Regionaal Archief Alkmaar

Programma van Eisen en Wensen

Bijlage 1 bij

Inkoopprocedure Project E-depot ’18

Regionaal Archief Alkmaar

Mei 2017

Opgesteld door Regionaal Archief Alkmaar ten behoeve van project E-depot’18	
Datum	4 mei 2017
Versie	1.0
Auteurs	Anje van der Lek Brigit Hoomans

Inhoud

Toelichting

De eisen in dit PvE zijn geordend volgens de hoofdfunctionaliteiten van het OAIS. Aansluitend aan deze functionele eisen zijn een aantal Algemene eisen geformuleerd. Begrippen uit het OAIS staan cursief beschreven. Waar van toepassing verwijzen we de geformuleerde eisen bovendien naar de Eisen Duurzaam Digitaal Depot (ED3) en het Toepassingsprofiel Metagegevens Lokale Overheden (TMLO).

Wij verzoeken u aan te geven in hoeverre u kunt voldoen aan de genoemde eisen en wensen, doormiddel van het invullen van het bijgevoegde Invulformulier PvE volgens de daarin vermelde invulinstructie.

1. Ingest

De *Ingest* omvat het proces van opname van informatieobjecten in het systeem tot en met het gereed maken van de *AIP*, het bestand dat in de *Archival Storage* wordt opgeslagen. In dit proces vinden diverse kwaliteitscontroles plaats en wordt gecontroleerd of de aangeleverde informatiebestanden voldoen aan aanleververeisten of andere afspraken die zijn gemaakt met de archiefvormer.

1.1.	Er is een ingestprocedure in het systeem ingericht, die tenminste de in het OAIS genoemde stappen doorloopt: *Receive Submission, Quality Assurance, Generate AIP, Generate Descriptive Info en Coördinate Updates*.	P
1.2.	Informatieobjecten die worden aangeleverd conform door het Nationaal archief gestelde standaarden kunnen worden opgenomen in het e-depot (op dit moment metagegevens conform het TMLO 1.1 aangeleverd in ToPX-XML formaat). Dit houdt in dat in de ingestprocedure kan worden gecontroleerd of de aangeboden informatieobjecten aan de aanleververeisten van het NA voldoen.	P
1.3.	Informatieobjecten kunnen ook worden aangeleverd conform andere, op een later moment door het RAA te definiëren aanlevervoorwaarden. Dit houdt in dat de ingestprocedure kan worden aangepast en ingericht op andere digitale collecties zoals bijvoorbeeld de beeldbank.	
1.4.	Informatieobjecten kunnen zowel per zaak / dossier (handmatig) als in bulk (geautomatiseerd) worden opgenomen in het e-depot.	P
	De volgende checks *(Quality Assurance)* kunnen automatisch worden uitgevoerd in het Ingest -proces. *Geef in uw documentatie aan welke tools hiervoor gebruikt worden. Beschrijf de procedure hiervoor, waarbij u ook aangeeft hoe het systeem fouten tijdens de ingestprocedure afhandelt.*	
1.5.	• Controle integriteit bestanden (checksum)	P
1.6.	• Controle juistheid toegekende bestandsformaten	P
1.7.	• Virus-controle en verwijderen van virussen in een quarantaine-omgeving	P

1.8.	• Controle validiteit aangeleverde bestanden (voldoet aangeleverde informatie aan de aanleverwoorwaarden, bijv valide ToPX bestand, geaccepteerde bestandformaten)	P
1.9.	• Controle op compleetheid van de ingest (volledigheid, alle objecten en alle metagegevens zijn ingestroomd)	P
1.10.	De ingestprocedure kan vanuit het beheer-dashboard (zie eis XX) worden opgestart / uitgevoerd en gevolgd.	P
1.11.	Indien er fouten / afwijkingen worden aangetroffen gedurende de ingest, krijgt de beheerder hiervan een notificatie.	P
1.12.	Er is een aparte quarantaine-omgeving waar de aangeleverde informatieobjecten gedurende het ingest proces in zijn opgeslagen.	P

2. Data Management

De functie *Data Management* staat voor de opslag en het beheer van metagegevens behorende bij de *AIP's*. Dit gaat om beschrijvende, technische en administratieve metagegevens. De *functie Data Management* wordt belegd in een database. Aanpassingen en beheer worden via de OAIS functie *Administration* geregeld.

2.1.	Metagevens behorende bij *AIP's* worden beheerd in een stabiele database. *Beschrijf wat voor type database u voor dit doel gebruikt. Geef daarbij aan of er aparte licenties nodig voor het gebruik / beheer van deze database.*	P
2.2.	Metagegevens zijn onlosmakelijk verbonden met de bijhorende informatieobjecten. *Beschrijf hoe deze onlosmakelijke verbondenheid wordt gegarandeerd.*	P
2.3.	Het is mogelijk metagegevens te wijzigen. Dit kan uitsluitend worden uitgevoerd door een beheerder. Van wijzigingen wordt gelogd wanneer en door wie deze zijn uitgevoerd. De oude waarde van gewijzigde metagegevens blijft bewaard, maar wordt aangemerkt als "vervallen".	P
2.4.	Het is mogelijk metagegevens toe te voegen.	P
	De functie *Data Management* ondersteunt de volgende open standaarden:	
2.5.	• datamodel TMLO[1], ToPX	P
2.6.	• CMIS (Content Management Interoperability Services)	P
2.7.	• ICA richtlijnen: ISAD(G), ISAAR(CPF) en EAD	P
2.8.	De functie *Data Management* kan ook andere datamodellen voor overige digitale collecties ondersteunen.	P

[1] Het datamodel TMLO wordt momenteel ontwikkeld op basis van het TMLO 1.1 en zal in beheer komen bij het Nationaal Archief. Zie voor meer informatie deze discussielijn op BREEDnetwerk: http://www.breednetwerk.nl/group/tmlo/forum/topics/informatie-en-uitnodiging-voor-doorontwikkeling-tmlo

2.9.	Beheer-activiteiten die een *AIP* betreffen (bijvoorbeeld conversie van een bestandformaat t.b.v. *Preservation Planning*), worden automatisch geregistreerd (gelogd) bij de administratieve metagegevens behorende bij de betreffende *AIP's* (TMLO 12 en 13: Event plan en Event geschiedenis).	
2.10.	Het systeem kan een persistant identifier (PID) aanmaken. Dit is een unieke, permanente digitale link als virtuele vindplaats van een digitaal object (TMLO 7: plaats; ED3 B 2.3). Voor de vindplaats van informatieobjecten wordt gebruik gemaakt van persistant identifiers volgens het Handle systeem (SURFSara)[2].	P
2.11.	Indien een in het systeem op te nemen digitaal object al een persistant identifier heeft, kan deze worden opgenomen als virtuele vindplaats (TMLO 7: plaats) van het betreffende digitale object.	P

3. Archival Storage

De functie *Archival Storage* regelt de permanente opslag van *AIP's*. De functie behandelt verzoeken van de functie *Access* om duplicaten van *AIP's* af te leveren, die als *DIP* aan de *Consumer* beschikbaar worden gesteld. Het Regionaal Archief Alkmaar is voornemens de voorzieningen voor *de Archival Storage* (servers e.d.) niet zelf aan te kopen, maar deze en het technisch beheer hierover uit te besteden. Het leveren van de opslagomgevingen en het technisch beheer hierover maakt deel uit van de opdracht.

3.1.	De leverancier stelt een een actuele beschrijving van de ICT-architectuur van het systeem beschikbaar. Voor de bewaaromgeving is een juist, actueel en volledig overzicht van de aanwezige systemen, hard- en software in hun onderlinge samenhang (ICTarchitectuur) aanwezig. (ED3 C1.1)	P
3.2.	Informatie wordt redundant opgeslagen (ten behoeve van *Error checking / Disaster recovery*)	P
3.3.	Hardware en opslagmedia worden planmatig en tijdig vervangen *(Replace Media;* ED3 1.5*). Beschrijf uw procedure hiervoor*	P
3.4.	Het systeem monitort continue op bitverval en repareert indien nodig *(Error Checking;* ED3 C1.4*). Beschrijf uw procedure hiervoor*	P
3.5.	De fysieke storage faciliteiten bevinden zich in Nederland.	P
3.6.	De storage faciliteiten vallen niet onder de Patriot Act (Dit kan het geval zijn als de (onder-)leverancier Amerikaans is of structureel activiteiten in Verenigde Staten ontplooit).	P

[2] Vanuit het project Persistant Identifiers heeft de Nationale Coalitie Digitale Duurzaamheid (NCDD) afspraken gemaakt met SURFsara, zodat ook erfgoedinstellingen sinds juni 2016 gebruik kunnen maken van hun PID-service (Handle Systeem). Het Handle systeem wordt door de projectgroep aangeraden voor digitale archieven. Zie de website van de NCDD: http://www.ncdd.nl/projecten/netwerk-digitaal-erfgoed/project-persistent-identifiers/

3.7.	Een volledige mirror (backup/kopie) van het e-depot is opgeslagen op een locatie in Nederland die geografisch is gescheiden van de hoofd storage *(Disaster Recovery;* ED3 C2.2, C2.3). Bij uitval van het primaire systeem, kan dienstverlening geheel worden overgenomen door het mirror systeem. *Geef aan waar deze co-loactie zich bevindt, of deze door een onderleverancier (welke) wordt geleverd, en beknopt hoe synchronisatie tussen de systemen is ingericht.*	P
3.8.	Het is mogelijk om (op termijn) gebruik te maken van een tiered storage systeem. (Goedkope, langzame storage naast duurdere, direct beschikbare storage)	
3.9.	Alle storage voorzieningen bevinden zich in een adequate serverruimte met onder meer klimaatbeheersing, alarm en brandmeldvoorziening, toegangscontrole, ordelijke bekabeling en noodstroomvoorziening (UPS). (ED3 C2.4).	P

4. Administration

De functie *Administration* in het OAIS is een zeer brede functie waar alle diensten/services en functies/taken die met het dagelijks beheer van alle overige functies samenhangen. Deze OAIS-functie omvat ook componenten die buiten de eisen aan het systeem vallen, zoals het maken van afspraken met de archiefvormers (*Negiotiate Submission Agreement*), vaststellen van standaarden en beleid (*Establish Standards and Policies*), etc. In dit PvE wordt in gegaan op eisen die de configuratie en het beheer van het systeem ondersteunen. Centraal in deze functie staat het beheer-dashboard: de interface waarmee beheertaken kunnen worden uitgevoerd.

Met beheerder wordt één of meerdere functionarissen in dienst van het RAA bedoeld, die systeemrechten krijgen toebedeeld om beheeractiviteiten te kunnen plannen, accorderen of uit te kunnen voeren.

Eisen aan het beheer met betrekking op een bepaalde OAIS-functie worden in dit PvE bij de betreffende OAIS-functie genoemd.

4.1.	Voor beheertaken is een alleen voor de beheerder toegankelijke webomgeving beschikbaar: het beheer-dashboard.	P
4.2.	Via het beheer-dashboard ontvangt de beheerder systeemnotificaties.	P
4.3.	Via het beheer-dashboard kan de beheerder instellen in welk geval er ook via andere kanalen (bijv e-mail of sms) notificaties worden verstuurd. *Beschrijf welke andere kanalen voor notificaties kunnen worden gebruikt.*	
4.4.	De beheerder moet zelfstandig, zonder tussenkomst van leverancier, gebruikers en beheerders aan kunnen maken en autoriseren.	P
4.5.	De beheerder kan alle (zowel openbare als niet openbare) in het e-depot opgenomen informatieobjecten en bijhorende metagegevens doorzoeken, raadplegen en downloaden.	P
4.6.	De beheerder moet zelfstandig, zonder tussenkomst van leverancier, een export uit het	P

	systeem kunnen maken.	
4.7.	De beheerder kan afgescheiden beheeromgevingen aanmaken voor de afzonderlijke zorgdragers.	P
	Vanuit het beheer-dashboard kunnen periodieke rapportages worden opgesteld ten behoeve van het management:	
4.8.	• Kwantitatieve informatie: (de groei van) het aantal opgenomen informatieobjecten, de gebruikte opslagcapaciteit, aantal uren video, etc	P
4.9.	• Aangetroffen risico's: virussen, ontdekte fouten bij ingest, verouderde bestandsformaten	P
4.10.	• Informatie betreffende gebruik: aantal raadplegingen, welke bestanden worden het meest geraadpleegd, vanuit welke toegang/interface	P
4.11.	• Uitgevoerde beheertaken (zowel automatisch als door beheerder uitgevoerd) met bijhorende resultaten.	P
4.12.	•Storage-beheer: welke storage is in gebruik, hoeveel capaciteit is nog beschikbaar, planning vervanging media.	P
4.13.	Alle beheer-activiteiten (zowel automatisch als door beheerder uitgevoerd) worden geregistreerd in een logfile.	P
4.14.	De logfile is te raadplegen via het beheer-dashboard.	P
4.15.	De logfile kan niet worden verwijderd of gewijzigd.	P

5. Preservation Planning

De functie *Preservation Planning* monitort het risico dat informatie-objecten ontoegankelijk / onbruikbaar worden en regelt de maatregelen die getroffen moeten worden om dit risico te beperken. Net als de functie *Administration* omvat *Preservation Planning* componenten die buiten de functionele eisen aan het systeem vallen, bijvoorbeeld het vaststellen van preserveringsbeleid (*Develop Preservation Strategies and Standards)* en het bijhouden van de stand van de technologie (*Monitor Technology)*. In dit PvE worden de functionele eisen aan het systeem genoemd die de functie *Preservation Planning* ondersteunen. (Deze eisen zijn tevens een invulling van de eisen gesteld in ED3 B3.1 en B3.2)

5.1.	Het systeem houdt bij welke bestandsformaten in gebruik zijn. Hier kunnen via het beheer-dashboard overzichten van worden gemaakt.	P
5.2.	Het is mogelijk via het beheer-dashboard in het systeem aan te geven welke uitvoersoftware met deze bestandsformaten moet worden geassocieerd.	P
5.3.	In het systeem kan (via beheer-dashboard) worden aangegeven welke bestandsformaten /geassocieerde software risicovol zijn (bijvoorbeeld omdat deze in onbruik zijn geraakt, licenties aflopen etc.)	P
5.4.	Het systeem checkt welke bestanden geassocieerd zijn met als risicovol benoemde	P

	bestandsformaten/software.	
5.5.	Het systeem heeft een monitor-functie die steekproefsgewijs en automatisch checkt of bestanden nog te openen zijn met de geassocieerde software. Indien dit niet mogelijk is, wordt het betreffende bestand of bestandformaat als risicovol aangemerkt.	P
5.6.	Bij door het systeem aangetroffen risico's krijgt de beheerder een notificatie.	P
	Het systeem kan, per individueel bestand en in bulk , de volgende maatregelen uitvoeren om gesignaleerde risico's te beperken:	
5.7.	• Conversie naar een ander bestandsformaat. Het originele bestand kan behouden blijven (of bestanden in verouderde formaten behouden blijven, bepaalt de beheerorganisatie in het preserveringsbeleid)	P
5.8.	• "Conversie on demand": Het vastleggen van een conversie-pad bij *AIP*'s met verouderde bestandsformaten, zodat als in de toekomst een verouderd bestandsformaat wordt opgevraagd, het systeem als DIP een bestand in een op dat moment gangbaar bestandsformaat levert.	
5.9.	•Emulatie: het systeem verwijst naar een emulatie-omgeving waar verouderde bestandsformaten in kunnen worden geopend.	
5.10.	De beheerder kan via het beheer-dashboard de benodigde maatregelen configureren en uitvoeren.	P

6. Access

De functie *Access* (Toegang) handelt informatieverzoeken af en stelt informatie aan de gebruiker beschikbaar in een vorm die voor de gebruiker leesbaar en bruikbaar is. Er kunnen verschillende toegangen worden geboden, aangepast aan verschillende doelgroepen of soorten gebruikers (*Designated Communities*), zoals algemeen publiek, aangesloten gemeenten, (web-)ontwikkelaars, onderzoekers, gebruikers van Open Data etc. Het is niet noodzakelijk dat al deze doelgroepen vanuit één toegang / interface bediend moeten worden, het is juist belangrijk dat het systeem een pluriforme waaier aan toegangen (zowel binnen het systeem als extern) kan bedienen.

De eisen betreffende de functie *Access* zijn onderscheiden in twee categorieën:

- **Eisen betreffende de algemene toegankelijkheid van informatie die is opgenomen in het systeem.**

  Het doel is om de informatie optimaal en machineleesbaar toegankelijk te maken voor allerlei externe toepassingen. Denk hierbij aan doorzoekbaarheid door zoekmachines zoals Google, data-aggregatoren zoals bijvoorbeeld Europeana, koppelingen met andere systemen, of andere toepassingen die zijn ontwikkeld op basis van open data.

  Door deze algemene toegankelijkheid kan in principe iedere web-ontwikkelaar een naar wens ontworpen toegang op het e-depot bouwen.

- **Eisen aan de component “webportaal publiek”**

  Naast deze algemene toegankelijkheid heeft het RAA de verantwoordelijkheid om de informatie toegankelijk aan te bieden voor individuele gebruikers. Het systeem moet daarom worden geleverd met een concrete basistoegang: een gebruiksvriendelijke, online webinterface (hierna: “webportaal publiek”) waarmee alle in het systeem opgenomen informatieobjecten kunnen worden geraadpleegd.

  Op de langere termijn wil het RAA dit webportaal verder ontwikkelen en optimaal integreren met andere zoekfunctionaliteit op de eigen website. Dit staat echter los van deze opdracht.

De hieronder genoemde eisen voor de functie *Access* zijn van toepassing op openbare informatie. De toegang tot niet-openbare infromatie wordt op een andere manier geregeld. Zie ‘toelichting en eisen bij Informatiebeveiliging’, p. 11.

De eisen met betrekking op Access *(Toegang) kunnen op gespannen voet staan met eisen mbt de informatiebeveiliging (zie toelichting en eisen bij* Informatiebeveiliging, *p. 11). Als dit het geval is, geeft u dat dan a.u.b. aan in de toelichting. Beschrijf ook –indien mogelijk- op welke manier u de toegankelijkheid kunt optimaliseren zonder de informatiebeveiliging geweld aan te doen.*		
Eisen betreffende de algemene toegankelijkheid van informatie die is opgenomen in het systeem.		
6.1.	Elke gebruiker kan een openbaar informatieobject met behulp van de persistent identifier (PID) via een beveiligde internetverbinding ophalen (downloaden).	P
6.2.	Elke gebruiker kan openbare informatieobjecten periodiek ophalen via koppelvlakken /API’s op basis van open uitwisselingsstandaarden, zoals OAI-PMH (Open Archive Initiative – Protocol for Metadata Harvesting), ResourceSync (Open Archives Initiative - ResourceSync Framework Specification) en JSON (JavaScript Object Notation). *Geef aan welke standaarden worden ondersteund.*	P
6.3.	Elke gebruiker kan openbare metagegevens over een informatieobject met behulp van de persistent identifier (PID) via een beveiligde internetverbinding ophalen (downloaden).	P
6.4.	Elke gebruiker kan openbare metagegevens over informatieobjecten periodiek ophalen via koppelvlakken /API’s op basis van open uitwisselingsstandaarden, zoals OAI-PMH (Open Archive Initiative – Protocol for Metadata Harvesting), ResourceSync (Open Archives Initiative - ResourceSync Framework Specification) en JSON (JavaScript Object Notation). *Geef aan welke standaarden worden ondersteund.*	P
6.5.	De in eis 6.2 en 6.4 bedoelde koppelvlakken/API’s zijn zonder registratie toegankelijk voor eenieder om de openbare informatieobjecten en metagegevens als open data te hergebruiken. *Geef aan of er een fair use policy wordt gehanteerd voor het gebruik van deze koppelvlakken/API’s. Welke kosten en/of limieten zijn er aan verbonden?*	P
6.6.	Externe zoekmachines (bijv. Google) kunnen de openbare informatie (content en metagegevens) indexeren.	P
Eisen aan de component “webportaal publiek”		

6.7.	Openbare informatieobjecten en metagegevens in het systeem zijn via een online webinterface (hierna: webportaal publiek) voor iedereen te doorzoeken, raadplegen en beschikbaar voor hergebruik (=te downloaden in bruikbaar bestandsformaat). Hiervoor is geen gebruikersaccount of anderszins registratie vereist. *Geef indien mogelijk een voorbeeld van de interface in de vorm van een schermafbeelding (evt mock-up).*	P
	Via het webportaal publiek is de inhoud van het e-depot te doorzoeken. Er zijn verschillende zoekmogelijkheden: *Benoem welke tools/ zoekmachines hiervoor worden ingezet. Indien gebruik wordt gemaakt van door onderleverancier geleverde zoektechnologie, benoem welke leverancier dat is en of er sprake is van licentiekosten.*	
6.8.	• Simpel zoeken: met de invoer van één zoekveld worden alle metagegevens en content doorzocht. Booleaanse operatoren worden ondersteund.	P
6.9.	• Geavanceerd zoeken: de gebruiker kan op basis van metagegevens d.m.v. van filters en meerdere zoekvelden de zoekopdracht specifiek afbakenen.	P
6.10.	• Full-text zoeken: de content van informatieobjecten in het e-depot kan worden doorzocht.	P
6.11.	• Zoeken op de kaart: als zoekhulpmiddel kunnen informatieobjecten met een geografische dekking (TMLO: 9.2) op een geografische kaart worden afgebeeld.	
6.12.	Zoekresultaten worden in een nader met het RAA af te stemmen, archivistische en gebruiksvriendelijke context gepresenteerd in het webportaal publiek. *Geef indien mogelijk een voorbeeld in de vorm van een schermafbeelding (evt mock-up) van een zoekresultaat.*	P
6.13.	De gevonden informatieobjecten zijn in een in het webportaal publiek geïntegreerde viewer te raadplegen. *Geef aan welke bestandsformaten door de viewer(s) worden ondersteund.*	

7. Vernietigen / verwijderen van informatie-objecten

De functies Vernietigen of Verwijderen komen niet voor in het OAIS. Omdat het RAA de voorkeur heeft voor de door KING geformuleerde variant 2: “E-Depot als digitale archiefruimte”, moet vernietiging van informatie in het e-depot wel mogelijk zijn. Daarom voegen wij deze functie toe aan het PvE.

Vernietiging van digitale archiefbescheiden houdt in dat de digitale informatie een zodanige bewerking ondergaat, dat de informatie niet meer te lezen of te herleiden is.
De archiefvormer geeft informatieobjecten die niet blijvend te bewaren zijn op grond van de vigerende selectielijst een bewaartermijn mee (onderdeel van TMLO 13: Event plan). Na het verstrijken van deze termijn moeten de informatieobjecten worden vernietigd. Dit geldt voor alle representaties van het te vernietigen informatieobject (SIP, AIP en DIP’s), ook in back-ups / mirror-

locatie. Metagegevens van informatieobjecten die vernietigd zijn, kunnen deels worden bewaard om als virtuele vernietigingslijst te dienen.

Verwijdering van archiefbescheiden houdt in dat informatieobjecten inclusief bijhorende metagegevens uit het e-depot worden verwijderd, maar mogelijk in een ander archiefsysteem worden opgenomen. Er gaat dan een export aan de verwijdering vooraf (zie eis 10.7).

7.1.	Informatieobjecten en bijhorende metagegevens kunnen uit het systeem worden verwijderd en/of vernietigd, uitsluitend als dit gebeurt conform een daartoe opgestelde procedure. Bij het verstrijken van de bewaartermijn krijgt de beheerder een notificatie en kan de vernietigingsprocedure in gang worden gezet. *Beschrijf welke methode wordt gebruikt voor het vernietigen van informatieobjecten.*	P
7.2.	Voor de verwijdering of vernietiging van informatieobjecten plaatsvindt, moet deze zijn geautoriseerd door zowel de beheerder als een bevoegde functionaris van de archiefvormer (4 ogen principe).	P
7.3.	Informatieobjecten en bijhorende metagegevens kunnen niet worden vernietigd voordat de bewaartermijn verstreken is.	P

8. Informatiebeveiliging

Informatiebeveiliging bestaat uit 3 aspecten:

1) Het tegengaan van informatieverlies door calamiteiten of onbedoeld/ongeoorloofd verwijderen van informatie;
2) Het tegengaan van onbedoelde of ongeoorloofde wijzigingen van informatie;
3) Het tegengaan van toegang tot in openbaarheid beperkte informatie door niet-geautoriseerden.

Toelichting op aspect 3: Beveiliging van en toegang tot niet-openbare informatie

Overheidsinformatie in het e-depot is in principe openbaar, en moet vrij toegankelijk zijn voor alle gebruikers. Overheidsinformatie kan onder voorwaarden in openbaarheid worden beperkt. Als dit het geval is, moet dat door de archiefvormer worden aangegeven in de metagegevens (TMLO 18, Openbaarheid). De belangrijkste eis mbt dit aspect is dat deze informatie *niet* mag worden ingezien door gebruikers die *niet* geautoriseerd zijn (eis 8.3).

Het regelen van toegang tot niet-openbare informatie door gebruikers die daarvoor *wel* geautoriseerd zijn, is zowel technisch als organisatorisch een zeer complexe aangelegenheid. In eerste instantie zullen we deze geautoriseerde toegang daarom buiten het e-depot houden. De eisen die wat betreft geautoriseerde toegang aan het systeem moeten worden gesteld, kunnen hierdoor beperkt blijven.

Toegang tot niet-openbare informatie aan geautoriseerde gebruikers zal op twee manieren worden geregeld:

- Er kan conform de huidige wet en regelgeving een verzoek worden gedaan voor het inzien van in openbaarheid beperkt archief bij de archivaris (of een WOB verzoek indien het gaat om niet overgedragen archief). Als dat wordt gehonoreerd, zal de beheerder de gewenste informatie downloaden uit het e-depot en beschikbaar stellen aan de aanvrager (eis 4.5).
- Geautoriseerde gebruikers zullen in de regel medewerkers van de archiefvormer zijn. Niet-openbare informatie kan via een koppeling met een informatiesysteem van de archiefvormer worden geraadpleegd (zie 'Koppelingen met bronsystemen' p. 12). Toegang en autorisaties worden geregeld door de archiefvormer.

Veel van deze aspecten zijn al geadresseerd bij de eisen met betrekking op de OAIS functies. Hieronder zijn nog enkele aanvullende eisen betreffende informatiebeveiliging opgenomen.

8.1.	Het systeem is ingericht conform de norm NEN-ISO/IEC 27001 voor informatiebeveiliging en de leverancier is hiervoor gecertificeerd.	P
8.2.	Informatie-uitwisseling met het systeem vindt uitsluitend plaats via beveiligde verbindingen.	P
8.3.	Informatie-objecten die in openbaarheid zijn beperkt (beperking is aangegeven in TMLO 18, Openbaarheid), kunnen niet worden geraadpleegd door ongeautoriseerde gebruikers. *Geef aan op welke manier deze toegang wordt afgeschermd.*	P
8.4.	Informatieobjecten die in openbaarheid zijn beperkt, kunnen via een koppeling via een informatiesysteem van de archiefvormer worden geraadpleegd.	

9. Koppelingen met bronsystemen

Ter voorbereiding op deze inkoopprocedure is een verkenning uitgevoerd om inzicht te krijgen in de behoeften van archiefvormers wat betreft het digitaal beheer van informatie in het e-depot. De rode draad in de antwoorden was de behoefte aan een goede aansluiting van het e-depot op gemeentelijke DMS en zaaksystemen. De archiefvormers wensen direct na afsluiten van een zaak (of soms zelfs nog eerder) digitale informatie automatisch te kunnen overdragen aan het e-depot. Ook wil men overgedragen informatie vanuit het eigen zaaksysteem kunnen blijven raadplegen.

Om deze wens te realiseren is een koppeling nodig tussen het gemeentelijke zaaksysteem of DMS, hierna *bronsysteem* genoemd.
Het is echter lastig om in dit PvE harde eisen te stellen aan de functionaliteit van deze koppeling, omdat veel eisen de functionaliteit van het bronsysteem betreffen en niet die van het e-depot. Hierbij komt, dat het niet om één bronsysteem gaat , maar om meerdere bronsystemen van verschillende archiefvormers en verschillende leveranciers.

Omdat het een belangrijke prioriteit is voor ons om het e-depot aan te laten sluiten op de bronsystemen, nemen we eisen aan een koppeling op in het PvE. Zoals eerder aangegeven zien wij het e-depot als ontwikkeltraject, en gaan er daarom vanuit dat aanbieders (nog) niet alle eisen en wensen kunnen inwilligen. Uw visie op een eventuele koppeling en eventuele eerdere ervaring met het realiseren van een dergelijke koppeling wordt meegenomen in de beoordeling.

Eerst volgt nu een schets van hoe wij een koppeling tussen e-depot en bronsysteem voor ons zien. Daaronder volgen enkele eisen.

Schets functionaliteit koppeling e-depot / bronsysteem:

- De overdracht van informatieobjecten naar het e-depot kan worden geïnitieerd vanuit het e-depot.
- Naar het e-depot overgedragen informatieobjecten kunnen vanuit het bronsysteem kunnen worden geraadpleegd.

Proces:

1. Start overdracht: automatisch op basis van business rules, of handmatig door geven van opdracht.

Voorbeelden:

- *een zaakdossier wordt automatisch aan het e-depot aangeboden vanuit het bronsysteem, op het moment dat een zaak wordt afgesloten (business rules).*
- *een informatieobject wordt aan het e-depot aangeboden op het moment dat een medewerker van de archiefvormer hier in het bronsysteem opdracht toe geeft.(opdracht)*

2. Er wordt een dataset klaargemaakt voor overdracht: informatieobject(en) en metagegevens worden klaargezet volgens de overeengekomen aanlevervoorwaarden.
3. E-depot ontvangt bericht dat dataset klaar staat.
4. Dataset wordt verstuurd over beveiligde verbinding.
5. Ingest in e-depot vindt plaats.
6. Als ingest voltooid is, ontvangt bronsysteem bericht.
7. Informatieobject wordt uit bronsysteem verwijderd.
8. Metagegevens behorende bij het informatieobject in het bronsysteem worden verwijderd óf bevroren (=onwijzigbaar gemaakt).
9. In het geval dat metagegevens worden bevroren, wordt het oude bestandspad naar het informatieobject vervangen door de persistant identifier (PID) (zie eis 2.4).

Verwijderen

Indien de metagegevens uit het bronsysteem worden verwijderd, staat er geen beschrijving/verwijzing van het overgedragen informatieobject meer in het bronsysteem. Het overgedragen informatieobject kan dan niet meer via het bronsysteem worden geraadpleegd. Dit scenario ligt voor de hand als raadplegen van informatieobjecten niet meer nodig is door medewerkers van de archiefvormer (in archieftermen: de statische fase).

Bevriezen

Indien de metagegevens niet worden verwijderd uit het bronsysteem, blijft er een beschrijving / verwijzing naar het informatieobject in het bronsysteem staan. Gebruikers vanuit de archiefvormer kunnen het dan raadplegen via het bronsysteem. Het bronsysteem kan het informatieobject dan ophalen dmv de PID.

Autorisaties voor toegang tot niet-openbare informatieobjecten kunnen op individueel en gebruikersgroepniveau vanuit het bronsysteem worden geregeld. (Zie *Toelichting op aspect 3: Beveiliging van en toegang tot niet-openbare informatie* 11)

Dit scenario ligt voor de hand als de informatieobjecten nog regelmatig worden geraadpleegd door medewerkers van de archiefvormer (in archieftermen: de semi-statische fase).

Gebruikers vanuit de archiefvormer kunnen hierdoor in hun eigen werkapplicatie zowel overgedragen als niet overgedragen informatieobjecten raadplegen. Ze hoeven dan niet in verschillende systemen te zoeken.

9.1.	Er is een koppelvlak tussen het systeem en het bronsysteem waarmee onderstaande eisen kunnen worden gerealiseerd.	P
9.2.	Het koppelvlak is generiek (=bruikbaar voor verschillende bronsystemen).	P
9.3.	Het koppelvlak is gebaseerd op open standaarden voor interoperabiliteit tussen DMS-CMS- en zaaksystemen: • CMIS (Content Management Interoperability Services) • standaarden ontwikkelt door KING: StUF, StUF-ZKN, RGBZ	P
9.4.	Een overdracht van informatieobjecten naar het e-depot kan vanuit het bronsysteem worden gestart: • door het geven van een opdracht • automatisch door vooraf geconfigureerde business rules	P
9.5.	Er is uitwisseling van berichten tussen het systeem en het bronsysteem: • Als over te dragen dataset klaarstaat • Als dataset in e-depot is opgenomen	P
9.6.	Vanuit het bronsysteem kan een in het e-depot opgenomen informatieobject via de Persistant identifier (PID) worden opgehaald.	P

10. Algemeen

	Performance	
10.1.	We verwachten garanties ten aanzien van de performance van het systeem, ook voor de langere termijn. *We verzoeken u specificaties en voorwaarden te formuleren waaraan de infrastructuur moet voldoen om deze performance te kunnen garanderen.*	P
10.2.	Grote bulkactiviteiten in een bepaalde functie hebben geen invloed op de performance van de andere functies..	P
	Schaalbaarheid	
10.3.	We verwachten garanties ten aanzien van de schaalbaarheid van de opslagcapaciteit van het systeem, ook voor de langere termijn. *We verzoeken u uw strategie op dit punt toe te lichten.*	P
	Continuïteit en dienstverlening	
10.4.	U heeft voldoende gekwalificeerde medewerkers beschikbaar om het implementatietraject (ontwikkeling, implementatie en aansluiting 10 gemeenten) in de periode september 2017 tm eind 2018 tot uitvoer te brengen.	P
10.5.	Na oplevering gaat een dienstverleningsovereenkomst in werking met afspraken over ondersteuning, beheer en regulier onderhoud. *We verzoeken u uw concept-DVO mee te leveren bij uw offerte.*	P
	In de dienstverleningsovereenkomst worden ten minste de volgende eisen betreffende	

	continuïteit opgenomen:	
10.6.	De leverancier claimt geen enkel eigendomsrecht op in het systeem opgenomen informatieobjecten en metagegevens.	P
10.7.	Alle, of een selectie van in het systeem opgenomen informatieobjecten en metagegevens kunnen volledig en zonder kosten worden geëxporteerd, in een zodanige vorm dat import/ingest in een ander systeem mogelijk is. *Geef aan of er een fair use policy wordt gehanteerd, welke kosten en/of limieten zijn er aan verbonden?*	P
10.8.	In geval van het plotseling wegvallen van of een onvoorziene beëindiging van de dienstverlening door de leverancier of een onderleverancier (bijvoorbeeld door faillissement of calamiteit), wordt de continuïteit van het systeem en dienstverlening gegarandeerd door een derde partij (escrow-regeling). Deze voorwaarde wordt nader uitgewerkt in een continuïteitsplan. (ED3 A1.2)	P
10.9.	De leverancier houdt een overzicht bij van alle wijzigingen in werkwijzen, procedures, soft- en hardware waarbij is vastgelegd wat de mogelijke invloed van de wijzigingen is op de digitale informatieobjecten. De leverancier stelt dit overzicht ter beschikking aan het RAA. (ED3 A3.3)	P
10.10	Het RAA streeft – binnen redelijke termijn na implementatie – naar certificering van zijn e-depot[3] De leverancier werkt mee aan onderzoeken en audits die i.h.k.v certificering worden uitgevoerd en stelt benodigde informatie beschikbaar.	P
	Helpfunctie en taal	
10.11	Het systeem heeft een Nederlandstalige gebruikersinterface voor de schermen, de functies en de meldingen.	P
10.12	Het systeem beschikt over een online Nederlandstalige helpfunctie.	
10.13	De helpfunctie is contextafhankelijk.	
10.14	De volledige systeemdocumentatie, handleidingen voor gebruikers en functioneel beheerders moeten voorafgaand aan de implementatie in de Nederlandse taal te worden opgeleverd.	P
10.15	Voorafgaand aan de implementatie biedt de leverancier een training aan beheerders van het systeem, op basis waarvan de beheerder zelfstandig met het systeem kan werken.	P
10.16	Voor de dagelijkse ondersteuning is een Helpdesk beschikbaar.	P

[3] Dit zal een certifering zijn op basis van de door de Nationale Coalitie Digitale Duurzaamheid voorgestelde certificeringsinstrumenten Data Seal of Approval, Nestor en ISO 16363. Zie http://www.ncdd.nl/kennis-en-advies/certificering/