



Justitiële Informatiedienst
Ministerie van Justitie en Veiligheid

Toelichting op de Vragenlijst Vooronderzoek CDD+

Versie 2025.v2.0

Datum	17 oktober 2025
Status	Definitief

Colofon

Afzendgegevens	Justitiële Informatiedienst Digitaliserings- en Archiveringsdienst (DAD) Henri Dunantweg 3 7201 EV Zutphen Postbus 337 7600 AH Almelo www.justid.nl
Contactpersoon	drs K.A.J. Leers
	T 088 99 89000 info@justid.nl
Auteurs	Justitiële Informatiedienst

Inhoud

Colofon 3

1 Introductie 7

- 1.1 Inleiding 7
- 1.2 Waarom een Vooronderzoek? 7
- 1.3 Wat gaan we doen? 7
- 1.4 Wanneer gaan we archiveren? 11
- 1.5 Waarom wil Justid zoveel weten? 12
- 1.6 Het vooronderzoek is afgerond. En dan? 12

2 Formele kaders 14

- 2.1 Inleiding 14
- 2.2 Uitgangspunten archiefbeheer 14
 - 2.2.1 Algemeen bestuursrecht 15
 - 2.2.2 Algemene regelgeving betreffende gegevens 15
 - 2.2.2.1 (1.1) De Verordening (EU) 2016/679 15
 - 2.2.2.2 (1.2) Wet politiegegevens (Wpg) 15
 - 2.2.2.3 (1.3) Wet justitiële en strafvorderlijke gegevens (Wjsg) en Besluit justitiële en strafvorderlijke gegevens (Bjsg) 16
 - 2.2.2.4 (1.4) Strafrecht 16
 - 2.2.2.5 (1.5) Specifieke wetgeving en jurisprudentie 16
 - 2.2.2.6 (1.6) Voorschriften (informatie)beveiliging 16
 - 2.2.2.7 (1.7) Mandaatregeling 16
 - 2.2.2.8 (1.8) Verantwoordelijkheden en archiefbeheer 17
 - 2.2.2.9 (1.9) Archiefbeheersregels 17
 - 2.2.2.10 (1.10) Selectielijst 17
 - 2.2.2.11 (1.12) Werkprocessen: hoofd- en deelprocessen 17

3 Fit-Gap Metadata 18

- 3.1 Kent elke organisatie metadata toe aan documenten? 18
- 3.2 Waarom zijn metadata belangrijk? 18
- 3.3 Welke soorten metadata zijn er? 18
 - 3.3.1 Voorbeelden 18
- 3.4 Toepassingsprofiel Metagegevens Rijksoverheid (TMR) 19
 - 3.4.1 Wat is de achtergrond van het TMR? 19
 - 3.4.2 Justitieel Archivistisch Metagegevensschema 19
- 3.5 Vragenlijst Vooronderzoek 19
 - 3.5.1 (2.1) Dossiernummer 20
 - 3.5.2 (2.2) Dossierstructuur 20
 - 3.5.3 (2.3) Documentclassificaties 20
 - 3.5.4 (2.4) Titel en onderwerp documenten 20
 - 3.5.5 (2.5) Events 20
 - 3.5.6 (2.6) Metadata van gerelateerde personen 21

4 Functionele en technische aspecten 22

- 4.1 Inleiding 22
- 4.2 (3.1) Servicepartij 22
- 4.3 (3.2) Autorisaties 22
- 4.4 (3.3 en 3.4) Toegang tot het CDD+ 22
- 4.5 (3.5) Uitwisselen in de keten 22
- 4.6 (3.6) Hoe groot wordt de belasting van de systemen? 23

- 4.7 (3.7) Welke bestandsformaten zijn er mogelijk? 23
- 4.7.1 Versies van pdf-bestanden 24
- 4.7.2 Welke bestandsformaten levert uw organisatie aan? 25
- 4.8 (3.8) Digitale ondertekening 25
- 4.9 (3.9) Dienst Intelligent Metadateren (DIM) 26
- 4.9.1 Waarvoor is DIM bedoeld? 26
- 4.9.2 Link met CDD+ 27

1 Introductie

Uw organisatie heeft besloten haar documenten te archiveren in het CDD+. Hiervoor is vooraf onderzoek nodig naar een aantal aspecten. Deze onderzoeksfase heet het *vooronderzoek*. De *Vragenlijst Vooronderzoek* is de basis van het uitvoeren van het vooronderzoek voor het aansluiten op het Centraal Digitaal Depot (CDD+) van de Justitiële Informatiedienst (Justid). Door middel van de Vragenlijst komen alle te onderzoeken onderwerpen langs.

Het vooronderzoek wordt zowel gedaan voor organisaties die hun bronsysteem direct willen aansluiten op het CDD+, alsook voor organisaties die papieren archieven digitaliseren en via de Dienst Intelligent Metadateren (DIM) hun documenten in het betreffende archief in het CDD+ willen opslaan.

De *Vragenlijst Vooronderzoek* wordt grotendeels ingevuld door Justid. Voor sommige aspecten is kennis en expertise nodig die alleen uw eigen organisatieonderdeel kan leveren. Wij verzoeken u de betreffende vragen te beantwoorden. Deze Toelichting biedt ondersteuning hierbij en geeft uitleg over het hoe en waarom van de vragen.

1.1 Inleiding

Archiveren, waarom eigenlijk?

Publieke organisaties moeten zich kunnen verantwoorden voor hun acties, juist omdat zij deze acties namens de burger uitvoeren. De wetgever stelt in de Archiefwet dat overheidsorganen verplicht zijn de 'onder hen berustende archiefbescheiden in goede, geordende en toegankelijke staat te brengen en te bewaren, alsmede zorg te dragen voor de vernietiging van de daarvoor in aanmerking komende archiefbescheiden'. Archiefstukken vormen het geheugen van een organisatie en zorgen ervoor dat een organisatie zich kan verantwoorden. Ze laten ook zien welke vragen en verzoeken de organisatie kreeg en welke besluiten genomen zijn. Een andere functie is die van het ondersteunen van de bedrijfsvoering en de primaire werkprocessen. Archief is een kennisbron die nodig is voor het uitvoeren van taken en is onmisbaar voor een transparante overheidsorganisatie.

1.2 Waarom een Vooronderzoek?

Het resultaat van het Vooronderzoek wordt samengevat in het *Rapport Vooronderzoek aansluiten op CDD+*. Dit rapport is voor Justid de basis om uw archief in het CDD+ in te richten, zodat het aan de geldende wet- en regelgeving voldoet, documenten en metadata op de juiste plek terechtkomen en de eventuele koppeling van uw bronsysteem aan het CDD+ technisch mogelijk is.

1.3 Wat gaan we doen?

De *Vragenlijst Vooronderzoek* gaat u samen met Justid invullen. Samen zorgen we ervoor dat de bovengenoemde aspecten met voldoende diepgang worden onderzocht, zodat het vooronderzoek kan worden afgerond. Uw organisatie draagt de eindverantwoordelijkheid voor hetgeen in het Rapport Vooronderzoek wordt vastgelegd.

We doen samen onderzoek naar drie onderwerpen:

- **Formele kaders**
We beginnen met het in kaart brengen van de wet- en regelgeving die van toepassing is op uw organisatie. Hierbij komen allerlei facetten aan de orde, van algemene regelgeving tot selectielijsten;
- **Metadata**
Vervolgens beschrijven we het gebruik van metadata. Om documenten gemakkelijk te kunnen vinden, de inhoud te kunnen interpreteren en het handelen in het verleden te kunnen reconstrueren zijn metagegevens van groot belang;
- **Functionele en technische aspecten**
We beschrijven welke techniek noodzakelijk is om informatieobjecten in het CDD+ te plaatsen en wat er nodig is om hergebruik te faciliteren.

Dienst Intelligent Metadateren (DIM)

Tevens is er een deel waarin gefocust wordt op DIM. De vragen richten zich op het gewenste gebruik van deze dienst. U kunt deze vragen overslaan als u geen gebruik gaat maken van DIM.

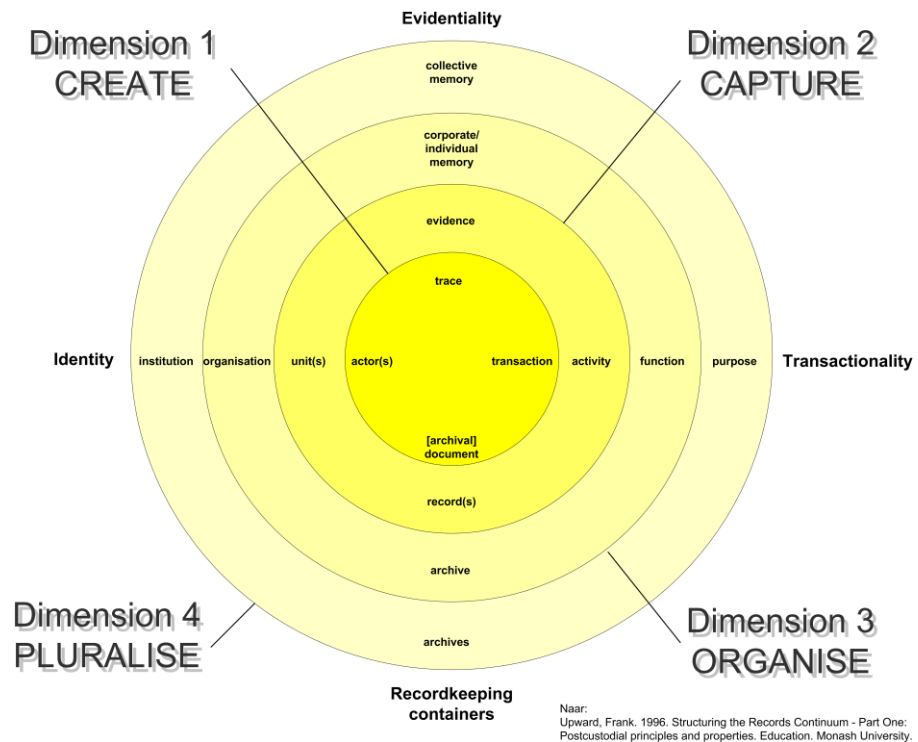
Records Continuum Model (RCM)

Een van de conceptuele modellen die ten grondslag liggen aan het CDD+ is het Records Continuum Model (RCM). Aan de hand van het RCM zijn de formele kaders, de metadata en de functionele en technische aspecten uitgewerkt. Voor het RCM is gekozen omdat in het informatiebeheer niet meer het document centraal staat als te onderzoeken object, maar het werkproces waarin het document wordt gebruikt of wordt gecreëerd. Aan het woord 'document' hangt sterk de betekenis van 'tekst op papier', maar in de Vragenlijst en Toelichting wordt document gebruikt in de breedste zin van het woord: als 'informatieobject' en als het informatieobject is gearhiveerd als 'archiefoobject'. Het RCM sluit beter aan op deze nieuwe denkwijze dan het voorheen gebruikte life cycle model.

Het RCM gaat uit van het principe dat archiefbeheer van informatieobjecten een continu proces is en verschillende belangengroepen kan dienen. Het RCM kent vier dimensies:

- 1 **Creëren:** in de eerste dimensie wordt het informatieobject gecreëerd;
- 2 **Borgen:** in de tweede dimensie wordt het informatieobject nadat ze haar uiteindelijke vorm heeft bereikt, als archiefoobject geregistreerd en in samenhang met andere archiefoobjecten gebracht;
- 3 **Organiseren:** in de derde dimensie wordt het archief gevormd. Hier wordt nagedacht over de wijze waarop de geborgen archiefoobjecten voor later gebruik moeten worden bewaard om de verantwoordings- en geheugenfunctie van de organisatie vorm te geven;
- 4 **Vermeerderen:** in de vierde dimensie worden de archiefoobjecten met derden gedeeld en worden de archieven in samenhang met andere archieven gebracht om het geheugen van de samenleving (collectief geheugen) te vormen.

Schematisch ziet dit er als volgt uit:



Figuur 1: Records Continuum Model

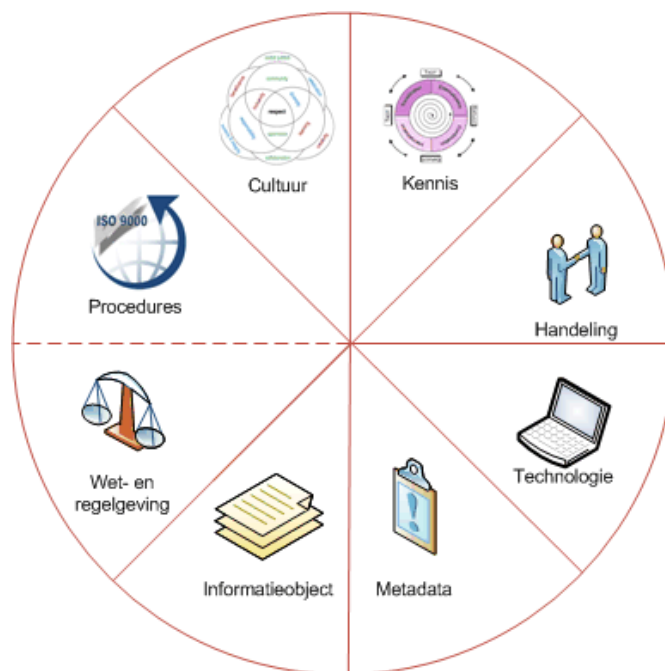
In het RCM volgt het uitwisselen van informatieobjecten pas nadat het informatieobject als archiefobject is zekergesteld, zodat de geheugen- en verantwoordingsfunctie van de organisatie is ingericht. In tegenstelling tot andere modellen hoort het uitwisselen van informatie- en archiefobjecten ook tot dit model.

Het model kent naast de dimensies ook vier assen, die overeenkomen met de vier eigenschappen van informatieobjecten. Aan deze eigenschappen kunnen vervolgens kwaliteitseisen worden gesteld:

- authenticiteit is een kwaliteitseis aan de identiteit van de (bevoegde) auteur, die op een bepaald tijdstip een bepaald informatieobject heeft ontvangen of opemaakt;
- betrouwbaarheid is een eis aan de handeling, die is uitgevoerd. Hoe gedetailleerder het werkproces is ingericht, hoe betrouwbaarder het informatieobject wordt;
- integriteit is een eis aan de intellectuele inhoud van hetgeen waarover het informatieobject getuigt. De getuigenis mag niet onbevoegd of onbedoeld worden gewijzigd;
- bruikbaarheid is een eis aan de interpreteerbaarheid van de verpakking. Verpakkingen (bijvoorbeeld kleitabletten of bestandsformaten) die niet meer bruikbaar zijn, maken het informatieobject waardeloos. Daarmee is het niet meer duurzaam toegankelijk.

De dimensies en assen van het records continuüm zijn vrij abstract. Daarom zijn ze vertaald naar de componenten van een archiveringssysteem:

- 1 kennis die nodig is om het archiveringssysteem intelligentie te verlenen en de daarin opgenomen informatieobjecten toegankelijk te maken;
- 2 handeling, een handeling of werkproces, die in de werkelijkheid plaatsvindt, of heeft plaatsgevonden;
- 3 technologie waarmee het archief wordt gevormd;
- 4 metadata, gegevens over het informatieobject, waarbij verschillende soorten te onderscheiden zijn: metadata uit de ontstaans- en beheercontext en technische metadata;
- 5 informatieobject(en);
- 6 wet- en regelgeving;
- 7 procedures die de administratieve organisatie beschrijven en/of geldige kwaliteitsprocedures die voor accreditatie en certificering nodig zijn;
- 8 normen en waarden, waarmee ieder mens op zijn unieke wijze de realiteit benadert. Dit valt samen te vatten onder de noemer 'zo doen wij dingen hier' en betreft de lokale cultuur expliciet in de archiefvorming.



Figuur 2: Archiveringssysteem

De componenten Wet- en regelgeving en procedures zijn onderdeel van het onderzoek naar de formele kaders, de componenten Informatieobjecten en Metadata van het vergelijken van de metadata, Handeling en Cultuur van de werkwijzen en werkprocessen, en Technologie en Kennis van functionele en technische aspecten. Op deze wijze worden alle aspecten van het RCM en het archiveringssysteem onderzocht tijdens het vooronderzoek, en is het mogelijk om een totaalbeeld te vormen van alle aspecten die relevant zijn voor het inrichten, beheren en gebruiken van het CDD+ door uw organisatie.

De resultaten van de drie (deel)onderzoeken worden vastgelegd in het Rapport Vooronderzoek, dat fungeert als fit-gap analyse voor de metadata, vastlegging van afspraken over onder andere de wijze waarop u het CDD+ gaat gebruiken

(bijvoorbeeld welke documenten u daar wel of niet in opneemt en wanneer) en als startpunt voor de volgende stappen van het aansluittraject.

1.4 Wanneer gaan we archiveren?

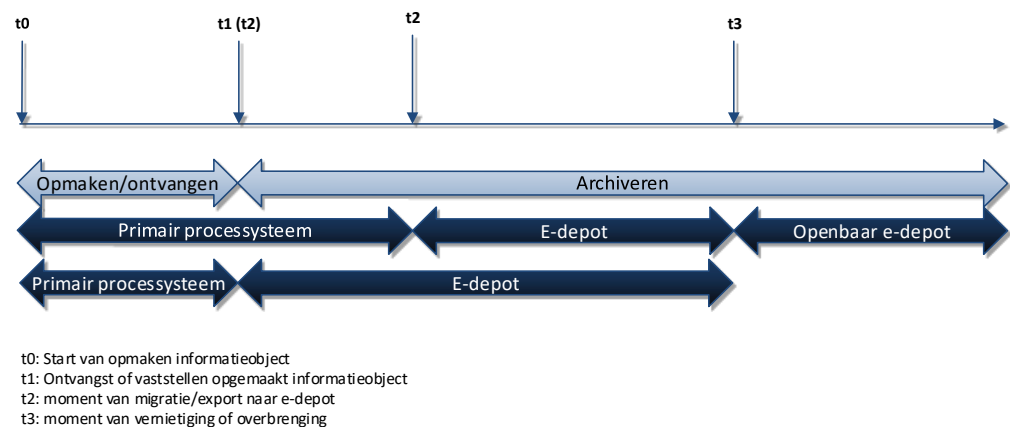
Een informatieobject wordt een archiefobject zodra het binnen een werkproces wordt ontvangen of opgemaakt door de organisatie.

Dit betekent niet dat een archiefobject dan direct in het CDD+ moet worden opgenomen. Dat kan ook het primaire processysteem (PPS) zijn, mits dit voldoet aan de (archief)wettelijke eisen die voor de daarin op te nemen archiefobjecten gelden.

Opslaan van archiefobjecten in het CDD+ kan onmiddellijk na creatie of ontvangst plaatsvinden, maar ook op een later tijdstip als een werkproces wordt beëindigd, een dossier wordt gesloten of een zaak is afgedaan. Deze keuze is aan uw organisatie, maar heeft wel gevolgen voor de opbouw van metadata in de beheercontext.

In het geval dat niet onmiddellijk na creatie opname in het CDD+ volgt, omdat bijvoorbeeld pas na het sluiten van een zaak wordt overgedragen aan het CDD+, dan heeft het CDD+ extra metadata nodig uit de beheercontext van het aanleverende systeem. Anders kan niet zeker worden gesteld dat het ontvangen informatieobject één op één overeenkomt met het in het verleden gecreëerde informatieobject, ofwel of het authentiek is. Als onmiddellijk na creatie het object in het CDD+ wordt opgenomen, dan bouwt het CDD+ voor de beheercontext een eventgeschiedenis op.

Het moment van migreren – meteen na creatie of op een later tijdstip – is dus bepalend voor de hoeveelheid metadata uit de beheercontext die moet worden aangeleverd. Hoe actueler dit gebeurt, hoe minder metadata uw PPS zelf uit de beheercontext dient op te slaan. Er zijn verschillende scenario's mogelijk waarbij ervoor gekozen kan worden om het archiefobject pas later naar het CDD+ te migreren. In Figuur 3 is de levensloop van een informatie-/archiefobject afgezet tegen de twee scenario's die mogelijk zijn.



Figuur 3: Processen en systemen

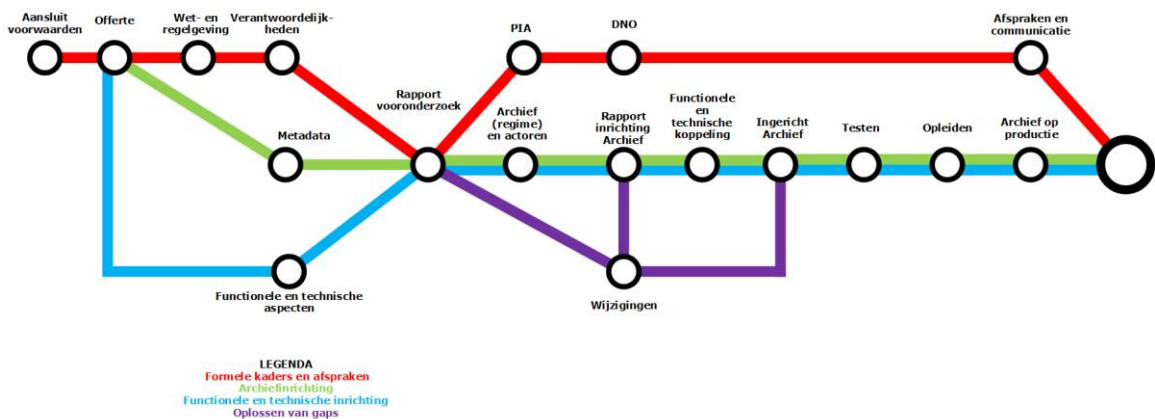
1.5 Waarom wil Justid zoveel weten?

Het antwoord op de vraag waarom Justid zoveel informatie vraagt varieert per onderwerp:

- Het in kaart brengen van de formele kaders schept helderheid over de relevante regelgeving, taken, verantwoordelijkheden en bewaartermijnen die gelden binnen uw organisatie. Daarmee kan worden bepaald of en welke maatregelen nog nodig zijn om aan alle regelgeving en interne afspraken te voldoen;
- Door de bij u beschikbare metadata en de metadatavelden in het CDD+ te vergelijken ontstaat er inzicht in de verschillen en overeenkomsten in metadata, en kan voor afwijkingen een oplossing worden bedacht. Dit zorgt ervoor dat informatieobjecten eenvoudig en zonder informatieverlies zijn over te zetten naar, en toegankelijk te maken zijn in, het CDD+;
- Kennis van uw ICT-infrastructuur is nodig om de koppeling tussen uw bronsysteem en het CDD+ te realiseren en het gebruik van informatieobjecten te faciliteren. Ook kunnen eventuele knelpunten vroegtijdig worden opgelost.

1.6 Het vooronderzoek is afgerond. En dan?

Het onderstaande schema geeft een overzicht van de vervolgstappen binnen het aansluittraject:



Figuur 4: Metrokaart aansluittraject CDD+

In figuur 4 ziet u de *Metrokaart aansluittraject van het CDD+*. In deze metrokaart worden alle stappen (metrostations) beschreven welke genomen moeten worden vanaf het begin van de aansluiting naar de inbeheername van het archief. De rode lijn beschrijft de formele kaders en afspraken, de groene lijn de archiefinrichting, de blauwe lijn de functionele en technische inrichting en de paarse lijn het oplossen van (mogelijke) gaps. Het *Rapport Vooronderzoek* vormt een knooppunt naar de volgende stappen in het aansluitproces.

Een vervolgstap is een Privacy Impact Assessment (PIA) die door u moet worden uitgevoerd. Een PIA is een onderzoek naar de gevolgen van de verwerking van persoonlijke gegevens op de privacy. Parallel hieraan wordt gestart aan de inrichting van het archief (inclusief eventuele wijzigingen die uit het traject voortkomen) en het opstellen van de DNO.

Tijdens de eerste bijeenkomst zal Justid het hele traject verder toelichten.

2 Formele kaders

2.1 Inleiding

In hoofdstuk 1 van de Vragenlijst Vooronderzoek brengen we de formele kaders in kaart. We beschrijven welke wet- en regelgeving van toepassing is op uw organisatie voor een bepaalde periode of proces. Het is van belang om te weten wat voor stukken u ter archivering gaat aanbieden en welke periode ze bestrijken.

Bij het onderzoek zullen belangrijke zaken aan het licht komen zoals:

- het achterhalen waar knelpunten zitten in wet- en regelgeving. Zijn er hiaten in de regelgeving?
- het in kaart brengen van wet- en regelgeving die van belang zijn voor de archiefinrichting (mandaten etc.).

Het is van belang de formele kaders waarbinnen uw organisatie functioneert in kaart te brengen in verband met het beheer van uw archiefbescheiden. Dit vormt belangrijke contextinformatie om onze dienstverlening aan u uit te kunnen voeren.

2.2 Uitgangspunten archiefbeheer

De Archiefwet 1995, het Archiefbesluit 1995 en de Archiefregeling zijn de basis voor het archiefbeheer. Archiefbeheersregels ex artikel 14 van het Archiefbesluit 1995 beschrijven per zorgdrager de verantwoordelijkheden voor de inrichting, methoden en middelen van het archiveringsstelsel en de uitvoering van de archiveringsfuncties.

In de archiefbeheersregels wordt rekening gehouden met de algemene en specifieke wet- en regelgeving. Een voorbeeld van algemene wetgeving is de Algemene wet bestuursrecht. Specifieke wetgeving kan bijvoorbeeld het Burgerlijk Wetboek zijn, het Wetboek van Burgerlijke Rechtsvordering, de Vreemdelingenwet 2000, de Penitentiaire beginselenwet of het Wetboek van Strafrecht of Strafvordering. Wat betreft gestructureerde gegevens kan de privacywetgeving (AVG, Wjsg, Wpg) van toepassing zijn. Selectielijsten behoren ook tot het regelgevend kader. Daarnaast zijn voor het archiefbeheer standaarden van toepassing zoals de NEN-ISO 23081, de NEN 15489 en NEN 16175-1, maar ook de Baseline waarbij deze normen betrokken zijn. Wat betreft bestandsformaten kan worden gedacht aan de ISO 19005 voor PDF/A-1 of de ISO 19005-2 voor PDF/A-2.

De Archiefbeheersregels van het bestuursorgaan of overheidsorgaan regelen de verantwoordelijkheden voor en de uitvoering van het archiefbeheer.

De verantwoordelijke voor het archiefbeheer bij een ketenpartner mag besluiten naast de eigen in gebruik zijnde primaire processystemen gebruik te maken van het CDD+ als archiefsysteem dat werkt binnen archiefwettelijke kaders.

Elk bestuursorgaan of overheidsorgaan heeft naast de beheersregels zijn handboek(en). In geval van vervanging van archiefbescheiden door digitalisering moet er een Handboek vervanging bestaan dat voldoet aan de eisen van artikel 26b van de Archiefregeling. Art. 26b Archiefregeling is strikt genomen alleen van toepassing op blijvend te bewaren archiefbescheiden, maar de meeste organisaties passen om pragmatische redenen dit artikel ook toe op te vernietigen archiefbescheiden.

In archiefbeheersregels worden de verantwoordelijkheden beschreven van het archiefbeheer, evenals de systemen en de functionaliteiten ervan. Met betrekking tot de verantwoordelijkheden tussen het CDD+ en de ketenpartners wordt gebruik gemaakt van een Diensten Niveau Overeenkomst (DNO).

Juridische context van uw organisatie
Hieronder volgen voorbeelden van wet- en regelgeving die van toepassing kunnen zijn op uw organisatie. Deze stukken tekst kunt u wellicht gebruiken bij het invullen van het hoofdstuk formele kaders van de Vragenlijst. De nummers tussen () verwijzen naar de nummers in de Vragenlijst.

2.2.1 *Algemeen bestuursrecht*

Archiefwet 1995 (Aw)

Vastgesteld dient te worden of de aan te sluiten partner een overheidsorgaan is in de zin van de Archiefwet, opdat duidelijk is dat de betrokken partner zich dient te houden aan deze wet en het onderliggend Archiefbesluit 1995 en de Archiefregeling. In verband met juridische procedures is het van belang authentieke en integere archiefbescheiden te kunnen raadplegen of beschikbaar te kunnen stellen.

Algemene wet bestuursrecht (Awb)

Deze wet heeft betrekking op overheidsorganen die tevens bestuursorganen zijn. Het betreft hier bijvoorbeeld dienstonderdelen van ministeries, maar geen rechtbanken. Een complicerende factor hierbij is dat het bestuursprocesrecht wel van toepassing is op de rechtbanken. Het gaat hier echter niet om archivering, maar om het door hen uit te voeren bedrijfsproces.

2.2.2 *Algemene regelgeving betreffende gegevens*

2.2.2.1 (1.1) De Verordening (EU) 2016/679

De Algemene verordening gegevensbescherming (AVG) regelt voor alle staten van de Europese Unie (EU) de bescherming van persoonsgegevens. Er wordt in de Verordening meer nadruk gelegd op de verantwoordelijkheid van organisaties zelf om de wet na te leven én om te kunnen aantonen dat zij zich aan de wet houden (accountability).

Organisaties hebben ook een documentatieplicht. Dit houdt in dat zij met documenten moeten kunnen aantonen dat zij de juiste organisatorische en technische maatregelen hebben genomen om aan de Verordening te voldoen.¹

2.2.2.2 (1.2) Wet politiegegevens (Wpg)

Deze wet beoogt met eerbiediging van de beginselen die de bescherming van de persoonlijke levenssfeer ten doel hebben, meer ruimte te bieden dan de overige wetgeving voor het verwerken van gegevens ten behoeve van een optimale uitvoering van de politietaak. Het is de vraag welke consequenties dit heeft voor het gebruiken en bewaren van de gegevens naast de eisen die voortvloeien uit de AVG. Zie tevens de tekst van Richtlijn (EU) 2016/680.

¹ Art 24, eerste lid, AVG

- 2.2.2.3 (1.3) Wet justitiële en strafvorderlijke gegevens (Wjsg) en Besluit justitiële en strafvorderlijke gegevens (Bjsg)
Deze wet is naast de AVG een speciale wet op het gebied van gegevensbescherming. Vastgesteld moet worden of deze van toepassing is op de te gebruiken gegevens van uw organisatie. Het is de vraag welke consequenties dit heeft voor het gebruiken en bewaren van de gegevens naast de eisen die voortvloeien uit de AVG.

Richtlijn (EU) 2016/680

Op dit vlak werd gepubliceerd: de Richtlijn (EU) 2016/680 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen en betreffende het vrije verkeer van die gegevens en intrekking van Kaderbesluit 2008/977/JBZ van de Raad. In Nederland heeft deze richtlijn invloed op de Wpg, Bpg, Wjsg en Bjsg.

Wederzijdse uitsluiting

De AVG en Richtlijn (EU) 2016/680 sluiten elkaar wederzijds uit. Een persoonsgegeven dat niet onder de Richtlijn valt, valt automatisch onder de AVG (art. 9 van de Richtlijn).

- 2.2.2.4 (1.4) Strafrecht
Specifiek op het gebied van het strafrecht is er wet- en regelgeving beschikbaar. Zoals het Besluit digitale processtukken Strafvordering.
Het besluit maakt het mogelijk om het strafproces op digitale wijze af te doen en in de rechtszaal gebruik te maken van digitale processtukken. Het doel is de kwaliteit van afhandeling van strafzaken te vergroten en een ongewenste uitstroom van strafzaken tegen te gaan.

- 2.2.2.5 (1.5) Specifieke wetgeving en jurisprudentie
Deze vraag is bedoeld voor organisaties die te maken hebben met bijzondere wetgeving en/of jurisprudentie die bij de Justitiële Informatiedienst onbekend is, maar wel van invloed kan zijn op de inrichting en het beheer van archieven.

- 2.2.2.6 (1.6) Voorschriften (informatie)beveiliging
Voor de Rijksdienst geldt de onderstaande regelgeving:
Besluit voorschrift informatiebeveiliging rijksdienst 2007 (Vir)
Besluit voorschrift informatiebeveiliging rijksdienst- bijzondere informatie (Virbi) 2025
Beveiligingsvoorschrift Rijksdienst 2013
Als uw organisatie hier niet toe behoort, dient de vraag gesteld te worden welke regelgeving dan wel geldt of dat uw organisatie zich hieraan conformeert.
Er kunnen nog specifiekere regelingen voorkomen. Bij het ministerie van Justitie en Veiligheid is bijvoorbeeld nog bekend:
De Kaderregeling VIRBI VenJ.

- 2.2.2.7 (1.7) Mandaatregeling

Hier kunt u aangeven welke mandaatregeling van toepassing is op uw organisatie. Wij verzoeken u vriendelijk om een hyperlink naar de mandaatregeling op te nemen of het nummer van de Staatscourant op te nemen waarin de regeling is gepubliceerd.

- 2.2.2.8 (1.8) Verantwoordelijkheden en archiefbeheer
Hier kunt u aangeven wie de zorgdrager is in de zin van de Archiefwet 1995. In veel gevallen zal dat de Minister van Justitie en Veiligheid zijn. Het antwoord op de tweede subvraag kan veelal worden beantwoord op basis van artikel 3, vijfde lid, de Archiefbeheersregels Veiligheid en Justitie 2014.
- In de derde subvraag kan worden aangegeven waar in uw organisatie het archiefbeheer wordt uitgevoerd. Dat kan bijvoorbeeld een archivaris of een afdeling DIV zijn.
- 2.2.2.9 (1.9) Archiefbeheersregels
De Archiefbeheersregels van het bestuursorgaan of overheidsorgaan regelen de verantwoordelijkheden voor en de uitvoering van het archiefbeheer. In uw antwoord op deze vraag kunt u aangeven welke beheersregels op uw organisatie van toepassing zijn.
- 2.2.2.10 (1.10) Selectielijst
Deze vragen zijn bedoeld om duidelijk te krijgen of de selectielijst actueel is, welke handelingen/werkprocessen van toepassing zijn en welke bewaartermijnen worden gehanteerd.
- 2.2.2.11 (1.12) Werkprocessen: hoofd- en deelprocessen
Archiefstukken worden gevormd in de context van de uitvoering van werkprocessen. In het CDD+ worden de hoofdprocessen benoemd en vastgelegd, plus de eventuele deelprocessen die daar onder vallen. Om uw archief zo compleet mogelijk te kunnen inrichten, worden hoofdproces en deelprocessen steeds in relatie gebracht met de producten die binnen het (deelproces van het) werkproces worden gecreëerd. Het hoofdproces dient als hulpmiddel om handelingen toe te kennen aan archiefobjecten. Een deelproces (in het CDD+ heet dit een proceselement) is een activiteit (of een samenstel van activiteiten) die leidt tot een document (product). Dit document is relevant voor de archivering.

3 Fit-Gap Metadata

3.1 Kent elke organisatie metadata toe aan documenten?

Het is haast ondenkbaar dat een document wordt opgeslagen zonder metadata. Zelfs als een document niet in een document management systeem (DMS) of primair processysteem (PPS) wordt opgeslagen maar 'gewoon' op een schijf binnen uw netwerk, wordt er - al dan niet automatisch - metadata aan toegekend. Denk bijvoorbeeld aan het opslaan van een eenvoudig Word-bestand. Metadata als 'gewijzigd', 'type' en 'grootte' worden weergegeven en vastgelegd zonder dat u deze metadata actief aan het document heeft meegegeven.

3.2 Waarom zijn metadata belangrijk?

Metadata zijn gegevens over gegevens. Ze zijn belangrijk om:

- authenticiteit van documenten te waarborgen (het document is wat het beweert te zijn)
- integriteit van documenten te waarborgen (het document is niet gewijzigd)
- documenten terug te vinden (bruikbaarheid en toegankelijkheid)
- documenten bruikbaar te houden (bruikbaarheid en leesbaarheid)
- documenten uit te wisselen (spreken van dezelfde 'taal')
- documenten te kunnen beheren
- de beveiliging van documenten te waarborgen
- de zorgvuldige omgang met documenten te bevorderen (wel of niet openbaar)

Het vastleggen van metadata is in een digitale omgeving nog veel belangrijker dan in een analoge omdat documenten vluchtiger en veranderlijker zijn.

Metadata zijn van groot belang bij het reconstrueren van gebeurtenissen. Eerder werd al uitgelegd waarom overheidsinstanties de plicht hebben om te archiveren. Verantwoording kunnen afleggen is een belangrijke functie van het duurzaam bewaren van documenten. Er moet gereconstrueerd kunnen worden wie, in welk werkproces en volgens welk mandaat, een bepaalde beslissing heeft genomen. Daarvoor is het nodig om ook de context van het document te beschrijven.

Terugzoeken van informatie kan gebeuren door uw eigen organisatie en geautoriseerde ketenpartners. Maar ook in de toekomst – als uw archief openbaar wordt – zullen er wellicht onderzoekers met allerlei vragen uw archief benaderen. Metadata bieden dan noodzakelijke ingangen voor onderzoek.

3.3 Welke soorten metadata zijn er?

Metadata kennen verschillende ontstaansmomenten en vormen.

Er zijn:

- metadata die iets zeggen over de ontstaanscontext van een document/dossier.
- metadata die iets zeggen over de beheerscontext van een document/dossier.
- technische metadata die iets zeggen over de vorm van een document/dossier.

De 'gebeurtenissen' in de levensloop van een document heten 'events'.

3.3.1 Voorbeelden

In de *ontstaanscontext* worden er allerlei metadata vastgelegd over een document zoals bijvoorbeeld wie (welke medewerker) het document opstelde, op welke datum en welke rol hij/zij had in de organisatie. Misschien is het document ergens in de workflow ook wel ondertekend of in elk geval vastgesteld? Dit soort metadata hoort bij de ontstaanscontext van een document.

In de *beheercontext* bestaan er metadata die iets zeggen over wat er verder met het document gebeurd is, bijvoorbeeld geconverteerd, beschikbaar gesteld en vernietigd. Deze 'gebeurtenissen' staan in het CDD+ als 'events' beschreven. In de beheercontext worden documenten gerubriceerd door middel van *classificaties/rubrieken* die in uw organisatie worden gebruikt. Denk bijvoorbeeld aan bepaalde types van documenten zoals beschikkingen, vonnissen, aanvragen etc. In de beheercontext zijn ook *technische metadata* erg belangrijk omdat zij informatie bieden over bestandsformaten, resolutie etc. Deze metadata worden in de regel automatisch tijdens het proces vastgelegd.

3.4 Toepassingsprofiel Metagegevens Rijksoverheid (TMR)

Metadata bestaan op elk aggregatieniveau: het archief als geheel, dossier, map en document. Binnen het CDD+ wordt met het Toepassingsprofiel Metagegevens Rijksoverheid gewerkt.

Binnen de overheid zijn er afspraken gemaakt over het gebruik van metadata. Bij de uitwisseling van documenten moeten partners immers kunnen vertrouwen op authenticiteit, integriteit, betrouwbaarheid en bruikbaarheid van documenten. Bovendien kunnen stukken efficiënter uitgewisseld worden wanneer partners dezelfde taal spreken. Metadata bestaan op elk aggregatieniveau: het archief als geheel, dossier, map en document.

3.4.1 *Wat is de achtergrond van het TMR?*

Het Toepassingsprofiel Metagegevens Rijksoverheid (TMR) is gebaseerd op de uitwerking van de ISO/NEN 23081 metadatastandaard. Het TMR, dat speciaal is ontwikkeld voor gebruik door de Rijksoverheid, behelst een aantal rijksbrede afspraken over de manier waarop gegevens worden vastgelegd.

Het CDD+ is qua metadata ingericht op basis van het TMR. Ketenpartners die archiveren en uitwisselen via het CDD+, metadateren hun documenten volgens het TMR.

Het toepassingsprofiel is gebaseerd op de Richtlijn Metagegevens Overheidsinformatie (RMO). De Richtlijn vormt het kader voor alle informatiebeheersystemen en geldt voor alle informatie die door de overheid bij de uitvoering van haar taken wordt ontvangen of gecreëerd (documenten, maar ook websites, databases, en het Geografisch Informatie Systeem (GIS)).² De Richtlijn maakt deel uit van de Nederlandse Overheid Referentie Architectuur (NORA), waarbinnen samenhang en samenwerking binnen de elektronische overheid wordt geborgd.

3.4.2 *Justitieel Archivistisch Metagegevensschema*

Justitie en Veiligheid (JenV) heeft een formeel vastgesteld metagegevensschema, conform art. 19.1 Archiefregeling, dat gebaseerd is op het TMR: het Justitieel Archivistisch Metagegevensschema (JAM).

3.5 Vragenlijst Vooronderzoek

² De Richtlijn kan beschouwd worden als een metagegevensschema zoals vermeld in artikel 19 van de Archiefregeling.

In het Vooronderzoek richten we ons op de verplichte metadata die nodig zijn voor een archief in het CDD+. Daarnaast brengen we de metadata over eventuele gerelateerde personen in kaart. De nummers tussen () verwijzen naar de nummers in de Vragenlijst.

3.5.1 (2.1) Dossiernummer

In het CDD+ moet het unieke kenmerk dat u toekent aan dossiers, zoals een nummer of een combinatie van een nummer met letters, worden vastgelegd. Het metadataveld dat hiervoor in het CDD+ is gereserveerd heet "dossiernummer".

3.5.2 (2.2) Dossierstructuur

De gebruikersinterface van CDD+ ondersteunt een structuur tot zeven niveaus diep. Het is van belang om te onderzoeken hoe dossiers binnen uw organisaties zijn opgebouwd.

Naam en onderwerp van een (sub) map

Binnen het CDD+ draagt elke (sub)map van het dossier een eigen naam en eventueel een eigen onderwerp.

3.5.3 (2.3) Documentclassificaties

De classificaties en rubrieken die in uw organisatie worden gebruikt op documentniveau worden hier in kaart gebracht.

Een drietal classificaties zijn verplicht op documentniveau:
VIR-rubriek (Voorschrift Informatiebeveiliging Rijksdienst)³
Documenttype (Toepassingsprofiel Metagegevens Rijksoverheid)⁴
Merking (deze rubriek kan worden toegepast bij documenten die alleen door geautoriseerde medewerkers geraadpleegd mogen worden)

3.5.4 (2.4) Titel en onderwerp documenten

Het is wenselijk om in het CDD+ titels en onderwerpen toe te kennen aan documenten in verband met de toegankelijkheid en terugvindbaarheid van gegevens.

3.5.5 (2.5) Events

Events zijn belangrijke metadata omdat zij aangeven wat er met een dossier of document door de tijd heen gebeurd is. Events kunnen het gevolg zijn van gebeurtenissen buiten het CDD+, maar ook het gevolg van een handeling in het CDD+. Events die buiten het CDD+ hebben plaatsgevonden, kunt u bij de documenten of dossiers aanleveren en opslaan. Gebeurtenissen die in het CDD+ plaatsvinden worden door het CDD+ zelf geregistreerd.

³ <https://wetten.overheid.nl/BWBR0022141/2007-07-01>

⁴ https://www.nationaalarchief.nl/sites/default/files/filed-file/Toepassingsprofiel_metagegevens_rijksoverheid.pdf, zie p12 Entiteittype

Bij elk event wordt naast het type een datum/tijd vastgelegd, de verantwoordelijke functionaris en eventueel een omschrijving. In de events-tabel kunt u aangeven of u de verplichte events kunt aanleveren.

3.5.6 (2.6) Metadata van gerelateerde personen

Gerelateerd persoon: Natuurlijk persoon en niet-natuurlijk persoon

Een gerelateerd persoon is de (rechts)persoon of betrokkene waarop een dossier of document van toepassing is. Het CDD+ biedt de mogelijkheid om *persoonsgegevens* vast te leggen. Persoonsgegevens kunnen *natuurlijke* en *niet-natuurlijke c.q. rechtspersonen* betreffen. Hier bestaan in het CDD+ diverse velden voor. In de gezamenlijke sessie met de Justitiële Informatiedienst komt uitgebreid aan de orde welke mogelijkheden dit voor uw organisatie biedt.

Als archiefvormer moet u een keuze maken óf en op welk niveau u persoonsgegevens wilt vastleggen: op het niveau van het dossier of van het document.

Bij elke persoon (natuurlijke- of rechtspersoon) is het vastleggen van minimaal één identificatiemiddel verplicht.

Indien u heeft aangegeven dat metadata over personen moet worden vastgelegd in het CDD+, kan gestart worden met het 'mappen' van de metadata uit uw systemen met de metadatavelden van het CDD+. Gebruik hiervoor het werkblad 'Gerelateerde Personen' van het document *Metadataschema t.b.v. Fit-gap Analyse*. Het invullen doet u samen met de Specialist Archiefbeheer van de Justitiële Informatiedienst.

Indien u geen uniek identificatiemiddel van een persoon kunt aanleveren, is er mogelijk een zogeheten gap. Overleg hierover met Justid om te bepalen welke actie nodig is.

4 Functionele en technische aspecten

4.1 Inleiding

In dit deel brengen we in kaart hoe de functionaliteiten en de technische infrastructuur er (op hoofdlijnen) uitziet. U maakt duidelijk hoe de aanlevering van digitale documenten gaat plaatsvinden, hoe de toegang tot het CDD+ gaat plaatsvinden, of er gebruik gaat worden gemaakt van uitwisseling in een keten en wat de belasting van de systemen zal zijn. Hierdoor kan Justid de eventuele koppeling tussen uw bronsysteem en het CDD+ realiseren en een advies geven over de mogelijke inrichting van het CDD+. De nummers tussen () verwijzen naar de nummers in de Vragenlijst.

4.2 (3.1) Servicepartij

Om de aansluiting soepel te laten verlopen, is het handig om te weten wie uw IT-servicepartij is.

4.3 (3.2) Autorisaties

Welke gebruikers krijgen toegang tot het archief in CDD+ en waar wordt dit geregeld?

4.4 (3.3 en 3.4) Toegang tot het CDD+

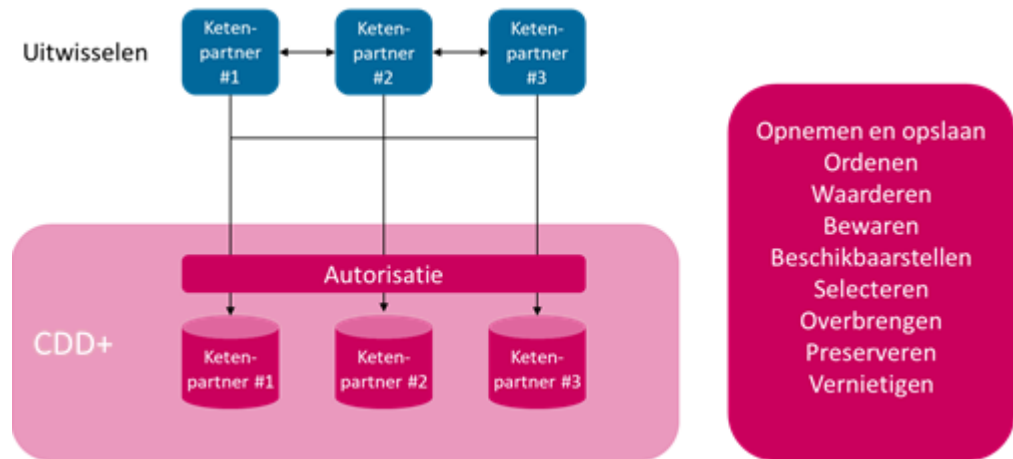
Er zijn twee soorten 'toegang' om gebruik te maken van het CDD+. De eerste optie is REST API's. Er is dan een koppeling nodig vanaf het primaire systeem van de klant naar het CDD+. Deze koppeling loopt via de centrale Justitie Berichten Service (JUBES).

De tweede optie is toegang via de Graphical User Interface (GUI), de webinterface. De GUI van het CDD+ is te benaderen via een URL. Alles wat via REST API's kan worden uitgevoerd op het CDD+ kan ook via de GUI (m.u.v. de notificaties). De GUI biedt daarnaast aanvullende (beheers)handelingen zoals het aanmaken van nieuwe gebruikersaccounts en voor de archivaris het verbijzonderen, overbrengen en het vernietigen van archiefstukken.

4.5 (3.5) Uitwisselen in de keten

Het CDD+ is in eerste instantie ontwikkeld als een archiefvoorziening. Het heeft zich ontwikkeld tot een dynamische uitwisselingsvoorziening. Een aansluiting van ketenpartners op het CDD+ heeft grote voordelen voor een keten, aangezien de mogelijkheid bestaat om documenten onderling uit te wisselen of beschikbaar te stellen aan andere ketenpartners. Dat is onder andere mogelijk door het principe van enkelvoudige opslag, meervoudig gebruik. In de vreemdelingenketen wordt hier al gebruik van gemaakt.

Uitwisselen kan uiteraard alleen als de betreffende ketenpartner zijn documenten duurzaam toegankelijk opslaat in CDD+.



Figuur 5: Het duurzaam bewaren en uitwisselen in het CDD+.

4.6 (3.6) Hoe groot wordt de belasting van de systemen?

Het is belangrijk om gegevens te verkrijgen over de (toekomstige) belasting van het CDD+. Verzamel in overleg met uw medewerkers (functioneel en technisch beheer) de informatie die wordt gevraagd in de tabel. Hiermee wordt inzicht verkregen in het verwachte toekomstige gebruik van het CDD+. Met deze gegevens kan de Justitiële Informatiedienst onderzoeken of de aantallen die aangeleverd gaan worden mogelijk zijn.

4.7 (3.7) Welke bestandsformaten zijn er mogelijk?

Documenten kunnen voorkomen in verschillende bestandsformaten. In de tabel in de Vragenlijst ziet u de indeling die voor het CDD+ wordt gehanteerd.

Categorie I

Documenten van categorie I worden niet alleen duurzaam opgeslagen, maar er wordt gezorgd dat deze documentformaten later nog steeds te openen zijn. Dit wordt gedaan door de ontwikkeling rondom deze formaten te monitoren. Zo zijn bijvoorbeeld benodigde lettertypes *embedded* in de bestanden. Niet elk duurzaam bestandsformaat valt automatisch in categorie I; er kan er ook voor gekozen zijn om het formaat op te nemen in categorie II en te converteren.

Categorie II

Bestandsformaten van categorie II worden geconverteerd naar bestanden van categorie I. Hiermee wordt voor bestanden in deze formaten gegarandeerd dat de inhoud in de toekomst nog steeds te benaderen is, zij het in een ander formaat. Het streven is om bestandsformaten (voor documenten en archivering) die voorkomen op de "Pas toe of leg uit" lijst van het Forum Standaardisatie op te nemen in categorie I of II, zodat alle, binnen de overheid gangbare en aangemoedigde bestandsformaten, gepreserveerd kunnen worden in het CDD+. Bestandsformaten die probleemloos kunnen worden omgezet naar een categorie I formaat kunnen worden opgenomen in categorie II. Doorgaans vereist dit dat de Justitiële Informatiedienst de beschikking heeft over software die het betreffende formaat kan openen. Bij minder gangbare bestandsformaten kan er daarom van een ketenpartner worden gevraagd om de Justitiële Informatiedienst te voorzien van de betreffende software. Het blijkt namelijk dat veel software vaak op detailniveau

afwijkt van de standaard voor het bestandsformaat. Het bestandsformaat blijft dan in categorie II zolang de software beschikbaar blijft. Is hij niet langer beschikbaar, dan verschuift het bestandsformaat naar categorie III.

Categorie III

Documenten van een bestandsformaat dat onder categorie III is ingedeeld, kunnen wel worden opgeslagen in het CDD+, maar er wordt geen waarborg gegeven dat deze documenten in de toekomst nog kunnen worden geopend. Daarnaast vallen ook bestanden in een formaat van categorie I of II die zijn voorzien van een elektronische handtekening of waarmerk in categorie III, aangezien deze niet geconverteerd kunnen worden, omdat dat leidt tot corruptie van de handtekening of het waarmerk. Gesloten, *proprietary* bestandsformaten zullen ook worden ingedeeld in categorie III. Dit zijn formaten waarvan de technische specificatie niet is vrijgegeven, en die alleen (eenvoudig) kunnen worden geopend met de software (of zelfs hardware) van de eigenaar van het formaat. Ook hier geldt dat de bestanden niet zonder meer geconverteerd kunnen worden.

Categorie IV

Documenten van een type uit categorie IV worden *niet* opgeslagen in het CDD+. In deze categorie vallen bestanden met actieve elementen, zoals een .exe bestand. Daarnaast vallen versleutelde bestanden en bestanden die door middel van een wachtwoord zijn beschermd in deze categorie. Aangezien deze bestanden niet kunnen worden ingezien, hebben ze geen plaats in het archief. Bestandstypes die nog niet expliciet zijn ingedeeld in een van de andere categorieën, vallen impliciet in categorie IV totdat ze wel zijn ingedeeld.



Figuur 6: Bestandsformaten in het CDD+

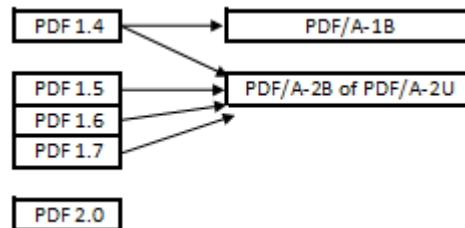
4.7.1

Versies van pdf-bestanden

Vaak heeft een nieuwe versie van een bestandsformaat meer functionaliteit dan de vorige. Dit betekent dat als een bestand oorspronkelijk is gemaakt met een nieuwe versie, en later wordt opgeslagen met een oude versie, er informatie verloren kan gaan. Dit moet dus vermeden worden. Echter, bij PDF-bestanden gaat dit vaak fout. Oude software herkent vaak niet dat het met een nieuwere bestandsversie te maken heeft, voert wel bewerkingen uit, en slaat het document op in een ouder formaat. Niet alleen leidt dit tot verlies van informatie, maar vaak ook tot een corrupte bestandsstructuur, waarin elementen van de oude en de nieuwe versie door elkaar heen lopen. Het risico bestaat dat deze bestanden in de toekomst niet goed leesbaar zijn. Het is dan ook van belang om te weten welke conversies er in uw organisatie plaatsvinden. Het gaat niet alleen om expliciete conversies; elke bewerking kan een conversie tot gevolg hebben als de betreffende software het bestand opslaat in een andere versie.

De versieproblematiek speelt ook bij de conversie van pdf naar pdfa. In figuur 7 wordt een overzicht gegeven van de veilige conversies tussen pdf en pdfa.

Zo heeft de jongste pdf-versie 2.0 meer functionaliteit dan de oudere pdf 1.4, 1.5, 1.6 en 1.7. Dit geldt ook voor de door Justid geaccepteerde duurzame versies: pdfa-1b en pdfa-2b. De eerste bevat minder functionaliteit dan de tweede. Als er binnen uw organisatie geconverteerd wordt, is het van belang om te onderzoeken of dit op de juiste wijze gebeurt.



Figuur 7: Converteren van pdf-bestanden.

Veilige conversies:

- Converteren van pdf 1.4 naar pdfa-1b wordt geaccepteerd.
- Converteren van pdf 1.4 naar pdfa-2b is gewenst.
- Converteren van pdf 1.5, pdf 1.6 en pdf 1.7 naar pdfa-2b of pdfa 2u is gewenst.

Af te raden conversies:

- Converteren van pdf 1.5, pdf 1.6 en pdf 1.7 naar pdfa-1b is ongewenst.
- Converteren van pdfa-1b naar pdfa-2b of 2u is ongewenst.
- Getekende pdf-documenten converteren naar pdfa is ongewenst.
- Pdf met bijlagen converteren naar pdfa is ongewenst.

Ongewenst is bovendien het 'terugconverteren' van een hogere pdf-versie naar een lagere versie in verband met het risico op informatieverlies (dus bijvoorbeeld van pdf 1.6 naar pdf 1.4).

Conversie niet mogelijk:

- Converteren van pdf 2.0 is niet mogelijk. Hier is nog geen equivalente pdfa versie voor beschikbaar

4.7.2 Welke bestandsformaten levert uw organisatie aan?

Welk bestandsformaat hebben de documenten die u aanlevert? Maak bij pdf-bestanden een duidelijk onderscheid tussen de verschillende pdf-versies. Mocht er een bestandsformaat ontbreken in de rij, dan noteert u dat onderaan de tabel in de Vragenlijst.

In een later stadium van de aansluiting zult u gevraagd worden om een representatieve steekproef van verschillende documenten van verschillende bronnen aan te leveren, om de compatibiliteit met het CDD+ te testen.

4.8 (3.8) Digitale ondertekening

Documenten zijn vaak ondertekend. In veel gevallen gaat het dan om een weergave van de natte handtekening: het document is uitgeprint, ondertekend en ingescand –

of er is simpelweg een afbeelding van de handtekening ingevoerd. In andere gevallen is er gebruikgemaakt van een digitale handtekening, die ongeldig wordt zodra het document na ondertekening nog wordt gewijzigd. Dit wordt gedaan door een controlegetal (een *hash*) te berekenen en op te nemen in de handtekening.

We onderscheiden twee soorten digitale handtekeningen:

- handtekeningen waarbij de hash in het document wordt opgenomen, en wordt beveiligd met encryptie gebaseerd op een *public key infrastructure* (PKI);
- handtekeningen waarbij de hash in een externe database wordt opgenomen.

In het eerste geval is de handtekening op echtheid te checken door de hash te controleren en het gebruikte PKI certificaat na te trekken. In het tweede geval vindt de controle plaats door de hash te vergelijken met de hash in de externe database.

Er is een conflict tussen deze digitale handtekeningen, die wijzigingen tegenhouden, en het preservatiebeleid, waarbij onder andere de bruikbaarheid van de documenten wordt geborgd door documenten te converteren naar andere formaten. Om te voorkomen dat dit tot problemen leidt, worden de gebruikte digitale handtekeningen hier geïnventariseerd.

4.9 (3.9) Dienst Intelligent Metadateren (DIM)

DIM staat voor Dienst Intelligent Metadateren en is een aanvullende dienst op het CDD+, waarvoor een aparte offerte moet worden opgesteld.

DIM is een systeem waarin (gedigitaliseerde) archiefstukken kunnen worden voorzien van metadata. Via deze dienst kunnen, zodra de metadata compleet is, documenten inclusief metadata naar het CDD+ worden verstuurd om daar duurzaam toegankelijk te worden opgeslagen voor zolang de bewaartermijn dat vereist.

DIM kan een oplossing bieden bij het digitaliseren van archieven waarvan de metadata nog niet (digitaal) beschikbaar is of nog niet volledig genoeg is om aan wet- en regelgeving en geldende standaarden te voldoen. Met behulp van DIM kunt u uw gescande documenten bekijken, ordenen en beschrijven, door ze op verschillende aggregatieniveaus van metadata te voorzien.

De metadata kan op drie manieren aan de documenten worden toegekend. Combinaties van deze drie methoden zijn ook mogelijk.

1. Er kan gebruik gemaakt worden van Artificial Intelligence (AI). Dit houdt in dat bepaalde metadata uit het gedigitaliseerde document kan worden gelezen. Met behulp van maatwerkregels die worden ingesteld per archief, kan worden bepaald hoe metadatavelden gevuld moeten worden.
2. De metadata kan tevens worden aangeleverd vanuit de archiefvormer die (deels) al metadata heeft opgeslagen in de eigen processystemen. Hiervoor is een importfunctionaliteit beschikbaar in DIM.
3. De metadata kan handmatig worden aangevuld. Hiervoor is in de DIM een viewer ingebouwd waarmee het digitale document en dossier kan worden bekeken. In overleg is het mogelijk om het handmatig metadateren door Justid te laten uitvoeren.

4.9.1 Waarvoor is DIM bedoeld?

De Dienst Intelligent Metadateren wordt aangeboden aan organisaties binnen Justitie en Veiligheid die (papier) documenten of dossiers van metadata willen

voorzien. Hierbij bieden wij tevens de optie om archiefstukken voor de organisatie te scannen én/of na het scannen op te nemen in een eigen archief in het CDD+.

Gedigitaliseerd archief kan direct vanuit de scanstraat van Justid in DIM worden opgenomen, maar het is ook mogelijk elders gescande documenten of dossiers in te lezen in DIM. De bijbehorende metadata (o.a. scandatum, document-id) kan tegelijk met de documenten/dossiers worden ingelezen.

4.9.2

Link met CDD+

DIM en CDD+ voldoen beide aan het Toepassingsprofiel Metagegevens Rijksoverheid (TMR). Dit betekent dat er voor alle metadatavelden die het TMR kent, plaats is in deze systemen. Tevens zijn er een aantal verplichte metadatavelden die gevuld moeten zijn voor opname in het CDD+. Deze verplichting komt overeen met de metadata die in het CDD+ verplicht zijn.