

Aspect	Nr.	Beschrijving van de eis/wens
Koppelingen en koppelvlakken		Het Collectiebeheersysteem voldoet, daar waar van toepassing, aan de GEMMA-standaarden welke zijn gepubliceerd op: standaarden.vng.nl Het Collectiebeheersysteem voldoet ook aan de verplichte standaarden welke voortvloeien uit de 'pas toe of leg uit'-lijst van Forum standaardisatie welke zijn gepubliceerd op https://www.forumstandaardisatie.nl/open-standaarden/verplicht. Het RAZU heeft naar aanleiding van

deze aanbesteding de beslisboom van het Forum standaardisatie ingevuld en de uitkomsten opgenomen in deze aansluitvoorwaarden, zie de kop *Vermoedelijk Relevante Standaarden*.

Het Collectiebeheersysteem biedt de mogelijkheid tot het realiseren van standaard koppelvlakken voor het koppelen met de nationale en internationale aggregatieplatforms, zoals Europeana, Netwerk Oorlogsbronnen en de Digitale Charterbank Nederland. Bij oplevering dient tenminste de Digitale Charterbank Nederland functioneel te zijn, gezien de charters van het RAZU hier reeds gepubliceerd zijn.

Overige kaders en technische aansluitvoorwaarden

Aspect	Nr.	Beschrijving van de eis/wens
Algemeen		Het Collectiebeheersysteem wordt als Software as a Service geleverd en is te benaderen/ gebruiken door middel van webbrowsers op zowel desktop- en laptop-computers, alsmede webbrowsers en/of 'apps' op mobiele apparaten (smartphones, tablets) en is indien nodig van een responsive design voorzien. Het Collectiebeheersysteem wordt middels het Internet ontsloten.
		Het Collectiebeheersysteem wordt onder de verantwoordelijkheid van Leverancier gehost.
		De functionele behoefte van het RAZU wordt door het Collectiebeheersysteem ingevuld middels configuratie van het Collectiebeheersysteem en vereist géén aanpassing van de programmacode van het Collectiebeheersysteem.
		Iedere App behorende bij het systeem is ontwikkeld voor browseronafhankelijk gebruik en ondersteunt in ieder geval de door browser-leveranciers ondersteunde versies van Microsoft Edge en Mozilla Firefox.
Gebruiksvriendelijkheid		Het Collectiebeheersysteem is één herkenbaar geheel; de schermen, de kleuren, de navigatie en andere basisfuncties zijn eenduidig herkenbaar.
		De schermen (invoer, raadpleeg en beheer) zijn overzichtelijk, duidelijk en eenvoudig opgezet, waardoor de meest voorkomende handelingen intuïtief uitgevoerd kunnen worden.

Technische aansluitvoorwaarden

De navigatie en bediening van het Collectiebeheersysteem is eenduidig. Dat wil zeggen dat deze op elke plaats binnen Het Collectiebeheersysteem op dezelfde wijze gebruikt en gedefinieerd zijn.

Het Collectiebeheersysteem voorziet in een gebruikersinterface met de mogelijkheid tot 'help'-ondersteuning voor gebruikers.

Koppelingen tussen Leverancier en het RAZU kunnen enkel tot stand gebracht worden via een beveiligde https-verbinding.

Voor de beveiliging van HTTPS-verbindingen wordt minimaal gebruikgemaakt van een TLS-certificaat dat gebruikmaakt van SHA-256 als hashfunctie en een RSA-sleutellengte van minimaal 2048 bits. Toepassing van sterkere hashfuncties (zoals SHA-384) of langere sleutels kan in overleg worden overwogen.

Voor de beveiliging van https-verbindingen wordt minimaal gebruik gemaakt van TLS 1.2. Oudere versies worden niet ondersteund.

Het RAZU vereist het gebruik van sterke authenticatie (Multi-Factor Authentication, MFA). Dit wordt voor medewerkers van het RAZU technisch afgedwongen via Azure Active Directory (Azure AD) Conditional Access. Authenticatie vindt plaats via standaarden zoals SAML 2.0 en/of OAuth 2.0, waarbij het authenticatieverzoeken doorstuurt naar de Identity Provider (IdP) van het RAZU.

De Leverancier dient deze methode van sterke authenticatie te ondersteunen.

Voor externe gebruikers (bijv. vrijwilligers) dwingt het collectiebeheersysteem een andere vorm van MFA af.

Het Collectiebeheersysteem voldoet bij oplevering aantoonbaar aan de normen en eisen die in de NIS2 of BIO2 (Baseline Informatiebeveiliging Overheid) zijn vastgelegd, inclusief de daaruit voortvloeiende bescherming van persoonsgegevens.

Informatie-veiligheid

Leverancier zal om het jaar een audit laten uitvoeren door een daartoe gelicenseerde externe partij op de eigen dienstverlening. Deze audit richt zich met name op het nakomen van de afspraken omtrent beveiliging en privacy en op kwetsbaarheden. De kosten voor deze audit zijn een integraal onderdeel van de offerte.

Een medewerker van het RAZU hoeft zich slechts eenmalig aan te melden bij de Identity Provider (Single Sign-On). Het Collectiebeheersysteem dient hier notie van te hebben en de medewerker niet nogmaals om inloggegevens te vragen. Het gebruik van IdP initiated SSO is niet toegestaan.

De volgende acties van medewerkers van het RAZU dienen gelogd te worden en herleidbaar te zijn naar natuurlijke personen:

Het muteren van data;

Het exporteren van data:

Ook data die het Collectiebeheersysteem verlaat en daarmee niet meer getraceerd kan worden dient gelogd te worden. Voorbeelden hiervan zijn het al dan niet automatisch versturen van e-mail, het maken van data-dumps en het uitwisselen van data met andere systemen;

Het verwijderen van data.

De log-regels dienen minimaal de volgende informatie weer te geven:

de gebeurtenis;

de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon;

het gebruikte apparaat;

het resultaat van de handeling;

een datum en tijdstip van de gebeurtenis.

Het opvragen van loggegevens dient automatisch uitgevoerd te kunnen worden zonder dat daar bij de Leverancier handmatige acties aan verbonden zijn. Eventueel kan de informatie ook op gezette tijden op voldoende wijze beveiligd naar het RAZU worden verstuurd.

Logbestanden dienen als leesbare tekst opgeslagen te worden in een standaardformaat zoals XML, CSV of JSON. Ieder bestand dient te zijn voorzien van informatie die een beschrijving geeft van de data in het bestand.

Het is niet toegestaan gevoelige informatie zoals persoonsgegevens, anders dan de gebruikersnaam of het gebruikers ID, op te slaan als gelogde informatie.

Leverancier dient log informatie ook zelf veilig te stellen. Tevens dient Leverancier te garanderen dat log informatie ouder dan 3 jaar verwijderd wordt, behalve voor de audittrail van individuele objecten in het collectiebeheersysteem welke bewaard dient te worden.

Wanneer Leverancier gebruik maakt van een shared omgeving, is de data van het RAZU niet te benaderen door derden die dezelfde shared omgeving gebruiken.

Het Collectiebeheersysteem biedt de mogelijkheid voor het instellen van meerdere autorisatieniveaus, waardoor inzage of mutatie van gegevens voor medewerkers van het RAZU beperkt of uitgebreid kan worden afhankelijk van de taak/functie/rol waarvoor zij gemachtigd zijn om specifieke gegevens in te zien of te wijzigen.

Het Collectiebeheersysteem is in staat een totaaloverzicht te presenteren waarop de autorisaties per functie(groep) weergegeven worden.

Het Collectiebeheersysteem beschikt over een adequate back-up voorziening die aansluit bij de gestelde eisen ten aanzien van RPO en RTO die leverancier in zijn SLA aanbiedt. Leverancier voert periodiek restore-testen uit om te controleren of de back-ups consistent en herstelbaar zijn.

Stabiliteit en continuïteit

Leverancier beschikt minimaal over een gescheiden acceptatie- en productieomgeving. Wijzigingen in de ene omgeving mogen geen invloed hebben op het functioneren van de andere omgeving.

De acceptatie- en productieomgeving worden aan de gelijknamige omgevingen binnen het RAZU gekoppeld. Wijzigingen aan de kant van het RAZU zullen altijd eerst in de acceptatieomgeving doorgevoerd worden, waarna getest kan worden of het Collectiebeheersysteem, inclusief de diverse koppelingen, nog naar behoren werkt.

Het RAZU is en blijft te allen tijde eigenaar van de data in het Collectiebeheersysteem.

Alle relevante documenten en (meta)data die betrekking hebben op aanvraag, mutatie, verlenging of beëindiging van een product/dienst worden opgeslagen.

Data

Het Collectiebeheersysteem beschikt over interoperabele (open standaarden) exportformaten voor alle gegevens die opgeslagen zijn in het Collectiebeheersysteem, zodat de data beschikbaar en toegankelijk is voor het RAZU.

Op verzoek van het RAZU zal de Leverancier binnen 24 uur alle data op een leesbare manier exporteren naar het RAZU, waar nodig vergezeld van documentatie over relevante onderdelen van het datamodel.

Leverancier verleent na afloop of bij tussentijdse beëindiging van de Overeenkomst kosteloos en onvoorwaardelijk medewerking aan een exit-strategie. Na gunning wordt de inhoud van deze strategie gezamenlijk vastgesteld door het RAZU en Leverancier (zie hiertoe ook het concept Overeenkomst).

Leverancier dient de data na afloop of bij tussentijdse beëindiging van de overeenkomst via interoperabele (open standaarden) exportformaten op verzoek van het RAZU beschikbaar te stellen aan, dan wel mee te werken aan de migratie van de data naar een nieuw Collectiebeheersysteem. Leverancier garandeert hierbij de volledigheid van de data. Na migratie of levering van de data, dient Leverancier op verzoek van het RAZU de data te verwijderen van haar systemen en deze te vernietigen. Voorgaande geldt uitdrukkelijk ook voor data bestaande uit persoonsgegevens.

Technische werkomgeving

De ICT-omgeving van het RAZU kan globaal als volgt worden gekenmerkt:

Binnen het RAZU wordt gebruik gemaakt van een werkplek gebaseerd Microsoft 365 E5. Medewerkers beschikken over een recente laptop voorzien van Windows 11 en centraal beheerd via Microsoft Intune.

Vermoedelijk relevante standaarden

Op basis van de beslisboom van het Forum standaardisatie zijn de volgende standaarden vermoedelijk relevant.

1 Digitoegankelijk (EN 301 549 met WCAG 2.1)

Door toepassing van Digitoegankelijk worden websites, webapplicaties en documenten voor iedereen toegankelijk, ook voor mensen met permanente, tijdelijke of situationele functiebeperkingen. Zo krijgt iedereen dezelfde toegang tot overheidsinformatie.

Let op: per 1 juli 2018 zijn overheidsorganisaties wettelijk verplicht om Digitoegankelijk (EN 301 549 en WCAG 2.1) te gebruiken voor de toegankelijkheid van websites en mobiele applicaties. Kijk voor meer informatie.

<https://www.forumstandaardisatie.nl/open-standaarden/digitoegankelijk-en-301-549-met-wcag-21>

2 DKIM

DKIM faciliteert van het vaststellen van organisatorische herkomst voor e-mail afkomstig van overheidsdomeinen, als deze over een onbeveiligde, publieke internetverbinding wordt verstuurd wanneer verdere authenticatie ontbreekt.

<https://www.forumstandaardisatie.nl/open-standaarden/dkim>

3 DMARC

DMARC is een standaard die het voor organisaties mogelijk maakt om te bepalen hoe e-mailproviders, die DMARC ondersteunen, omgaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het eigen domein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie.

<https://www.forumstandaardisatie.nl/open-standaarden/dmarc>

4 DNSSEC

DNSSEC zorgt voor de beveiliging van DNS door aan het DNS-record een digitale handtekening toe te voegen en deze bij uitwisseling te verifiëren.

<https://www.forumstandaardisatie.nl/open-standaarden/dnssec>

5 HTTPS en HSTS

HTTPS en HSTS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowser).

Let op: per 1 juli 2023 zijn overheidsorganisaties wettelijk verplicht om HTTPS en HSTS te gebruiken voor beveiligen van publiek toegankelijke websites en webapplicaties. Kijk voor meer informatie.

<https://www.forumstandaardisatie.nl/open-standaarden/https-en-hsts>

6 IPv6

IPv6 en IPv4 standaardiseren communicatie op netwerkniveau over organisatiegrenzen heen tussen organisaties, individuele eindgebruikers, apparaten, diensten en sensoren.

<https://www.forumstandaardisatie.nl/open-standaarden/ipv6>

7 NEN-ISO/IEC 27001

NEN-ISO/IEC 27001 specificeert de eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information

Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.

Gebruik de ICO Wizard om uw eisenpakketten te selecteren die passen bij de producten/diensten die u aanbesteedt. De ICO-Wizard bevat een uitgebreid pakket van informatiebeveiligingseisen die een rol spelen bij aanbestedingen en inkopen. Met behulp van selectievelden kunnen eisenpakketten worden geselecteerd die passen bij specifieke inkoopsegmenten of combinaties daarvan, en kunnen nadere verfijningen daarop worden toegepast. De eisen in de Wizard zijn gebaseerd op een stevig fundament dat is ontleend aan de markstandaard ISO27002.

<https://www.forumstandaardisatie.nl/open-standaarden/nen-isoiec-27001>

8 NEN-ISO/IEC 27002

NEN-ISO/IEC 27002 omvat "best practices" op het gebied van het organiseren van informatiebeveiliging voor een organisatie, bestaande uit het beheer van bedrijfsmiddelen, veilig personeel, toegangsbeveiliging, cryptografie, fysieke beveiliging en beveiliging van de omgeving, beveiliging in de bedrijfsvoering, communicatiebeveiliging, leveranciersrelaties, beheer van informatiebeveiligingsincidenten, informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer, naleving en de acquisitie, ontwikkeling en het onderhoud van informatiesystemen.

9 NL GOV Assurance profile for OAuth 2.0

NL GOV Assurance profile for OAuth 2.0 zorgt ervoor dat de autorisatie van gebruikers van REST APIs van de overheid op een uniforme en eenduidige wijze plaatsvindt.

<https://www.forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oauth-20>

10 ODF

<https://www.forumstandaardisatie.nl/open-standaarden/odf>

11 OpenAPI Specification

Een OpenAPI Specification (OAS) beschrijft de eigenschappen van de data die een API als input accepteert en als output teruggeeft. Met OAS 3.0 kunnen zowel mensen als machines de dataset attributen van een REST API vinden, bekijken en verwerken zonder toegang tot de programmatuur en zonder aanvullende documentatie.

<https://www.forumstandaardisatie.nl/open-standaarden/openapi-specification>

12 PDF (NEN-ISO)

<https://www.forumstandaardisatie.nl/open-standaarden/pdf-nen-iso>

13 REST-API Design Rules

De standaard REST-API Design Rules geeft een verzameling basisregels voor structuur en naamgeving waarmee de overheid op een uniforme en eenduidige manier REST-API's aanbiedt ten behoeve van het ontsluiten van overheidsinformatie en/of functionaliteit.

<https://www.forumstandaardisatie.nl/open-standaarden/rest-api-design-rules>

14 RPKI

Met Resource Public Key Infrastructure (RPKI) kan de rechtmatige houder van een blok IP-adressen een autoritatieve, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routing vanaf haar netwerk. Deze verklaringen kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen die onrechtmatige routing negeren.

<https://www.forumstandaardisatie.nl/open-standaarden/rpki>

15 SAML

SAML standaardiseert federatieve (web)browser-gebaseerde single-sign-on (SSO). Dat wil zeggen dat een gebruiker na eenmalig inloggen via zijn browser toegang krijgt tot verschillende diensten van verschillende partijen.

<https://www.forumstandaardisatie.nl/open-standaarden/saml>

16 security.txt

security.txt moet worden toegepast op alle systemen die via HTTPS publiek benaderbaar zijn, zodat securitycontactinformatie duidelijk is.

<https://www.forumstandaardisatie.nl/open-standaarden/securitytxt>

17 SKOS

SKOS betreft het in een gestructureerde vorm op het Web publiek beschikbaar stellen van een 'niet geformaliseerd' Knowledge Organization System (KOS), met als doel kennis over de betekenissen en samenhang van de onderliggende begrippen te ordenen en toegankelijk te maken.

<https://www.forumstandaardisatie.nl/open-standaarden/skos>

18 SPF

Met SPF kan worden gecontroleerd of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden.

<https://www.forumstandaardisatie.nl/open-standaarden/spf>

19 STARTTLS en DANE

STARTTLS in combinatie met DANE gaan afluisteren of manipuleren van mailverkeer door internetcriminelen tegen.

<https://www.forumstandaardisatie.nl/open-standaarden/starttls-en-dane>

20 TLS

TLS beveiligt met behulp van certificaten de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie.

<https://www.forumstandaardisatie.nl/open-standaarden/tls>