelijk per aanroepende applicatie.
E3A.5	Eis		De levensduur van id-, access- en refresh tokens (OAuth/OIDC) is verschillend instelbaar, ook per omgeving (TAP).
E3A.6	Eis		Het CIAM-systeem biedt single sign-on (SSO), waarbij een eindgebruiker slechts eenmaal hoeft in te loggen voor de toegang tot alle aangesloten applicaties.
E3A.7	Eis		De duur van de SSO-sessie is instelbaar, ook per omgeving (TAP).
W3A.2	Wens	3	Applicaties kunnen uitgezonderd worden van het SSO-domein (bijvoorbeeld middels een force authentication parameter).
E3A.8	Eis		Het CIAM-systeem biedt de mogelijkheid om eindgebruikers van zowel webapplicaties als native apps te authenticeren.
E3A.9	Eis		Het CIAM-systeem ondersteunt twee soorten logout functies, namelijk een lokale logout uit de applicatie, waarbij de tokens worden opgeruimd, en een globale logout, waarbij de SSO-sessie wordt opgeruimd.

F3A.3	Funct. vraag	15	Het CIAM-systeem ondersteunt wachtwoordloos inloggen, bijvoorbeeld via het scannen van een QR-code.
W3A.4	Wens	6	Het CIAM-systeem biedt de eindgebruiker de mogelijkheid om in te loggen met een tweede factor via een app op een mobiel apparaat. De koppeling van het account aan de tweede factor geschiedt in een veilig registratieproces.
W3A.5	Wens	3	Het CIAM-systeem biedt de mogelijkheid om onderdeel te zijn van een federatie, zodat ook geauthentiseerde eindgebruikers van federatieve IdP's (bijv. SURF) toegang kunnen krijgen tot aan het CIAM-systeem gekoppelde applicaties.
W3A.6	Wens	3	Op het inlogscherm wordt getoond voor welke applicatie de eindgebruiker op dat moment probeert in te loggen.

3.B Pseudoniemen

De KB wil niet dat derde partijen een profiel van haar eindgebruikers kunnen opbouwen door over applicaties heen gegevens van de eindgebruiker te koppelen. Daarom dient het CIAM-systeem per eindgebruiker per op het systeem aangesloten applicatie een pseudoniem te genereren. Deze functionaliteit gaat over verschillende identifiers en niet over verschillende accounts per gebruiker: aan een en hetzelfde account worden meerdere identifiers in de vorm van pseudoniemen gekoppeld. Als een eindgebruiker dus op tien verschillende applicaties heeft ingelogd, dan zijn er tien verschillende pseudoniemen aan het account gekoppeld in het CIAM-systeem.

3B	Type		Omschrijving
E3B.1	Eis		Het CIAM-systeem genereert voor elk account een identifier in de vorm van een pseudoniem voor elke applicatie waarop de eindgebruiker inlogt.
E3B.2	Eis		De pseudoniemen wijzigen niet bij wijziging van account- of klantgegevens.
E3B.3	Eis		Als een applicatie (op basis van een access token) informatie over de eindgebruiker opvraagt, dan wordt dit pseudoniem aan de applicatie doorgegeven als identifier van de gebruiker.
E3B.4	Eis		Het pseudoniem kan ook onderdeel zijn van een SAML- of id-token.

4. Autorisatie

Aan toegang tot diensten die door de KB geleverd worden zijn doorgaans voorwaarden gebonden. Soms is dat alleen een akkoord op de gebruiksvoorwaarden, soms is dat (ook) een geldig abonnement. Het systeem moet een gebruiker kunnen autoriseren door te bepalen of deze gebruiker ook bepaalde rechten heeft.

4	Type		Omschrijving
E4.1	Eis		Het CIAM-systeem kan alle gegevens vastleggen die nodig zijn om een eindgebruiker wel of geen autorisatie te geven voor een aangesloten dienst.
E4.2	Eis		Nieuwe of gewijzigde autorisatiegegevens kunnen via API's worden doorgegeven aan het CIAM-systeem.
E4.3	Eis		Het CIAM-systeem bevat een autorisatiefunctie waarmee de aangesloten applicatie of dienst autorisatie opvraagt.
E4.4	Eis		De autorisatieregels/business rules kunnen per aangesloten applicatie of dienst verschillen.
E4.5	Eis		Een Functioneel Beheerder kan autorisatieregels per dienst beheren.

5. Selfservice accountcreatie en -beheer

Gebruikers moeten via selfservice hun wachtwoord opnieuw kunnen instellen of hun gebruikersnaam kunnen opvragen. De link naar deze functie is beschikbaar op het loginscherm. Na inloggen kunnen gebruikers hun account via selfservice beheren.

5	Type	Punten	Omschrijving
W5.1	Wens	3	Het CIAM-systeem biedt selfservice schermen waarmee de eindgebruiker diens eigen klantgegevens kan onderhouden.
5A	**Type**	**Punten**	**Wachtwoord of gebruikersnaam vergeten**
E5A.1	Eis		De eindgebruiker kan voor wachtwoordherstel de gebruikersnaam invullen, waarna het CIAM-systeem een notificatie stuurt naar het bij het account geregistreerde contactgegeven.
E5A.2	Eis		De notificatie van het systeem bevat een link naar het wachtwoordherstelscherm, waar de eindgebruiker een nieuw wachtwoord kan instellen.
W5A.1	Wens	3	Na invoeren van het nieuwe wachtwoord, wordt een knop getoond om door te gaan naar het loginscherm.
W5A.2	Wens	3	Na succesvolle authenticatie wordt de eindgebruiker doorgestuurd naar de applicatie of dienst, waar die vandaan kwam.
E5A.3	Eis		Vanaf het loginscherm kan de eindgebruiker, met behulp van diens contactgegeven behorend bij het account, de gebruikersnaam opvragen. De gebruikersnaam wordt op een veilige en vertrouwelijke manier met de eindgebruiker gedeeld.
5B	**Type**	**Punten**	**Gebruikersnaam wijzigen**
E5B.1	Eis		Na inloggen op de selfservice accountbeheer functie, kan de eindgebruiker diens gebruikersnaam wijzigen in een zelfgekozen andere

			gebruikersnaam, waarbij dezelfde eisen aan de gebruikersnaam gelden als bij registratie.
E5B.2	Eis		Na wijziging van de gebruikersnaam heeft de eindgebruiker nog steeds een actieve sessie.
5C	**Type**	**Punten**	**Wachtwoord wijzigen**
E5C.1	Eis		Na inloggen op de selfservice accountbeheer functie, kan de eindgebruiker diens wachtwoord wijzigen, waarbij dezelfde eisen aan het wachtwoord gelden als bij registratie en wachtwoord vergeten.
E5C.2	Eis		Na wijziging van het wachtwoord heeft de eindgebruiker nog steeds een actieve sessie.
5D	**Type**	**Punten**	**E-mailadres wijzigen**
E5D.1	Eis		Na inloggen op de selfservice accountbeheer functie, kan de eindgebruiker diens bij het account behorende e-mailadres wijzigen.
E5D.2	Eis		De syntax van de invoer wordt gecontroleerd en moet voldoen aan die van een e-mailadres.
E5D.3	Eis		Het nieuwe emailadres wordt geverifieerd (bijvoorbeeld middels een door het systeem verzonden e-mail met een activatielink die na een ingestelde periode vervalt).
E5D.4	Eis		Indien de activatielink ongebruikt vervalt, dient de e-mailadreswijziging te vervallen en het oude e-mailadres teruggezet te worden.
5E	**Type**	**Punten**	**Account verwijderen**
E5E.1	Eis		Na inloggen op de accountbeheerfunctie kan de eindgebruiker diens account via selfservice verwijderen.
E5E.2	Eis		Bij het verwijderen van een account (via selfservice) wordt een melding getoond met de vraag of de eindgebruiker het zeker weet en een tekst met uitleg van de consequenties en de optie om door te gaan of te annuleren.
E5E.3	Eis		Het account wordt op dat moment nog niet definitief uit het CIAM-systeem verwijderd, maar krijgt een status in de trant van 'grace/soft deleted'.
E5E.4	Eis		Na een instelbare periode wordt het account alsnog definitief uit het CIAM-systeem verwijderd.
F5E.1	Funct. vraag	10	Het CIAM-systeem biedt eindgebruikers die hun account hebben verwijderd, de mogelijkheid om binnen een te configureren termijn het account te herstellen, bijvoorbeeld met hun tweede factor authenticatie (indien 2FA is geïmplementeerd uiteraard).

6. Beheer door KB-medewerkers

Binnen het CIAM-systeem moeten gegevens niet alleen door eindgebruikers zelf maar ook door KB-medewerkers kunnen worden beheerd.

6.A Accountbeheer

Bij het accountbeheer door medewerkers van de KB moet onderscheid gemaakt kunnen worden in verschillende beheerrollen met verschillende rechten. Bijvoorbeeld: wie mag accounts aanmaken of verwijderen, wie alleen inzien of aanpassen, wie mag rapportages uit het systeem opvragen, etc. Dit moet ook instelbaar zijn op verschillende niveaus: een Klantenservicemedewerker beheert 1 klantrecord tegelijk, een Functioneel Beheerder kan meerdere klantrecords (selecties) beheren en voor sommige medewerkers is read-only van 1 klantrecord voldoende.

De toegang tot deze ondersteuning- en beheertaken in het CIAM-systeem moet goed te beveiligen zijn om ongeautoriseerd gebruik uit te sluiten.

6A	Type	Punten	Omschrijving
W6A.1	Wens	3	Het CIAM-systeem levert een grafische gebruikersinterface voor Functioneel Beheer en Klantenservicemedewerkers.
E6A.1	Eis		Een Functioneel Beheerder kan in het CIAM-systeem verschillende beheerrollen met verschillende beheerrechten/ autorisaties configureren en toewijzen of intrekken.
E6A.2	Eis		Een Klantenservicemedewerker kan gebruikersaccounts en -gegevens zoeken en sorteren. Hierbij kan gezocht of gefilterd worden op alle velden van een gebruikersaccount en van de klantgegevens.
E6A.3	Eis		Een Klantenservicemedewerker kan een account, accountstatus, autorisatiegegevens en klantgegevens bewerken en verwijderen.
E6A.4	Eis		Een Klantenservicemedewerker kan de status van een account wijzigen, bijvoorbeeld door een door een eindgebruiker verwijderd account met ‘grace/soft-deleted’ status weer actief te maken, zodat er weer mee kan worden ingelogd.
E6A.5	Eis		Een Klantenservicemedewerker heeft de mogelijkheid om een account te verbinden met, of te ontkoppelen van, de klantgegevens van een specifieke eindgebruiker.
E6A.6	Eis		Een Functioneel Beheerder kan dezelfde gegevensbewerkingen doen als de Klantenservicemedewerker, maar dan in bulk.
E6A.7	Eis		Een Functioneel Beheerder kan gebruikersaccounts en klantgegevens aanmaken, bewerken en verwijderen in bulk (onder andere, maar niet beperkt tot testdata).

6.B. Monitoring op basis van logging

Naast accountbeheer moeten Functioneel Beheerders ook toegang hebben tot functionele/ informatieve logging.

6B	Type	Punten	Omschrijving
E6B.1	Eis		Het CIAM-systeem biedt een Functioneel Beheerder informatie over de huidige performance en eventuele verstoringen (actueel en historisch).
W6B.1	Wens	3	Het CIAM-systeem stuurt een Functioneel Beheerder een notificatie wanneer er performance issues of verstoringen zijn.
W6B.2	Wens	3	Een Functioneel Beheerder kan de notificaties die het CIAM-systeem verstuurt naar de eindgebruikers tekstueel aanpassen.
W6B.3	Wens	3	Een Functioneel Beheerder kan een onderhouds- of storingsmelding plaatsen (of laten doen) en wijzigen bij onderhoud of problemen.
W6B.4	Wens	3	Het CIAM-systeem biedt een instelbaar logniveau, zonder serviceonderbreking.
W6B.5	Wens	3	Het CIAM-systeem biedt een Functioneel Beheerder de mogelijkheid de loggegevens in te zien en downloaden.
W6B.6	Wens	3	Bij het opvragen van de logging zijn minimaal de volgende filtermogelijkheden beschikbaar: 1. Op basis van aangesloten applicatie 2. Op basis van eindgebruiker-ID 3. Op basis van IP-adres van een eindgebruiker 4. Op basis van tijdsperiode

6.C. Onboarding van aan te sluiten applicaties of diensten

Tot slot moet het via functioneel beheer mogelijk zijn de diensten/applicaties van (soms externe) leveranciers eenvoudig te onboarden zodat ze met behulp van het CIAM-systeem kunnen authenticeren.

6C	Type	Punten	Omschrijving
W6C.1	Wens	6	Onboarding van diensten: Een Functioneel Beheerder kan een serviceprovider middels configuratie en zonder maatwerk aansluiten op het CIAM-systeem.
W6C.2	Wens	6	De Leverancier van een aan te sluiten dienst kan het onboardingsproces via een self-service mechanisme voorbereiden zodat het minder bewerkelijk is voor de functioneel beheerder van de KB.

7 Dataschoning en datauitvoer

Accounts moeten conform de GDPR/AVG automatisch opgeschoond kunnen worden volgens door KB op te stellen regels.

7A	Type	Punten	Omschrijving
E7A.1	Eis		Het CIAM-systeem voert geautomatiseerde opschoning uit op gegevens die voldoen aan de criteria om te mogen worden verwijderd (tenminste op basis van verstreken tijd sinds de laatste succesvolle inlogpoging). De criteria zullen worden aangeleverd door de KB.
W7A.1	Wens	3	Het CIAM-systeem biedt de mogelijkheid om opschoning van accounts te doen (mede) op basis van gegevens uit een ander KB-systeem via een bestandsimport of API.

Daarnaast kan alle account-, rechten- en klantdata regelmatig worden aangeleverd aan het datawarehouse van de KB zodat de wettelijke rapportagetaken uitgevoerd kunnen worden.

7B	Type		Omschrijving
E7B.1	Eis		Het CIAM-systeem moet in staat zijn de gehele set aan eindgebruikersgegevens, exclusief wachtwoorden, op regelmatige basis aan te leveren aan het datawarehouse van de KB.
E7B.2	Eis		Een Functioneel Beheerder moet in staat zijn selecties van eindgebruikersgegevens te exporteren ten behoeve van analyse en rapportages.
E7B.3	Eis		Bij data uitvoer of data duplicatie moet het mogelijk zijn gegevens (deels) te anonimiseren.

8. Provisioning

De KB zoekt een CIAM-systeem dat aangesloten diensten kan provisionen met gebruikersgegevens. Dit is onder andere nodig bij de registratie van KB-leden in het KB-bibliotheeksysteem.

8	Type	Punten	Omschrijving
E8.1	Eis		Het CIAM-systeem heeft een voorziening om klantgegevens van een subset van de klanten realtime door te geven aan een extern systeem, bijvoorbeeld NAW-gegevens en een identifier van eindgebruikers aan bijvoorbeeld het bibliotheeksysteem van de KB.

9 API’s en protocollen

De KB zoekt een leverancier die alle klantgegevens en aansluitconfiguraties via een API kan laten bewerken. Bijvoorbeeld ten behoeve van KB-beheerapplicaties en applicaties van derden die de KB ontsluit. We volgen de relevante richtlijnen van de Nederlandse overheid en we gebruiken waar mogelijk open standaarden. Voor zover beschikbaar bouwen we op (industrie)standaarden. Dat zijn voor inloggen minimaal OpenID Connect, OAuth 2 en SAML 2.

9	Type	Punten	Omschrijving
E9.1	Eis		Alle API's, met uitzondering van de API's waarvoor we een specifieke standaardvragen, werken volgens het REST/JSON principe.
E9.2	Eis		Het CIAM-systeem ondersteunt volgens het OAuth 2.0 protocol gekoppelde applicaties.
E9.3	~~Eis~~		Vervallen ~~Het NL GOV Assurance profile for OAuth 2.0 wordt ondersteund (https://www.forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oauth-20)~~
E9.4	Eis		Het CIAM-systeem ondersteunt volgens het OpenID Connect protocol gekoppelde applicaties.
E9.5	~~Eis~~		Vervallen ~~Het NL GOV Assurance Profile for OIDC wordt ondersteund (https://www.forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oidc)~~
E9.6	Eis		Het CIAM-systeem ondersteunt volgens het SAML 2.0 protocol gekoppelde applicaties
W9.1	Wens	6	Het CIAM-systeem bevat een SCIMv2 API voor CRUD-operaties op gebruikersgegevens

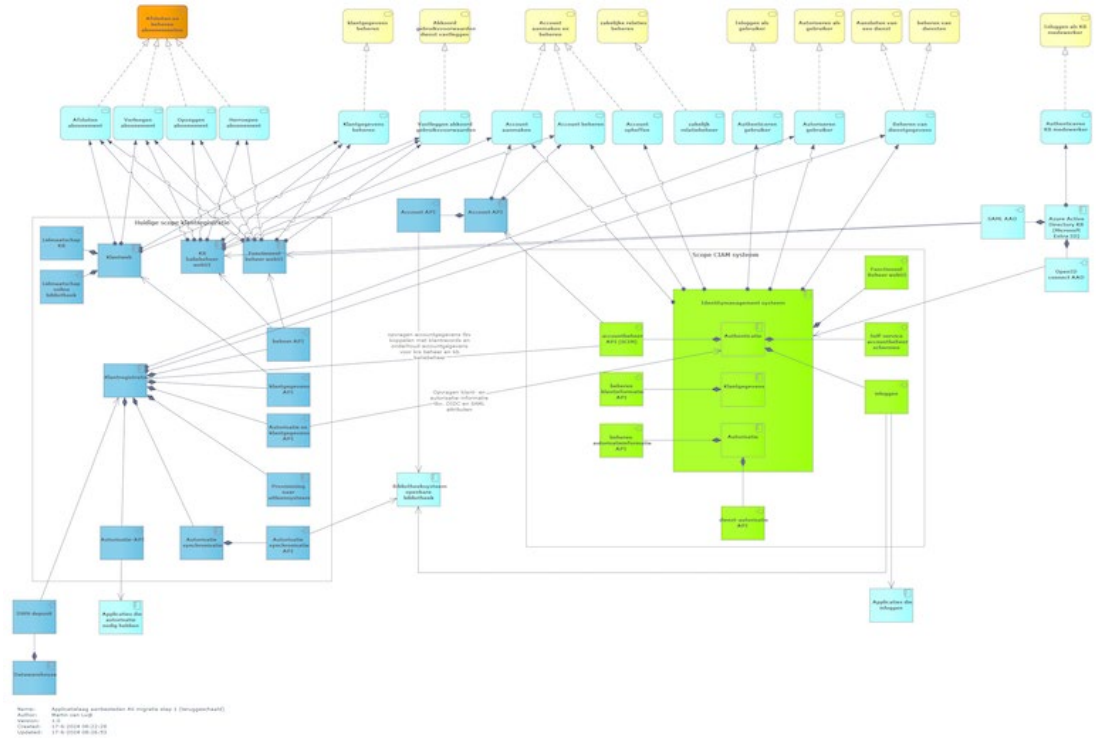
10. Implementatie & uitfasering

10.A. Implementatie en migratie

De KB wenst een gedegen implementatie en migratie waarbij de eindgebruikers van de authenticatie- en autorisatie functionaliteit geen tot minimale hinder ondervinden en waarbij zekerheid wordt geboden dat het platform per 1 januari 2026 volledig functioneel is. Volledig functioneel wil hier zeggen dat alle beoogde functies van de CIAM-voorziening geaccepteerd en bruikbaar zijn voor de eindgebruikers en beheerders, inclusief een volledige migratie van de huidige accounts en klantgegevens en van de aangesloten applicaties of diensten naar de nieuwe CIAM-voorziening.

Daarbij gelden de volgende randvoorwaarden:

- De KB wil eerst de authenticatiefunctie van het CIAM-systeem in gebruik nemen (uiterlijk 12 maanden na gunning). In een latere fase of fasen worden klantinformatie en de autorisatiefunctie in gebruik genomen. De situatie op applicatielaag-niveau na de eerste fase zou dan de volgende zijn:



Afbeelding3: illustratie van applicatielaag na fase 1, detailtekening wordt toegestuurd.

- Vanwege het grote aantal (externe) aangesloten applicaties/diensten, moet de migratie van de authenticatiefunctie op één moment in de tijd (dus niet gefaseerd) gebeuren.
- De Inschrijver is verantwoordelijk voor de migratie van de accounts en de (big-bang) overgang van de aangesloten applicaties of diensten, zie bijlage Q (te verkrijgen na het tekenen van een geheimhoudingsverklaring). De KB verzorgt de eventueel benodigde aanpassingen van de aansluitingen op de (SCIM) API.

10A	Type		Omschrijving
E10A.1	Eis		Inschrijver zorgt binnen 3 maanden na gunning voor een met de KB afgestemd migratie- en implementatieplan dat gericht is op een efficiënte en effectieve implementatie van de authenticatiefunctie in het CIAM-systeem waarvan de ingebruikname uiterlijk 6-9 maanden na gunning plaatsvindt.
E10A.2	Eis		De Inschrijver biedt naast een Productieomgeving ook een Test en een Acceptatie-omgeving waarlangs nieuwe releases in overleg met de KB worden gedeployed.
E10A.3	Eis		Inschrijver stelt, na de ingebruikname van de authenticatiefunctie, met de KB een plan op voor het (eventueel in een aantal fasen) verplaatsen van de klantgegevens en de autorisatiefunctie naar het CIAM-systeem.
E10A.4	Eis		Ten behoeve van verdere integraties of toepassingen ná de bovenstaande implementaties, biedt de Inschrijver op verzoek van de KB kennis en assistentie voor veranderingen in het gebruik van het CIAM-systeem.

10.B. Uitfasering (exitplan)

De KB zoekt een Inschrijver die kan voorzien in een effectieve, gefaseerde exit strategie van het CIAM-systeem en de KB aan het einde van het contract helpt om over te stappen op een volgende oplossing. Het exitplan beschrijft de wijze waarop de dienstverlening van de Inschrijver wordt beëindigd.

10B	Type		Omschrijving
E10B.1	Eis		Inschrijver verklaart dat hij bij het beëindigen van de overeenkomsten bereidwillig medewerking zal verlenen bij een soepele overgang van de dan bestaande dienstverlening naar de KB en/of een (nieuwe) contractpartij, waarover geen extra kosten in rekening kunnen worden gebracht bij de KB, anders dan de exitkosten die vermeld kunnen worden in het Prijzenblad.
E10B.2	Eis		Het exitplan wordt initieel opgesteld door de Inschrijver voorafgaand aan de ingebruikname van het CIAM-systeem. Het exitplan wordt periodiek herzien en indien relevant geactualiseerd. Periodiek is (minimaal) jaarlijks of wanneer de situatie daartoe aanleiding geeft.
E10B.3	Eis		Het exitplan bevat een gedetailleerde weergave van alle uit te voeren activiteiten om de exit transitie tot een succes te maken. Dit omvat ondermeer de wijze waarop Inschrijver zorgdraagt dat Opdrachtgever (of een door de Opdrachtgever aangewezen derde partij) de beschikking krijgt over de in de Oplossing opgeslagen gegevens en eventuele documenten.
E10B.4	Eis		De doorlooptijd van de exit transitie is (maximaal) 3 maanden na de aanvang van de transitie.
E10B.5	Eis		Na afsluiting van de exit transitie zal door Inschrijver de gehele omgeving worden 'geschoond', met andere woorden alle gegevens worden vernietigd/verwijderd, inclusief backups. Inschrijver levert hier bewijs van en zal op geen enkele wijze gegevens of informatie

			achterhouden. De geheimhoudingsplicht van de Inschrijver blijft ook na de exit transitie bestaan.
E10B.6	Eis		Inschrijver houdt rekening met een minimale overgangstermijn van 6 maanden na contracteinde. In deze periode behoudt de KB het recht om het CIAM-systeem op die wijze te gebruiken zoals deze zich op de datum van contracteinde voordeed. Hiermee wil de KB borgen dat eventueel lopende procedures afgerond kunnen worden en dat bij implementatie van een opvolgend CIAM-systeem op de informatie teruggevallen kan worden. De aanvullende kosten hiervoor worden bij de prijstelling opgenomen.

11. Training, e-learning, handleidingen en overige documentatie

De Inschrijver zorgt voor training en documentatie voor verschillende rollen binnen de KB, inclusief een trainingsaanpak. Er dienen 2 groepen getraind te worden: één groep van functioneel beheerders, productowner en productmanager (max 10 personen) en één groep van klantenservicemedewerkers (maximaal 20 personen).

11	Type	Punten	Omschrijving
E11.1	Eis		De Inschrijver voorziet in trainingsmateriaal en documentatie op basis waarvan softwareontwikkelaars van de KB (en van KB-partners) aansluitingen kunnen maken op het CIAM-systeem.
E11.2	Eis		De Inschrijver voorziet in trainingsmateriaal en documentatie geschikt voor de Functioneel Beheer rol.
E11.3	Eis		De Inschrijver voorziet in trainingsmateriaal en documentatie geschikt voor de Klantenservicerol.
F11.1	Funct. vraag	10	Inschrijver zorgt voor een trainingsaanpak en opleiding van beheerders en klantenservicemedewerkers.

12. Performance en schaalbaarheid

Het CIAM-systeem is hét inlogsysteem voor de eindgebruikers van de KB en van alle openbare bibliotheken. Het wordt daarom gevoed met klantgegevens en autorisatie-informatie vanuit de ledenadministratiesystemen van alle lokale openbare bibliotheken. Dit betekent dat het systeem miljoenen accounts, inlogpogingen en API-requests aan moet kunnen.

Een aanzienlijk deel van de eindgebruikers van de openbare bibliotheken maakt ook gebruik van de landelijke diensten van de KB, waar we klantinformatie voor bewaren en waar we autorisaties voor doen. Er wordt de komende jaren een groei voorzien in aantal gebruikers (en daarmee in aantal accounts en inlogpogingen) én in het aantal aangesloten diensten of applicaties (en daarmee in het aantal API-requests).

Omschrijving	Huidige omvang	Geschatte maximale omvang
Accounts	4,5 miljoen	8 miljoen
Actieve accounts	500.000-700.000	1.000.000-2.000.000
Inlogpogingen	100 miljoen per jaar	200 miljoen per jaar
Piekbelasting inloggen	50 per seconde	100 per seconde
API requests (anders dan inloggen)	10 miljoen per jaar	20 miljoen per jaar
Piekbelasting API requests	50 per seconde	75 per seconde
Zwaartepunt belasting API requests	1 miljoen/24h rond de maandovergangen	1 miljoen/24h rond de maandovergangen
Aangesloten diensten	70	150+

12	Type		Omschrijving
E12.1	Eis		Het CIAM-systeem moet kunnen omgaan met 4 tot 8 miljoen eindgebruikers/klantaccounts.
E12.2	Eis		Het CIAM-systeem moet kunnen omgaan met 100 tot 150 miljoen inlogpogingen per jaar doen.
E12.3	Eis		Het CIAM-systeem moet kunnen omgaan met 10-20 miljoen API requests per jaar.
E12.4	Eis		Het CIAM-systeem moet 50 logins en 50 API requests per seconde aankunnen.
E12.5	Eis		De responsetijd tussen aanvragende applicaties en de authenticatievoorziening mag per authenticatieverzoek niet langer duren dan 0,5 seconde, gemeten vanaf de device van de eindgebruiker. Met responstijd wordt bedoeld de doorlooptijd van het hele inlogproces, uitgezonderd de tijd die een gebruiker nodig heeft voor het invoeren van credentials, waarbij rekening wordt gehouden met de typische snelheden van consumenten-niveau breedband en mobiele dataverbindingen.

Van de openbare bibliotheekleden is de KB niet de beheerder van de klantgegevens, deze worden via API-calls aangeleverd door de diverse bibliotheeksystemen van de openbare bibliotheken. De levering van klant- en autorisatie-informatie is niet gelijk verdeeld over de tijd. Alle gegevens worden minimaal eens per jaar ververst, met pieken van 0,5M tot 1M API calls rond de maandovergangen.

12	Type	Punten	Omschrijving
F12.1	Funct. vraag	15	De levering van klant- en autorisatie-informatie aan het CIAM-systeem is niet gelijk verdeeld over de tijd. Alle gegevens worden minimaal eens per jaar ververst, met pieken van 0,5M tot 1M API calls rond de maandovergangen. Het CIAM-systeem voorziet in een vorm van

			autoscaling om ook op piekmomenten een goede performance te kunnen blijven bieden.

13. Servicemanagement

13.A. SLA

De KB zoekt een Inschrijver die het dienstverleningsniveau kan leveren wat past bij een identityprovider voor de hele bibliotheekbranche. Daarnaast moeten de ontwikkel- en kwaliteitsborgingsprocessen van de KB goed ondersteund worden. Dit is belangrijk voor enerzijds controleren dat nieuwe releases van het CIAM-systeem correct samenwerken met onze andere systemen en anderzijds om nieuwe software van KB-zijde gecontroleerd live te kunnen brengen.

13A	Type	Punten	Omschrijving
E13A.1	Eis		Opdrachtnemer sluit met Opdrachtgever een Service Level Agreement voor het Beheer van het CIAM-systeem (voor productie-, acceptatie- en testomgeving). Deze Service Level Agreement (SLA) dient in conceptversie bij de inschrijving geleverd te worden, als bijlage van de overeenkomst.
E13A.2	Eis		Het minimale beschikbaarheidspercentage van het CIAM-systeem, exclusief tijd voor gepland onderhoud is 99,90 % per maand.
E13A.3	Eis		De Inschrijver biedt uiterlijk de volgende reactie- en Functieherstelttijden (oplostijden) voor de verschillende prioriteitsniveaus van servicemeldingen: Reactietijden: • P1: 15 minuten • P2: 2 uur • P3: 1 werkdag • P4: in overleg • P5: in overleg Functieherstelttijden: • P1: 80% binnen 4 uur; de overige 20% binnen 24 uur • P2: 90% binnen 1 werkdag; de overige 10% binnen 3 werkdagen • P3: 90% binnen 2 werkdagen; de overige 10% binnen 4 werkdagen • P4: 90% binnen 5 werkdagen; de overige 10% binnen 10 werkdagen • P5: 90% binnen 10 werkdagen; de overige 10% binnen 1 maand

E13A.4	Eis		Voor Servicemeldingen met prioriteit 1 of 2 verwacht de KB een bereikbaarheid van de Inschrijver van 24 uur per dag, 7 dagen in de week, het hele jaar door.
E13A.5	Eis		Voor Servicemeldingen met prioriteit 3 of lager verwacht de KB een bereikbaarheid van de Inschrijver op werkdagen (tijden nader af te stemmen).
E13A.6	Eis		In de SLA wordt uitgewerkt hoe wordt omgegaan met geplande en ongeplande (bijvoorbeeld bij een security incident) onderhoudsvensters. In ieder geval meldt Inschrijver geplande downtime (bijvoorbeeld als gevolg van onderhoudswerkzaamheden of het installeren van een nieuwe release) minimaal 48 uur van tevoren bij de KB.
E13A.7	Eis		Voordat de CIAM-systeem oplossing in beheer wordt genomen, worden in de definitieve SLA minimaal de volgende punten concreet en in detail uitgewerkt (waarbij relevante eisen in dit PvE van toepassing blijven): Incidentmatrix, escalatiematrix, rapportages (dienstverlening), wijzigingenbeheer, overlegstructuur en evaluaties.
E13A.8	Eis		Voordat het CIAM-systeem in beheer wordt genomen, zal de Inschrijver met de KB afspraken maken over de invulling van een Dossier Afspraken en Procedures (DAP), waarin operationele afspraken worden gemaakt die gedurende de inrichting van het CIAM-systeem en tijdens de looptijd van de overeenkomst van toepassing zijn.
E13A.9	Eis		Monitoring: bij uitval van (een component van) het CIAM-systeem wordt de KB d.m.v. e-mail/sms geïnformeerd. De situaties waarop Inschrijver moet monitoren worden in de SLA beschreven.
W13A.1	Wens	3	Bij zeer urgente situaties, bijvoorbeeld bij een datalek of een P1-verstoring, is Inschrijver bereikbaar via een noodnummer.

13.B. Servicelevel Rapportages

Inschrijver zorgt voor 24/7 monitoring van, maandelijkse rapportage over en regelmatige bespreking van de behaalde service levels.

13B	Type	Punten	Omschrijving
E13B.1	Eis		Inschrijver zorgt voor monitoring van de servicelevels zoals afgesproken in het SLA en levert hier rapportages over. Oplevering 1 x per maand binnen 10 werkdagen na afloop van de rapportageperiode.
W13B.1	Wens	3	Inschrijver levert maandelijks een voortgangsrapport op over de in opdracht van de KB uitgevoerde werkzaamheden. Oplevering 1 x per maand binnen 10 werkdagen na afloop van de rapportageperiode.
W13B.2	Wens	3	Inschrijver dient te rapporteren over geplande en uitgevoerde Security hardening werkzaamheden inclusief de status van de opvolging/ afhandeling van geconstateerde bevindingen. Oplevering 1 x per maand binnen 10 werkdagen na afloop van de rapportageperiode.

E13B.2	Eis		Inschrijver dient in samenspraak met de KB een overlegstructuur inclusief periodiek overleggen in te richten om minimaal de overeengekomen opgeleverde rapportages, eventuele issues en ontwikkelingen rond de geleverde dienstverlening te bespreken.
W13B.3	Wens	3	Inschrijver zorgt in het geval van technische escalaties voor een vast contactpersoon.
W13B.4	Wens	3	Inschrijver organiseert minimaal één keer per jaar een workshop waarin de ontwikkelingen in de SaaS-roadmap worden doorgesproken.

14. Gebruiksvriendelijkheid en Toegankelijkheid

Laagdrempelige toegang tot al haar diensten is een groot goed voor de KB. Daarom worden de internationale standaarden hiervoor aangehouden, zodat online diensten zo eenvoudig mogelijk te gebruiken zijn, ook door minder digitaal vaardigen. Omdat de authenticatievoorziening ook door andere organisaties dan de KB gebruikt wordt, is het wenselijk de eindgebruikerschermen in meerdere merkuitvoeringen te kunnen tonen.

14	Type	Punten	Omschrijving
E14.1	Eis		Het CIAM-systeem voldoet steeds aantoonbaar aan de eisen voor digitale toegankelijkheid zoals omschreven in de meest actuele versie van de Europese standaard EN 301 549, waarvan de internationale richtlijnen voor toegankelijkheid, de Web Content Accessibility Guidelines, deel uitmaken. De KB vraagt hierbij WCAG-niveau AA.
E14.2	Eis		Opdrachtnemer kan bij oplevering bewijs overleggen dat de opgeleverde dienst voldoet aan genoemde toegankelijkheidseisen voor de eindgebruiker interfaces. Dit betekent dat er voor oplevering van de dienst getest is volgens een betrouwbare evaluatiemethode: WCAG-EM of een gelijkwaardige methode. Mocht de dienst niet (volledig) voldoen, dan worden de toegankelijkheidsproblemen alsnog door de leverancier opgelost.
E14.3	Eis		De gebruikersinterface en beheerinterface van het CIAM-systeem ondersteunen de actuele versies van de gangbare mobiele, tablet en desktop-browsers (Minimaal Edge, Firefox, Safari en Chrome).
E14.4	Eis		De gebruikersinterface en beheerinterface van het CIAM-systeem zijn responsive naar alle scherm- en window formaten.
E14.5	Eis		In de eindgebruikersinterfaces moet de eindgebruiker de taal kunnen selecteren waarin de teksten worden getoond, waarbij minimaal tussen Nederlands (default) of Engels gekozen kan worden.
W14.1	Wens	3	Alle teksten in de beheerinterfaces zijn beschikbaar in het Nederlands.
W14.2	Wens	3	Alle eindgebruikersschermen kunnen worden aangepast aan de eisen van de KB als het gaat om opmaak, velden, links naar achterliggende functies of informatie en logo. Zie https://login.kb.nl voor een voorbeeld van het huidige loginscherm.
W14.3	Wens	3	De eindgebruikersschermen moeten in meerdere opmaken/merkuitvoeringen parallel gebruikt kunnen worden (multi branding).

15. Privacy, techniek en veiligheid

15.A. Privacy

Als deelnemer van het ‘Public Spaces’ initiatief is de privacy van alle eindgebruikers in het bibliotheeknetwerk voor de KB essentieel. Dat heeft impact op de voorwaarden voor hosting, cookies en datamanagement.

15A	Type		Omschrijving
E15A.1	Eis		Inschrijver verwerkt gegevens van KB alleen binnen de EER (Europese Economische Ruimte). Vindt doorgifte van persoonsgegevens (inclusief backups) buiten de EER plaats, dan is hiervoor expliciete toestemming van KB vereist en moet er sprake zijn van een passend beschermingsniveau. Van een passend beschermingsniveau is sprake als Inschrijver of Subverwerker: - De gegevens verwerkt enkel in een land dat beschikt over een adequaat beschermingsniveau op grond van het adequaatheidsbesluit (Adequacy decisions) van de Europese Commissie (eventueel met aanvullende maatregelen); - Is gecertificeerd overeenkomstig de "Transatlantic Data Privacy Framework" en de gegevensverwerking vallen onder de reikwijde van de certificering; - Er wereldwijd Binding Corporate Rules, die zijn goedgekeurd door de EDPB, worden gehanteerd; - De EU Standard Contractual Clauses is ondertekend (plus aanvullende maatregelen genomen zijn, zoals aanbevolen door de EDPB).
E15A.2	Eis		Het CIAM-systeem dient vrij te zijn van third party tracking cookies, uitgezonderd die van de door de KB gehanteerde analyticstool (momenteel Matomo).
E15A.3	Eis		Inschrijver dient te waarborgen dat de KB te allen tijde eigenaar blijft van de gegevens welke binnen het CIAM-systeem wordt verwerkt en/of zijn opgeslagen.
E15A.4	Eis		Opdrachtnemer is niet gerechtigd om de verkregen data, informatie en/of andere inzichten welke voortkomen uit het aangaan van deze Overeenkomst te gebruiken voor andere doeleinden (waaronder productverbetering) zonder nadrukkelijke schriftelijke toestemming door Opdrachtgever.
E15A.5	Eis		Inschrijver zorgt ervoor dat de gegevens van KB tijdens transport, bewerking en opslag duurzaam geïsoleerd zijn van beheerfuncties aan de kant van Inschrijver en anderen die gebruikmaken van dezelfde infrastructuur.
E15A.6	Eis		Het verlenen van toegang tot persoonsgegevens aan medewerkers van de Opdrachtnemer wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.
E15A.7	Eis		Opdrachtnemer werkt mee met het uitvoeren van een Data Protection Impact Assessment (DPIA) volgens het model van Opdrachtgever.

15.B. Techniek en veiligheid

Als identityprovider voor een heel bibliotheeknetwerk stelt de KB logischerwijs hoge eisen aan haar IT-landschap. Dit leidt tot strenge voorwaarden op het gebied van standaarden, beveiliging, risicomanagement en datamanagement.

15B	Type	Punten	Omschrijving
W15B.1	Wens	3	Het CIAM-systeem heeft een OpenID Certification van de OpenID Foundation (waarmee interoperabiliteit beter gegarandeerd wordt).
E15B.1	Eis		Inschrijver zorgt ervoor dat de vanuit het CIAM-systeem verzonden e-mails herkenbaar zijn, op basis van domeinnaam van de KB, als e-mail van de KB.
E15B.2	Eis		De emailfunctionaliteit voldoet blijvend aan aanvullende beveiligingsmaatregelen als SPF, DKIM, DMARC en STARTTLS + DANE.
E15B.3	Eis		Het CIAM-systeem maakt standaard gebruik van veilige communicatieprotocollen zoals HTTPS, SSH en SFTP. Waar HTTPS wordt toegepast vindt dit plaats conform de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' v2.1 van het NCSC, wat betekent dat minimaal TLS 1.2 en bij voorkeur TLS 1.3 (dan wel nieuwer) wordt toegepast.
E15B.4	Eis		Binnen het CIAM-systeem worden gegevens versleuteld opgeslagen (data-at-rest) op basis van adequate encryptiestandaarden (minimaal AES-256). Dit is ook van toepassing op back-ups.
E15B.5	Eis		Inschrijver beveiligt de SaaS-dienst afdoende, onder andere middels preventieve maatregelen (zoals firewalls en anti-DDoS voorzieningen) en detectieve maatregelen (zoals een SIEM).
E15B.6	Eis		Componenten waaruit het CIAM-systeem bestaat (zoals (Cloud)platforms, hypervisors, containerplatforms, (besturings)systemen, database platforms) dienen door Inschrijver afdoende te zijn gehardened aan de hand van CIS benchmarks of hardening best-practices van individuele fabrikanten (comply or explain).
E15B.7	Eis		Daar waar de Inschrijver X.509-certificaten gebruikt van de KB wil de KB deze certificaten zelf kunnen aanmaken, verlengen of intrekken.
E15B.8	Eis		Inschrijver zal een recente samenvatting van een Business Continuity test voor de CIAM SaaS-dienst overleggen.
E15B.9	Eis		Inschrijver is verantwoordelijk voor het uitvoeren van security monitoring van het CIAM-systeem. Inschrijver voorziet in een security monitoring-systeem en onderhoudt deze, die in staat is om alle relevante loggegevens, activiteiten en gebeurtenissen binnen het systeem te monitoren. Het security monitoring-systeem moet proactief zijn en in staat zijn om verdachte activiteiten, afwijkend gedrag en beveiligingsincidenten te detecteren. Het dient te beschikken over analyse- en algoritmemogelijkheden om potentiële bedreigingen te identificeren.
E15B.10	Eis		Inschrijver heeft een Security Operations Center (SOC) of een vergelijkbaar team, dat verantwoordelijk is voor het 24/7 monitoren en reageren op security-gerelateerde gebeurtenissen en incidenten.

E15B.11	Eis		Waar in het CIAM-systeem gebruik wordt gemaakt van cookies bevatten deze nooit persoonlijke informatie en vindt de uitwisseling altijd via een beveiligde verbinding (HTTPS+HSTS) plaats.
E15B.12	Eis		Waar in het CIAM-systeem gebruik wordt gemaakt van cookies met gevoelige gegevens dienen deze voorzien te zijn van de 'secure' en 'httponly' flags.
E15B.13	Eis		Het CIAM-systeem ondersteunt IP-whitelisting op de SCIM-interface.
W15B.2	Wens	3	Het CIAM-systeem ondersteunt IP-whitelisting op andere APIs.
E15B.14	Eis		Inschrijver zorgt ervoor dat medewerkers van KB zich kunnen authenticeren bij het CIAM-systeem met behulp van Single Sign On (SSO) die loopt via de authenticatie management oplossing (Microsoft Entra ID) van KB. Toegang tot het CIAM-systeem is enkel mogelijk na succesvolle login en Multi Factor Authenticatie (MFA).
W15B.3	Wens	3	Voor noodgevallen is er een 'enveloppenprocedure' om KB-medewerkers voor de duur van de noodsituatie directe toegang te geven tot hun taken in het CIAM-systeem (bijvoorbeeld als het Microsoft Entra ID van de KB-beheerders niet functioneert). Ook deze procedure moet veilige authenticatiemethoden gebruiken.

15.C. Risicomanagement, logging, backup&restore

15C	Type	Punten	Omschrijving
E15C.1	Eis		Het CIAM-systeem dient aantoonbaar geen kwetsbaarheden/ kritische beveiligingsrisico's te bevatten zoals beschreven in de meest recente OWASP top 10 (https://owasp.org/).
E15C.2	Eis		Het CIAM-systeem heeft in de afgelopen 12 maanden aantoonbaar succesvol een (pen)test doorstaan langs de lijnen van de OWASP Application Security Verification Standard (ASVS) c.q. Certified Secure Checklists.
E15C.3	Eis		Inschrijver heeft de organisatie en verantwoordelijkheden voor het risicomanagementproces voor de beveiliging van clouddiensten opgezet en onderhoudt deze.
E15C.4	Eis		Inschrijver dient structureel risicoanalyses uit te voeren in het bouw- en implementatietraject, bij grote onderhoudstrajecten en bij significante wijzigingen in de geleverde Oplossing/ Dienstverlening.
E15C.5	Eis		Inschrijver dient aantoonbaar onderkende risico's vast te leggen voorzien van de geplande mitigerende maatregelen inclusief een verwachte implementatie/ oplosdatum en actiehouder.
E15C.6	Eis		Inschrijver dient de KB op de hoogte te stellen, via het overeengekomen communicatiekanaal en tijdslijnen, van risico's die een directe impact op de opdrachtgever (kunnen) hebben.
E15C.7	Eis		Inschrijver voorziet in actuele, niet-muteerbare logging van gebeurtenissen met betrekking tot de activiteiten van beheerders binnen het CIAM-systeem. De vastgelegde gebeurtenis omvat

			minimaal de datum en tijd van de verrichte handeling, met een duidelijke beschrijving van de activiteit van de beheerder.
E15C.8	Eis		De logging bevat net voldoende gegevens om te kunnen bepalen welke beheerder een bepaalde actie heeft uitgevoerd (en dus geen wachtwoorden of emailadressen van beheerders).
E15C.9	Eis		Het CIAM-systeem logt en toont alle acties, die zijn uitgevoerd door het systeem ongeacht of deze succesvol zijn geweest of niet (failures), t.b.v. auditdoeleinden. Dit betreft minimaal de acties rond provisioning, identiteitenwijzigingen, account/autorisatie wijzigingen en autorisatie/account aanvragen.
E15C.10	Eis		Het CIAM-systeem dient audit/ logbestanden minimaal 6 en maximaal 12 maanden te bewaren voor toekomstig onderzoek en toegangscontrole. In geval van een (vermoed) informatiebeveiligingsincident dient de gelogde incidentinformatie minimaal drie jaar bewaard te worden.
E15C.11	Eis		In geval van een (vermoed) informatiebeveiligingsincident dient de gelogde incidentinformatie minimaal drie jaar bewaard te worden.
E15C.12	Eis		Inschrijver garandeert adequate back-up- en restorevoorzieningen van het CIAM-systeem, waarbij het creëren van back-ups geen verstorende werking heeft op de dienstverlening.
E15C.13	Eis		Inschrijver voorziet in een back-up voorziening van het CIAM-systeem die niet geraakt wordt door een incident.
E15C.14	Eis		In het geval een restore van gegevens in het CIAM-systeem nodig is, kan de afgesproken dienstverlening binnen 8 uur (Recovery Time Objective) worden gecontinueerd. Er mag sprake zijn van maximaal 24 uur dataverlies (Recovery Point Objective). Indien restores data-inconsistentie veroorzaken (bijvoorbeeld met gekoppelde systemen) dan zijn er aanvullende recovery procedures.
E15C.15	Eis		In het geval een restore van gegevens in het CIAM-systeem nodig is, mag sprake zijn van maximaal 24 uur dataverlies (Recovery Point Objective). Indien restores leiden tot data-inconsistentie (bijvoorbeeld met gekoppelde systemen) dan zijn er aanvullende recovery procedures.
E15C.16	Eis		Inschrijver dient periodiek, minimaal eens per jaar, aan te tonen dat de back-up en restore voorziening correct functioneert en voldoet aan de maximale hersteltijden en het maximaal toegestaan gegevensverlies. De Inschrijver legt de resultaten hiervan vast in een rapport dat aan de KB beschikbaar wordt gesteld.

16. Juridische, financiële en overige Inkoopvoorwaarden

De KB stelt een aantal juridische voorwaarden aan de samenwerking. Ook gelden er eisen aan de tarieven van de Inschrijver en aan de wijze waarop wordt gecommuniceerd en gefactureerd. Daarnaast wenst de KB de mogelijkheid te hebben verdere ontwikkeling of ondersteuning bij het gebruik van de oplossing bij Inschrijver uit te vragen. Tot slot stelt de KB nog enkele voorwaarden bij verlenging of beëindiging van de samenwerking.

16	Type	Omschrijving
E16.1	Eis	Door het indienen van de inschrijving gaat Inschrijver akkoord met de tekst van de overeenkomst en de algemene voorwaarden, zoals vastgesteld na de laatste nota van inlichtingen.
E16.2	Eis	Door het indienen van een inschrijving maken de door Inschrijver opgegeven antwoorden op de kwalitatieve gunningcriteria automatisch en direct deel uit van de eisen die gesteld worden aan de uitvoering van de opdracht.
E16.3	Eis	De overeenkomst incl. bijbehorende bijlagen prevaleert te allen tijde boven de voorwaarden opgenomen in een offerte of opdrachtbevestiging m.b.t. aanvullende werkzaamheden.
E16.4	Eis	In het CIAM-systeem worden door de Inschrijver, in opdracht van de KB, persoonsgegevens verwerkt. Op die verwerking van persoonsgegevens is de AVG van toepassing. Voordat Inschrijver overgaat tot het verwerken van persoonsgegevens van KB, dient de verwerkersovereenkomst te zijn afgesloten.
E16.5	Eis	De algemene en/of verkoopvoorwaarden van Inschrijver worden nadrukkelijk van de hand gewezen. In de inschrijving van Inschrijver wordt niet (deels) naar andere juridische voorwaarden verwezen.
E16.6	Eis	Inschrijver voert werkzaamheden uit in lijn met de geldende wet- en regelgeving, waaronder de AVG-wetgeving en meldt proactief aan de KB incidenten betrekkende de beveiliging van de persoonsgegevens.
E16.7	Eis	De door Inschrijver aangeboden tarieven zijn 'all-in', dat wil zeggen inclusief (niet gelimiteerd) salariskosten, overheadkosten, kosten voor gebruik apparatuur, software, licenties, testkosten, kosten van keuringen, verzekeringen, reis- en verblijfskosten, reistijd, belastingen, heffingen, administratieve kosten, kosten voor overleg, kosten voor certificering of kosten voor Verklaringen Omtrent Gedrag. Dit betekent dat uitsluitend de opgegeven prijzen en het tarief in rekening kan worden gebracht zoals opgegeven in het prijsblad.
E16.8	Eis	Alle communicatie tussen Inschrijver en de aanbestedende dienst vindt plaats in de Nederlandse en/of Engelse taal.
E16.9	Eis	Inschrijver zorgt ervoor dat alle medewerkers die op welke wijze dan ook contact hebben met de KB de Nederlandse en/of Engelse taal in woord en geschrift beheersen.
E16.10	Eis	De KB krijgt een vast beslissingsbevoegd contactpersoon (accountmanager) bij Inschrijver toegewezen voor alle vragen en/of opmerkingen met betrekking tot de overeenkomst en de uitvoering van de opdracht. Deze contactpersoon dient tijdens kantooruren telefonisch en per email bereikbaar te zijn, waarbij deze binnen 5 werkdagen inhoudelijk reageert op email, telefonisch contact en/of voicemailberichten. Indien de contactpersoon langer dan 5 werkdagen afwezig is wordt de KB hiervan op de hoogte gebracht op het moment dat de KB contact opneemt met de contactpersoon.
E16.11	Eis	Opdrachtnemer zal geen communicatie-uitingen doen over het contract of de relatie met Opdrachtgever zonder schriftelijke toestemming van Opdrachtgever.
E16.12	Eis	Gedurende de looptijd van de Opdracht vindt minimaal eenmaal per jaar een strategisch en tactisch evaluatieoverleg plaats tussen een binnen de KB aangewezen functionaris en de accountmanager van Inschrijver. Inschrijver is verantwoordelijk voor de schriftelijke vastlegging van de overleggen met de afgesproken acties en verbeterpunten en het (digitaal) aanleveren hiervan uiterlijk één week na het overleg. De KB is verantwoordelijk voor de agenda van dit overleg.

E16.13	Eis	De KB verwacht in de toekomst opdrachten te geven voor hulp bij ontwikkelingen in het gebruik van de oplossing. In dat geval zal aan Inschrijver een ureninschatting worden gevraagd voor de betreffende hulp. Indien de urenopgave acceptabel wordt geacht kan KB besluiten een opdracht te verstrekken.
E16.14	Eis	Na schriftelijke acceptatie van de urenopgave door de KB dient de verdere ontwikkeling binnen de door de Inschrijver opgegeven doorlooptijd verricht of gedurende de afname periode uitgevoerd te worden. Deze doorlooptijd wordt niet als fatale termijn beschouwd.
E16.15	Eis	Facturatie van de verdere ontwikkeling kan alleen plaatsvinden na volledige uitvoering en acceptatie van de uitvoering door de KB, tenzij schriftelijk anders overeengekomen.
E16.16	Eis	Facturen worden uitsluitend onder vermelding van het inkoopordernummer als e-factuur, volgens de UBL 2.1 standaard, via Peppol of digitaal in pdf-formaat aan digifez@kb.nl verstuurd.
E16.17	Eis	Indien een factuur niet voldoet aan de Aanbestedingsstukken genoemde voorwaarden wordt de Opdrachtnemer hiervan binnen 14 kalenderdagen na ontvangst schriftelijk op de hoogte gebracht. De betreffende factuur wordt pas in behandeling genomen op het moment dat deze voldoet aan de in de Aanbestedingsstukken genoemde voorwaarden.
E16.18	Eis	De KB is gerechtigd om indien er sprake is van door Inschrijver verschuldigde bedragen (crediteringen) deze te verrekenen met bedragen die Inschrijver verschuldigd is aan de KB.
E16.19	Eis	Inschrijver brengt de KB, zodra Inschrijver weet of behoort te weten dat de nakoming van de opdracht niet of niet tijdig of niet naar behoren plaatsvindt, onmiddellijk schriftelijk én telefonisch op de hoogte onder vermelding van de omstandigheden.
E16.20	~~Eis~~	Vervallen ~~Indien de overeenkomst binnen de looptijd wordt ontbonden, om reden van een onjuiste calculatie, op grond van een onvoldoende prestatie of andere tekortkomingen die aan Inschrijver kunnen worden toegerekend, is Inschrijver verplicht tot vergoeding van de schade die door de annulering ontstaat. Onder schade wordt in dit verband mede verstaan het verschil tussen de met Inschrijver overeengekomen prijs en de eventueel hogere prijs, verbonden aan het doen uitvoeren van de opdracht door een derde, zulks te berekenen over de nog resterende looptijd van de overeenkomst. Indirecte- en gevolgschade zoals bedrijfsstagnatie vallen hier niet onder.~~